Penggunaan Algoritma *Advanced Encryption Standard* (Algoritma Rijndael) pada Sistem Keamanan di Bidang Perbankan

Muhammad Hanif A. Nasution - 18219077 (*Author*)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 18219077@std.stei.itb.ac.id

***Abstract*—Transaksi digital merupakan hal yang cukup umum dilakukan oleh seluruh masyarakat. Seluruh jenis bank, baik bank konvensional, maupun bank digital memiliki fitur untuk melakukan transaksi secara daring darimanapun dan kapanpun. Tentu, kemudahan ini mengundang berbagai masalah baru seperti peretasan data transaksi. Bahkan, peretasan tersebut dapat dilakukan sampai ke data pengguna bank tersebut yang dapat menyebabkan kerugian yang sangat besar. Oleh karen itu, umumnya, setiap sistem yang dimiliki oleh perbankan menggunakan sebuah metode enkripsi yang disebut *Advanced Encryption Standard*. Penggunaan AES dapat mengurangi masalah peretasan. Hal ini disebabkan oleh sulitnya memecahkan hasil enkripsi dari metode tersebut. Jenis AES yang digunakan pada perbankan adalah AES 128 bit atau 256 bit. Alasan penggunaan jenis tersebut adalah tingkat keamanan yang sangat tinggi.**

***Keywords*—AES, enkripsi, perbankan, 256 bit**

I. PENDAHULUAN

Transaksi digital adalah sebuah kegiatan transaksi yang dilakukan tanpa membutuhkan penggunaan kertas atau uang. Jenis transaksi ini memungkinkan seseorang untuk melakukan transaksi kapanpun dan dimanapun tanpa harus bertemu. Kemudahan ini membuat jenis transaksi ini menjadi salah satu jenis transaksi yang paling sering dilakukan. Namun, transaksi digital membutuhkan keamanan dalam melakukannya karena berisiko terjadinya pencurian dan peretasan data transaksi. Hal ini dapat menyebabkan kerugian yang tak terkira dari pelaku transaksi.

Dahulu, banyak bermunculan perkataan mengenai keamanan dari transaksi digital. Banyak narasi mengenai ketidakamanan transaksi digital dibandingkan transaksi luring. Sebelumnya, hal tersebut merupakan narasi yang benar karena perkembangan teknologi dahulu tidak semaju sekarang. Pada tangga 27 November sampai dengan 15 Desember 2013, terjadi salah satu insiden peretasan terbesar pada transaksi digital. Perusahaan Target mengumumkan mengenai 70 juta akun pengguna berhasil diretas. Tidak lama setelah itu, 56 juta kartu kredit pada perusahaan Home Depot berhasil diretas pada penyerangan selama 5 bulan. 1,1 juta kartu kredit berhasil diretas pada penyerangan selama 3 bulan.

Berkaca dari kasus-kasus yang sudah dibahas sebelumnya, banyak perusahaan berusaha mengembangkan teknologi yang digunakan dalam keamanan transaksi secara digital. Salah satu metode keamanan transaksi yang digunakan pada transaksi di dunia perbankan adalah penggunaan *Advanced Encryption Standard*. Pembahasan mengenai AES akan dijelaskan pada bab selanjutnya.

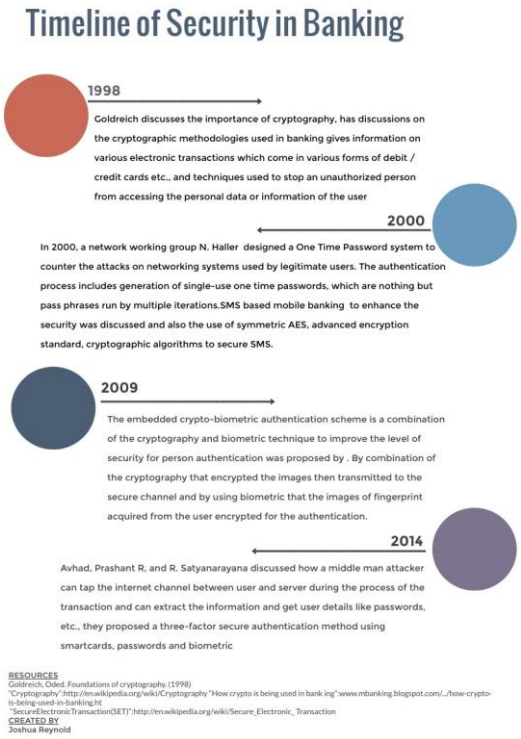


Fig. 1. Sejarah Perkembangan Sistem Keamanan Perbankan

(sumber: https://medium.com/@joshuareynolds/cryptography-and-security-in-banking-2cce7691e70f)

Sebelumnya, pada tahun 1970an, perbankan menggunakan *Data Encryption Standard* (DES) sebagai metode kriptografi untuk mengamankan data-datanya. Namun, masih terdapat peretasan yang berhasil dilakukan. Pada tahun 2002, muncul

dua metode kriptografi baru yang merupakan hasil pengembangan dari DES. Dua metode tersebut adalah *Triple* DES dan *Advanced Encryption Standard*. Pada tahun-tahun berikutnya, keamanan pada data perbankan dienkripsi dengan menggunakan kedua metode tersebut. AES sering disebut sebagai Algoritma Rijndael memiliki tingkat keamanan yang hampir mustahil dipecahkan. Oleh karena itu penggunaan AES terus berlanjut digunakan pada keamanan data perbankan.

