IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH

SKRIPSI

Diajukan untuk Memenuhi Sebagian Syarat

Guna Memperoleh Gelar Sarjana S1

Dalam Ilmu Matematika

Oleh:

Ivvan Nuzulul Huda

NIM: 1508046027

MATEMATKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN WALISONGO SEMARANG

2021

PERNYATAAN KEASLIAN NASKAH

Yang bertanggung jawab di bawah ini:

Nama : Ivvan Nuzulul Huda

NIM : 1508046027

Program Studi : Matematika

Menyatakan bahwa skripsi yang berjudul:

IMPLEMENTASI ALGORITMA KRIPTOGRAFI

ADVANCED ENCRYPTION STANDARD

PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH

Secara keseluruhan adalah hasil penelitian / karya saya sendiri, kecuali bagian tertentu yang dirujuk sumbernya.

Semarang, 26 April 2021

Ivvan Nuzulul Huda

NIM : 1508046027

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI WALISONGO SEMARANG
FAKULTAS SAINS DAN TEKNOLOGI
Alamat: Jl. Prof. Dr. Hamka Km. 1 Semarang Telp. 024 76433366 Semarang 50185

PENGESAHAN

Naskah skripsi berikut ini:

Judul : **IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH**

Penulis : **Ivvan Nuzulul Huda**

NIM :150804027

Jurusan : Matematika

Telah diujikan dalam sidang *munaqosyah* oleh Dewan Penguji Fakultas Sains dan Teknologi Universitas Islam Negeri Walisongo Semarang dan dapat diterima sebagai salah satu syarat memperoleh gelar sarjana dalam Ilmu Matematika.

Semarang, 10 Mei 2021

DEWAN PENGUJI

Penguji I,

Emy Siswanah, M.Sc.
NIP. 19870202 201101 2 014

Penguji II,

Minhayati Saleh, M.Si
NIP. 19760426 200604 2 001

Penguji III,

Budi Cahyono, S.Pd., M.Si
NIP. 19801215 200912 1 003

Penguji IV,

Siti Maslihah, M.Si.
NIP. 19770611 201101 2 004

Pembimbing I,

Dr. Saminanto, M.Sc
NIP. 19720604 200312 1 002

Pembimbing II,

Nur Cahyo Hendro W, S.T., M.Kom
NIP. 19731222 200604 1 001

NOTA DINAS

Semarang, 22 April 2021

Yth.

Dekan Fakultas Sains dan Teknologi

UIN Walisongo Semarang

di Semarang

Assalamu'alaikum Wr. Wb.

Dengan ini diberitahukan bahwa Saya telah melakukan bimbingan, arahan, dan koreksi naskah skripsi dengan:

Judul : **IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH**

Penulis : **Ivvan Nuzulul Huda**

NIM :150804027

Jurusan : Matematika

Saya memandang bahwa naskah skripsi tersebut sudah dapat diajukan kepada Fakultas Sains dan Teknologi UIN Walisongo Semarang untuk diujikan dalam Sidang Munaqosah.

Wassalamu'alaikum Wr. Wb.

Pembimbing I,

Dr. Saminanto, S. Pd, M. Sc.

NIP. 19720604 200312 1 002

NOTA DINAS

Semarang, 26 April 2021

Yth.

Dekan Fakultas Sains dan Teknologi

UIN Walisongo Semarang

di Semarang

Assalamu'alaikum Wr. Wb.

Dengan ini diberitahukan bahwa Saya telah melakukan bimbingan, arahan, dan koreksi naskah skripsi dengan:

Judul : **IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH**

Penulis : **Ivvan Nuzulul Huda**

NIM :150804027

Jurusan : Matematika

Saya memandang bahwa naskah skripsi tersebut sudah dapat diajukan kepada Fakultas Sains dan Teknologi UIN Walisongo Semarang untuk diujikan dalam Sidang Munaqosah.

Wassalamu'alaikum Wr. Wb.

Pembimbing II,

Nur Cahyo Hendro W., ST., M. Kom.

NIP. 19731222 200604 1 001

MOTTO

...فَاسْتَبِقُوا الْخَيْرٰتِ...

“Maka Berlomba-lombalah dalam Kebaikan”

(Q.S. Al-Baqarah: 148)

PERSEMBAHAN

Alhamdulillah 'ala kulli ini'matillah, washolatu wassalamu 'ala Rosulillah, laa haula wala quwwata illa billahil 'aliyyil 'adzim...

Puji Syukur yang dapat Hamba panjatkan kepadamu Ya *Rabb*,
Tuhan semesta alam, Tuhan Penguasa Jagat Raya ini atas segala nikmat yang telah engkau berikan kepada hambamu yang kerdil ini.
Waktu terasa begitu cepat berlalu
Hingga saatnya berpisah dengan kampus hijauku
Tidak ada satu waktu pun yang terbuang rugi
di kampus yang menjunjung tinggi tridarma perguruan tinggi
Kuliah, organisasi, dan lomba
yang selalu menghiasi hari-hariku untuk hari yang tak biasa
tapi sekarang,
aku harus meninggalkanmu untuk masa depan yang benderang
Harapan dan doa
untuk kampus tercinta,
semoga semakin jaya
dan semakin mengangkasa
Aamiin

Untuk karya yang sederhana ini, saya persembahkan kepada:

1. Ayahku Tersayang dan Ibuku Tercinta, Bapak Niamushomad dan Ibu Jariyah yang selalu mendoakan di sepertiga malamnya untuk kesejahteraan putra dan putrinya.
2. Kakakku tercinta, Mamas Imam yang selalu membantu ketika diri ini kesulitan.
3. Kedua Adikku tersayang, Putri Amaliyah dan Puji Nur Hisbiyah.

ABSTRAK

Ivvan Nuzulul Huda (1508046027), 2021. Implementasi Algoritma Kriptografi *Advanced Encryption Standard* pada Sistem Informasi Pondok Pesantren An-Najah. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Walisongo Semarang.

Di era yang sangat pesat perkembangan teknologi dan informasi, sistem informasi seperti hal wajib bagi suatu organisasi atau instansi. Sebab, sistem informasi dapat memberikan suatu nilai tambah terhadap produksi, pengambilan keputusan, kualitas, proses, manajemen, dan pemecahan masalah, serta keunggulan kompetitif yang berguna bagi kegiatan bisnis. Tidak dapat dipungkiri bahwa kerap keamanan dalam pembuatan sebuah sistem informasi selalu di urutan sehabis tampilan, padahal segi keamanan adalah jendela utama bagi sistem informasi untuk mengamankan data yang terkandung di dalamnya. Penelitian ini bertujuan untuk mengamankan data pada sistem informasi pondok pesantren di kabupaten Sragen

dengan menggunakan algoritma kriptografi *Advanced Encryption Standard* (*AES*).

Penelitian ini menggunakan metode *Research and Development* dengan modifikasi model pengembangan tiga langkah yaitu definisi, desain, dan *develop* atau pengembangan. Penguji ahli merupakan dosen matematika yang kompeten dalam bidan ilmu kriptografi dan pembuat dari sistem informasi. Hasil penelitian ini menunjukkan bahwa produk dalam penelitian ini dinyatakan valid melalui uji validitas produk dengan kategori nilai "Sangat Baik", praktis dalam mengimplementasikan ke dalam sistem informasi melalu uji kepraktisan produk dengan kategori nilai "Sangat Baik", serta efektif yang diuji melalui uji keefektifan produk dengan kategori nilai "Sangat Baik".

Kata Kunci: Sistem Informasi, Kriptografi, *Advanced Encyption Standard*.

KATA PENGANTAR

Bismillahirrahmanirrahim.

Alhamdulillahirabbil 'alamiin. Puji syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat, hidayah, serta karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir (skripsi) yang berjudul **IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* PADA SISTEM INFORMASI PONDOK PESANTREN AN-NAJAH** ini dengan lancar. Sholawat serta salam penulis sampaikan kepada junjungan kita, nabi Muhammad SAW yang kita nantikan syafaatnya di *yaumul qiyamah* nanti.

Pada kesempatan ini, penulis ingin mengucapkan banyak terima kasih kepada pihak yang membantu hingga terselesaikannya penyusunan tugas akhir (skripsi) ini. Untuk itu penulis mengucapkan terima kasih kepada:

1. Allah SWT yang telah memberikan kemudahan dalam segala hal sehingga laporan ini dapat terselesaikan.
2. Prof. Dr. KH. Imam Taufiq, M. Ag. Selaku Rektor UIN Walisongo Semarang.
3. Dr. H. Ismail, M. Ag. Selaku Dekan Fakultas Sains dan Teknologi.
4. Emy Siswanah, M. Sc., selaku Ketua Jurusan Matematika.

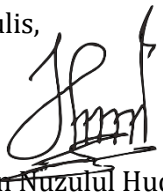
5. Aunur Rohman, M. Pd., selaku Sekretaris Jurusan Matematika.
6. Hj. Muthohiroh, selaku pengasuh Pondok Pesantren Raudlatut Tholibin yang selalu sabar mendidik santrinya.
7. KH. Mustaghfirin, KH. Abdul Kholiq, Lc., dan Abah Qolyubi, M. Ag., Selaku Pengasuh Pondok Pesantren Raudlatut Thalibin yang senantiasa mengajar, mengarahkan, dan mendidik santri-santrinya.
8. Dr. KH. Minanul Aziz Syathori, M. Ag. selaku pengasuh Pondok Pesantren An-Najah yang telah memberikan izin penelitian dalam penulisan ini.
9. Dr. Saminanto, M. Sc. Selaku Pembimbing I yang telah membimbing dan mengarahkan penulis dengan ikhlas dan sabar dalam penyusunan skripsi.
10. Nur Cahyo Hendro Wibowo, S.T., M. Kom. Selaku Pembimbing II yang telah memberikan bimbingan dan dukungan dengan sepenuh hati dalam penyusunan skripsi.
11. Siti Maslihah, M. Si. selaku dosen wali atau orang tua akademik penulis yang telah sabar dan ikhlas membimbing penulis.
12. Any Muanalifah, M. Si. selaku penguji ahli yang ikhlas, sabar, dan memberikan validasi terhadap validitas produk dalam penelitian.
13. Imam Abdul Aziz, S. Kom. Selaku pembuat sistem informasi sekaligus penguji ahli yang sabar dan responsif dalam

menanggapi penulis serta memberikan penilaian terhadap kepraktisan dan keefektifan produk dalam penelitian.

14. Seluruh Dosen dan Staf Fakultas Sains dan Teknologi yang membantu proses penyelesaian skripsi.
15. Sahabat Penulis yang banyak memberikan motivasi dan dukungan kepada penulis.
16. Adek Penulis, Yulia Alfiatur Rokhmaniyah dan Ana Alfiatur Rohmah yang selalu mendoakan, menyemangati, dan membantu mempersiapkan keperluan penulis dalam penulisan skripsi.
17. Teman-teman jurusan Matematika angkatan 2015 yang telah berjuang bersama melewati masa-masa perkuliahan dan menjadikan kehidupan kampus lebih berwarna.
18. Keluarga Besar UKM RISALAH yang telah memberikan pelajaran dalam mengelola sebuah organisasi serta memberikan pengalaman yang sangat berarti dan semoga menjadi berguna di masyarakat kelak.
19. Keluarga Besar Pondok Pesantren Raudlatut Thalibin yang telah menjadi keluarga selama kuliah di kota Atlas (Semarang).
20. Alfu Lail Jatisari Mijen, Grup Al-Banjari yang hanya mengikuti perlombaan secara *online*.
21. Serta semua pihak yang tidak dapat disebutkan satu per satu yang telah membantu kelancaran penulisan skripsi ini.

Penulis sangat menyadari bahwa skripsi ini masih jauh dari kata sempurna, sehingga perlu adanya kritik dan saran yang membangun. Semoga skripsi ini dapat bermanfaat bagi semua pihak yang terkait.

Semarang, 26 April 2021
Penulis,



Ivvan Nuzulul Huda
NIM : 1508046027

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Zaman ini perkembangan teknologi informasi dan komunikasi bertambah sangat pesat. Salah satunya perkembangan sistem informasi. Banyak langkah manusia yang berhubungan dengan sistem informasi. Tidak semata-mata di negara maju yang memiliki sistem informasi seperti Korea Selatan. Amerika, Singapura, Jepang dan, Tiongkok. Sistem informasi di Indonesia juga telah diterapkan berbagai tempat seperti di dunia pendidikan, pemerintahan atau instansi. Sistem informasi memberikan nilai tambah terhadap produksi, pengambilan keputusan, kualitas, proses, manajemen, dan pemecahan masalah, serta keunggulan kompetitif bagi kegiatan bisnis (Kroeke, 1992).

Sistem informasi merupakan sesuatu sistem yang terdiri atas berbagai komponen baik komputasi maupun manual dalam menghimpun, menaruh, serta mengelola informasi untuk pemakainya. Menurut (Wilkison, 1992) sistem informasi adalah kerangka kerja yang mengoordinasikan sumber daya (manusia, komputer) untuk mengubah masukan (*input*) menjadi informasi, guna mencapai sasaran-sasaran perusahaan.

Permasalahan keamanan ialah salah satu aspek terutama dari suatu sistem data. Permasalahan keamanan kerap kali kurang menemukan atensi dari para perancang serta pengelola sistem data. Kerap kali permasalahan keamanan terletak di urutan sehabis tampilan, apalagi terletak pada urutan terakhir dalam catatan yang dikira bernilai. Sehingga banyak terjalin pencurian informasi data oleh pihak- pihak yang tidak bertanggung jawab. Sehingga timbul sebutan ilmu kriptografi.

Kriptografi merupakan ilmu serta seni buat melindungi keamanan pesan yang dikirim dari sesuatu tempat ke tempat yang lain. Secara Universal, kriptografi dipecah menjadi dua, yakni kriptografi simetris serta kriptografi asimetris. Kriptografi simetris merupakan algoritma dengan satu kunci untuk enkripsi serta dekripsi. Sebaliknya kriptografi asimetris merupakan dengan dua kunci untuk enkripsi dan dekripsinya..

Banyak algoritma kriptografi yang digunakan untuk mengamankan data atau informasi. Di antaranya algoritma *Data Encryption Standard* (*DES*), *Advanced Encryption Standard* (*AES*), RSA, El-Gamal, RC4, dan sebagainya.

Advanced Encryption Standard (*AES*) yaitu enkripsi dengan satu kunci yang diadopsi oleh pemerintah Amerika Serikat. Algoritma kriptografi ini terdiri dari tiga blok *cipher,*

yaitu *AES*-128 dengan panjang kunci 128 bit, *AES*-192 dengan panjang kunci 192 bit, dan *AES-256* dengan panjang kunci 256 bit. *AES* telah dianalisis serta digunakan di seluruh dunia.

Pondok pesantren An-Najah Gondang adalah lembaga pendidikan agama yang terletak di Gondang Kabupaten Sragen yang sedang merancang sebuah sistem informasi untuk memudahkan pengelolaan transaksi dari para santri. Imam Abdul Aziz adalah perancang dan pembuat sistem informasi tersebut. Fitur yang diunggulkan dalam sistem informasi tersebut adalah transaksi pembayaran dan transaksi menabung baik secara *offline* maupun *online*. Transaksi pembayaran dan transaksi menabung secara *offline* yang dimaksudkan adalah santri datang dan melakukan transaksi langsung kepada pengurus yang memiliki akun di sistem informasi kemudian pengurus melaporkan dan mencatat transaksi tersebut pada sistem informasi secara *online*. Sedangkan transaksi secara *online* adalah santri melakukan pembayaran melalui transfer bank dengan ketentuan yang telah disepakati oleh pengurus pondok pesantren. Selain itu, fitur lain dari sistem informasi pondok pesantren An-Najah yang lain adalah fitur *chat* atau pesan yang memungkinkan adanya konsultasi langsung dari santri kepada admin secara *online* mengenai masalah yang

dihadapi santri ketika melakukan transaksi baik pembayaran maupun menabung.

Sistem informasi pondok pesantren An-Najah memiliki beberapa tingkat *role* akses yaitu santri, administrator, dan super administrator. Setiap *role* akses memiliki menu dan fitur yang berbeda. *Role* santri hanya memiliki menu *chat* atau pesan, transaksi pembayaran atau menabung, menampilkan catatan transaksi, dan menu pengguna yang menampilkan profil santri tersebut, sedangkan fitur yang tersedia untuk *role* santri adalah fitur *chat*, transaksi pembayaran, transaksi menabung, dan ganti *password*. *Role* administrator memiliki menu dan fitur seperti role santri dengan beberapa tambahan yaitu menu data santri, verifikasi, jenis pembayaran, dan info transaksi sukses, gagal maupun pending, sedangkan fitur yang ditambahkan adalah fitur penambahan data santri, log semua transaksi, dan verifikasi *online*. *Role* super administrator memiliki menu dan fitur yang sama seperti *role* administrator hanya ditambahkan fitur data admin yang memungkinkan untuk menambah nama admin untuk *role* administrator.

Sistem informasi pondok pesantren saat ini masih dalam tahap pengembangan dari berbagai segi seperti segi keamanan. Keamanan dalam sistem informasi pondok pesantren An-Najah masih belum terjamin, karena sistem

informasi tersebut belum memiliki enkripsi di berbagai fiturnya. Oleh karena itu, sistem informasi ini perlu adanya enkripsi untuk menunjang keamanan bagi pengguna.

Berdasarkan hasil rekomendasi riset yang telah dilakukan peneliti, sistem informasi pada pondok pesantren An-Najah membutuhkan pengamanan data khususnya pada *database* dalam sistem informasi tersebut. Hal itu disebabkan karena tidak adanya pengamanan pada *database* tersebut.

Berdasarkan uraian di atas, penulis mengambil judul **"Implementasi Algoritma Kriptografi *Advanced Encryption Standard* pada Sistem Informasi Pondok Pesantren An-Najah"**.

B. Identifikasi Masalah

Identifikasi masalah yang ada pada penelitian ini adalah tidak ada satu pun pengamanan data pada sistem informasi pondok pesantren An-Najah.

C. Pembatasan Masalah

Pembatasan masalah dalam penulisan ini agar tidak menyimpang dari permasalahan, maka ruang lingkup pembahasannya dibatasi antara lain:

1. Enkripsi pada *id* transaksi, *password*, *chat*, dan nomor rekening
2. Menggunakan algoritma enkripsi *AES* 128-bit.

3. *Input*-an berupa *plaintext* dengan *output* berupa *ciphertext*.

D. Rumusan Masalah

Permasalahan yang ingin diselesaikan adalah bagaimana pengembangan keamanan sistem informasi menggunakan algoritma kriptografi AES (*Advanced Encyiption Standard*) yang valid, praktis, dan efektif pada sistem informasi pondok pesantren An-Najah.

E. Tujuan Penelitian

Tujuan dalam penelitian ini adalah mengamankan data pada sistem informasi pondok pesantren An-Najah menggunakan algoritma *Advanced Encryption Standard*.

F. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Keamanan *database* pada sistem informasi pondok pesantren An-Najah
2. Menerapkan ilmu yang diajarkan di bangku kuliah dalam kehidupan sehingga tidak hanya teori saja.

G. Asumsi Pengembangan

Penelitian ini berasumsi bahwa produk yang telah diimplementasikan pada sistem informasi akan membuat sistem informasi lebih terjamin keamanannya dari pihak yang tidak berwenang.

H. Spesifikasi Produk yang Dikembangkan

Spesifikasi yang diharapkan pada penelitian ini yaitu:

1. Produk menggunakan bahasa pemrograman *PHP.*
2. Produk yang diimplementasikan tidak membebani sistem.
3. Produk hanya dapat mengenkripsi pesan asli (*plaintext*).
4. Produk ini memenuhi uji validitas, kepraktisan, dan keefektifan.

BAB II

LANDASAN TEORI

A. Landasan Teori

1. Sistem Informasi

   a. Pengertian Sistem Informasi

      Abdul Kadir (2014) dalam karyanya yang berjudul "Pengenalan Sistem Informasi Edisi Revisi" menyebutkan bahwa sistem informasi merupakan sistem yang mencakup sejumlah komponen, ada yang diproses, dan dimaksudkan untuk mencapai suatu sasaran tertentu.

      Sistem informasi menurut para ahli didefinisikan sebagai berikut:

      1) Alter (1992)

         Sistem informasi merupakan campuran dari aturan kerja, data, manusia seta teknologi yang saling berkaitan dalam mencapai cita-cita organisasi.

      2) Bondar dan Hopwood (1993)

         Sistem informasi merupakan kolaborasi antara *hardware* dan *software* untuk mewujudkan terciptanya data yang bermanfaat.

3) Gelinas, Oram, dan Wiffins (1990)

Sistem informasi merupakan suatu sistem yang bertujuan untuk mengolah, menyimpan, mengumpulkan serta menyediakan informasi.

4) Hail (2001)

Sistem informasi ialah langkah-langkah mengumpulkan data, kemudian diproses menjadi data dan disebarkan kepada pengguna.

5) Wilkinson

Sistem informasi ialah sistem yang mengoordinasikan pengguna dan komputer yang bertujuan untuk menjadikan data menjadi informasi yang bermanfaat dalam mencapai tujuan tertentu.

b. Aplikasi Sistem Informasi

Aplikasi sistem informasi bisa kita temukan di bermacam bidang serta digunakan untuk menanggulangi bermacam kegiatan. Aplikasi bisa berupa desktop maupun *website*. Aplikasi desktop terbuat dengan memakai perkakas pengembangan. Di lingkungan Windows, aplikasi dapat dibangun menggunakan Visual Basic, Delphi atau semacamnya. Di lingkungan Linux, dapat dibangun menggunakan C++, Gambas dan sebagainya. Sedangkan aplikasi

yang berbentuk web dibangun menggunakan ASP, PHP, dan JSP. Dalam hal ini, semua browser dapat digunakan untuk mengakses aplikasi web.

Aplikasi sistem informasi berbentuk web sangat diminati oleh banyak perusahaan, karena mudahnya akses ke internet. Selain itu, aplikasi sistem informasi yang berbasis web memberikan kemudahan dalam hal peluncuran aplikasi baru karena aplikasi hanya diletakkan pada server serta tidak perlu di *install* pada klien. Sebagai keterkaitannya, aplikasi web digunakan untuk memberikan layanan informasi atau sebagai media dalam bertransaksi, baik itu transaksi pembayaran, jual beli, bahkan aplikasi web digunakan sebagai sistem informasi untuk instansi pondok pesantren.

c. Komponen Sistem Informasi

Komponen dalam sistem informasi adalah sebagai berikut:

1) Perangkat keras yang mencangkup alat-alat yang bersifat fisik seperti komputer, printer, dan sebagainya.
2) Perangkat lunak, yaitu instruksi untuk memproses data pada perangkat keras.

3) Prosedur, yaitu aturan-aturan untuk menghasilkan keluaran yang diinginkan.
4) Manusia, yakni pihak yang bertanggung jawab terhadap semua proses dalam pengembangan sistem informasi.
5) Basis data (*database*), ialah sekumpulan tabel, ikatan, serta suatu yang berkaitan dengan penyimpanan data.
6) Jaringan komputer dan komunikasi data, ialah suatu sistem untuk meningkatkan sumber yang dipakai bersama-sama atau diakses oleh beberapa pemakai.

Praktik yang ada di lapangan, tidak seluruhnya sistem informasi memenuhi keenam komponen tersebut. Sebagai contoh, sistem informasi pribadi yang hanya membutuhkan pengguna dan perangkatnya tanpa harus ada jaringan komputer maupun komunikasi data.

d. Klasifikasi Sistem Informasi

Klasifikasi yang biasa digunakan dalam sistem informasi antara lain didasarkan pada:

1) Tingkat Organisasi

Sistem informasi pada tingkat organisasi diklasifikasikan menjadi tiga bagian, yaitu sistem

informasi perusahaan, departemen, serta sistem informasi antar organisasi

Sistem informasi perusahaan yaitu sistem informasi yang dapat digunakan antar departemen. Contohnya adalah sistem informasi yang ada di perguruan tinggi dengan mengintegrasikan bagian-bagian seperti pengajar, kemahasiswaan, dan keuangan.

Sistem informasi departemen yaitu sistem informasi yang dipakai pada suatu departemen. Contohnya adalah sistem informasi departemen SDM yang bertujuan memantau kinerja pegawai dan menangani pelamar pekerjaan.

Sistem informasi antar organisasi yaitu sistem informasi yang menghubungkan antar organisasi. Contoh dari sistem informasi ini yaitu sistem informasi pada perusahaan kereta api yang memungkinkan penjualan tiket tanpa harus datang langsung ke perusahaan untuk membeli tiket.

2) Area Fungsional

Sistem informasi fungsional merupakan suatu sistem informasi untuk membagikan data kepada kelompok tertentu dalam sebuah

perusahaan. Contoh dari sistem informasi ini yaitu sistem informasi keuangan, akuntansi, pemasaran, dan lain sebagainya.

3) Dukungan yang diberikan

Sistem informasi ini dikelompokkan sebagai berikut:

- Sistem informasi manajemen.
- Sistem otomasi perkantoran.
- Sistem informasi eksekutif.
- Sistem pendukung cerdas.
- Sistem pendukung kelompok.
- Sistem pemroses transaksi.
- Sistem pendukung keputusan.

4) Arsitektur Sistem Informasi

Sistem informasi ini dikelompokkan sebagai berikut:

- Sistem komputer pribadi.
- Sistem berbasis *mainframe*.
- Sistem komputasi jaringan.

e. Keamanan dalam Sistem Informasi

Keamanan adalah hal penting dalam pengoperasian suatu sistem informasi untuk mencegah ancaman-ancaman ketika terdeteksi adanya kesalahan sistem.

Ancaman aktif dan pasif adalah ancaman yang dapat terjadi pada sistem informasi. Ancaman aktif adalah ancaman yang terjadi karena adanya kejahatan pada perangkat sistem informasi. Sedangkan ancaman pasif adalah ancaman yang terjadi karena bencana alam, kegagalan sistem, maupun kesalahan manusia.

Bencana alam ialah faktor yang tidak dapat diprediksi yang bisa mengancam suatu sistem informasi. Kebakaran, gempa bumi, banjir, gunung meletus, dan lainnya dapat menghancurkan sumber daya pada sistem informasi dalam waktu yang sangat singkat.

Kesalahan manusia contohnya adalah kesalahan dalam pengoperasian sistem sehingga dapat mengancam integritas sistem dan data. Pemasukan data yang salah dapat merusak dan mengacaukan sistem. Begitu pula penghapusan data, pelabelan yang salah dapat membawa dampak yang buruk jika terganggu dalam sistem.

Kegagalan komponen dan perangkat sistem informasi juga dapat menyebabkan masalah yang besar mulai dari data yang tidak konsisten bahkan dapat merusak data. Selain itu, variasi tegangan listrik dalam komponen dan perangkat sistem informasi juga sangat

perlu untuk diamankan karena dapat membuat peralatan-peralatan terbakar.

Ancaman lain dari keamanan sistem informasi yaitu kecurangan dan kejahatan komputer. Sistem yang berbasis komputer sangat rawan terhadap aksi kecurangan serta pencurian. Contohnya penyalahgunaan kartu VISA ataupun semacamnya lewat jalur internet telah merebak di seluruh dunia, termasuk di Indonesia. Seseorang bisa menggunakan kartu tersebut untuk berbelanja di situs-situs *online* menggunakan kepemilikan orang lain. Kasus pembobolan rekening nasabah bank juga adalah salah satu bentuk kecurangan dan pencurian dalam sistem informasi.

Cara yang sering digunakan untuk menyelundupkan sesuatu ke dalam sistem ada enam macam (Bornar dan Hopwood, 1993), yaitu:

1) Pemanipulasian Masukan

   Pemanipulasian masukan adalah metode yang sangat sering dipakai dalam kejahatan dalam komputer, karena metode ini tidak perlu ketrampilan khusus maupun tingkat tinggi.

2) Penggantian Program

Penggantian program yang biasa dilakukan oleh para ahli teknologi informasi bisa menjadi ancaman terhadap informasi yang memungkinkan program yang dipasang telah dilengkapi dengan celah-celah yang dapat dijadikan jalan untuk merusak dan memanipulasi data.

3) Penggantian Data secara Langsung

Penggantian data dapat dilakukan oleh orang yang mempunyai akses langsung terhadap basis data. perihal ini dapat terjadi jika seorang pemrogram memiliki hak akses untuk mengolah data di basis data.

4) Pencurian Data

Pencurian data biasa dilakukan oleh orang dalam untuk tujuan dijual, sebagai contoh, seorang anak muda berhasil memasang program yang disebut "*invisible KeyLogger Stealt*" di komputer-komputer yang ditujukan untuk publik di 14 toko yang memungkinkan pelanggan mengakses internet. Perangkat lunak tersebut dapat mencatat setiap ketikan di *keyboard*. Dalam satu tahun, perangkat lunak tersebut

dapat merekam lebih dari 450 nama pemakai berserta kata sandinya. Kemudian, informasi tersebut digunakan untuk mengakses bank.

5) Sabotase

Sabotase bisa dilakukan dengan banyak cara. Istilah yang umum dalam sabotase ini adalah aktivitas *hacking*. Banyak aktivitas *hacking* yang terjadi di dunia yang sekarang ini karena mereka beranggapan "tidak ada sistem yang aman".

Berbagai teknik yang digunakan untuk melakukan *hacking* adalah sebagai berikut:

- *Sniffing*

  Sebuah jaringan tentunya banyak paket data yang bolak balik. Data tersebut dapat berupa apa saja, mulai dari waktu, IP *address*, protokol, dan nama jaringan. Bahkan informasi sensitif seperti *cookies*, *username*, dan *password*. Paket data tersebut dapat di-*capture* atau di rekam. Kegiatan tersebut dinamakan *sniffing*.

- SQL *Injection*

  SQL *Injection* merupakan suatu kegiatan peretasan dengan mengubah perintah SQL

pada *database*. Terdapat dua jenis dalam SQL *Injection*, yaitu *Blind* SQL *Injection* yang bertujuan untuk melihat isi *database* dan *Advandced* SQL *Injection* yang bertujuan untuk mengakses server, termasuk mengakses *shell* dan memasang *backdoor*.

- *Spoofing*

  Spoffing adalah kegiatan *hacking* dengan melakukan pemalsuan alamat web atau *e-mail* yang bertujuan menjebak pengguna agar memasukkan informasi pribadi ke dalam alamat web palsu tersebut seperti *password* atau nomor kartu kredit.

- *Denial of Service* (DoS)

  DoS ialah suatu metode penyerangan terhadap suatu sistem dengan jalur menghabiskan sumber energi sistem tersebut sehingga tidak dapat diakses lagi.

- Virus

  Virus adalah kode ganas yang dapat menggandakan dirinya dengan tujuan menginfeksi program-program yang telah diidentifikasi virus tersebut.

Virus ada yang hanya menyembunyikan *file* dan memindahkan *file*. Virus jenis ini tidak terlalu berbahaya tetapi sangat mengganggu bagi pengguna. Selain itu virus juga ada yang sangat bahaya sebab dapat menghapus berkas-berkas ekstensi tertentu serta dapat memformat *hard disk*. Ada pula virus yang baru-baru ini tersebar, yaitu virus *Ransomware* yang dapat mengunci berkas-berkas pada komputer korban dan dijadikan sebagai alat untuk mengancam korban.

- Cacing (*Worm*)

  Worm atau cacing ialah suatu aplikasi yang dapat menginfeksi komputer-komputer lain yang berada pada suatu jaringan.

- Bom Waktu

  Bom waktu adalah sebuah program yang akan bereaksi dalam waktu tertentu sesuai dengan pengaturan pada program tersebut. Contoh dari program ini yaitu program yang dapat menghapus seluruh data pada suatu alat penyimpanan ataupun program yang

dapat mengatur lalu lintas macet pada suatu waktu yang telah ditetapkan.

- Kuda Trojan (*Trojan Horse*)

  Program ini adalah program tersembunyi yang dapat disusupkan ke dalam sebuah sistem. *Trojan* ini akan aktif ketika menghidupkan suatu program yang telah terinfeksi kuda *trojan* ini

  Klien dan server adalah bagian dari *trojan horse*. Bagian klien merupakan bagian target peretasan yang dapat dijalankan oleh peretas melalui komputernya. Sedangkan bagian server merupakan bagian yang disusupi kuda *trojan* dan harus dijalankan oleh komputer klien.

6) Penyalahgunaan dan Pencurian Sumber Daya Komputasi

   Kegiatan ini dapat dilakukan oleh pegawai yang secara ilegal mencuri dan menjual informasi demi kelancaran bisnis pribadi

f. Sistem Informasi yang Baik

1) Kemudahan Akses

   Sistem informasi dibuat untuk memudahkan pengguna dalam memperoleh

informasi agar informasi dapat diterima dengan mudah. Sehingga informasi terjamin mudah dalam mengaksesnya.

2) Akurasi

Akurasi adalah faktor yang wajib dipenuhi oleh suatu sistem informasi. Ketidakakuratan informasi bisa mengakibatkan kegagalan sistem yang dapat merugikan bagi pemilik sistem. Pengambilan keputusan dalam sistem informasi harus benar-benar akurat mengingat kegagalan sistem dapat membahayakan sistem.

3) Keamanan

Keamanan adalah faktor penting dalam sebuah sistem informasi sehingga keamanan harus diperhatikan. Ada beberapa kontrol yang dapat mengamankan sistem informasi yang dapat kita lihat tabel yang ada pada lampiran.

2. Kriptografi

a. Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi yaitu ilmu dan seni dalam mengamankan pesan dari pengirim ke penerima

tanpa diketahui pihak lain. Sedangkan menurut (Rifki Sadikin, 2012) dalam bukunya yang berjudul "Kriptografi untuk Keamanan Jaringan" menjelaskan bahwa kriptografi ialah ilmu yang berdasarkan informasi teknik matematika untuk berurusan dengan keamanan informasi seperti keutuhan data, kerahasiaan, dan autentikasi entitas.

b. Sejarah Kriptografi

Sejarah kriptografi sangat panjang dan menarik. Kriptografi telah lama digunakan semenjak 4000 tahun yang lalu yang diperkenalkan oleh orang-orang Mesir *hieroglyph* untuk mengirim pesan ke pasukan militer yang terletak di lapangan dan tidak terbaca oleh pihak lawan meski pembawa pesan tersebut tertangkap oleh musuh.

Pada era Romawi kuno, terdapat kisah antara Julius Caesar dan seorang Jendral yang sedang ada di medan perang. Kisah ini menceritakan tentang cara mengirim pesan antara Julius Caesar dengan Jendral tersebut tanpa diketahui oleh pihak musuh. Cara yang digunakan Julius Caesar yaitu dengan mengacak pesan yang hendak dikirim menjadi pesan yang hanya diketahui Jendral tersebut. Metode yang dilakukan adalah mengganti susunan yang terdapat pada alfabet

dengan menggeser empat langkah ke kanan yang artinya huruf “a” diganti dengan huruf “d”, huruf “b” diganti dengan huruf “e”, dan seterusnya.

Ilustrasi di atas menggambarkan bahwa kriptografi kerap digunakan untuk aktivitas-aktivitas rahasia dalam proses kirim pesan. Yang dilakukan Julius Caesar yang mengubah tatanan alfabet menjadi tak terbaca disebut sebagai *encryption* atau enkripsi, sedangkan yang dilakukan sang jenderal adalah menyusun dan merapikan kembali tatanan alfabet yang tak terbaca menjadi terbaca dan dipahami disebut dengan *decryption* atau dekripsi. Pesan awal dan pesan yang sudah dirapikan biasa disebut dengan *plaintext* dan pesan yang tidak dapat dibaca dan dipahami biasa disebut dengan *ciphertext*.

Pada zaman Romawi juga terdapat alat untuk membuat pesan rahasia yaitu Scytale. *Scytale* adalah alat pembuat pesan rahasia dengan media pita panjang dari daun papirus dengan kayu berbentuk silinder. Metode yang digunakan yaitu menulis pesan pada pita papirus yang digulung pada kayu yang berbentuk silinder. Setelah itu pita dilepaskan dan dikirim.

Cara membaca *Scytale* yaitu dengan melilitkan kembali pita tersebut dengan kayu yang berbentuk silinder dan memiliki diameter yang sama. Kunci dari penyandian ini yaitu diameter kayu silinder tersebut. Tetapi penyandian *Scytale* dapat dipecahkan dengan menerka jumlah huruf yang dapat ditulis pada kayu silinder yang digunakan.

Pada era perang dunia yang kedua, terdapat suatu alat buatan Jerman yang dapat mengenkripsi pesan dari pimpinan perang kala itu (Hitler) kepada tentaranya yang diberi nama enigma. mereka menduga bahwa alat tersebut tidak akan ada yang bisa memecahkan kodenya. Tetapi ternyata dugaannya tersebut salah, alat tersebut lambat laun dapat dipecahkan kode-kodenya.

Enigma yang digunakan Jerman dapat mengenkripsi satu pesan yang mempunyai bermilyar-milyar kemungkinan untuk mendekripsikannya. Sehingga Jerman kembali percaya diri bahwa enigma yang dibuat tidak dapat dipecahkan. Tetapi percaya diri tersebut pudar karena pihak sekutu kembali dapat memecahkan enigma yang dibuat oleh Jerman.

Kriptografi dahulu hanya digunakan oleh pihak militer dalam mengamankan komunikasi antar anggota dan pasukan dari pihak luar. Akan tetapi mereka juga mempelajari kode-kode rahasia yang dimiliki oleh negara lain sehingga kriptografi semakin berkembang sesuai perkembangan era.

Namun sekarang kriptografi tidak hanya di kalangan militer saja, tetapi setiap individu juga menginginkan komunikasi mereka aman dari pihak lain.

c. Algoritma Kriptografi

Algoritma menurut bahasa berarti proses perhitungan. Algoritma berasal dari nama penulis buku yang sangat terkenal, yaitu Abu Ja'far Muhammad Ibnu al-Khawarizmi (al-Khawarizmi dibaca oleh orang barat sebagai *algorism*) dan sekarang berubah menjadi *algorithm*.

Menurut terminologi, algoritma adalah langkah-langkah sistematis dalam menyelesaikan suatu masalah. Sedangkan algoritma kriptografi adalah langkah-langkah sistematis dalam mengamankan pesan antara pengirim dan penerima dari pihak ketiga.

Algoritma kriptografi memiliki tiga fungsi dasar, yaitu:

1) Enkripsi

   Enkripsi adalah proses mengamankan pesan yang akan dikirimkan dengan mengubah pesan asli (*plaintext*) menjadi pesan yang tidak dapat dibaca (*ciphertext*).

2) Dekripsi

   Dekripsi adalah proses pengembalian pesan yang tidak dapat dibaca menjadi pesan asli.

3) Kunci

   Kunci yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Jenis kunci ada dua bagian, yaitu kunci rahasia (*private key*) dan kunci publik (*public key*).

Keamanan dari kriptografi didapat dengan merahasiakan kunci algoritma itu sendiri. Karena, kunci memiliki fungsi yang sama dengan *password* yang harus dijaga agar pihak lain tidak dapat mengakses milik kita.

d. Macam-macam Algoritma Kriptografi

Berdasarkan kuncinya, kriptografi dibedakan menjadi tiga bagian, yaitu:

1) Algoritma Simetris

Algoritma simetris ialah algoritma dengan kunci tunggal yang artinya kunci tersebut dapat digunakan untuk enkripsi maupun dekripsi.

Secara umum, *cipher* yang termasuk dalam algoritma kriptografi simetri beroperasi dalam mode blok atau biasa disebut *block cipher*, yaitu enkripsi dan dekripsi dilakukan terhadap satu blok data yang berukuran tertentu.

Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma di bawah ini:

- *Data Encryption Standard* (DES)
- *Advanced Encryption Standard* (AES)
- *International Data Encryption Algoritma* (IDEA)
- RC2, RC4, RC5, RC6

2) Algoritma Asimetris

Algoritma asimetris adalah algoritma dengan kunci ganda yang artinya satu kunci untuk enkripsi pesan dan satu kunci yang lain untuk dekripsi pesan.

Keamanan algoritma asimetris lebih terjamin dari pada menggunakan algoritma simetris, akan tetapi estimasi waktu algoritma asimetris jauh lebih lama daripada algoritma simetris. Contoh algoritma kriptografi asimetris di antaranya adalah:

- *Digital Signature Algorithm* (DSA)
- RSA
- Diffie-Hellman

3) Fungsi *Hash*

Fungsi *hash* biasa disebut dengan fungsi satu arah yang berarti fungsi ini hanya memiliki enkripsi saja, tanpa memiliki dekripsinya. Fungsi ini biasanya dipakai dalam pembuatan sidik jari pada suatu pesan. Sidik jari ini digunakan untuk mengidentifikasi pesan tersebut asli dari orang yang diinginkan atau pesan tersebut palsu.

e. Kriptografi Klasik

Kriptografi klasik adalah kriptografi yang tidak memakai proses komputasi, biasanya kriptografi ini menggunakan algoritma kriptografi simetris atau dengan satu kunci. Ciri-ciri kriptografi ini adalah sebagai berikut:

1) Berbasis karakter
2) Tanpa bantuan komputer
3) Menggunakan Algoritma kriptografi simetris

Teknik dalam kriptografi klasik ini meliputi:

1) Teknik Substitusi

Teknik substitusi atau teknik pergantian karakter satu dengan karakter lainnya. Dalam teknik ini terdapat empat istilah substitusi kode, yaitu:

- *Monoalphabet*: setiap karakter teks kode menggantikan karakter teks asli.
- *Polyalphabet*: setiap karakter teks kode dapat menggantikan lebih dari satu macam karakter teks asli.
- *Monograf*: satu enkripsi dilakukan terhadap satu karakter teks asli.
- *Polugraph*: satu enkripsi dilakukan terhadap lebih dari satu karakter teks asli.

2) Teknik Transposisi

Teknik transposisi ini menggunakan permutasi karakter sehingga dengan teknik ini pesan yang asli tidak dapat dibaca kecuali memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula. Teknik ini

menggunakan enam kunci untuk melakukan permutasi *cipher*.

Varian lain dari teknik ini dapat menggunakan pola spiral, segitiga, diagonal, maupun zig-zag. Banyaknya varian pola dalam teknik ini dapat meningkatkan keamanan pesan dari pihak lain yang tidak berhak. Maka, teknik ini adalah dasar dari terbentuknya algoritma kriptografi modern.

f. Kriptografi Modern

Kriptografi modern yaitu suatu algoritma yang mempunyai kerumitan sangat tinggi sehingga dalam pengoperasiannya harus menggunakan komputer. Kriptografi ini berbeda dengan kriptografi klasik dikarenakan pengoperasian enkripsinya menggunakan bantuan komputer.

Setiap karakter pada kriptografi modern harus dikonversikan terlebih dahulu ke dalam urutan digit biner (bits) yaitu 1 dan 0, konversi ini sudah ada dalam *schema encoding* ASCII (*American Standard Code for Information Interchange*). Urutan bit yang akan mewakili *plaintext* yang kemudian dienkripsi untuk mendapatkan *ciphertext* dalam bentuk urutan bit.

3. Algoritma *Advanced Encryption Standard (AES)*

   a. Pengertian Algoritma Kriptografi *AES*

      Advanced Encryption Standard (AES) adalah kriptografi modern dengan algoritma kriptografi simetris pengganti *Data Encryption Standard* (DES) yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. Algoritma ini dikembangkan oleh Joan Daeman dan Vincent Rinjment yang memenangkan sayembara pengganti algoritma DES. alasan terpilihnya algoritma AES ini karena dapat bertahan terhadap serangan analisis dan serangan secara *brute force*, memiliki biaya komputasi dan memori yang efisien, serta bersifat terbuka, fleksibel, dan sederhana.

      Algoritma kriptografi *Advanced Encryptios Standard* memiliki panjang blok 126 bit dengan panjang kunci yang bervariasi yaitu 128 bit, 192 bit, serta 258 bit. Proses dalam algoritma ini berulang setiap putarannya yang biasa disebut ronde. Banyaknya ronde dalam algoritma kriptografi ini juga bervariasi tergantung panjang kuncinya. Berikut hubungan panjang kunci dan banyaknya ronde.

      Tabel 2. 1 Hubungan panjang kunci dan jumlah ronde

No.	Panjang Kunci AES	Jumlah Ronde (Nr)
1.	128 bit	10
2.	192 bit	12
3.	256 bit	14

b. Unit Data *AES*

Algoritma kriptografi *Advanced Encryption Standard* menggunakan 5 unit data: bit, *byte*, *word*, blok, dan *state*. Bit merupakan satuan data terkecil, yaitu nilai digit sistem biner. Sedangkan *byte* berukuran 8 bit, *word* berukuran 4 *byte* (32 bit), blok berukuran 16 *byte* (128 bit) sedangkan *state* adalah blok yang ditata sebagai matriks *byte* berukuran 4x4.

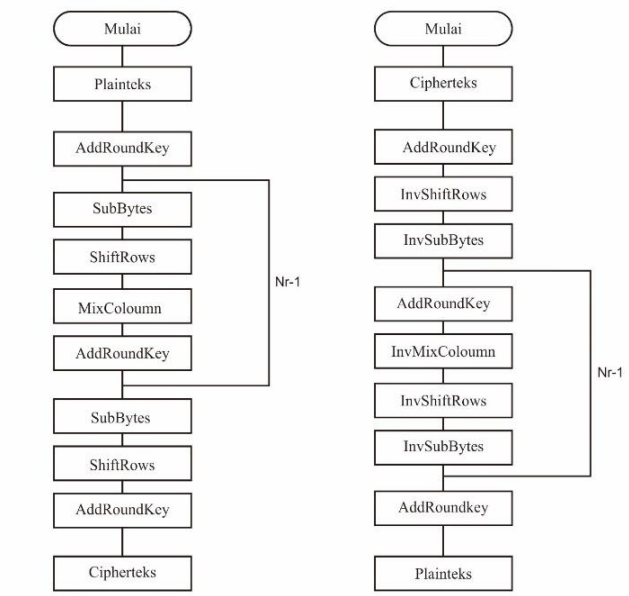
c. Struktur Enkripsi dan Dekripsi *AES*

Proses di dalam algoritma kriptografi AES merupakan transformasi terhadap *state*. Enkripsi AES adalah transformasi terhadap *state* secara berulang dalam beberapa ronde. *State* yang menjadi keluaran ronde k menjadi masukan untuk ronde k+1.

Secara garis besar, proses enkripsi diawali dengan mengonversikan setiap karakter ke dalam bentuk biner dan dimasukkan ke dalam sebuah *state*. Setelah karakter dimasukkan ke dalam *state*, dalam memulai ronde ke-0, karakter-karakter tersebut

harus dicampur dengan kunci ronde ke-0 atau biasa disebut transformasi *AddRoundKey.* Memasuki ronde ke-1 sampai ke-Nr dengan Nr adalah jumlah ronde, masing-masing karakter dalam *state* akan melalui empat transformasi, yakni *SubBytes, ShiftRowa, MixColumg,* dan *AddRoundKey*. Penecualian pada ronde terakhir, langkah yang dilakukan yaitu menghilangkan langkah transformasi *MixColumn*.

Dekripsi dari algoritma *Advanced Encryption Standard* yaitu *invers* dari proses enkripsinya. Setiap transformasi dasar *AES* memiliki transformasi *invers*, yaitu: *InvSubBytes*, *InvShiftRows*, dan *InvMixColoumn*. *AddRoundKey* merupakan transformasi yang bersifat *selfinvers* dengan syarat menggunakan kunci yang sama.



Gambar 2. 1 Diagram Proses Enkripsi dan Dekripsi

d. Transformasi-transformasi *AES*

1) *SubBytes*

Transformasi *SubBytes* dan *invers*-nya (transformasi *InvSubBytes)* adalah transformasi pertukaran setiap *byte* dengan tabel substitusi (S-*Box)*, yaitu dengan cara menginterpretasikan *byte* sebagai dua bilangan heksadesimal, kemudian digit kiri menunjukkan indeks baris dan digit kanan menunjukkan indeks kolom di tabel substitusi.

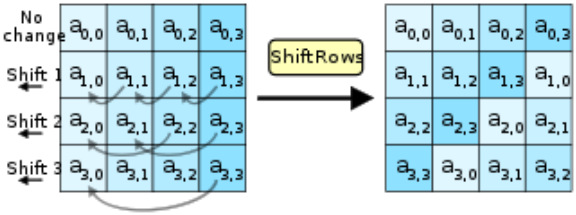
Tabel 2. 2 Tabel Substitusi (*S-Box*)

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2) *ShiftRows*

Transformasi *ShiftRows* adalah transformasi yang mengubah posisi *byte* tanpa mengganti nilainya. *ShiftRows* dilakukan dengan menjalankan operasi *circular shift left* atau menggeser ke kiri sebanyak i pada baris ke-i pada *state*.