II. LANDASAN TEORI

A. *Advanced Encryption Standard*

Advanced Encryption Standard (AES) adalah sebuah metode kriptografi yang dikembangkan pada tahun 2002 untuk menyempurnakan metode kriptografi sebelumnya, *Data Encryption Standard*. AES memiliki nama lain yaitu Algoritma Rijndael karena berasal dari penemunya yaitu Joan Daemen dan Vincent Rijmen.

AES merupakan kriptografi yang termasuk ke dalam tipe *iterative* (non-Feistel). Jenis kriptografi ini berdasarkan pada teori substitusi dan permutasi. AES dilakukan komputasinya pada skala bytes. Hal ini mempengaruhi anggapan besar suatu teks yang biasanya disebut memiliki panjang 128 bits menjadi sepanjang 16 bytes. Byte-byte ini disusun ke dalam empat kolom dan empat baris untuk diproses sebagai matriks.

Jumlah *rounds* dari AES ditentukan pada panjang dari kunci yang digunakan. Perbedaan tersebut dapat dilihat pada tabel berikut.

Jumlah *Rounds*	**Panjang Key**
10 rounds	128-bit keys
12 rounds	192-bit keys
14 rounds	256-bit keys

Penggambaran dari skema struktur AES digambarkan pada berikut.

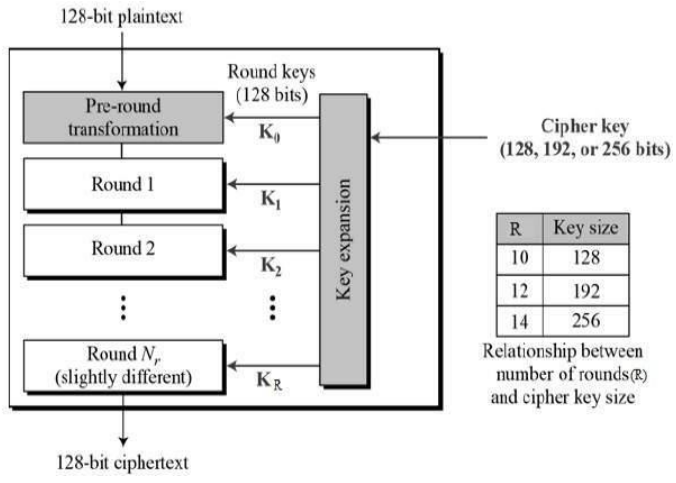


Fig. 2. Skema dari Struktur AES

(sumber: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm)

Beberapa fitur dari AES adalah sebagai berikut:

1. Kunci yang simetris dan blok yang simetri
2. Data sebesar 128 bit, kunci sebesar 128/192/256 bit
3. Lebih aman daripada *Triple* DES
4. Dapat diimplementasikan pada Java dan Python

AES pada panjang kunci 128 bit memiliki kemungkinan kunci sebanyak 2^{128} atau sekitar 3,4 x 10^{38}. Komputer tercepat hanya bisa mencoba 10^6 kunci setiap detik. Oleh karena itu, dibutuhkan kurang lebih 5,4 x 10^{24} tahun untuk mencoba seluruh kunci yang ada.

Selain itu, AES memiliki beberapa variasi, yaitu:

1. ECB (*Electronic Code Book*)
2. CBC (*Cipher Block Chaining*)
3. CFB (*Cipher Feed Back*)
4. OFB (*Output Feed Back*)
5. CTR (*Counter*)
6. GCM (*Galois/Counter Mode*)

Setiap variasi dari AES memiliki kekurangan dan kelebihan masing-masing. Namun, pada dokumen kali ini, penulis hanya memfokuskan pada AES tanpa variasi.

B. Enkripsi AES

Proses enkripsi dari AES yang umum (128 bit blok dan 128 bit key) memiliki total 10 rounds dan setiap round memiliki empat proses, yaitu:

1. Byte Substitution

   Melakukan substitusi 16 input byte dengan melihat kepada tabel S-Box. Hasilnya akan berbentuk matriks 4x4.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 3. Tabel S-B0x

(sumber: PPT Perkuliahan)

2. Shiftrows

   Setiap dari keempat baris akan digeser ke kiri. Setiap element yang terjatuh akan diisi pada baris paling kiri. Beberapa peraturan dari pemindahan adalah sebagai berikut:

1. Baris pertama tidak digeser
2. Baris kedua digeser satu posisi ke kiri
3. Baris ketiga digeser dua posisi ke kiri
4. Baris keempat digeser tiga posisi ke kiri

3. MixColumns

   Seluruh kolum dari 4 bytes ditransformasi menggunakan fungsi matematik. Fungsi ini menerima input empat byte dari satu kolum dan menghasilkan empat byte baru yang mengganti kolum aslinya. Hasilnya menghasilkan matriks baru bersisi 16 bytes baru.