Transformasi *invers* terhadap *ShoftRows* disebut *InvShiftRows*. Transformasi ini dilakukan dengan menjalankan operasi *circular shift right* atau menggeser ke kanan sebanyak i pada baris ke-i pada *state*.

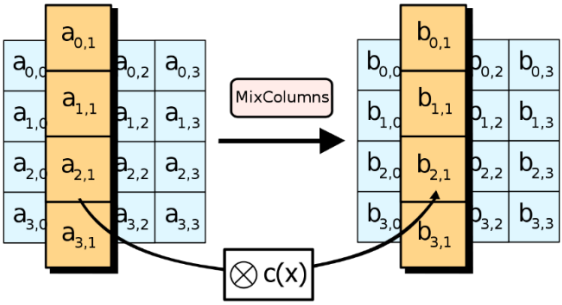


Gambar 2. 2 Proses Transformasi *ShiftRows*

3) *MixColoumn*

Transformasi *MixColoumn* adalah mencampur nilai kolom-kolom pada dalam *state* elemen pada *state* keluaran atau dengan bahasa mudahnya mengalikan matriks yang telah ditentukan dengan kolom-kolom yang ada pada *state*.

Invers dari transformasi *MixColoumn* adalah transformasi *InvMixColoumn*. Transformasi ini menggunakan perkalian matriks konstan dengan *state*. Konstan yang dimaksud adalah *invers* dari matriks yang telah ditentukan pada transformasi *MixColoumn*.



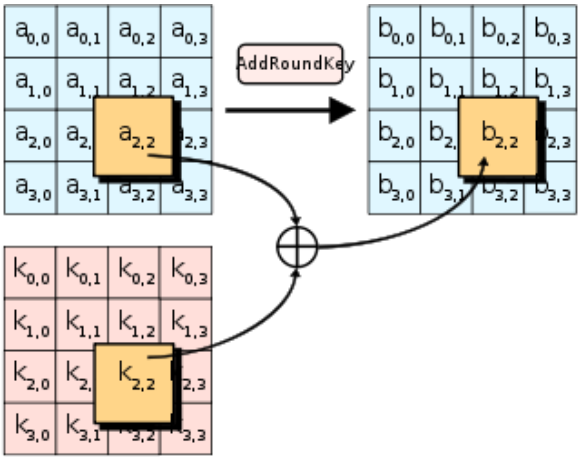
Gambar 2. 3 Proses Transformasi *MixColumn*

4) *AddRoundKey*

Transformasi *AddRoundKey* adalah transformasi yang mencampur suatu *state* masukan dengan kunci ronde menggunakan

operasi eksklusif OR (⊕). Setiap elemen pada *state* masukan yang merupakan sebuah *byte* dikenakan operasi eksklusif OR dengan *byte* pada posisi yang sama di kunci ronde.

Transformasi *AddRoundKey* merupakan transformasi yang bersifat *self invers*, yaitu transformasi *invers* sama dengan transformasi aslinya asalkan menggunakan kunci ronde yang sama.



Gambar 2. 4 Proses Transformasi *AddRoundKey*

e. Ekspansi Kunci *AES*

Ekspansi kunci algoritma *Advanced Encryption Standard* dibuat dengan melakukan *cipher key* sehingga menghasilkan *key schedule*. Pembuatan ekspansi kunci memerlukan $Nb(Nr + 1)$ kata yang

dapat digunakan pada *AES* dengan panjang kunci 128 bit. Proses ini dinamakan *key schedule*.

Key schedule terdiri dari *array* 4 *byte word* linier yang dinotasikan dengan [wi]. *Rotword* adalah menukar bit paling atas ke bit paling bawah secara siklik. *Subword* adalah fungsi yang mengambil 4 *byte* kata dan melakukan transformasi *SubBytes. Rcon* () adalah untuk menghasilkan putaran yang tetap dari larik kata dan berisi nilai yang dihasilkan oleh $[xi - 1, \{00\}, \{00\}, \{00\}]$ dengan $xi - 1$ dari i ke 1.

Proses perputaran kunci dimulai dari pengambilan kolom pertama pada kunci dan dilakukan proses *rotword.* Setelah didapatkan *rotword* maka hasilnya diproses menggunakan *Subword*. Hasil dari *Subword* kemudian di-XOR-kan dengan *Rcon* sehingga didapatkan *sub key* yang baru.

f. Keamanan Algoritma *AES*

Desain dan kekuatan dari semua panjang kunci dari algoritma *Advanced Encryption Standard* (yaitu 128, 192, dan 256) cukup untuk melindungi informasi rahasia hingga tingkat *secret*. Informasi *top secret* akan membutuhkan penggunaan panjang kunci 192 atau 256. Implementasi AES dalam produk yang dimaksudkan untuk melindungi sistem keamanan

nasional dan / atau informasi harus ditinjau dan disertifikasi oleh NSA sebelum diakuisisi dan digunakan.

AES memiliki kerangka kerja aljabar yang cukup sederhana. Pada tahun 2002, serangan teoritis yang disebut XSL *attack* oleh Nicolas Courtoid dan Josef Pieprzyk yang dimaksudkan untuk menunjukkan kelemahan dalam algoritma AES, sebagian karena kompleksitas komponen *nonlinear* yang rendah. Sejak saat itu, makalah lain menunjukkan bahwa serangan itu tidak dapat dilakukan.

Pada akhir proses pemilihan AES, pengembang dari algoritma Twofish yaitu Bruce Schneler menulis bahwa walaupun dia pikir serangan akademik yang berhasil pada Rinjdael akan dikembangkan suatu hari nanti, dia tidak percaya ada orang yang akan menemukan serangan untuk membaca lalu lintas Rinjdael.

Pada 3 Agustus 2009, serangan baru dilakukan oleh Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, dan Adi Shamir bertentangan dengan AES-256 yang hanya menggunakan dua kunci terkait dari 2^{39} kali untuk memulihkan kunci 256-bit lengkap dari versi 9 ronde atau 2^{45} kali untuk versi 10

ronde dengan jenis serangan sub kunci terkait yang lebih kuat, atau 2^{70} kali untuk versi 11 ronde. AES 256-bit menggunakan 14 ronde, jadi serangan ini tidak efektif terhadap AES penuh.

Pada bulan November 2009, serangan *known key distinguishing attack* untuk pertama kalinya terhadap AES 128 versi 8 ronde. Kunci ini adalah peningkatan *rebound* atau serangan *start* dari tengah terhadap permutasi seperti AES yang memandang dua putaran permutasi berturut-turut sebagai penerapan yang disebut super *sbox*. Super *sbox* ini bekerja pada versi 8 ronde AES 128, dengan kompleksitas waktu 2^{48} dan kompleksitas memori 2^{32}. AES 128 bit menggunakan 10 ronde atau putaran, jadi serangan ini tidak efektif terhadap AES-128 penuh.

Berbagai serangan telah dilakukan untuk memecahkan algoritma kriptografi *Advanced Encryption Standard*. Hingga saat ini, tidak ada serangan praktis yang memungkinkan seseorang untuk membaca data yang telah dienkripsi oleh algoritma kriptografi AES.

B. Kajian Penelitian yang Relevan

1. Jurnal Teknik Informatika Vol. 11 No. 2 dengan judul "*Rancangan Aplikasi Pengamanan Data dengan Algoritma Advanced Encryption Standard (AES)*" oleh Angga Aditya Permana dan Desi Nurnaningsih. Hasil dari penelitian ini adalah aplikasi untuk membuat enkripsi *file-file* yang terdapat pada sistem komputer yang berupa *file* dokumen, MP3, PDF dan gambar. Penelitian ini menggunakan aplikasi Microsoft Visual Studio 2010 dengan menggunakan bahasa pemrograman .NET. Perbedaan dengan penelitian skripsi ini adalah bahasa pemrograman dan penerapannya yang berbeda. Bahasa pemrograman yang digunakan pada penelitian skripsi ini adalah bahasa pemrograman PHP dan menerapkannya pada sebuah sistem informasi, sedangkan pada jurnal ini menggunakan bahasa pemrograman .NET dan menerapkannya pada sebuah aplikasi.
2. Jurnal dari ResearchGate: Seminar Nasional Aplikasi Teknologi Informasi 2012 (SNATI 2012) ISSN 1907-5022 dengan judul "*Implementasi Algoritma Rinjdael untuk Enkripsi dan Dekripsi pada Citra Digital*" oleh R. Kristoforus JB dan Stefanus Aditya BP. Jurnal ini penulis mengimplementasikan kriptografi pada citra digital. Perangkat lunak yang dibangun adalah perangkat lunak

enkripsi dan dekripsi dengan algoritma *Rinjdael* untuk citra digital menggunakan metode *Waterfall*. Hasil dari penelitian ini, penulis dapat mengimplementasikan algoritma *Rinjdael* untuk keamanan dan kerahasiaan citra digital dengan format *file* citra *bitmap*. Perbedaan jurnal ini dengan penelitian penulis adalah jurnal ini hanya mengenkripsi citra digital dan mengubahnya kembali ke bentuk semula, sedangkan penelitian penulis yaitu mengimplementasikan enkripsi dan dekripsi berupa teks pada sebuah sistem informasi.

3. Jurnal dari STMIK Mardira Indonesia: Jurnal Computech & Bisnis volume :4 Nomor: 2 ISSN 1978-9629 dengan judul "*Implementasi Algoritma Rinjdael pada Pembuatan Kunci Lisensi Program Pengubah Atribut File*" oleh Budiantoro dan Nanan Rohman. Dalam jurnal ini penulis mengamati algoritma enkripsi pelaksanaan *Rinjdael* pada program yang diuji yaitu program kunci lisensi dan penulis meneliti tentang langkah-langkah dalam enkripsi dan dekripsi algoritma *Rinjdael* seperti *AddRoundKey, Subbytes, ShiftRows, MixColumn* dan akan dilakukan penelitian tentang pelaksanaan program pembuat lisensi yang menghasilkan enkripsi menggunakan berkas lisensi algoritma *Rijdael*. Perbedaan jurnal ini dengan penelitian penulis adalah pada objeknya, jurnal ini

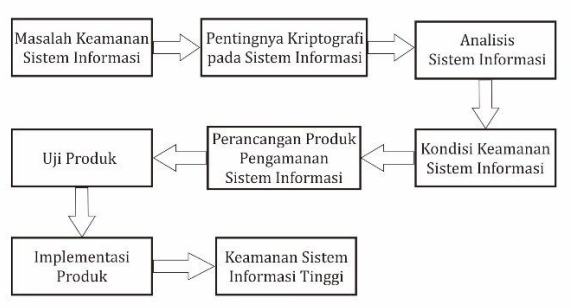
mengimplementasikan algoritma kriptografi *Advanced Encyiption Standard* pada program pengubah atribut *file*, sedangkan penelitian penulis mengimplementasikan algoritma kriptografi *Advanced Encryption Standard* pada sistem informasi.

C. Kerangka Berpikir

Pengamanan pada sebuah sistem informasi adalah suatu hal yang harus dilakukan bagi seorang perancang sistem informasi dalam suatu perusahaan atau instansi. Pengamanan tersebut akan sangat membantu dalam menciptakan sistem informasi yang baik. Metode dalam pengamanan data pada sistem informasi yang berbasis komputer dapat dilakukan dengan menerapkan kriptografi sebagai pertahanan awal pada sebuah sistem informasi. Oleh sebab itu, peneliti ingin mengimplementasikan kriptografi tersebut ke dalam sistem informasi yang ada pada suatu pondok pesantren.

Penelitian ini bertujuan untuk mengamankan data pada sistem informasi di suatu pondok pesantren menggunakan algoritma kriptografi *Advanced Encryption Standard*. Sehingga setelah dilakukannya penelitian ini, diharapkan akan ada peneliti lain yang dapat meningkatkan keamanan sistem informasi dari segi jaringannya.

Alur penelitian ini dapat dilihat dalam diagram alur berikut ini:



Gambar 2. 5 Kerangka Berpikir

D. Pertanyaan Penelitian

1. Bagaimana rancangan produk kriptografi *Advanced Encryption Standard*?
2. Bagaimana validitas dari produk kriptografi *Advanced Encryption Standard*?
3. Bagaimana kepraktisan dalam penerapan produk kriptografi *Advanced Encryption Standard*?
4. Bagaimana keefektifan produk kriptografi *Advanced Encryption Standard* dalam sistem informasi?

BAB III

METODE PENELITIAN

A. Model Pengembangan

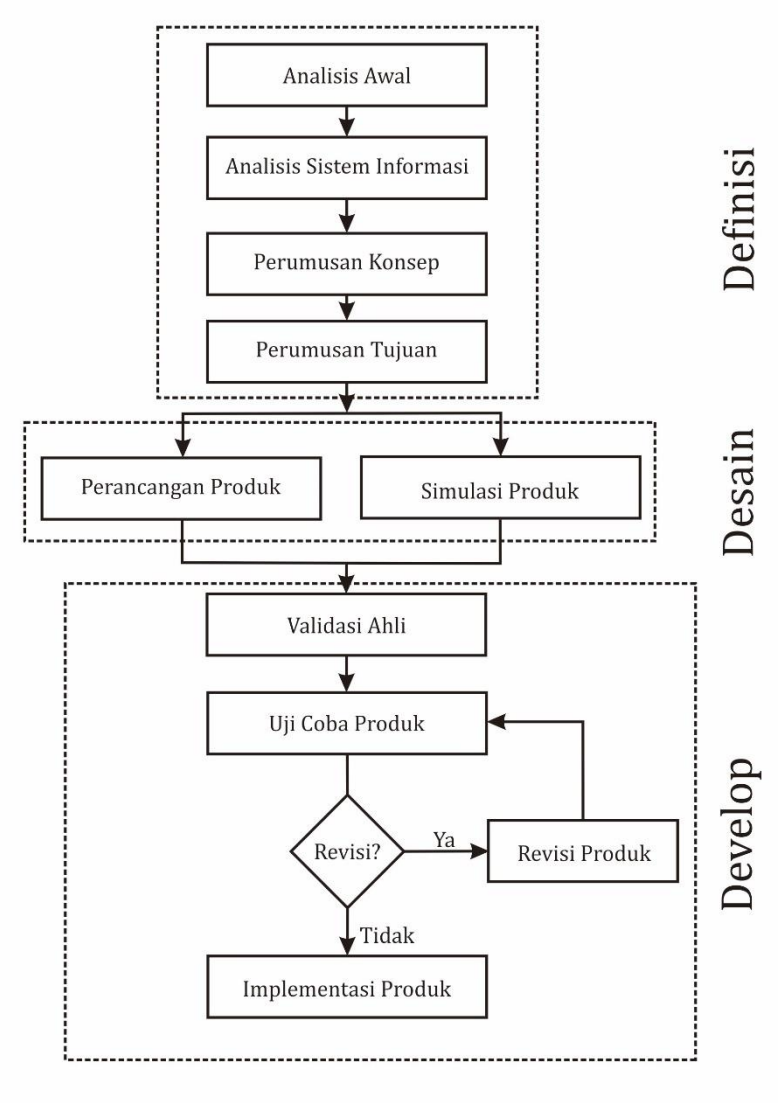
Penelitian ini menggunakan modifikasi model pengembangan 4D menjadi 3D dengan menghilangkan langkah yang keempat *Disseminate*, sehingga langkah pada penelitian ini hanya sebatas yaitu *Define, Design,* dan *Develop*. Pengembangan yang dimaksud dalam penelitian ini adalah mengimplementasikan algoritma kriptografu *AES* (*Advanced Encryption Standard*) pada sistem informasi di pondok pesantren An-Najah. Diharapkan penelitian yang dihasilkan dapat digunakan untuk mengamankan data pada *database* di sistem informasi pondok pesantren An-Najah.

Tahapan dalam metode penelitian ini ada tiga, yaitu *define* (pendefinisian), *design* (perancangan), dan *develop* (pengembangan). Tahap *define* (pendefinisian) adalah pembuatan rancangan awal melalui studi literatur meliputi buku referensi, artikel-artikel yang terkait, dan penelitian yang mendukung untuk penelitian ini. Tahap *design* (perancangan) dilakukan dengan cara merancang desain yang akan dikembangkan berdasarkan potensi dan masalah sesuai dengan teori yang dipahami. Pada tahap ini juga dilakukan penyusunan instrumen penelitian dan validasinya.

Metode ini peneliti pilih karena sesuai untuk mengembangkan produk kriptografi pada sistem informasi. Produk yang dikembangkan kemudian diuji tingkat validitas, keefektifan, dan kepraktisan untuk mengetahui peningkatan keamanan pada sebuah sistem informasi.

B. Prosedur Pengembangan

Metode penelitian pada penelitian ini adalah metode penelitian modifikasi dari 4D menjadi 3D dengan menghilangkan langkah keempat. Sehingga tahapan penelitian ini dapat digambarkan seperti diagram alir berikut ini:



Gambar 3. 1 Desain Pengembangan Produk Kriptografi

1. *Define* (Pendefinisian)

Pada tahap ini, langkah-langkah yang akan dilakukan peneliti dalam pengembangan keamanan sistem informasi pondok pesantren An-Najah adalah sebagai berikut:

a. Identifikasi Masalah

Identifikasi masalah dalam penelitian ini yaitu mengidentifikasi perkembangan sistem informasi di pondok pesantren An-Najah yang berkaitan dengan keamanan dalam sistem informasi tersebut. Adapun langkah-langkah yang dilakukan sebagai berikut:

1) Analisis Awal

Langkah identifikasi masalah yang pertama ini bertujuan untuk mengetahui masalah-masalah yang ada pada sistem informasi yang dijadikan objek penelitian terutama dalam bidang keamanan data. Tahap ini akan dilihatkan fakta tentang keamanan pada sistem informasi dengan permasalahannya sehingga peneliti dapat menentukan pengembangan keamanan yang sesuai dengan sistem informasi.

2) Analisis Sistem Informasi

Analisis sistem informasi ini bertujuan untuk mengetahui segala proses yang ada dalam sistem informasi. Cara yang dilakukan peneliti adalah membongkar isi dari sistem informasi sehingga peneliti mendapatkan informasi sebagai landasan awal pembuatan produk keamanan pada sistem informasi. Analisis sistem informasi meliputi bahasa pemrograman, *library*, dan jenis *database* yang digunakan.

3) Perumusan Konsep

Langkah perumusan konsep ini bertujuan menganalisis langkah-langkah yang akan dijalankan produk pada saat mengamankan data baik dalam proses enkripsi maupun proses dekripsi. Konsep produk dibuat dengan cara menentukan alur utama dalam mengamankan sistem informasi dalam bentuk diagram.

4) Perumusan Tujuan

Perumusan ini bertujuan untuk menentukan indikator pencapaian pada produk yang akan dibuat sesuai dengan rumusan masalah dalam penelitian ini.

b. Tinjauan Pustaka

Pada tahap ini, peneliti mencari bahan bacaan untuk mengkaji penelitian sebelumnya dan mencari teori-teori yang berkaitan dengan penelitian yaitu sistem yang baik, pentingnya keamanan dalam informasi, serta hal-hal yang berhubungan dengan pengembangan penelitian.

2. *Design* (Perancangan)

Pada tahap perancangan, peneliti membuat rancangan awal produk sesuai dengan identifikasi masalah dan teori-teori yang telah dirumuskan pada tahap pendefinisian. Langkah dalam tahap ini meliputi:

a. Perancangan produk

Tahap perancangan produk ini bertujuan memperoleh rancangan produk untuk mengembangkan sistem informasi yang sesuai dengan informasi yang telah diterima. Perancangan produk ini meliputi: penyusunan instrumen penelitian, pemilihan bahasa pemrograman, dan pemilihan perangkat lunak yang akan digunakan pada pembuatan produk kriptografi ini.

b. Simulasi produk

Tahap simulasi ini bertujuan untuk menyimulasikan proses pengamanan pada sistem informasi secara manual dari awal sampai akhir.

3. *Develop* (Pengembangan)

Tahap ini bertujuan untuk menghasilkan produk yang melalu dua tahapan, yaitu tahap penilaian ahli dan tahap uji coba pengembangan.

a. Validasi Ahli (*Ecpert Appraisal*)

Penilaian para ahli terhadap produk bertujuan untuk menilai apakah produk sesuai dengan kriteria penilaian pengembangan terhadap potensi dan masalah yang telah dirumuskan. Kemudian untuk mengetahui kelebihan dan kelemahan dari produk sehingga produk dapat direvisi sesuai dengan masukan dari para ahli untuk membuat produk lebih tepat, efektif, mudah digunakan, dan memiliki kualitas yang tinggi.

b. Uji Coba Pengembangan (*Development Testing*)

Uji coba pengembangan merupakan kegiatan pengujian produk pada sasaran subjek yang sesungguhnya. Uji coba produk dilakukan untuk mengetahui kesesuaian dan manfaat produk dalam penelitian ini. Hasil uji coba produk

digunakan untuk memperbaiki produk hingga diperoleh produk yang tepat, efektif, mudah digunakan, dan memiliki kualitas yang tinggi.

Dalam konteks pengembangan produk, kegiatan pengembangan (*develop*) dilakukan langkah-langkah sebagai berikut:

1) Validasi Produk oleh Ahli

   Hal-hal yang divalidasi meliputi kinerja produk dan keefektifan produk. Validasi produk ini dilakukan untuk mengetahui kelemahan dari produk sehingga produk dapat diperbaiki dan dikatakan layak/baik untuk dikembangkan. Validasi yang dilakukan pada penelitian ini meliputi: uji validitas, uji kepraktisan, dan uji keefektifan sehingga diharapkan produk sesuai dengan teori-teori yang ada, praktis dalam mengimplementasikan dan efektif dalam penggunaan produk.

2) Revisi Produk

   Setelah para ahli menilai produk melalui diskusi maka akan diketahui kelemahan dari produk dan dilakukan revisi produk untuk memperbaiki kelemahan dan kesalahan sehingga produk dapat dikembangkan

dengan sempurna. Pada tahap ini peneliti merevisi produk sesuai dengan saran perbaikan dari para ahli.

3) Uji Coba Produk

Setelah proses revisi, produk diuji coba pada sistem untuk mengetahui kesesuaian dan manfaat produk dalam penelitian ini.

4) Revisi Produk

Setelah uji coba produk secara terbatas, produk direvisi kembali untuk memperbaiki masalah-masalah yang ditemukan saat uji coba. Revisi produk diperbaiki kembali berdasarkan saran dari uji coba produk. Revisi ini bertujuan menyempurnakan kembali produk sehingga dapat diimplementasikan pada kondisi nyata berdasarkan uji coba.

5) Implementasi Produk

Setelah produk diuji coba dan direvisi, kemudian produk diimplementasikan pada sistem yang akan dikembangkan untuk diuji keefektifan dan kesesuaian produk pada objek penelitian. Apabila objek penelitian lebih baik dari sebelumnya maka produk yang dikembangkan dinyatakan efektif dan sesuai.

C. Desain Uji Coba Produk

1. Desain Uji Coba

   Penelitian ini adalah pengembangan produk yang dilakukan secara individu. Kegiatan yang dilakukan dalam penelitian ini yaitu melakukan observasi terhadap sistem informasi secara langsung, menganalisis sistem informasi, membuat produk algoritma kriptografi *Advanced Encryption Standard*, menguji kelayakan produk dengan cara melakukan validasi kepada beberapa pakar. Hasil validasi dalam penelitian ini harus bernilai baik atau sangat baik.

   Desain awal produk ini adalah sebuah *script* yang dapat diimplementasikan pada sistem informasi dengan bahasa pemrograman yang sama dan dapat mengamankan data pada sistem informasi tersebut.

   Uji coba produk ini dilakukan dengan mengimplementasikan langsung terhadap sistem informasi. Proses enkripsi dan dekripsi adalah proses yang harus terpenuhi dalam uji coba ini. Jika kedua proses tersebut berjalan dengan lancar dan tanpa ada masalah baik berupa *bug* atau kesalahan sistem maka uji coba produk dinyatakan berhasil.

2. Subjek Penelitian

   Subjek penelitian dalam penelitian ini adalah dosen Matematika yang berspesifikasi pada bidang

kriptografi sebagai penguji ahli dalam uji validitas produk dan pembuat sistem informasi sebagai penguji ahli dalam bidang keefektifan dan kepraktisan produk.

3. Teknik dan Instrumen Pengumpulan Data

a) Uji Validitas Produk Kriptografi

Lembar validitas produk kriptografi ini bertujuan untuk mengetahui validitas produk algoritma kriptografi *Advanced Encryption Standard* yang dikembangkan dalam mengembangkan sistem informasi.

Prosedur pengembangan validitas produk kriptografi untuk meningkatkan keamanan pada sistem informasi adalah sebagai berikut.

a. Menentukan indikator yaitu rasionalisasi produk kriptografi, landasan teori pengembangan, fase pengembangan, karakteristik produk, dan keutuhan data produk.
b. Menjabarkan setiap indikator menjadi nomor pernyataan dan kriteria penilaiannya.
c. Menyusun lembar uji dengan susunan judul, tujuan, kisi-kisi, bentuk instrumen, cara penggunaan, petunjuk penggunaan, pernyataan penilaian, komentar dan saran,

indikator penilaian, dan kesimpulan penilaian.

Teknik penggunaan uji validitas produk ini adalah menyerahkan *script* dan produk kepada penguji ahli yang berkualifikasi akademik di bidang kriptografi untuk dimintakan penilaian. Penyusunan instrumen uji ini menggunakan skala *likert* dengan lima kategori nilai, yaitu: (1) tidak baik, sehingga produk tidak dapat digunakan dan harus diganti, (2) kurang baik sehingga belum dapat digunakan dan masih memerlukan konsultasi, (3) cukup baik sehingga produk dapat digunakan tetapi dengan banyak revisi, (4) baik sehingga dapat digunakan dengan sedikit revisi, dan (5) sangat baik sehingga produk dapat digunakan tanpa revisi.

b) Uji Keefektifan Produk Kriptografi

Lembar uji keefektifan produk kriptografi ini bertujuan untuk mengetahui efektivitas produk yang dikembangkan dalam meningkatkan keamanan pada sistem informasi.

Prosedur pengembangan uji keefektifan produk kriptografi untuk meningkatkan keamanan pada sistem informasi adalah sebagai berikut.

1) Menentukan indikator yaitu kondisi produk kriptografi *Advanced Encryption Standard*, proses enkripsi kriptografi *Advanced Encryption Standard*, dan kerahasiaan produk kriptografi *Advanced Encryption Standard.*
2) Menjabarkan setiap indikator menjadi nomor pernyataan dan kriteria penilaiannya.
3) Menyusun lembar uji dengan susunan judul, tujuan, kisi-kisi, bentuk instrumen, cara penggunaan, petunjuk penggunaan, pernyataan penilaian, komentar dan saran, indikator penilaian, dan kesimpulan penilaian.

Teknik penggunaan uji keefektifan produk ini adalah menyerahkan *script* dan produk kepada penguji ahli yaitu pembuat sistem informasi untuk dimintakan penilaian. Penyusunan instrumen uji ini menggunakan skala *likert* dengan lima kategori nilai, yaitu: (1) tidak baik, sehingga produk tidak dapat digunakan dan harus diganti, (2) kurang baik sehingga belum dapat digunakan dan masih memerlukan konsultasi, (3) cukup baik sehingga

produk dapat digunakan tetapi dengan banyak revisi, (4) baik sehingga dapat digunakan dengan sedikit revisi, dan (5) sangat baik sehingga produk dapat digunakan tanpa revisi.

c) Uji Kepraktisan Produk Kriptografi

Lembar uji keefektifan produk kriptografi ini bertujuan untuk mengetahui kepraktisan produk yang dikembangkan dalam meningkatkan keamanan pada sistem informasi.

Prosedur pengembangan uji kepraktisan produk kriptografi untuk meningkatkan keamanan pada sistem informasi adalah sebagai berikut.

1) Menentukan indikator yaitu kesesuaian produk kriptografi *Advanced Encryption Standard*, penggunaan produk kriptografi *Advanced Encryption Standard,* keutuhan data produk kriptografi *Advanced Encryption Standard,*, dan keaslian data produk kriptografi *Advanced Encryption Standard.*
2) Menjabarkan setiap indikator menjadi nomor pernyataan dan kriteria penilaiannya.

3) Menyusun lembar uji dengan susunan judul, tujuan, kisi-kisi, bentuk instrumen, cara penggunaan, petunjuk penggunaan, pernyataan penilaian, komentar dan saran, indikator penilaian, dan kesimpulan penilaian.

Teknik penggunaan uji kepraktisan produk ini adalah menyerahkan *script* dan produk kepada penguji ahli yaitu pembuat sistem informasi untuk dimintakan penilaian. Penyusunan instrumen uji ini menggunakan skala *likert* dengan lima kategori nilai, yaitu: (1) tidak baik, sehingga produk tidak dapat digunakan dan harus diganti, (2) kurang baik sehingga belum dapat digunakan dan masih memerlukan konsultasi, (3) cukup baik sehingga produk dapat digunakan tetapi dengan banyak revisi, (4) baik sehingga dapat digunakan dengan sedikit revisi, dan (5) sangat baik sehingga produk dapat digunakan tanpa revisi.

4. Teknik Analisis Data

a. Teknik Analisis untuk Uji Validitas

Penelitian ini akan dianalisis secara kualitatif. Data yang dianalisis adalah hasil penilaian uji validitas produk.

Hasil penilaian data yang dianalisis digunakan untuk menilai validitas produk kriptografi, dengan langkah sebagai berikut.

1) Merekap semua penilaian dari indikator ke dalam tabel.
2) Mencari rata-rata nilai setiap aspek pernyataan yang dinilai.

   $\bar{X} = \frac{\sum x}{N}$

   Keterangan:

   $\bar{X}$ = Nilai rata-rata

   $\sum x$ = Jumlah skor

   N = Jumlah indikator
3) Menentukan validitas produk kriptografi dengan cara mencocokkan rata-rata penilaian terhadap kategori yang telah ditentukan sebagai berikut.

   Tabel 3. 1 Kriteria Penilaian Validitas

No.	Nilai	Keterangan
1.	$1{,}00 \leq \bar{X} \leq 1{,}80$	Tidak baik
2.	$1{,}80 < \bar{X} \leq 2{,}60$	Kurang baik
3.	$2{,}60 < \bar{X} \leq 3{,}40$	Cukup baik
4.	$3{,}40 < \bar{X} \leq 4{,}20$	Baik
5.	$4{,}20 < \bar{X} \leq 5{,}00$	Sangat baik

Keterangan:

a) Produk dikatakan valid apabila $\bar{X}$ dari pernyataan terkait dalam kategori baik atau sangat baik.
b) Produk dikatakan tidak valid apabila $\bar{X}$ dari pernyataan terkait dalam kategori tidak baik, kurang baik, dan cukup baik.

b. Teknik Analisis untuk Uji Kepraktisan

Penelitian ini akan dianalisis secara kualitatif. Data yang dianalisis adalah hasil penilaian uji kepraktisan produk.

Hasil penilaian data yang dianalisis digunakan untuk menilai kepraktisan produk kriptografi, dengan langkah sebagai berikut.

1) Merekap semua penilaian dari indikator ke dalam tabel.
2) Mencari rata-rata nilai setiap aspek pernyataan yang dinilai.

$$\bar{X} = \frac{\sum x}{N}$$

Keterangan:

$\bar{X}$ = Nilai rata-rata

$\sum x$ = Jumlah skor

N = Jumlah indikator

3) Menentukan kepraktisan produk kriptografi dengan cara mencocokkan rata-rata penilaian terhadap kategori yang telah ditentukan sebagai berikut.

Tabel 3. 2 Kriteria Penilaian Kepraktisan

No.	Nilai	Keterangan
1.	$1{,}00 \leq \bar{X} \leq 1{,}80$	Tidak baik
2.	$1{,}80 < \bar{X} \leq 2{,}60$	Kurang baik
3.	$2{,}60 < \bar{X} \leq 3{,}40$	Cukup baik
4.	$3{,}40 < \bar{X} \leq 4{,}20$	Baik
5.	$4{,}20 < \bar{X} \leq 5{,}00$	Sangat baik

Keterangan:

a) Produk dikatakan praktis apabila $\bar{X}$ dari pernyataan terkait dalam kategori baik atau sangat baik.

b) Produk dikatakan tidak praktis apabila $\bar{X}$ dari pernyataan terkait dalam kategori tidak baik, kurang baik, dan cukup baik.

c. Teknik Analisis untuk Uji Keefektifan

Penelitian ini akan dianalisis secara kualitatif. Data yang dianalisis adalah hasil penilaian uji keefektifan produk.

Hasil penilaian data yang dianalisis digunakan untuk menilai efektivitas produk kriptografi, dengan langkah sebagai berikut.

1) Merekap semua penilaian dari indikator ke dalam tabel.
2) Mencari rata-rata nilai setiap aspek pernyataan yang dinilai.

   $\bar{X} = \frac{\sum x}{N}$

   Keterangan:

   $\bar{X}$ = Nilai rata-rata

   $\sum x$ = Jumlah skor

   N = Jumlah indikator
3) Menentukan validitas produk kriptografi dengan cara mencocokkan rata-rata penilaian terhadap kategori yang telah ditentukan sebagai berikut.

   Tabel 3. 3 Kriteria Penilaian Keefektifan

No.	Nilai	Keterangan
1.	$1{,}00 \leq \bar{X} \leq 1{,}80$	Tidak baik
2.	$1{,}80 < \bar{X} \leq 2{,}60$	Kurang baik
3.	$2{,}60 < \bar{X} \leq 3{,}40$	Cukup baik
4.	$3{,}40 < \bar{X} \leq 4{,}20$	Baik
5.	$4{,}20 < \bar{X} \leq 5{,}00$	Sangat baik

   Keterangan:

a) Produk dikatakan efektif apabila $\bar{X}$ dari pernyataan terkait dalam kategori baik atau sangat baik.
b) Produk dikatakan tidak efektif apabila $\bar{X}$ dari pernyataan terkait dalam kategori tidak baik, kurang baik, dan cukup baik.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil Pengembangan Produk Awal

1. Tahap Pendefinisian

   Pada tahap pendefinisian ini bertujuan untuk menganalisis dan mengidentifikasi masalah untuk memperoleh berbagai informasi yang berkaitan dengan produk yang akan dikembangkan.

   a. Analisis Awal

      Pada langkah ini, peneliti melakukan observasi pada sistem informasi di pondok pesantren An-Najah untuk mengetahui masalah-masalah yang ada pada sistem informasi terutama dalam bidang keamanan data.

      Dari hasil observasi dan diskusi dengan pembuat sistem informasi, peneliti memperoleh informasi yaitu dalam sistem informasi yang telah dibuat, tidak ada satu pun enkripsi pada semua data yang ada dalam sistem informasi. Berdasarkan informasi tersebut, peneliti memilih produk kriptografi *Advanced Encryption Standard* (*AES*) sebagai enkripsi pada sistem informasi tersebut. Kriptografi *AES* tersebut merupakan kriptografi simetris yang telah

diakui aman dan cepat dalam proses enkripsi maupun dekripsinya.

b. Analisis Sistem Informasi

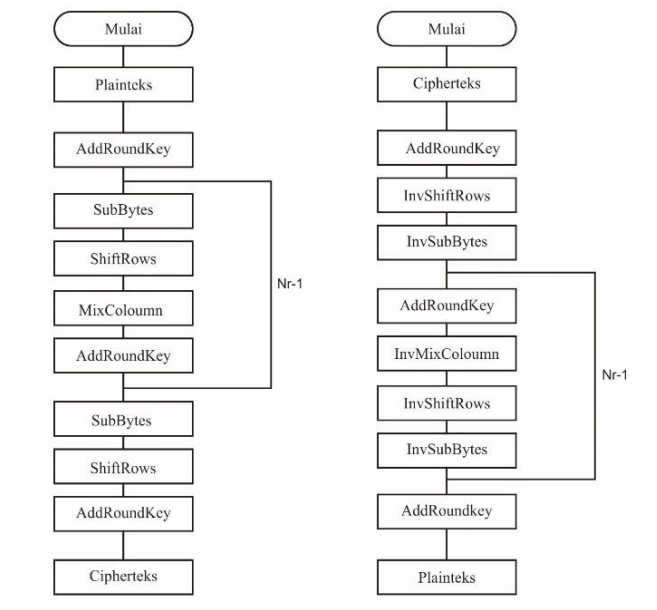
Pada langkah ini, peneliti melakukan observasi terhadap sistem informasi untuk mengetahui segala proses yang ada dalam sistem informasi.

Dari observasi yang dilakukan, peneliti menemukan beberapa informasi tentang proses yang terjadi pada sistem informasi tersebut di antaranya 1). Bahasa pemrograman yang terdapat dalam sistem informasi terdiri dari *HTML*, *PHP*, dan *Javascript*. 2). *Library* yang digunakan adalah *JQuery*. 3). *Database* disimpan pada *MySQL* dikarenakan masih tahap pengembangan dan belum dimuat dalam laman web.

c. Perumusan Konsep

Pada langkah ini, peneliti akan menganalisis langkah-langkah yang akan dijalankan produk pada saat proses enkripsi. Analisis ini bertujuan untuk menyusun langkah-langkah yang akan dijalankan program berdasarkan analisis awal.

Berdasarkan teori-teori yang terdapat pada algoritma kriptografi *Advanced Encryption Standard*, maka diperoleh algoritma sebagai berikut:



Gambar 4. 1 Konsep Ekripsi dan Dekripsi

d. Perumusan Tujuan

Pada langkah ini, peneliti membuat indikator pencapaian pada produk yang akan dibuat peneliti sesuai dengan rumusan masalah dalam penelitian ini. Adapun uraian tujuan produk dalam penelitian ini sebagai berikut.

Tabel 4. 1 Tujuan Produk

No.	Tujuan Produk
1.	Produk efektif pada sistem informasi
2.	Produk praktis dalam penggunaan
3.	Produk dapat diuji coba
4.	Produk dapat mengamankan data

2. Tahap Perancangan

Pada tahap perancangan ini, peneliti membuat rancangan awal produk yang akan dikembangkan sesuai dengan identifikasi masalah yang telah dirumuskan pada tahap pendefinisian. Selain itu, pada tahap ini peneliti juga membuat instrumen penelitian yang digunakan untuk mendukung terlaksananya uji coba produk. Langkah-langkah pada tahap perancangan ini adalah sebagai berikut.

a. Perancangan Produk

Langkah ini bertujuan membuat rancangan produk kriptografi *Advanced Encryption Standard* untuk mengembangkan sistem informasi sehingga diperoleh rancangan sesuai dengan informasi yang telah diterima.

1) Penyusunan instrumen penelitian

Pada langkah ini, peneliti menyusun instrumen penelitian yang akan digunakan sebagai alat ukur pengujian dalam penelitian ini. Penelitian ini memiliki tiga uji yaitu uji validitas, uji kepraktisan, dan uji keefektifan yang akan diberikan kepada penguji.

Tujuan dari langkah ini adalah menyusun alat ukur untuk mengetahui validitas produk, kepraktisan dalam implementasi produk, dan keefektifan dalam penggunaan produk.

2) Pemilihan bahasa pemrograman

Pada langkah ini, peneliti memilih bahasa pemrograman yang sesuai dengan sistem informasi yang akan menjadi objek penelitian. Berdasarkan analisis pada sistem informasi, diperoleh informasi tentang bahasa pemrograman yang digunakan adalah bahasa pemrograman PHP, sehingga dalam penelitian ini bahasa yang digunakan adalah bahasa pemrograman PHP.

3) Pemilihan perangkat lunak

Pemilihan perangkat lunak pada penelitian ini meliputi perangkat lunak yang berfungsi

sebagai penulisan *script* dalam bahasa pemrograman PHP, server lokal, dan perangkat lunak sebagai *database*.

Perangkat lunak yang digunakan peneliti dalam penulisan *script* adalah Microsoft Studio Code, sedangkan untuk server lokal dan *database*, peneliti menggunakan perangkat lunak XAMPP.

b. Simulasi Produk

Pada tahap ini, peneliti akan menyimulasikan proses enkripsi algoritma kriptografi *Advanced Encryption Standard* pada ronde 0 dan ronde 1. Misalkan peneliti mengambil sebuah *plaintext* dan kunci sebagai berikut.

Plaintext = UIN WALISONGO

Kunci = SIAnnajahgondang

Langkah pertama yang dilakukan adalah mengubah *plaintext* dan kunci ke dalam bentuk blok 4x4 dan mengubah ke dalam bentuk heksadesimal.

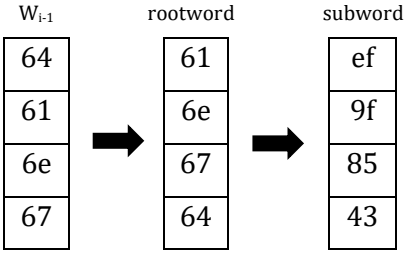
Plaintext =

U	W	S	O	=	55	57	53	4f
I	A	O			49	41	4f	00
N	L	N			4e	4c	4e	00
	I	G			20	49	47	00

Kunci =

S	n	h	d	=	53	6e	68	64
I	a	g	a		49	61	67	61
A	j	o	n		41	6a	6f	6e
n	a	n	g		6e	61	6e	67

Langkah kedua yaitu membuat pembangkit kunci atau *Key* Ekspansi. *Key* ekspansi adalah melaksanakan kunci kode untuk menghasilkan suatu kunci skedul. Kunci ekspansi yang diperlukan algoritma *AES* yaitu Nb(Nr+1) kata dengan Nb adalah jumlah blok dan Nr adalah jumlah putaran sehingga untuk algoritma *AES* 128-bit memerlukan 4(10+1) = 44 kata. Untuk membuat satu putaran *key* skedul, diperlukan
langkah-langkah sebagai berikut:



Langkah Pertama

W_{i-4}		Hasil Subword		Rcon		Round Key 1
53	⊕	ef	⊕	01	=	bd
49		9f		00		d6
41		85		00		c4
6e		43		00		2d

Langkah Kedua

Proses pencarian nilai sebagai berikut. (lakukan pada setiap baris)

53 = 0 1 0 1 0 0 1 1

ef = 1 1 1 0 1 1 1 1

01 = 0 0 0 0 0 0 0 1 ⊕

bd = 1 0 1 1 1 1 0 1

6e		bd		D3
61	⊕	d6	=	B7
6a		c4		Ae
61		2d		4c

Langkah Ketiga

Proses pencarian nilai sebagai berikut. (lakukan pada setiap baris)

6e = 0 1 1 0 1 1 1 0

bd = 1 0 1 1 1 1 0 1 ⊕

d3 = 1 1 0 1 0 0 1 0

W_{i-4}		W_{i-1}		
68	⊕	D3	=	Bb
67		B7		D0
6f		Ae		C1
6e		4c		22

Langkah Keempat

Proses pencarian sebagai berikut. (lakukan pada setiap baris)

68 = 0 1 1 0 1 0 0 0

D3= 1 1 0 1 0 0 1 1 ⊕

bb = 1 0 1 1 1 0 1 1

W_{i-4}		W_{i-1}		
64	⊕	Bb	=	Df
61		D0		B1
6e		C1		c1
67		22		45

Langkah Kelima

Proses pencarian nilai sebagai berikut. (lakukan pada setiap baris)

bb = 1 0 1 1 1 0 1 1

64 = 0 1 1 0 0 1 0 0 ⊕

df = 1 1 0 1 1 1 1 1

Ketika semua langkah diulang-ulang sampai banyaknya putaran, maka akan menghasilkan skedul kunci sebagai berikut:

53	6e	68	64	bd	d3	bb	df	77	a4	1f	c0
49	61	67	61	d6	b7	d0	b1	af	18	c8	79
41	6a	6f	6e	c4	ae	C1	af	aa	04	c5	6a
6e	61	6e	67	2d	4c	22	45	b3	ff	dd	98
Ronde 0				Ronde 1				Ronde 2			
61	7e	be	3f	5e	20	94	61	57	09	29	b7
b5	7d	04	0d	b8	c5	c1	b5	76	ce	0b	ca
e8	2d	47	81	69	44	03	e8	6c	35	71	72
f6	2b	b3	a7	51	7a	c9	f6	ac	fd	87	4c
Ronde 3				Ronde 4				Ronde 5			
03	0a	23	94	51	5b	78	ec	d3	88	f0	1c
36	f8	f3	39	58	a0	53	6a	95	35	66	0c
73	46	37	45	b4	f2	c5	80	35	c7	02	82
05	f8	7f	31	27	df	a0	91	e9	36	96	07
Ronde 6				Ronde 7				Ronde 8			
36	be	4e	52	35	8b	c5	97				
86	b3	d5	d9	2f	9c	49	90				
f0	37	35	b7	45	72	47	f0				
75	43	d5	d2	75	36	e3	31				
Ronde 9				Ronde 10							

Tabel 4. 2 Tabel *Rcon*

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Langkah ketiga yaitu proses enkripsi. Adapun algoritma dalam kriptografi *Advanced Enctyption Standard* adalah sebagai berikut:

1. Melakukan transformasi *AddRoundKey* dengan cara melakukan operasi XOR antara *plaintext* dengan *cipherkey* seperti contoh berikut ini:

55	57	53	4f
49	41	4f	00
4e	4c	4e	00
20	49	47	00

$\oplus$

53	6e	68	64
49	61	67	61
41	6a	6f	6e
6e	61	6e	67

=

06	39	3b	2b
00	20	28	61
0f	26	21	6e
4e	28	29	67

Proses pencarian nilai *AddRoundKey*. (lakukan pada setiap baris dan kolom yang sama)

55 = 0 1 0 1 0 1 0 1

53 = 0 1 0 1 0 0 1 1 $\oplus$

06 = 0 0 0 0 0 1 1 0

2. Melakukan transformasi *SubBytes* dengan cara melakukan operasi substitusi tak linear yang beroperasi secara mandiri pada setiap *byte* dengan menggunakan tabel s-Box seperti contoh berikut:

06	39	3b	2b
00	20	28	61
0f	26	21	6e
4e	28	29	67

=

6f	12	e2	f1
63	b7	34	ef
76	f7	fd	9f
2f	34	a5	85

3. Melakukan transformasi *ShiftRows*. Pada operasi ini - *byte-byte* yang ada pada baris terakhir *state* digeser secara memutar dengan jumlah pergeseran acak, tetapi baris pertama tidak digeser seperti contoh berikut:

6f	12	e2	f1
63	b7	34	ef
76	f7	fd	9f
2f	34	a5	85

=

6f	12	e2	f1
b7	34	ef	63
fd	9f	76	f7
85	2f	34	a5

4. Melakukan transformasi *MixColumn*. Operasi ini beroperasi pada *state* kolom dengan memperlakukan setiap kolom sebagai *polinomial*. Transformasi ini dapat digambarkan dengan perlakuan matriks seperti di bawah ini:

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

×

6f
b7
fd
85

=

64
c8
b7
0e

Proses pencarian transformasi *mixcolumn* sebagai berikut.

02 x 6f

03 x b7

01 x Fd

01 x 85

1. {02 . 6f}

6f = 0 1 1 0 1 1 1 1

{6f . 02}= 1 1 0 1 1 1 1 0

2. {03 . b7}

b7 = 1 0 1 1 0 1 1 1

03 = 1 1

= 1 0 + 0 1

{03 . b7}= (1 0 ⊕ 0 1) (1 0 1 1 0 1 1 1)

= (1 0 1 1 0 1 1 1 . 1 0) ⊕ (1 0 1 1 0 1 1 1 . 0 1)

= 0 1 1 0 1 1 1 0 ⊕ 0 0 0 1 1 0 1 1 ⊕ 1 0 1 1 0 1 1 1

= 1 1 0 0 0 0 1 0

(67 . 02) 1 1 0 1 1 1 1 0

(67 . 03) 1 1 0 0 0 0 1 0

fd = 1 1 1 1 1 1 0 1

85 = 1 0 0 0 0 1 0 1

64 = 0 1 1 0 0 1 0 0

Sehingga jika matriks tersebut dikalikan dengan satu *state* akan menghasilkan sebagai berikut:

64	83	ad	ea
c8	ef	72	c3
b7	89	bd	cc
0e	90	93	cd

Jika seluruh langkah-langkah tersebut diulang sampai banyaknya putaran, maka hasil akan terlihat seperti pada tabel yang terdapat pada lampiran.

B. Hasil Uji Coba Produk

1) Validasi Validitas Produk

Validasi validitas produk ini bertujuan untuk mengetahui validitas produk algoritma *Advanced Encryption Standard* yang telah dikembangkan untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah. Validasi ini dilakukan oleh ahli kriptografi.. Instrumen yang digunakan menggunakan skala *likert* dengan lima kategori penilaian terhadap validitas produk. Aspek penilaian ini meliputi Rasionalisasi Pengembangan, Landasan Teori, Fase Pengembangan, Karakteristik, Keutuhan Data. Adapun hasil penilaian dari validasi ini adalah sebagai berikut.

Tabel 4. 3 Penilaian Validasi Validitas

No.	Aspek Penilaian	Nilai	Kategori
1.	Rasionalisasi Pengembangan	5	Sangat Baik
2.	Landasan Teori	5	Sangat Baik
3.	Fase Pengembangan	4,7	Sangat Baik
4.	Karakteristik Produk	4	Sangat Baik
5.	Keutuhan Data	5	Sangat Baik
Rata-rata Nilai		4,74	Sangat Baik

Hasil penilaian validitas produk secara keseluruhan mendapatkan nilai 4,74 dari nilai maksimal 5 dengan komentar dan saran perbaikan yaitu "Program yang dibuat sudah sangat baik sekali dan dapat meningkatkan keamanan sistem informasi pondok pesantren An-Najah, Untuk saran sebaiknya perlu juga dihitung kompleksitas dari algoritma yang dibuat. Dalam membuat sistem keamanan kita juga harus memperhatikan tingkat keamanan algoritma uang dibuat".

Berdasarkan kategori nilai validitas produk, maka produk dinyatakan "Sangat Baik" untuk diimplementasikan pada sistem informasi.

2) Validasi Kepraktisan Produk

Validasi kepraktisan produk ini bertujuan untuk mengetahui kepraktisan produk algoritma *Advanced Encryption Standard* yang telah dikembangkan untuk

meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah. Validasi ini dilakukan oleh pembuat sistem informasi atau *Superadministrator* sistem informasi. Instrumen yang digunakan menggunakan skala likert dengan lima kategori penilaian terhadap kepraktisan produk. Aspek penilaian ini meliputi kesesuaian produk, penggunaan produk, keutuhan data, dan keaslian data pada produk. Adapun hasil penilaian dari validasi ini adalah sebagai berikut:

Tabel 4. 4 Penilaian Validasi Kepraktisan

No.	Aspek Penilaian	Nilai	Kategori
1.	Penggunaan Produk	5	Sangat Baik
2.	Proses Instalasi	5	Sangat Baik
3.	Keutuhan Data	5	Sangat Baik
4.	Keaslian Data	5	Sangat Baik
Rata-rata Nilai		5	Sangat Baik

Hasil penilaian validasi kepraktisan produk secara keseluruhan mendapatkan nilai 5 dari nilai maksimal 5. Berdasarkan kategori nilai validasi kepraktisan, maka produk dinyatakan “Sangat Baik” untuk diimplementasikan pada sistem informasi.

3) Validasi Keefektifan Produk

Validasi keefektifan produk ini bertujuan untuk mengetahui efektivitas produk algoritma kriptografi *Advanced Encryption Standard* yang telah dikembangkan untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah. Validasi ini dilakukan oleh pembuat sistem informasi atau *superadministrator* sistem informasi. Instrumen yang digunakan menggunakan skala *likert* dengan lima kategori penilaian terhadap keefektifan produk. Aspek penilaian keefektifan produk meliputi, kondisi produk, proses enkripsi, dan kerahasiaan data. Adapun penilaian dari validasi ini adalah sebagai berikut:

Tabel 4. 5 Penilaian Validasi Keefektifan

No.	Aspek Penilaian	Nilai	Kategori
1.	Kondisi produk	4,7	Sangat Baik
2.	Proses Enkripsi	5	Sangat Baik
3.	Kerahasiaan Data	5	Sangat Baik
Rata-rata Nilai		4,9	Sangat Baik

Hasil penilaian validasi keefektifan produk secara keseluruhan mendapatkan nilai 4,9 dari nilai maksimal 5 dengan komentar dan saran perbaikan yaitu “enkripsi sangat bagus, akan tetapi terkadang terjadi tulisan

"\n\n" ketika di dekripsi. Jadi alangkah baiknya sebelum di dekripsi perlu di *replace* dulu karakter "\n\n\n" biar tidak muncul ketika di dekripsi".

Berdasarkan kategori nilai validasi keefektifan, maka produk dinyatakan "Sangat Baik" untuk diimplementasikan pada sistem informasi.

4) Uji Coba Produk

Setelah produk melalui tahap validasi dan dinyatakan layak/baik digunakan sebagai pengamanan pada sistem informasi, kemudian produk di uji coba dengan mengimplementasikan produk pada sistem informasi pondok pesantren An-Najah untuk mendapatkan hasil kesesuaian antara produk dengan sistem informasi. Adapun hasil uji coba produk algoritma *Advanced Encryption Standard* adalah sebagai berikut.

Tabel 4. 6 Uji Coba

Butir Uji	Hasil yang diharapkan	Hasil yang diamati	Keterangan
Enkripsi *Password*	Data dapat dienkripsi sehingga menghasilkan *output ciphertext*	Data berhasil dienkripsi sehingga menghasilkan *output ciphertext*	Sukses
Enkripsi *id transaksi*			
Enkripsi *id pembayaran*			
Enkripsi *chat*			
Dekripsi *Password*	Data dapat didekripsi sehingga menghasilkan *output plaintext*	Data berhasil didekripsi sehingga menghasilkan *output plaintext*	Sukses
Dekripsi *id transaksi*			
Dekripsi *id pembayaran*			
Dekripsi *chat*			

Berdasarkan hasil uji coba, produk berjalan sesuai dengan yang diharapkan sehingga produk dapat diimplementasikan pada sistem informasi tanpa kendala.

5) Perbandingan Sebelum dan Sesudah Implementasi Algoritma Kriptografi pada Sistem Informasi

a. Estimasi Waktu

Tabel 4. 7 Perbandingan Estimasi Waktu (detik)

Proses	Banyak Huruf	Sebelum	Sesudah
Mengirim	13 Huruf	0,0000018	0,001026
	27 Huruf	0,000006	0,001902
	54 Huruf	0,0000062	0,002927
	81 Huruf	0,000007	0,004262
Menerima	24 Huruf	0,0000038	0,001494
	44 Huruf	0,000019	0,0020
	88 Huruf	0,000021	0,003889
	128 Huruf	0,000023	0,004482

Berdasarkan tabel di atas, perbandingan waktu antara sebelum dan sesudah produk diimplementasikan pada sistem informasi tidak jauh berbeda dan masih berkisar antara 0,001-0,004 detik. Hal ini dapat disimpulkan bahwa, produk tidak membebani sistem informasi dan terbukti efektif pada sistem informasi.

b. Keamanan Data

Tabel 4. 8 Perbandingan Kata Sebelum dan setelaj implementasi Produk

KATA	
Sebelum	Setelah
UIN WALISONGO	UwfqwpV0eDpB0spm5c1hAA==
UIN WALISONGO SEMARANG	TdVBDVJT5gThJXLdLZIoDHN5kivqDGr2tctIhAKbU0g=
Sistem Informasi Pondok Pesantren An-Najah	ZaYbhBDaScxsPV8GFASK7aRTSfB1dtQ/2wRZFQvcIsEpXaV4NXjj+VZ4M4rm4VBJ
Sistem Akademik UIN Walisongo Semarang	KfdJ8VhaGH/TKR54Bj0+RMBRlmY1ZNSPMIgd9nt1Y4DSdcjtNHSqrGI/YmD+9GYR

Berdasarkan tabel di atas, perbandingan kata antara sebelum dan sesudah produk diimplementasikan sangat terlihat perbedaannya. Kata sebelum produk diimplementasi sangat jelas dan dapat dibaca oleh pihak lain. Sedangkan ketika

produk telah diimplementasikan pada sistem informasi, kata yang sangat jelas tersebut berubah bentuk menjadi kata yang tidak beraturan sehingga pihak lain tidak dapat membaca atau menggunakan kata tersebut.

Hal ini menunjukkan bahwa, sistem informasi jauh lebih aman ketika produk dipasang pada sistem informasi tersebut.

C. Revisi Produk

Produk yang telah diuji coba selanjutnya direvisi sesuai dengan arahan dari penguji produk. Berdasarkan saran dari *validator* uji keefektifan yaitu me-*replace* hasil dekripsi yang masih memiliki *null* karakter menjadi hasil dekripsi yang sebenarnya, maka peneliti merevisi produk dengan menambahkan *script* untuk me-*replace* hasil yang masih memiliki *null* karakter. Berikut adalah *script* sebelum dan setelah direvisi sesuai saran dari *validator*.

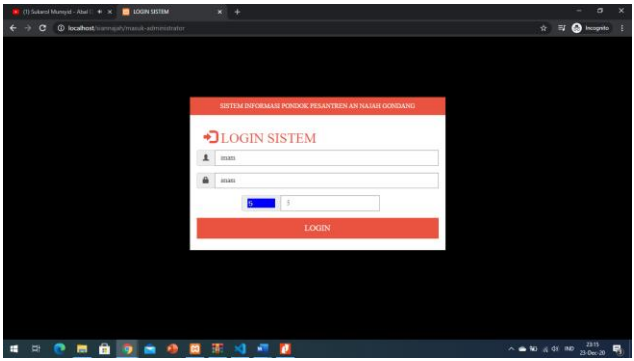
Tabel 4. 9 Revisi *script* produk

Sebelum direvisi	Setelah direvisi
`return ($x);`	`return preg_replace('~[^a-zA-Z0-9 @.]+~', '',$x);`

D. Kajian Produk Akhir

Pada penelitian ini, peneliti membuat produk algoritma kriptografi *Advanced Encryption Standard* dengan panjang kunci 128 bit. Produk ini bertujuan untuk mengamankan data pada *database* sistem informasi pondok pesantren An-Najah. Pengamanan data yang dimaksud adalah pengamanan data *password*, *id* transaksi, *id* pembayaran, dan *chat*. Berikut adalah tampilan data asli pada salah satu menu yang terdapat pada sistem informasi dengan data yang telah diamankan pada *database*.

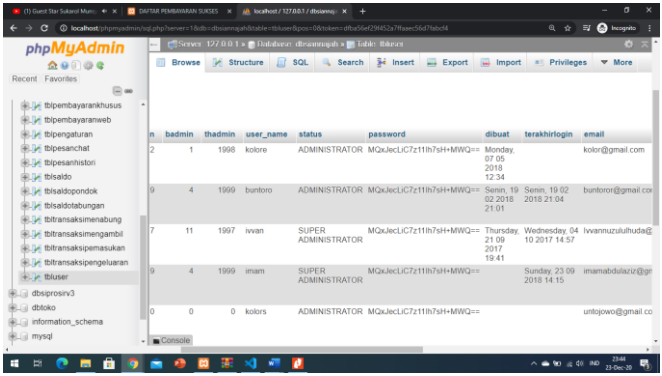
1. Tampilan Halaman Masuk



Gambar 4. 2 Tampilan Halaman Masuk

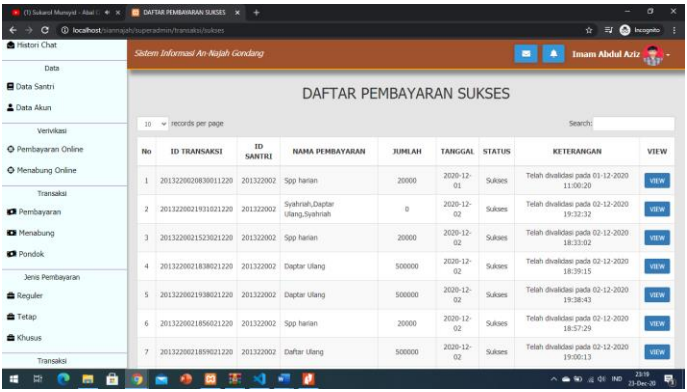
Halaman masuk berisi *form login* yang terdiri dari *username*, *password*, dan *captcha*. Salah satu *username* yang terdaftar pada *database* sistem informasi adalah ”imam” dengan *password* “imam”. Seperti yang terlihat pada gambar, terdapat perbedaan antara *password* yang

terdapat pada *form login* dengan *password* yang terdapat pada *database*. Hal ini disebabkan karena *password* yang terdapat pada *database* telah terenkripsi menggunakan produk kriptografi *Advanced Encryption Standard* yang telah dibuat pada penelitian ini. Berikut adalah data yang terdapat pada *database*.



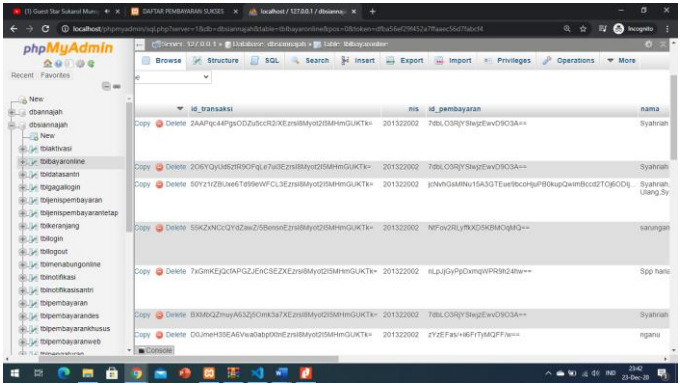
Gambar 4. 3 Tampilan *database tbluser*

2. Menu Pembayaran Sukses



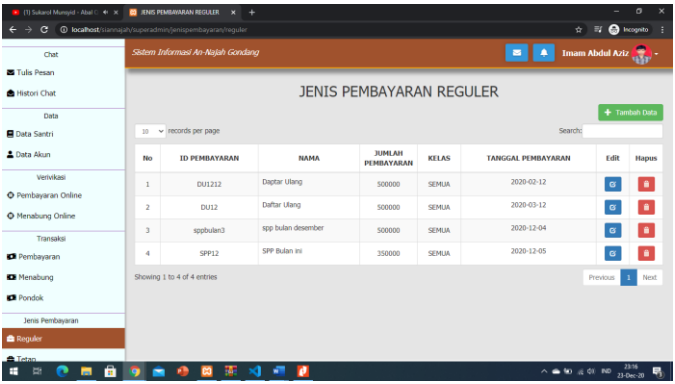
Gambar 4. 4 Tampilan Menu Pembayaran Sukses

Menu Daftar pembayaran sukses adalah salah satu menu pada sistem informasi yang menampilkan daftar semua pembayaran yang sukses divalidasi oleh admin sistem informasi pondok pesantren An-Najah. Menu tersebut memiliki beberapa kolom yaitu No., *Id* transaksi, Ide Santri, Nama Pembayaran, Jumlah, status, Keterangan, dan View. Data *id transaksi* yang terdapat pada menu daftar pembayaran sukses berbentuk *plaintext* atau kata yang dapat dibaca. Berbeda dengan yang terdapat pada *database*, *id transaksi* berupa *ciphertext* atau kata yang tidak dapat dibaca, hal ini dikarenakan *id* transaksi yang terdapat pada *database* sudah dienkripsi menggunakan produk yang telah dibuat pada penelitian ini. Berikut adalah gambar data pada *database*.



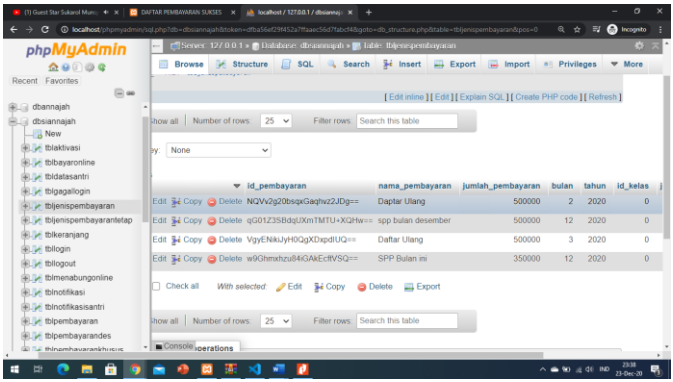
Gambar 4. 5 Tampilan *database tblbayaronline*

3. Menu Jenis Pembayaran Reguler



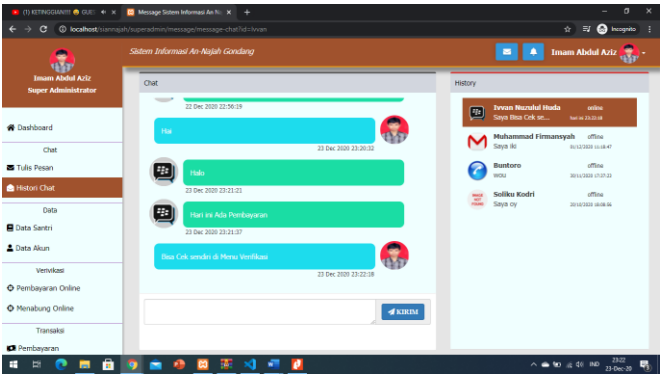
Gambar 4. 6 Tampilan Menu Jenis Pembayaran Reguler

Menu jenis pembayaran reguler adalah salah satu menu pada sistem informasi yang menampilkan jenis pembayaran reguler atau pembayaran rutin setiap bulannya. Menu ini terdiri dari beberapa kolom yaitu No., *Id* Pembayaran, Nama, Jumlah Pembayaran, Kelas, Tanggal Pembayaran, Edit, dan Hapus. Data *id* pembayaran yang terdapat pada jenis pembayaran reguler berbentuk *plaintext* atau kata yang dapat dibaca, sedangkan data *id* pembayaran yang terdapat pada *database* berbentuk *ciphertext* atau kata yang tidak dapat dibaca. Hal ini dikarenakan data *id* pembayaran yang terdapat pada *database* sudah terenkripsi menggunakan produk yang telah dibuat pada penelitian ini. Berikut adalah data yang terdapat pada *database* sistem informasi.



Gambar 4. 7 Tampilan *database tbljenispembayaran*

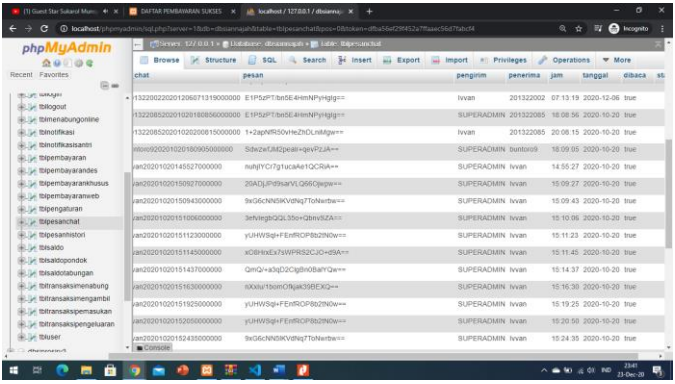
4. Tampilan Menu *Chat*



Gambar 4. 8 Tabel Menu *Chat*

Menu *chat* atau pesan adalah salah satu menu yang terdapat pada sistem informasi pondok pesantren An-Najah yang menampilkan pesan antar *user* atau pengguna sistem informasi. Data *chat* atau pesan yang terdapat pada tampilan menu *chat* masih berupa *plaintext* atau

kata yang dapat dibaca, berbeda dengan data *chat* yang terdapat pada *database* sistem informasi yaitu berupa *ciphertext* atau kata yang tidak dapat dibaca. Hal ini disebabkan data *chat* yang terdapat pada *database* sudah terenkripsi menggunakan produk yang telah dibuat pada penelitian ini. Berikut adalah tampilan data yang terdapat pada *database* sistem informasi.



Gambar 4. 9 Tampilan *database tblpesanchat*

Hasil dari penelitian skripsi ini adalah algoritma kriptografi *Advanced Encryption Standard* yang telah dibuat menggunakan bahasa pemrograman *PHP* telah berhasil diimplementasikan pada sistem informasi pondok pesantren An-Najah sehingga data tidak dapat dibaca oleh pihak-pihak yang tidak bertanggung jawab.

E. Keterbatasan Penelitian

1. Keterbatasan Objek Penelitian

   Penelitian ini hanya terbatas pada sebagian kecil dari sistem informasi. Objek yang dijadikan penelitian dalam sistem informasi ini hanya pada *chat*, *id* transaksi, *id* pembayaran, dan *password*. Keterbatasan tersebut peneliti ambil karena data tersebut adalah data yang paling vital dalam sistem informasi dan tidak membebani sistem untuk melakukan proses yang lebih berat.

2. Keterbatasan Algoritma

   Algoritma yang dipakai dalam penelitian ini adalah algoritma kriptografi *Advanced Encryption Standard* atau *AES* dengan panjang kunci 128 bit. Sebenarnya masih banyak algoritma kriptografi yang lebih kuat daripada *AES* akan tetapi peneliti mengambil algoritma tersebut karena lebih praktis, aman, dan ringan untuk sebuah sistem.

BAB V

PENUTUP

A. Simpulan Tentang Produk

Berdasarkan hasil dan pembahasan penelitian implementasi algoritma kriptografi *Advanced Encryption Standard* pada sistem informasi pondok pesantren An-Najah dapat disimpulkan bahwa produk Algoritma kriptografi *Advanced Encryption Standard* dinyatakan Valid dalam meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah melalui uji validitas produk dengan kategori nilai "Sangat Baik", produk algoritma kriptografi *Advanced Encryption Standard* juga dinyatakan Praktis dalam mengimplementasikan produk ke dalam sistem informasi pondok pesantren An-Najah melalui uji kepraktisan produk dengan kategori nilai "Sangat Baik", dan produk algoritma kriptografi *Advanced Encryption Standard* dinyatakan efektif pada sistem informasi pondok pesantren An-Najah melalui uji keefektifan produk dengan kategori nilai "Sangat Baik".

B. Saran Pemanfaatan Produk

Saran pemanfaatan produk dari hasil penelitian ini sebagai berikut:

1. Penggunaan produk sebaiknya diterapkan pada data penting yang lain, sehingga data pada *database* lebih aman dari gangguan pihak ketiga.

2. Kemudahan dalam penerapan produk seharusnya dapat menjadikan produk dapat digunakan pada sistem informasi lain yang memiliki bahasa pemrograman yang sama.

C. **Diseminasi dan Pengembangan Produk Lebih Lanjut**

Algoritma kriptografi *Advanced Encryption Standard* adalah algoritma kriptografi standar untuk pengamanan suatu data, masih banyak algoritma k riptografi yang lebih aman daripada algoritma ini. Jadi, saran untuk penelitian selanjutnya yaitu menggunakan kriptografi lain yang jauh lebih kuat keamanannya dengan menggunakan bahasa pemrograman yang sesuai dengan objek penelitian.

DAFTAR PUSTAKA

Ariyus, Dony. 2006. *Kriptografi*: *Keamanan Data dan Komunikasi*. Yogyakarta: Penerbit Graha Ilmu.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*: *Teori, Analisis, dan Implementasinya*. Yogyakarta: Penerbit Andi.

Asriyanik. 2017. *Studi terhadap Advanced Encryption Standard* (*AES*) *dan Algoritma Knapsack dalam Pengamanan Data*. Jurnal SANTIKA : Jurnal Ilmiah Sains dan Teknologi. Vol. 7 (1): 553-561.

Budianroto dan Nanan Rohman. 2010. *Implementasi Algoritma Enkripsi Rinjdael pada Pembuatan Kunci Lisensi Program Pengubah Atribut File*. Jurnal Computech & Bisnis. Vol. 4 (2): 59-69.

Chan, Arief Subrata. 2014. *Penerapan Kriptografi Rinjdael dalam Mengamankan File Menggunakan Interface USB Flashdisk (Memori External)*. Pelita Informatika Budi Darma. Vol. 6 (3): 11-15.

Dharmawan, Eka Adhitya, dkk. 2013. *Perlindungan Web pada Login Sistem Menggunakan Algoritma Rinjdael*. Jurnal EECCIS. Vol. 7 (1): 77-84.

Handoyo, Joko dan Yulleo Muchti Subakti. 2020. *Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard* (*AES*). Jurnal SITECH. Vol. 3 (2): 144-152.

JB, R. Kristoforus dan Stefanus Aditya BP. 2012. *Implementasi Algoritma Rinjdael untuk enkripsi dan dekripsi pada citra digital*. Seminar Nasional Aplikasi Teknologi Informasi 2012 (SNATI 2912). Yogyakarta, 15-16 Juni 2012.

Kadir, Abdul. 2014. *Pengenalan Sistem Informasi Edisi Revisi*. Yogyakarta: Penerbit Andi.

Kromodiemoljo, Sentot. 2010. *Teori & Aplikasi Kriptografi*. SPK IT Consulting.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit INFORMATIKA.

Nurdiansyah, Yanuar, dkk. 2018. *Sistem Informasi Kartu Pegawai Elektronik (SI-KPE) Berbasis Web dan Mobile KPE Berbasis Android dengan Menggunakan Metode AES-128*. Informatics Journal. Vol. 3 (4): 93-101.

Pabokort, Fresly Nandar, dkk. 2015. *Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokunen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard.* Jurnal Informatika Mulawarman. Vol. 10 (1): 20-31.

Permana, Angga Aditya dan Desi Nurnaningsih. 2018. *Rancangan Aplikasi Pengamanan Data dengan Algoritma Advanced Encryption Standard (AES)*. Jurnal Teknik Informatika. Vol. 11 (2): 177-186.

Primartha, Rifkie. 2018. *Security Jaringan Komputer Berbasis CEH*. Bandung: Penerbit Informatika.

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Penerbit Andi.

Sofana, Iwan dan Rifkie Primartha. 2019. *Network Security dan Cyber Security*: *Teori dan Praktik Cisco CCNA, Linux, Windows, Amazon AWS, Android*. Bandung: Penerbit Informatika.

Surian, Didi. 2006. *Algoritma Kriptografi AES Rinjdael*. TESLA, Jurnal Teknik Elektro. Vol. 8 (2): 97-101.

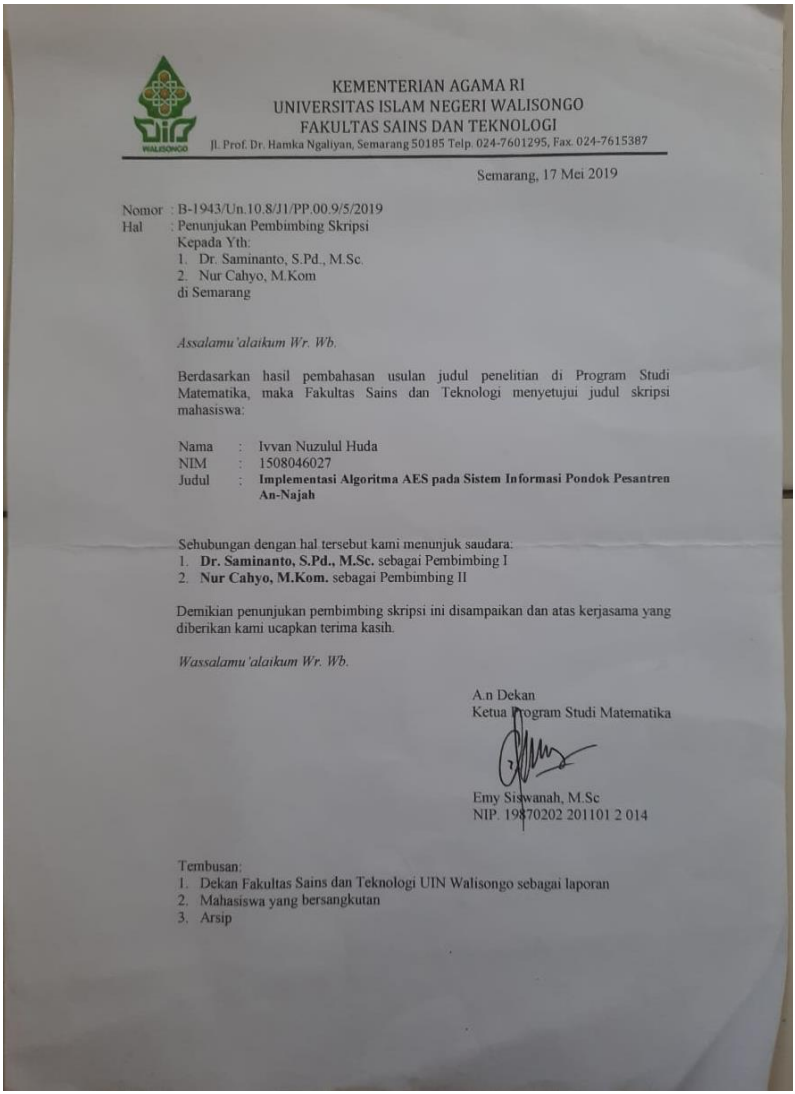
Tullah, Rahmat, dkk. 2016. *Perancangan Aplikasi Kriptografi File dengan Metode Algoritma Advanced Encryption Standard* (*AES*). Vol. 6 (2): 24-30.

Widyastuti, Susi, dkk. 2019. *Implementasi Kriptografi AES dalam Pengamanan Data Seleksi Peserta JAMKESMAS*. Jurnal INTECH. Vol. 1 (2): 13-22.

Zam, Efvy. 2011. *Buku Sakti Hacker*. Jakarta Selatan: PT. Transmedia.

LAMPIRAN

Lampiran 1 Surat Penunjukan Dosen Pembimbing



KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI WALISONGO
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Prof. Dr. Hamka Ngaliyan, Semarang 50185 Telp. 024-7601295, Fax. 024-7615387

Semarang, 17 Mei 2019

Nomor : B-1943/Un.10.8/J1/PP.00.9/5/2019
Hal : Penunjukan Pembimbing Skripsi
Kepada Yth:
1. Dr. Saminanto, S.Pd., M.Sc.
2. Nur Cahyo, M.Kom
di Semarang

Assalamu'alaikum Wr. Wb.

Berdasarkan hasil pembahasan usulan judul penelitian di Program Studi Matematika, maka Fakultas Sains dan Teknologi menyetujui judul skripsi mahasiswa:

Nama : Ivvan Nuzulul Huda
NIM : 1508046027
Judul : **Implementasi Algoritma AES pada Sistem Informasi Pondok Pesantren An-Najah**

Sehubungan dengan hal tersebut kami menunjuk saudara:
1. **Dr. Saminanto, S.Pd., M.Sc.** sebagai Pembimbing I
2. **Nur Cahyo, M.Kom.** sebagai Pembimbing II

Demikian penunjukan pembimbing skripsi ini disampaikan dan atas kerjasama yang diberikan kami ucapkan terima kasih.

Wassalamu'alaikum Wr. Wb.

A.n Dekan
Ketua Program Studi Matematika

Emy Siswanah, M.Sc
NIP. 19870202 201101 2 014

Tembusan:
1. Dekan Fakultas Sains dan Teknologi UIN Walisongo sebagai laporan
2. Mahasiswa yang bersangkutan
3. Arsip

Lampiran 2 Surat Permohonan Validator

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI
WALISONGO SEMARANG
FAKULTAS SAINS DAN TEKNOLOGI

Jalan Prof. Dr. H. Hamka Kampus II Ngaliyan Semarang 50185
Telepon (024) 76433366, Website: fst.walisongo.ac.id

5 Februari 2021

No : B.0449/Un 10.8/J1/TL.99/02/2021
Hal : Surat Permohonan Validator

Yth.
Any Muanalifah, M. Si.
Di tempat

Assalamu'alaikum Wr. Wb.

Berdasarkan pertimbangan dari dosen pembimbing, maka diperlukan uji validitas pada skripsi mahasiswa:

Nama : **Ivvan Nuzulul Huda**
NIM : **1508046027**
Judul : **Implementasi Algoritma Kriptografi *Advanced Encryption Standard* pada Sistem Informasi Pondok Pesantren An-Najah**

Oleh karena itu kami meminta Ibu **Any Muanalifah, M. Si.** sebagai **Validator Uji Kepraktisan dan Uji Keefektifan** pada instrumen produk algoritma kriptografi *Advanced Encryption Standard* tersebut.

Demikian surat permohonan ini kami sampaikan, atas perkenan dan kerjasama Bapak/Ibu kami ucapkan terima kasih.

Wassalamu'alaikum Wr.Wb.

Ketua Prodi Matematika

Siswanah, M.Sc
NIP. 198702022011012014

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI
WALISONGO SEMARANG
FAKULTAS SAINS DAN TEKNOLOGI

Jalan Prof. Dr. H. Hamka Kampus II Ngaliyan Semarang 50185
Telepon (024) 76433366, Website: fst.walisongo.ac.id

5 Februari 2021

No : B.0449/Un 10.8/J1/TL.99/02/2021
Hal : Surat Permohonan Validator

Yth.
Imam Abdul Aziz, S. Kom
Di tempat

Assalamu'alaikum Wr. Wb.

Berdasarkan pertimbangan dari dosen pembimbing, maka diperlukan uji kepraktisan dan uji keefektifan pada skripsi mahasiswa:

Nama	:	**Ivvan Nuzulul Huda**
NIM	:	**1508046027**
Judul	:	**Implementasi Algoritma Kriptografi *Advanced Encryption Standard* pada Sistem Informasi Pondok Pesantren An-Najah**

Oleh karena itu kami meminta Bapak **Imam Abdul Aziz, S. Kom.** sebagai **Validator Uji Kepraktisan dan Uji Keefektifan** pada instrumen produk algoritma kriptografi *Advanced Encryption Standard* tersebut.

Demikian surat permohonan ini kami sampaikan, atas perkenan dan kerjasama Bapak/Ibu kami ucapkan terima kasih.

Wassalamu'alaikum Wr.Wb.

Ketua Prodi Matematika

Iis Siswanah, M.Sc
NIP. 19870202011012014

Lampiran 3 Surat Permohonan Izin Riset

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI WALISONGO SEMARANG
FAKULTAS SAINS DAN TEKNOLOGI
Alamat: Jl.Prof. Dr. Hamka Km. 1 Semarang Telp. 024 76433366 Semarang 50185

Nomor : B.0343/Un.10.8/D1/TL.00/01/2021 Semarang, 27 Januari 2021
Lamp : Proposal Skripsi
Hal : Permohonan Izin Riset

Kepada Yth.
Pimpinan Pondok Pesantren An-Najah
di tempat

Assalamu'alaikum Wr. Wb.

Diberitahukan dengan hormat dalam rangka penulisan skripsi, bersama ini kami sampaikan bahwa mahasiswa di bawah ini:

Nama : Ivvan Nuzulul Huda
NIM : 1508046027
Fakultas/Jurusan : Sains dan Teknologi / Matematika
Judul Sekripsi : Implementasi Algoritma Kriptografi *Advanced Encryption Standard* pada Sistem Informasi Pondok Pesantren An-Najah

Pembimbing : 1. Dr. Saminanto, M.Sc
2. Nur Cahyo Hendro Wibowo, M.Kom.

Mahasiswa tersebut membutuhkan data-data dengan tema/judul skripsi yang sedang disusun, oleh karena itu kami mohon mahasiswa tersebut di ijinkan melaksanakan Riset di pondok pesantren yang Bapak/Ibu pimpin.

Demikian atas perhatian dan kerjasamanya disampaikan terima kasih.

Wassalamu'alaikum Wr. Wb.

A.n. Dekan,
Wakil Dekan I

Dr. Saminanto

Tembusan Yth.
1. Dekan Fakultas Sains dan Teknologi UIN Walisongo (sebagai laporan)
2. Arsip

Lampiran 4 Tabel ASCII

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

Lampiran 5 Kontrol terhadap sistem informasi

No.,	Macam Kontrol	Contoh Tindakan
1.	Kontrol administratif	• Mempublikasikan prosedur dan standar • Perekrutan personel secara berhati-hati
2.	Kontrol pengembangan dan pemeliharaan sistem	• Mengkaji pasca implementasi • Memastikan bahwa pemeliharaan yang dilakukan terotorisasi
3.	Kontrol operasi	• Mengontrol akses terhadap pusat data • Mengontrol pemeliharaan peralatan-peralatan • Melindungi dari virus
4	Proteksi terhadap pusat data secara fisik	• Mengontrol lingkungan • Menyiapkan sumber listrik darurat
5.	Kontrol perangkat keras	• Ssistem komputer *fault-tolerant*

6.	Kontrol terhadap akses komputer	• Mengiddentifikasi dan melakukan otentikasi terhadap pemakai
7.	Kontrol terhadap akses informasi	• Enkripsi
8.	Kontrol terhadap perlindungan terakhir	• Rencana pemulihan terhadap bencana • Asuransi
9.	Kontrol aplikasi	• Kontrol terhadap masukan, pemrosesan, dan keluaran • Kontrol terhadap basis data

Lampiran 6 Langkah setiap ronde pada *AES*

Ronde	Mulai Ronde				SubBytes				ShiftRows				MixColumn				Kunci				AddRoundKey			
0	55	57	53	4f													53	6e	68	64	06	39	3b	2b
	49	41	4f	00													49	61	67	61	00	20	28	61
	4e	4c	4e	00													41	6a	6f	6e	0f	26	21	6e
	20	49	47	00													6e	61	6e	67	4e	28	29	67
1	06	39	3b	2b	6f	12	e2	f1	6f	12	e2	f1	64	83	ad	ea	bd	d3	bb	df	d9	1b	0c	d1
	00	20	28	61	63	b7	34	ef	b7	34	ef	63	c8	Ef	72	c3	d6	b7	d0	b1	55	58	59	21
	0f	26	21	6e	76	f7	fd	9f	fd	9f	76	f7	b7	89	bd	cc	c4	ae	23	af	69	dc	7c	3c
	4e	28	29	67	2f	34	a5	85	85	2f	34	a5	0e	90	93	cd	2d	4c	6e	45	c7	8f	ee	88
2	d9	1b	0c	d1	35	af	fe	3e	35	af	fe	3e	00	15	28	b6	77	a4	1f	c0	77	8a	6e	0d
	55	58	59	21	fc	6a	cb	fd	6a	cb	fd	fc	2e	c2	f8	5d	af	18	c8	79	ba	da	b4	1d
	69	dc	7c	3c	f9	86	10	eb	10	eb	f9	86	71	7c	7f	fb	aa	04	c5	6a	82	fc	ba	c7
	c7	8f	ee	88	c6	73	28	c4	c4	c6	73	28	cd	64	ad	68	b3	ff	Dd	98	05	a2	26	f0
3	77	8a	6e	0d	f5	7e	9f	d7	f5	7e	9f	d7	70	d0	de	a4	c5	61	7e	be	b5	bc	85	4b
	ba	da	b4	1d	f4	57	8d	a4	57	8d	a4	f4	dd	45	d9	1f	ad	b5	7d	4	7d	f0	be	1c
	82	fc	ba	c7	13	b0	f4	c6	f4	c6	13	b0	fb	c3	53	79	ec	e8	2d	47	32	31	7e	1d
	05	a2	26	f0	6b	3a	f7	8c	8c	6b	3a	f7	f5	18	5a	d3	9	f6	2b	b3	ad	e9	52	60

4	b5	bc	85	4b	d5	65	97	b3	d5	65	97	b3	1d	08	cf	a0	3f	5e	20	94	22	4c	97	3e
	7d	f0	be	1c	ff	8c	ae	9c	8c	ae	9c	ff	12	40	3c	94	0d	b8	c5	c1	05	f8	0a	c5
	32	31	7e	1d	23	c7	f3	a4	f3	a4	23	c7	b7	Cf	6f	21	81	69	44	03	4e	55	2b	da
	ad	e9	52	60	95	1e	00	d0	d0	95	1e	00	a0	04	d9	f6	a7	51	7a	c9	07	c5	5b	3f
5	22	4c	97	3e	93	29	88	b2	93	29	88	b2	7a	6c	b4	f4	57	09	29	b7	2d	60	5a	b0
	05	f8	0a	c5	6b	41	67	a6	41	67	a6	6b	69	Db	b4	da	76	ce	0b	ca	1a	15	03	88
	4e	55	2b	da	2f	fc	f1	57	f1	57	2f	fc	73	08	81	5d	6c	35	71	72	e8	81	f0	03
	07	c5	5b	3f	c5	a6	39	75	75	c5	a6	39	07	42	71	28	ac	fd	87	4c	58	27	da	66
6	2d	60	5a	b0	d8	d0	be	e7	d8	d0	be	e7	ff	d6	d7	c0	03	0a	23	94	fc	2d	44	e7
	1a	15	03	88	a2	59	7b	c4	59	7b	c4	a2	27	c1	e3	bf	36	f8	f3	39	e0	39	a4	c2
	e8	81	f0	03	9b	0c	8c	7b	8c	7b	9b	0c	67	57	18	05	73	46	37	45	a4	a5	2f	e1
	58	27	da	66	6a	cc	57	33	33	6a	cc	57	73	fb	a4	32	05	f8	7f	31	c5	47	7a	03
7	fc	2d	44	e7	b0	d8	1b	94	b0	d8	1b	94	23	d0	05	3a	51	5b	78	ec	72	75	c8	3b
	e0	39	a4	c2	e1	12	49	25	12	49	25	e1	2e	ff	8b	95	58	a0	53	6a	88	5f	79	f7
	a4	a5	2f	e1	49	06	15	f8	15	f8	49	6	b0	2a	57	1a	b4	f2	c5	80	b1	79	92	8c
	c5	47	7a	03	a6	a0	da	7b	7b	a6	a0	da	d7	9d	0c	ef	27	df	a0	91	1d	4a	ba	7e
8	72	75	c8	3b	40	9d	e8	e2	40	9d	e8	e2	76	e7	1f	bd	d3	88	f0	1c	a5	a8	9d	d6
	88	5f	79	f7	c4	cf	b6	68	cf	b6	68	c4	20	e2	14	3d	95	35	66	0c	72	d7	cb	48

	b1	79	92	8c	c8	b6	4f	64	4f	64	c8	b6	6d	ad	6a	34	35	c7	02	82	2a	d3	68	d4
	1d	4a	ba	7e	a4	d6	f4	f3	f3	a4	d6	f4	ca	44	56	bc	e9	36	96	07	54	0b	a2	bb
9	a5	a8	9d	d6	06	c2	5e	f6	06	c2	5e	f6	b1	3f	a7	8e	36	be	4e	52	87	68	ca	39
	72	d7	cb	48	40	0e	1f	52	0e	1f	52	40	d6	04	2d	4a	86	b3	d5	d9	b9	b7	30	3f
	2a	d3	68	d4	e5	66	45	48	45	48	e5	66	84	e5	a0	03	f0	37	35	b7	57	1a	95	83
	54	0b	a2	bb	20	2b	3a	ea	ea	20	2b	3a	6b	e6	34	53	75	43	d5	d2	fb	09	d6	81
10	87	68	ca	39	17	45	74	12	17	45	74	12					35	8b	c5	97	22	ce	b1	85
	b9	b7	30	3f	56	a9	04	75	a9	04	75	56					2f	9c	49	90	86	98	3c	c6
	57	1a	95	83	5b	a2	2a	ec	2a	ec	5b	a2					45	72	47	f0	6f	9e	1c	52
	fb	09	d6	81	0f	01	f6	0c	0c	0f	01	f6					75	36	e3	31	79	39	e2	c7

Lampiran 7 Lembar Uji Validitas Produk

LEMBAR UJI VALIDITAS
KOMPONEN PRODUK ALGORITMA KRIPTOGRAFI
***ADVANCED ENCRYPTION STANDARD* (*AES*)**
UNTUK MENINGKATKAN KEAMANAN PADA SISTEM INFORMASI
PONDOK PESANTREN AN-NAJAH

Tujuan

Lembar uji validitas komponen produk algoritma kriptografi *Advanced Encryption Standard* ini disusun untuk mengetahui validasi produk algoritma kriptografi *Advanced Encryption Standard* yang telah dikembangkan untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah.

Kisi-kisi Uji Validitas Komponen Produk Algoritma Kriptografi *AES*

Pengembangan kisi-kisi validasi produk algoritma kriptografi *AES* untuk mendapatkan data tentang validasi produk algoritma kriptografi *AES* yang dikembangkan. Kisi-kisi ini memuat tiga komponen pokok yang dijabarkan dalam bentuk indikator-indikator. Berdasarkan indikator-indikator tersebut selanjutnya dikembangkan rumusan pernyataan untuk memperoleh penilaian. Indikator-indikator tersebut dirumuskan dalam Tabel 1 berikut.

Tabel 1. Kisi-kisi Lembar Validasi Komponen Produk Kriptografi *AES*

No.	Indikator Validasi Model Produk Kriptografi *AES*	No. Pernyataan
1.	Rasionalisasi Pengembangan Produk Kriptografi *Advanced Encryption Standard*.	1, 2, 3
2.	Landasan Teori Pengembangan Produk Kriptografi *Advanced Encryption Standard*.	4
3.	Fase Pengembangan Produk Kriptografi *Advanced Encryption Standard*.	5, 6, 7
4.	Karakteristik Produk Kriptografi *Advanced Encryption Standard*.	8
5.	Keutuhan Data Produk Kriptografi *Advanced Encryption Standard*	9

Bentuk Instrumen

Penyusunan instrumen validasi produk algoritma kriptografi *AES* ini menggunakan skala likert. Masing-masing pernyataan yang tersedia memiliki lima macam pilihan jawaban yang

merupakan penilaian terhadap validitas produk algoritma kriptografi *AES* untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah.

Cara Penggunaan

Hasil penilaian lembar validasi ini direpresentasikan dalam bentuk nilai x. Rata-rata (x) yang diperoleh menunjukkan tingkat validitas produk algoritma kriptografi *AES* untuk meningkatkan keamanan pada sistem informasi. Kriteria untuk menentukan penilaian secara umum dijabarkan dalam Tabel 2 berikut.

Tabel 2. Kriteria Penilaian

No.	Nilai	Keterangan
1.	$1{,}00 \leq x \leq 1{,}80$	Tidak baik
2.	$1{,}80 < x \leq 2{,}60$	Kurang baik
3.	$2{,}60 < x \leq 3{,}40$	Cukup baik
4.	$3{,}40 < x \leq 4{,}20$	Baik
5.	$4{,}20 < x \leq 5{,}00$	Sangat baik

Petunjuk Penggunaan

Berilah skor pada butir-butir lembar validasi komponen produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan keamanan pada sistem informasi dengan cara melingkari nilai (1, 2, 3, 4, atau 5) sesuai dengan kriteria penilaian pada masing-masing nomor pertanyaan.

LEMBAR UJI VALIDITAS
KOMPONEN PRODUK ALGORITMA KRIPTOGRAFI
***ADVANCED ENCRYPTION STANDARD* (AES)**
UNTUK MENINGKATKAN KEAMANAN PADA SISTEM INFORMASI
PONDOK PESANTREN AN-NAJAH

Nama Penilai	: Any Muanalifah
Jabatan	: Dosen Matematika
Tempat Tugas	: UIN Walisongo

Petunjuk Penilaian Validasi

1. Mohon Bapak/Ibu berkenan memberikan penilaian terhadap model produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan keamanan pada sistem informasi yang telah dikembangkan.
2. Penilaian produk algoritma kriptografi *Advanced Encryption* Standard untuk meningkatkan keamanan pada sistem informasi meliputi aspek :
   a. Rasionalisasi Pengembangan Produk Kriptografi *Advanced Encryption Standard.*
   b. Landasan Teori Pengembangan Produk Kriptografi *Advanced Encryption Standard*.
   c. Fase Pengembangan Produk Kriptografi *Advanced Encryption Standard*.
   d. Penilaian Produk Kriptografi *Advanced Encryption Standard*.
   e. Keutuhan Data Produk Kriptografi *Advanced Encryption Standard*.
3. Dimohon Bapak/Ibu memberi nilai pada butir-butir pengembangan produk algoritma kriptografi *Advanced Encryption Standard* dengan cara melingkari nilai (1, 2, 3, 4, atau 5) sesuai dengan kriteria penilaian pada masing-masing nomor pertanyaan.
4. Saran-saran yang Bapak/Ibu berikan, mohon dituliskan pada naskah yang perlu direvisi, atau dituliskan pada lembar saran yang telah disediakan.

Penilaian Produk Kriptografi *Advanced Encryption Standard*

A. Penilaian Aspek Rasionalisasi Pengembangan Produk *AES*

1. Rasionalisasi produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan kemanan pada sistem informasi pomdok pesantren An-Najah.

Lemah	Kuat
Tidak menunjukkan adanya alasan yang kuat pentingnya melakukan pengamanan *database* pada sistem informasi pondok pesantren An-Najah	Menunjukkan adanya alasan yang kuat untuk melakukan pengamanan *database* pada sistem informasi pondok pesantren An-Najah.

2. Keterkaitan masalah keamanan dengan sistem informasi

Lemah	Kuat
Tidak adanya keterkaitan antara masalah keamanan *database* dengan sistem informasi yang ada pada pondok pesantren An-Najah	Adanya keterkaitan yang kuat antara masalah keamanan *database* dengan sistem informasi pondok pesantren An-Najah..

3. Pentingnya pengembangan produk *AES* pada sistem informasi pondok pesantren An-Najah

Lemah	Kuat
Tidak menunjukkan pentingnya pengembangan produk *AES* untuk meningkatkan keamanan *database* pada sistem informasi pondok pesantren An-Najah.	Menunjukkan pentingnya pengembangan produk *AES* untuk meningkatkan keamanan *database* pada sistem informasi pondok pesantren An-Najah.

B. Penilaian Aspek Landasan Teori Pengembangan Produk *AES*

4. Kesesuaian landasan teori *AES* dengan produk algoritma kriptografi *AES* yang dikembangkan pada sistem informasi

Tidak sesuai	Sesuai
Langkah pada produk algoritma yang dibuat tidak sesuai dengan teori yang ada.	Langkah pada produk algoritma yang dibuat sudah sesuai dengan teori yang ada.

C. Penilaian Aspek Fase Pengembangan Produk Kriptografi *AES*

5. Fase pengembangan produk kriptografi *AES*

Tidak sistematis	Sistematis
Penerapan algoritma *AES* yang dikembangkan pada sistem informasi dengan menggunakan bahasa pemrograman PHP yang tidak sistematis	Penerapan algoritma *AES* yang dikembangkan pada sistem informasi dengan menggunakan bahasa pemrograman PHP yang sistematis.

6. Efisiensi produk algoritma kriptografi *AES*

Tidak efisien	Efisien
Penerapan algoritma kriptografi *AES* yang dikembangkan pada sistem informasi tidak efisien.	Penerapan algoritma kriptografi *AES* yang dikembangkan pada sistem informasi sudah efisien.

7. Validitas produk kriptografi *AES*

Rendah	Tinggi
Tidak terukur dengan jelas cara menentukan validitas, kepraktisan dan keefektifannya	Terukur sangat jelas cara menentukan validitas, kepraktisan dan keefektifannya

D. Penilaian Produk Kriptografi *AES*

8. Karakteristik produk kriptografi *AES*

Negatif	Positif
Tidak memberikan dampak untuk meningkatkan keamanan sistem informasi	Sangat memberikan dampak untuk meningkatkan keamanan sistem informasi

E. Penilaian Keutuhan Data Produk Kriptografi *AES*

9. Keutuhan data kriptografi *AES*

Rendah	Tinggi
Data tidak utuh sesuai dengan algoritma yang telah dibangun	Data sesuai dengan algoritma yang telah dibangun.

Komentar dan saran perbaikan

Program yang dibuat sudah sangat baik sekali dan dapat meningkatkan keamanan sistem Informasi Pesantren An Najah.

Untuk saran sebaiknya perlu juga dihitung kompleksitas dari algoritma yang dibuat

Dalam membuat sistem keamanan kita juga harus memperlihatkan tingkat keamanan algoritma yang dibuat.

Indikator Penilaian Validasi

No.	Nilai	Keterangan
1.	$1{,}00 \leq x \leq 1{,}80$	Tidak baik
2.	$1{,}80 < x \leq 2{,}60$	Kurang baik
3.	$2{,}60 < x \leq 3{,}40$	Cukup baik
4.	$3{,}40 < x \leq 4{,}20$	Baik
5.	$4{,}20 < x \leq 5{,}00$	Sangat baik

Kesimpulan penilaian

Setelah mengisi tabel penilaian, dimohon Bapak/Ibu melingkari angka di bawah ini sesuai dengan penilaian Bapak/Ibu.

Produk algoritma kriptografi *Advanced Encryption Standard* ini:

1. Tidak baik, sehingga belum dapat digunakan, harus diganti
2. Kurang baik, sehingga belum dapat digunakan, masih memerlukan konsultasi
3. Cukup baik, sehingga dapat digunakan tetapi dengan banyak revisi.
4. Baik, sehingga dapat digunakan tetapi dengan sedikit revisi.
5. Sangat baik, sehingga dapat digunakan tanpa revisi

Birmingham, 15 February 2021

Penilai,

(Any Muanalifah)

Lampiran 8 Lembar Uji Kepraktisan

LEMBAR UJI KEPRAKTISAN
KOMPONEN PRODUK ALGORITMA KRIPTOGRAFI
***ADVANCED ENCRYPTION STANDARD* (*AES*)**
UNTUK MENINGKATKAN KEAMANAN PADA SISTEM INFORMASI
PONDOK PESANTREN AN-NAJAH

Tujuan

Lembar uji kepraktisan komponen produk algoritma kriptografi *Advanced Encryption Standard* ini disusun untuk mengetahui kepraktisan produk algoritma kriptografi *Advanced Encryption Standard* yang telah dikembangkan untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah.

Kisi-kisi Uji Kepraktisan Komponen Produk Algoritma Kriptografi *AES*

Pengembangan kisi-kisi validasi produk algoritma kriptografi *AES* untuk mendapatkan data tentang kepraktisan produk algoritma kriptografi *AES* yang dikembangkan. Kisi-kisi ini memuat tiga komponen pokok yang dijabarkan dalam bentuk indikator-indikator. Berdasarkan indikator-indikator tersebut selanjutnya dikembangkan rumusan pernyataan untuk memperoleh penilaian. Indikator-indikator tersebut dirumuskan dalam Tabel 1 berikut.

Tabel 1. Kisi-kisi Lembar Validasi Komponen Produk Kriptografi *AES*

No.	Indikator Validasi Model Produk Kriptografi *AES*	No. Pernyataan
1.	Penggunaan Produk Kriptografi *Advanced Encryption Standard*	1, 2, 3
2.	Proses Instalasi Produk Kriptografi *Advanced Encryption Standard*	4
3.	Keutuhan Data Produk Kriptografi *Advanced Encryption Standard.*	5
4.	Keaslian Data Produk Kriptografi *Advanced Encryption Standard.*	6

Bentuk Instrumen

Penyusunan instrumen uji kepraktisan produk algoritma kriptografi *AES* ini menggunakan skala likert. Masing-masing pernyataan yang tersedia memiliki lima macam pilihan jawaban yang merupakan penilaian terhadap validitas produk algoritma kriptografi *AES* untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah.

Cara Penggunaan

Hasil penilaian lembar validasi ini direpresentasikan dalam bentuk nilai x. Rata-rata (x) yang diperoleh menunjukkan tingkat kepraktisan produk algoritma kriptografi *AES* untuk meningkatkan keamanan pada sistem informasi. Kriteria untuk menentukan penilaian secara umum dijabarkan dalam Tabel 2 berikut.

Tabel 2. Kriteria Penilaian

No.	Nilai	Keterangan
1.	$1{,}00 \leq x \leq 1{,}80$	Tidak baik
2.	$1{,}80 < x \leq 2{,}60$	Kurang baik
3.	$2{,}60 < x \leq 3{,}40$	Cukup baik
4.	$3{,}40 < x \leq 4{,}20$	Baik
5.	$4{,}20 < x \leq 5{,}00$	Sangat baik

Petunjuk Penggunaan

Berilah skor pada butir-butir lembar validasi komponen produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan keamanan pada sistem informasi dengan cara melingkari nilai (1, 2, 3, 4, atau 5) sesuai dengan kriteria penilaian pada masing-masing nomor pertanyaan.

LEMBAR UJI KEPRAKTISAN
KOMPONEN PRODUK ALGORITMA KRIPTOGRAFI
***ADVANCED ENCRYPTION STANDARD* (AES)**
UNTUK MENINGKATKAN KEAMANAN PADA SISTEM INFORMASI
PONDOK PESANTREN AN-NAJAH

Nama Penilai	:	Imam Abdul Aziz, S. Kom.
Jabatan	:	Pembuat Sistem Informasi
Tempat Tugas	:	Pondok Pesantren An-Najah

Petunjuk Penilaian Validasi

1. Mohon Bapak/Ibu berkenan memberikan penilaian terhadap model produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan keamanan pada sistem informasi yang telah dikembangkan.
2. Penilaian produk algoritma kriptografi *Advanced Encryption* Standard untuk meningkatkan keamanan pada sistem informasi meliputi aspek :
   a. Penggunaan Produk Kriptografi *Advaned Encryption Standard.*
   b. Proses Instalasi Produk Kriptografi *Advaned Encryption Standard.*
   c. Keutuhan *Data* Produk Kriptografi *Advanced Encryption Standard.*
   d. Keaslian Data Produk Kriptografi *Advanced Encryption Standard*
3. Dimohon Bapak/Ibu memberi nilai pada butir-butir pengembangan produk algoritma kriptografi *Advanced Encryption Standard* dengan cara melingkari nilai (1, 2, 3, 4, atau 5) sesuai dengan kriteria penilaian pada masing-masing nomor pertanyaan.
4. Saran-saran yang Bapak/Ibu berikan, mohon dituliskan pada naskah yang perlu direvisi, atau dituliskan pada lembar saran yang telah disediakan.

Penilaian Produk Kriptografi *Advanced Encryption Standard*

A. Penilaian Aspek Penggunaan Produk Kriptografi *AES*

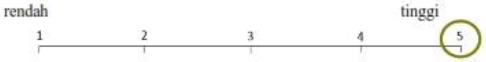
1. Kemudahan dalam penggunaan produk

Rendah	Tinggi
Penggunaan produk sulit untuk dipahami dan diterapkan	Produk sangat mudah untuk dipahami dan mudah untuk diterapkan

2. Kondisi produk saat dijalankan

Rendah	Tinggi
Produk tidak berjalan dengan baik dan masih terdapat *bug*..	Produk berjalan sesuai dengan tujuan pembuatan.

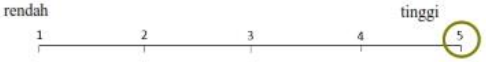
3. Fungsi produk kriptografi *AES*



Rendah	Tinggi
Tidak dapat berfungsi dengan baik	Berfungsi sangat baik dan sesuai dengan tujuan pembuatan produk.

B. Penilaian Aspek Instalasi Produk Kriptografi *AES*

4. Proses instalasi produk kriptografi *AES*



Rendah	Tinggi
Sulit dalam mengimplementasikan pada sistem informasi.	Produk dapat di instalasi dengan mudah karena memiliki bahasa pemrograman yang sama

C. Penilaian Keutuhan Data Produk Kriptografi *AES*

5. Keutuhan data kriptografi *AES*

Rendah	Tinggi
Data tidak utuh sesuai dengan algoritma yang telah dibangun	Data sesuai dengan algoritma yang telah dibangun.

D. Penilaian Aspek Keaslian Data Produk Kriptografi *AES*

6. Keaslian data kriptografi *AES*

Rendah	Tinggi
Tidak sesuai dengan data yang telah ditetapkan sebelumnya	Sesuai dengan data yang telah ditetapkan.

Komentar dan saran perbaikan

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Indikator Penilaian Validasi

No.	Nilai	Keterangan
1.	$1{,}00 \leq x \leq 1{,}80$	Tidak baik
2.	$1{,}80 < x \leq 2{,}60$	Kurang baik
3.	$2{,}60 < x \leq 3{,}40$	Cukup baik
4.	$3{,}40 < x \leq 4{,}20$	Baik
5.	$4{,}20 < x \leq 5{,}00$	Sangat baik

Kesimpulan penilaian

Setelah mengisi tabel penilaian, dimohon Bapak/Ibu melingkari angka di bawah ini sesuai dengan penilaian Bapak/Ibu.

Produk algoritma kriptografi *Advanced Encryption Standard* ini:

1. Tidak baik, sehingga belum dapat digunakan, harus diganti
2. Kurang baik, sehingga belum dapat digunakan, masih memerlukan konsultasi
3. Cukup baik, sehingga dapat digunakan tetapi dengan banyak revisi.
4. Baik, sehingga dapat digunakan tetapi dengan sedikit revisi.
5. Sangat baik, sehingga dapat digunakan tanpa revisi

Brebes ....., 5 Januari 2021

Penilai,

(Imam Abdul Aziz, S. Kom)

Lampiran 9 Lembar Uji Efektivitas

LEMBAR UJI EFEKTIVITAS
KOMPONEN PRODUK ALGORITMA KRIPTOGRAFI
***ADVANCED ENCRYPTION STANDARD* (*AES*)**
UNTUK MENINGKATKAN KEAMANAN PADA SISTEM INFORMASI
PONDOK PESANTREN AN-NAJAH

Tujuan

Lembar uji efektivitas komponen produk algoritma kriptografi *Advanced Encryption Standard* ini disusun untuk mengetahui efektivitas produk algoritma kriptografi *Advanced Encryption Standard* yang telah dikembangkan untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah.

Kisi-Kisi Uji Efektivitas Komponen Produk Algoritma Kriptografi *AES*

Pengembangan kisi-kisi uji efektivitas produk algoritma kriptografi *AES* untuk mendapatkan data tentang keefektifan produk algoritma kriptografi *AES* yang dikembangkan. Kisi-kisi ini memuat tiga komponen pokok yang dijabarkan dalam bentuk indikator-indikator. Berdasarkan indikator-indikator tersebut selanjutnya dikembangkan rumusan pernyataan untuk memperoleh penilaian. Indikator-indikator tersebut dirumuskan dalam Tabel 1 berikut.

Tabel 1. Kisi-kisi Lembar Uji Efektivitas Komponen Produk Kriptografi *AES*

No.	Indikator Validasi Model Produk Kriptografi *AES*	No. Pernyataan
1.	Kondisi Produk Kriptografi *Advanced Encryption Standard*	1, 2, 3
2.	Proses Enkripsi Kriptografi *Advanced Encryption Standard*	4, 5
3.	Kerahasiaan Kriptografi *Advaned Encryption Standard.*	6, 7

Bentuk Instrumen

Penyusunan instrumen uji keefektifan produk algoritma kriptografi *AES* ini menggunakan skala likert. Masing-masing pernyataan yang tersedia memiliki lima macam pilihan jawaban yang merupakan penilaian terhadap keefektivitasan produk algoritma kriptografi *AES* untuk meningkatkan keamanan pada sistem informasi pondok pesantren An-Najah.

Cara Penggunaan

Hasil penilaian lembar validasi ini direpresentasikan dalam bentuk nilai x. Rata-rata (x) yang diperoleh menunjukkan tingkat efektivitas produk algoritma kriptografi *AES* untuk meningkatkan keamanan pada sistem informasi. Kriteria untuk menentukan penilaian secara umum dijabarkan dalam Tabel 2 berikut.

Tabel 2. Kriteria Penilaian

No.	Nilai	Keterangan
1.	$1{,}00 \leq x \leq 1{,}80$	Tidak baik
2.	$1{,}80 < x \leq 2{,}60$	Kurang baik
3.	$2{,}60 < x \leq 3{,}40$	Cukup baik
4.	$3{,}40 < x \leq 4{,}20$	Baik
5.	$4{,}20 < x \leq 5{,}00$	Sangat baik

Petunjuk Penggunaan

Berilah skor pada butir-butir lembar validasi komponen produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan keamanan pada sistem informasi dengan cara melingkari nilai (1, 2, 3, 4, atau 5) sesuai dengan kriteria penilaian pada masing-masing nomor pertanyaan.

LEMBAR UJI EFEKTIVITAS
KOMPONEN PRODUK ALGORITMA KRIPTOGRAFI
***ADVANCED ENCRYPTION STANDARD* (AES)**
UNTUK MENINGKATKAN KEAMANAN PADA SISTEM INFORMASI
PONDOK PESANTREN AN-NAJAH

Nama Penilai	:	Imam Abdul Aziz, S. Kom.
Jabatan	:	Pembuat Sistem Informasi
Tempat Tugas	:	Pondok Pesantren An-Najah

Petunjuk Penilaian Validasi

1. Mohon Bapak/Ibu berkenan memberikan penilaian terhadap model produk algoritma kriptografi *Advanced Encryption Standard* untuk meningkatkan keamanan pada sistem informasi yang telah dikembangkan.
2. Penilaian produk algoritma kriptografi *Advanced Encryption* Standard untuk meningkatkan keamanan pada sistem informasi meliputi aspek :
   a. Kondisi Produk Kriptografi *Advanced Encryption Standard.*
   b. Proses Enkripsi Produk Kriptografi *Advanced Enrcryption Standard.*
   c. Kerahasiaan Kriptografi *Advaned Encryption Standard.*
3. Dimohon Bapak/Ibu memberi nilai pada butir-butir pengembangan produk algoritma kriptografi *Advanced Encryption Standard* dengan cara melingkari nilai (1, 2, 3, 4, atau 5) sesuai dengan kriteria penilaian pada masing-masing nomor pertanyaan.
4. Saran-saran yang Bapak/Ibu berikan, mohon dituliskan pada naskah yang perlu direvisi, atau dituliskan pada lembar saran yang telah disediakan.

Penilaian Produk Kriptografi *Advanced Encryption Standard*

A. Penilaian Aspek Kondisi Produk Kriptografi *AES*

1. Kondisi produk saat dijalankan

Rendah	Tinggi
Produk tidak berfungsi dengan baik dan masih terdapat *bug*..	Produk berfungsi sesuai dengan tujuan pembuatan.

2. Produk tidak menyebabkan kinerja melambat

Rendah	Tinggi
Produk sangat memperlambat kinerja dari sistem informasi.	Kinerja sistem informasi masih stabil dan tidak memperlambat kinerja sistem.

3. Produk tidak menyebabkan *crash* pada komputer

Rendah	Tinggi
komputer mengalami *crash* saat membuka sistem informasi.	Tidak terdapat hambatan berupa *crash*, hang atau kondisi lain saat dapat membuka sistem informasi.

B. Penilaian Proses Enkripsi Data Produk Kriptografi *AES*

4. Waktu yang dibutuhkan dalam melakukan enkripsi

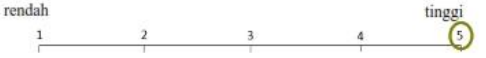
Rendah	Tinggi
Tidak memberikan kecepatan yang tinggi untuk meningkatkan keefektifan sistem informasi	Kecepatan yang diproses sangat tinggi sehingga dapat meningkatkan keefektifan sistem informasi

5. Dapat mengamankan data pada *database*

Rendah	Tinggi
Data pada *database* masih sama dan tanpa perubahan yang signifikan sehingga dapat dengan mudah diketahui datanya.	Dapat mengubah data secara signifikan dan tidak dapat dibaca sehingga data aman dari pencurian data.

C. Penilaian Kerahasiaan Data Produk Kriptografi *AES*

6. Kerahasiaan data kriptografi *AES*



Rendah	Tinggi
Data sangat tidak rahasia dan rentan untuk diketahui kerahasiaannya	Data sangat rahasia dan sulit untuk diketahui kerahasiaannya

7. Panjang kunci kriptografi *AES*

Pendek	Panjang
Panjang kunci terlalu pendek sehingga rawan untuk ditembus dari pihak luar.	Kunci sangat panjang sehingga keamanan data terjamin.

Komentar dan saran perbaikan

enkripsi sangat bagus, akan tetapi terkadang terjadi tulisan "\n\n" ketika di dekripsi. Jadi alangkah baiknya sebelum di dekripsi perlu di replace dulu karakter "\n\n\n" biar tidak muncul ketika di dekripsi

Indikator Penilaian Validasi

No.	Nilai	Keterangan
1.	$1{,}00 \leq x \leq 1{,}80$	Tidak layak
2.	$1{,}80 < x \leq 2{,}60$	Kurang layak
3.	$2{,}60 < x \leq 3{,}40$	Cukup layak
4.	$3{,}40 < x \leq 4{,}20$	Layak
5.	$4{,}20 < x \leq 5{,}00$	Sangat layak

Kesimpulan penilaian

Setelah mengisi tabel penilaian, dimohon Bapak/Ibu melingkari angka di bawah ini sesuai dengan penilaian Bapak/Ibu.

Produk algoritma kriptografi *Advanced Encryption Standard* ini:

1. Tidak baik, sehingga belum dapat digunakan, harus diganti
2. Kurang baik, sehingga belum dapat digunakan, masih memerlukan konsultasi
3. Cukup baik, sehingga dapat digunakan tetapi dengan banyak revisi.
4. Baik, sehingga dapat digunakan tetapi dengan sedikit revisi.
5. Sangat baik, sehingga dapat digunakan tanpa revisi

Brebes, 5 Januari 2021

Penilai,

Imam Abdul Aziz, S. Kom.

Lampiran 10 Script Algoritma Kriptografi *Advanced Encryption Standard*

```
<?php

class AES{
    private static $sBox = array(
        0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc
5,
        0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x7
6,
        0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf
0,
        0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc
0,
        0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xc
c,
        0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x1
5,
        0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9
a,
        0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x7
5,
        0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa
0,
        0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x8
4,
        0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5
b,
        0x6a, 0xcb, 0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xc
f,
        0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x8
5,
```

```
        0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa
8,
        0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf
5,
        0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd
2,
        0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x1
7,
        0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x7
3,
        0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x8
8,
        0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xd
b,
        0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5
c,
        0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x7
9,
        0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa
9,
        0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x0
8,
        0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc
6,
        0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8
a,
        0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0
e,
        0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9
e,
        0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x9
4,
```

```
        0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xd
f,
        0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x6
8,
        0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x1
6
    );
    private static $InvsBox = array(
        0x52, 0x09, 0x6a, 0xd5, 0x30, 0x36, 0xa5, 0x3
8,
        0xbf, 0x40, 0xa3, 0x9e, 0x81, 0xf3, 0xd7, 0xf
b,
        0x7c, 0xe3, 0x39, 0x82, 0x9b, 0x2f, 0xff, 0x8
7,
        0x34, 0x8e, 0x43, 0x44, 0xc4, 0xde, 0xe9, 0xc
b,
        0x54, 0x7b, 0x94, 0x32, 0xa6, 0xc2, 0x23, 0x3
d,
        0xee, 0x4c, 0x95, 0x0b, 0x42, 0xfa, 0xc3, 0x4
e,
        0x08, 0x2e, 0xa1, 0x66, 0x28, 0xd9, 0x24, 0xb
2,
        0x76, 0x5b, 0xa2, 0x49, 0x6d, 0x8b, 0xd1, 0x2
5,
        0x72, 0xf8, 0xf6, 0x64, 0x86, 0x68, 0x98, 0x1
6,
        0xd4, 0xa4, 0x5c, 0xcc, 0x5d, 0x65, 0xb6, 0x9
2,
        0x6c, 0x70, 0x48, 0x50, 0xfd, 0xed, 0xb9, 0xd
a,
        0x5e, 0x15, 0x46, 0x57, 0xa7, 0x8d, 0x9d, 0x8
4,
```

```
        0x90, 0xd8, 0xab, 0x00, 0x8c, 0xbc, 0xd3, 0x0
a,
        0xf7, 0xe4, 0x58, 0x05, 0xb8, 0xb3, 0x45, 0x0
6,
        0xd0, 0x2c, 0x1e, 0x8f, 0xca, 0x3f, 0x0f, 0x0
2,
        0xc1, 0xaf, 0xbd, 0x03, 0x01, 0x13, 0x8a, 0x6
b,
        0x3a, 0x91, 0x11, 0x41, 0x4f, 0x67, 0xdc, 0xe
a,
        0x97, 0xf2, 0xcf, 0xce, 0xf0, 0xb4, 0xe6, 0x7
3,
        0x96, 0xac, 0x74, 0x22, 0xe7, 0xad, 0x35, 0x8
5,
        0xe2, 0xf9, 0x37, 0xe8, 0x1c, 0x75, 0xdf, 0x6
e,
        0x47, 0xf1, 0x1a, 0x71, 0x1d, 0x29, 0xc5, 0x8
9,
        0x6f, 0xb7, 0x62, 0x0e, 0xaa, 0x18, 0xbe, 0x1
b,
        0xfc, 0x56, 0x3e, 0x4b, 0xc6, 0xd2, 0x79, 0x2
0,
        0x9a, 0xdb, 0xc0, 0xfe, 0x78, 0xcd, 0x5a, 0xf
4,
        0x1f, 0xdd, 0xa8, 0x33, 0x88, 0x07, 0xc7, 0x3
1,
        0xb1, 0x12, 0x10, 0x59, 0x27, 0x80, 0xec, 0x5
f,
        0x60, 0x51, 0x7f, 0xa9, 0x19, 0xb5, 0x4a, 0x0
d,
        0x2d, 0xe5, 0x7a, 0x9f, 0x93, 0xc9, 0x9c, 0xe
f,
```

```
        0xa0, 0xe0, 0x3b, 0x4d, 0xae, 0x2a, 0xf5, 0xb
0,
        0xc8, 0xeb, 0xbb, 0x3c, 0x83, 0x53, 0x99, 0x6
1,
        0x17, 0x2b, 0x04, 0x7e, 0xba, 0x77, 0xd6, 0x2
6,
        0xe1, 0x69, 0x14, 0x63, 0x55, 0x21, 0x0c, 0x7
d
    );
    private static $ltable = array(
        0x00, 0xff, 0xc8, 0x08, 0x91, 0x10, 0xd0, 0x3
6,
        0x5a, 0x3e, 0xd8, 0x43, 0x99, 0x77, 0xfe, 0x1
8,
        0x23, 0x20, 0x07, 0x70, 0xa1, 0x6c, 0x0c, 0x7
f,
        0x62, 0x8b, 0x40, 0x46, 0xc7, 0x4b, 0xe0, 0x0
e,
        0xeb, 0x16, 0xe8, 0xad, 0xcf, 0xcd, 0x39, 0x5
3,
        0x6a, 0x27, 0x35, 0x93, 0xd4, 0x4e, 0x48, 0xc
3,
        0x2b, 0x79, 0x54, 0x28, 0x09, 0x78, 0x0f, 0x2
1,
        0x90, 0x87, 0x14, 0x2a, 0xa9, 0x9c, 0xd6, 0x7
4,
        0xb4, 0x7c, 0xde, 0xed, 0xb1, 0x86, 0x76, 0xa
4,
        0x98, 0xe2, 0x96, 0x8f, 0x02, 0x32, 0x1c, 0xc
1,
        0x33, 0xee, 0xef, 0x81, 0xfd, 0x30, 0x5c, 0x1
3,
```

```
        0x9d, 0x29, 0x17, 0xc4, 0x11, 0x44, 0x8c, 0x8
0,
        0xf3, 0x73, 0x42, 0x1e, 0x1d, 0xb5, 0xf0, 0x1
2,
        0xd1, 0x5b, 0x41, 0xa2, 0xd7, 0x2c, 0xe9, 0xd
5,
        0x59, 0xcb, 0x50, 0xa8, 0xdc, 0xfc, 0xf2, 0x5
6,
        0x72, 0xa6, 0x65, 0x2f, 0x9f, 0x9b, 0x3d, 0xb
a,
        0x7d, 0xc2, 0x45, 0x82, 0xa7, 0x57, 0xb6, 0xa
3,
        0x7a, 0x75, 0x4f, 0xae, 0x3f, 0x37, 0x6d, 0x4
7,
        0x61, 0xbe, 0xab, 0xd3, 0x5f, 0xb0, 0x58, 0xa
f,
        0xca, 0x5e, 0xfa, 0x85, 0xe4, 0x4d, 0x8a, 0x0
5,
        0xfb, 0x60, 0xb7, 0x7b, 0xb8, 0x26, 0x4a, 0x6
7,
        0xc6, 0x1a, 0xf8, 0x69, 0x25, 0xb3, 0xdb, 0xb
d,
        0x66, 0xdd, 0xf1, 0xd2, 0xdf, 0x03, 0x8d, 0x3
4,
        0xd9, 0x92, 0x0d, 0x63, 0x55, 0xaa, 0x49, 0xe
c,
        0xbc, 0x95, 0x3c, 0x84, 0x0b, 0xf5, 0xe6, 0xe
7,
        0xe5, 0xac, 0x7e, 0x6e, 0xb9, 0xf9, 0xda, 0x8
e,
        0x9a, 0xc9, 0x24, 0xe1, 0x0a, 0x15, 0x6b, 0x3
a,
```

```
        0xa0, 0x51, 0xf4, 0xea, 0xb2, 0x97, 0x9e, 0x5
d,
        0x22, 0x88, 0x94, 0xce, 0x19, 0x01, 0x71, 0x4
c,
        0xa5, 0xe3, 0xc5, 0x31, 0xbb, 0xcc, 0x1f, 0x2
d,
        0x3b, 0x52, 0x6f, 0xf6, 0x2e, 0x89, 0xf7, 0xc
0,
        0x68, 0x1b, 0x64, 0x04, 0x06, 0xbf, 0x83, 0x3
8
    );
    private static $atable = array(
        0x01, 0xe5, 0x4c, 0xb5, 0xfb, 0x9f, 0xfc, 0x1
2,
        0x03, 0x34, 0xd4, 0xc4, 0x16, 0xba, 0x1f, 0x3
6,
        0x05, 0x5c, 0x67, 0x57, 0x3a, 0xd5, 0x21, 0x5
a,
        0x0f, 0xe4, 0xa9, 0xf9, 0x4e, 0x64, 0x63, 0xe
e,
        0x11, 0x37, 0xe0, 0x10, 0xd2, 0xac, 0xa5, 0x2
9,
        0x33, 0x59, 0x3b, 0x30, 0x6d, 0xef, 0xf4, 0x7
b,
        0x55, 0xeb, 0x4d, 0x50, 0xb7, 0x2a, 0x07, 0x8
d,
        0xff, 0x26, 0xd7, 0xf0, 0xc2, 0x7e, 0x09, 0x8
c,
        0x1a, 0x6a, 0x62, 0x0b, 0x5d, 0x82, 0x1b, 0x8
f,
        0x2e, 0xbe, 0xa6, 0x1d, 0xe7, 0x9d, 0x2d, 0x8
a,
```

```
        0x72, 0xd9, 0xf1, 0x27, 0x32, 0xbc, 0x77, 0x8
5,
        0x96, 0x70, 0x08, 0x69, 0x56, 0xdf, 0x99, 0x9
4,
        0xa1, 0x90, 0x18, 0xbb, 0xfa, 0x7a, 0xb0, 0xa
7,
        0xf8, 0xab, 0x28, 0xd6, 0x15, 0x8e, 0xcb, 0xf
2,
        0x13, 0xe6, 0x78, 0x61, 0x3f, 0x89, 0x46, 0x0
d,
        0x35, 0x31, 0x88, 0xa3, 0x41, 0x80, 0xca, 0x1
7,
        0x5f, 0x53, 0x83, 0xfe, 0xc3, 0x9b, 0x45, 0x3
9,
        0xe1, 0xf5, 0x9e, 0x19, 0x5e, 0xb6, 0xcf, 0x4
b,
        0x38, 0x04, 0xb9, 0x2b, 0xe2, 0xc1, 0x4a, 0xd
d,
        0x48, 0x0c, 0xd0, 0x7d, 0x3d, 0x58, 0xde, 0x7
c,
        0xd8, 0x14, 0x6b, 0x87, 0x47, 0xe8, 0x79, 0x8
4,
        0x73, 0x3c, 0xbd, 0x92, 0xc9, 0x23, 0x8b, 0x9
7,
        0x95, 0x44, 0xdc, 0xad, 0x40, 0x65, 0x86, 0xa
2,
        0xa4, 0xcc, 0x7f, 0xec, 0xc0, 0xaf, 0x91, 0xf
d,
        0xf7, 0x4f, 0x81, 0x2f, 0x5b, 0xea, 0xa8, 0x1
c,
        0x02, 0xd1, 0x98, 0x71, 0xed, 0x25, 0xe3, 0x2
4,
```

```
        0x06, 0x68, 0xb3, 0x93, 0x2c, 0x6f, 0x3e, 0x6
c,
        0x0a, 0xb8, 0xce, 0xae, 0x74, 0xb1, 0x42, 0xb
4,
        0x1e, 0xd3, 0x49, 0xe9, 0x9c, 0xc8, 0xc6, 0xc
7,
        0x22, 0x6e, 0xdb, 0x20, 0xbf, 0x43, 0x51, 0x5
2,
        0x66, 0xb2, 0x76, 0x60, 0xda, 0xc5, 0xf3, 0xf
6,
        0xaa, 0xcd, 0x9a, 0xa0, 0x75, 0x54, 0x0e, 0x0
1
    );

    # Key Schedule (Key Ekspansi)
    private $w = array();
    # Vektor 16 Bit
    private $iv;
    # Blok pada data AES
    private static $Nb = 4;
    # Blok pada key AES;
    private $Nk;
    # Banyaknya Putaran (Round)
    private $Nr;
    # Matriks keadaan dalam Cipher AES dengan Nb Kolo
m dan 4 Baris
    private $s = array(array());

    # Function Paling Awal
    public function __construct($z, $iv = null){
        $this->iv = $iv;
        $this->Nk = strlen($z)/4;
```

```
        $this->Nr = $this->Nk + self::$Nb + 2;
        if (strlen($this->iv) != 16) {
            die('Vektor bukan 16 bit Karakter');
        }
        if ($this->Nk !=4 && $this->Nk != 6 && $this-
>Nk != 8) {
            die('Key bukan 128, 192 atau 256 Bit');
        }
        $this->Nr = $this->Nk + self::$Nb + 2;
        $this->KeyExpansion($z);
    }

    # Function Paling Akhir
    public function __destruct()
    {
        unset($this->w);
        unset($this->s);
        # unset yaitu menghilangkan Variabel
    }

    function enkripsi($x)
    {
        $t = ''; // Untuk Menampung 16 Byte Sementara
        $y = ''; // Cipher text yang dikembalikan
        $y_blok = $this-
>iv; // Untuk Menahan output sementara dari cipher te
xt (16 Byte)
        $x_size = strlen($x); // Menghitung Jumlah Hu
ruf

        # Menggunakan ECB
```

```
        # Mengembil 16 Byte untuk di enkripsi dan dit
ampung ke hasil cipher sementara
        for ($i=0; $i < $x_size; $i += 16) {
            for ($j=0; $j < 16 ; $j++) {
                if ($i+$j < $x_size) {
                    $t[$j] = $x[$i+$j];
                }
                else
                {
                    $t[$j] = chr(0);
                }
            }
            $y_blok = $this->enkripsiBlok($t);
            $y .= $y_blok;
        }
        return base64_encode($y);
    }

    function dekripsi($y)
    {
        $y = base64_decode($y);
        $t = ''; // Untuk Menampung 16 Byte Sementara
        $x = ''; // Mengembalikan ke Plain Text
        $y_blok = $this->iv;
        $x_blok = '';

        $y_size = strlen($y);

        # Menggunakan Mode ECB
        for ($i=0; $i < $y_size ; $i+= 16) {
            for ($j=0; $j < 16 ; $j++) {
                if ($i+$j < $y_size) {
```

```
                    $t[$j] = $y[$i+$j];
                }
                else
                {
                    $t[$j] = chr(0);
                }
            }
            $x_blok = $this->dekripsiBlok($t);
            $x .= $x_blok;
        }
        return preg_replace('~[^a-zA-Z0-
9 @.]+~', '',$x);

    }

    function enkripsiBlok($x)
    {
        $y = ''; // 16 Byte untuk disimpan

        # Menempatkan inputan x pada sebuah Matriks d
engan urutan Kolom
        # Merubah string ke bilangan ASCII
        for ($i=0; $i < 4*self::$Nb ; $i++) {
            $this->s[$i%4][($i-
$i%self::$Nb)/self::$Nb] = ord($x[$i]);
        }

        # Add Round Key Ke 1
        $this->AddRoundKey(0);


        for ($i=1; $i < $this->Nr ; $i++) {
```

```
            # Sub Bytes Ke 1 sampai Nr-1
            $this->SubBytes();

            # Shift Rows Ke 1 sampai Nr-1
            $this->ShiftRows();

            # Mix Coloumn Ke 1 sampai Nr-1
            $this->MixColoumn();

            # Add Round Key Ke 2 - Nr
            $this->AddRoundKey($i);

        }

        # Sub Bytes Ke Nr
        $this->SubBytes();

        # Shift Rows Ke Nr
        $this->ShiftRows();

        # Add Round Key Ke Nr
        $this->AddRoundKey($i);

        for ($i=0; $i < 4*self::$Nb ; $i++) {
            $y .= chr($this->s[$i%4][($i-
$i%self::$Nb)/self::$Nb]);
        }
        return $y;
    }

    function dekripsiBlok($y)
    {
```

```
        $x = ''; // 16 Byte Untuk Di Simpan

        for ($i=0; $i < 4*self::$Nb ; $i++) {
            $this->s[$i%4][($i-
$i%self::$Nb)/self::$Nb] = ord($y[$i]);
        }

        # Add Round Key
        $this->AddRoundKey($this->Nr);

        for ($i = $this->Nr - 1; $i > 0 ; $i--) {
            # Invers Shift Rows
            $this->InvShiftRows();

            # Invers Sub Bytes
            $this->InvSubBytes();

            # Add Round key
            $this->AddRoundKey($i);

            # Invers Mix Coloumn
            $this->InvMixColoumn();
        }
        # Invers Shift Rows
        $this->InvShiftRows();

        # Invers Sub Bytes
        $this->InvSubBytes();

        # Add Round Key
        $this->AddRoundKey($i);
```

```
        for ($i=0; $i < 4*self::$Nb ; $i++) {
            $x .= chr($this->s[$i%4][($i-
$i%self::$Nb)/self::$Nb]);
        }
        return $x;
    }

    function AddRoundKey($round)
    {
        $temp = ''; // Sementara
        for ($i=0; $i < 4 ; $i++) {
            for ($j=0; $j < self::$Nb ; $j++) {
                # Mengambil W Kolom Pertama sampai Nb
                $temp = $this-
>w[$round*self::$Nb + $j] >> (3-$i)*8;
                # Menampilkan Nilai Asli
                $temp %= 256;
                # Membuat Positif temp
                $temp = ($temp < 0 ? (256 + $temp) :
$temp); // if dan Else
                # XOR state dengan Nilai Byte perkolo
m
                $this->s[$i][$j] ^= $temp;

            }
        }
    }

    function SubBytes()
    {
        # SubBytes adalah Mensubstitusikan State deng
an xBox
```

```
        for ($i=0; $i < 4 ; $i++) {
            for ($j=0; $j < self::$Nb ; $j++) {
                $this->s[$i][$j] = self::$sBox[$this-
>s[$i][$j]];
            }
        }
    }

    function ShiftRows()
    {
        # Shift Rows adalah Menggeser Baris sebanyak
n-1 kearah kiri
        $temp = array();
        for ($i=0; $i < 4 ; $i++) {
            for ($j=0; $j < self::$Nb ; $j++) {
                $temp[$j] = $this-
>s[$i][($i+$j)%self::$Nb];
            }
            for ($j=0; $j < self::$Nb ; $j++) {
                $this->s[$i][$j] = $temp[$j];
            }
        }
    }

    function MixColoumn()
    {
        $s0 = $s1 = $s2 = $s3 = '';
        for ($i=0; $i < self::$Nb ; $i++) {
            $s0 = $this->s[0][$i];
            $s1 = $this->s[1][$i];
            $s2 = $this->s[2][$i];
            $s3 = $this->s[3][$i];
```

```
            $this->s[0][$i] = $this-
>mult(0x02, $s0) ^ $this->mult(0x03, $s1) ^ $this-
>mult(0x01, $s2) ^ $this->mult(0x01, $s3);
            $this->s[1][$i] = $this-
>mult(0x01, $s0) ^ $this->mult(0x02, $s1) ^ $this-
>mult(0x03, $s2) ^ $this->mult(0x01, $s3);
            $this->s[2][$i] = $this-
>mult(0x01, $s0) ^ $this->mult(0x01, $s1) ^ $this-
>mult(0x02, $s2) ^ $this->mult(0x03, $s3);
            $this->s[3][$i] = $this-
>mult(0x03, $s0) ^ $this->mult(0x01, $s1) ^ $this-
>mult(0x01, $s2) ^ $this->mult(0x02, $s3);
        }
    }

    function mult($a, $b)
    {
        # Menambahkan ltable dari kedua inputan
        $sum = self::$ltable[$a] + self::$ltable[$b];
        # Menunjukan Nilai Asli dari Inputan dengan M
odulo
        $sum %= 255;
        # Substitusikan ke atable
        $sum = self::$atable[$sum];
        return ($a == 0 ? 0 : ($b == 0 ? 0 : $sum));
    }
    function KeyExpansion($z){
        # Konstanta Rcon
        static $Rcon = array(
            0x00000000,
            0x01000000,
```

```
            0x02000000,
            0x04000000,
            0x08000000,
            0x10000000,
            0x20000000,
            0x40000000,
            0x80000000,
            0x1b000000,
            0x36000000,
            0x6c000000,
            0xd8000000,
            0xab000000,
            0x4d000000,
            0x9a000000,
            0x2f000000
        );

        $temp = 0;
        # Kelompokan Key z dengan memisahkan perhuruf
 pada sebuah Matriks
        for ($i = 0; $i < $this-
>Nk; $i++) { //(Nk adalah number kata (128, 192, 256
bit))
            $this->w[$i] = 0;
            # Mengisi seluruh Kunci yang diperluas w
            # Dengan mendorong 4 bytes kedalam Kata w

            # Menambahkan byte baris pertama
            $this-
>w[$i] = ord($z[4*$i]); //ord untuk memecahkan karakt
er ke bilangan ASCII
```

```
            # Membuat Ruangan baru untuk Baris Selanj
utnya
            $this->w[$i] <<= 8;

            # Menambahkan Byte baris Kedua
            $this-
>w[$i] += ord($z[4*$i+1]); //ditambah 2

            # Membuat Ruangan baru untuk Baris Selanj
utnya
            $this->w[$i] <<= 8;

            # Menambahkan Byte Baris Ketiga
            $this-
>w[$i] += ord($z[4*$i+2]); //ditambah 3
            $this->w[$i] <<= 8;
            # Menambahkan Byte Baris Ketiga
            $this-
>w[$i] += ord($z[4*$i+3]); // ditambah 4
        }

        for (; $i < self::$Nb*($this-
>Nr+1); $i++) { //Nb*(Nr+1)

            # Mengambil Kolom Ke-4
            $temp = $this->w[$i-1];

            if ($i%$this->Nk == 0) {
                $temp = $this->subWord($this-
>rotWord($temp)) ^ $Rcon[$i/$this->Nk];
            } elseif ($this->Nk > 6 && $i%$this-
>Nk == 4) {
```

```
                $temp = $this->subWord($temp);
            }

            $this->w[$i] = $this->w[$i-$this-
>Nk] ^ $temp;

            self::make32BitWord($this->w[$i]);
        }
    }

    function InvShiftRows()
    {
        # Pergeseran Siklik Terbalik pada 3 Baris Ter
akhir dari Matrikx
        $temp = array();
        for ($i=0; $i < 4 ; $i++) {
            for ($j=0; $j < self::$Nb ; $j++) {
                $temp[($i+$j)%self::$Nb] = $this-
>s[$i][$j];
            }
            for ($j=0; $j < 4 ; $j++) {
                $this->s[$i][$j] = $temp[$j];
            }
        }
    }

    function InvSubBytes()
    {
        # Mensubstitusikan State ke Invers xBox
        for ($i=0; $i < 4 ; $i++) {
            for ($j=0; $j < self::$Nb ; $j++) {
```

```
                $this-
>s[$i][$j] = self::$InvsBox[$this->s[$i][$j]];
            }
        }
    }

    function InvMixColoumn()
    {
        $s0 = $s1 = $s2 = $s3 = '';
        for ($i=0; $i < self::$Nb ; $i++) {
            $s0 = $this->s[0][$i];
            $s1 = $this->s[1][$i];
            $s2 = $this->s[2][$i];
            $s3 = $this->s[3][$i];

            # Perkalian dengan Invers Matrika Mix Col
oumn
            # Invers Mix Coloumn adalah
            /*
            14 9 13 11
            11 14 9 13
            13 11 14 9
            9 13 11 14
            */
            $this->s[0][$i] = $this-
>mult(0x0e, $s0) ^ $this->mult(0x0b, $s1) ^ $this-
>mult(0x0d, $s2) ^ $this->mult(0x09, $s3);
            $this->s[1][$i] = $this-
>mult(0x09, $s0) ^ $this->mult(0x0e, $s1) ^ $this-
>mult(0x0b, $s2) ^ $this->mult(0x0d, $s3);
```

```
            $this->s[2][$i] = $this-
>mult(0x0d, $s0) ^ $this->mult(0x09, $s1) ^ $this-
>mult(0x0e, $s2) ^ $this->mult(0x0b, $s3);
            $this->s[3][$i] = $this-
>mult(0x0b, $s0) ^ $this->mult(0x0d, $s1) ^ $this-
>mult(0x09, $s2) ^ $this->mult(0x0e, $s3);

        }
    }

    function rotWord($w){
        # Rot Word adalah menggeser keatas Kolom Tera
khir satu kali
        # Mengambil Bit Pertama pada w
        $temp = $w >> 24;
        # Berikan Ruang untuk mengisi Baris
        $w <<= 8;
        # Membuat 32 bit word untuk mengantisipasi te
rlalu besar bit nya
        self::make32BitWord($w);
        # Untuk Melakukan Pergeseran Diperlukan temp
yang positif
        $temp += $temp < 0 ? 256 : 0; //membuat posit
if
        # Menambahkan Temp Positif
        $w += $temp;

        # Tampilkan hasil w
        return $w;
    }
    function subword($w){
```

```
        # Sub Word yaitu Mensubstitsikan setiap Bytes
 yang telah di Rot Word ke xBox Rinjdael
        $temp = 0;
        for ($i = 0; $i < 4; $i++) {
            # Mengambil 8 Bit Pertama
            $temp = $w >> 24; // put the first 8-
bits into temp
            # Temp Harus Positif
            $temp += $temp < 0 ? 256 : 0;
            # Memberikan Ruang untuk Mensubstitusikan
 w
            $w <<= 8;
            self::make32BitWord($w);
            # Menambahkan Byte yang telah disubstitus
ikan
            $w += self::$sBox[$temp];
        }
        self::make32BitWord($w);

        return $w;
    }

    private static function make32BitWord(&$w)
    {
        // Menjadi fungsi pembuat 32 bit
        $w &= 0x00000000FFFFFFFF;
    }
}

$Aes = new AES('SIAnNajahgondang', 'siannajahgondang'
);
?>
```

Lampiran 11 Profil Pondok Pesantren

Profil Pondok Pesantren

Nama Pondok	: Pondok Pesantren An-Najah
Nama Pengasuh	: KH. Minanul Aziz Syatori
Alamat	: Jl. Merbabu No. 20, Jl. Gondang Tani Selatan No. Rt. 19, Gondang Tani, Kec. Gondang, Kabupaten Sragen, Jawa Tengah 57254
Desa/Kelurahan	: Gondang Tani
Kecamatan	: Gondang
Kabupaten	: Sragen
Provinsi	: Jawa Tengah

Lampiran 12 Riwayat Hidup

RIWAYAT HIDUP

A. Identitas Diri

1. Nama Lengkap : Ivvan Nuzulul Huda
2. Tempat & Tgl. Lahir : Brebes, 17 November 1997
3. Alamat Rumah : Dusun Kedawon, Ds. Rengaspendawa, Kec. Larangan, Kab. Brebes
4. HP : 087835224600
5. E-Mail : ivannuzululhuda@gmail.com

B. Riwayat Pendidikan

1. Pendidikan Formal
   a. MI Miftahul Athfal 01 Kedawon (2003-2009)
   b. MTs Assalafiyah Sitanggal (2009-2012)
   c. MA Nahdlatul Ulama Gondang (2012-2015)
   d. UIN Walisongo Semarang (2015-2021)
2. Pendidikan Non-Formal
   a. Pondok Pesantren An-Najah Gondang
   b. Pondok Pesantren Raudlatut Tholibin

C. Prestasi Akademik

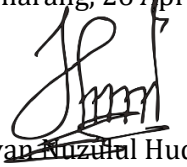
-

D. Karya Ilmiah

-

Demikian data riwayat hidup ini Saya buat dengan keadaan sebenarnya.

Semarang, 26 April 2021



Ivvan Nuzulul Huda

NIM : 1508046027