4. Addroundkey

   Seluruh 16 bytes dari matriks akan dilakukan XOR pada 128 bits dari kunci di round tersebut. Setelah itu, Kembali dimulai round selanjutnya.

C. Dekripsi AES

Dekripsi AES menggunakan keempat langkah yang terdapat pada proses enkripsi. Namun, keempat langkah ini dibalik urutannya.

D. Data Encryption Standard

DES adalah sebuah algoritma kriptografi yang diterbitkan oleh National Institute of Standards and Technology (NIST). Pada awalnya, standard inii digunakan oleh sistem keamanan perbankan. Namun, terdapat beberapa kendala yang menyebabkan algoritma ini ditinggalkan. Salah satunya adalah algoritma ini berhasil dipecahkan dengan waktu kurang dari satu hari. Hal ini tentu membuat para bank susah untuk menggunakan algoritma ini.

Berbeda dengan AES, DES menggunakan 16 Round struktur Feisel. Besar dari bloknya adalah 64 bit dan key sebesar 56 bit. Struktur dari algoritma DES adalah sebagai berikut.

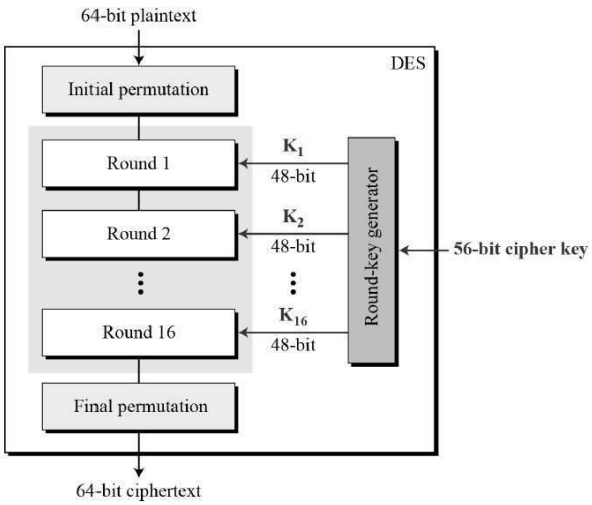


Fig. 4. Struktur dari DES

(sumber:https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm)

Langkah-langkah dari enkripsi DES adalah sebagai berikut:

1. *Initial* dan *Final* Permutasi

   Permutasi yang dilakukan berasal dari P-boxes yang merupakan inverse dari satu sama lain. *Initial* dan *Final* adalah sebagai berikut.

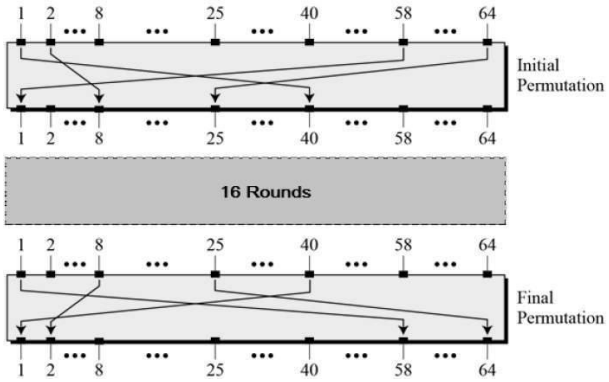


Fig. 5. *Initial* dan *Final* Permutasi

(sumber:https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm)

2. Fungsi Round

   Inti utama dari kriptografi ini adalah fungsi DES. Fungsi ini mengaplikasikan 48 bit kunci kepada 32 bit untuk menghasilkan 32 bit.

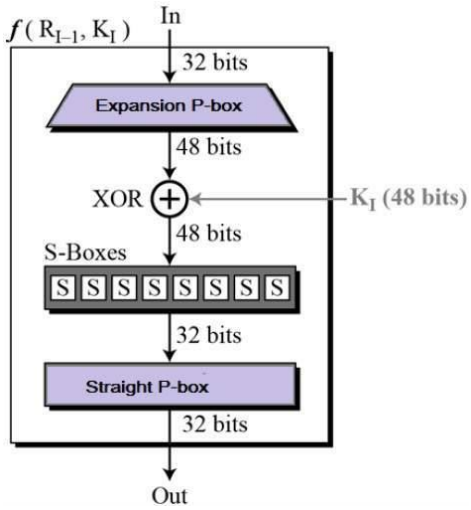


Fig. 6. Fungsi DES

(sumber:https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm)

3. Membangkitkan Kunci

   Tahapan pembangkitan kunci dilakukan dengan metode sebagai berikut.

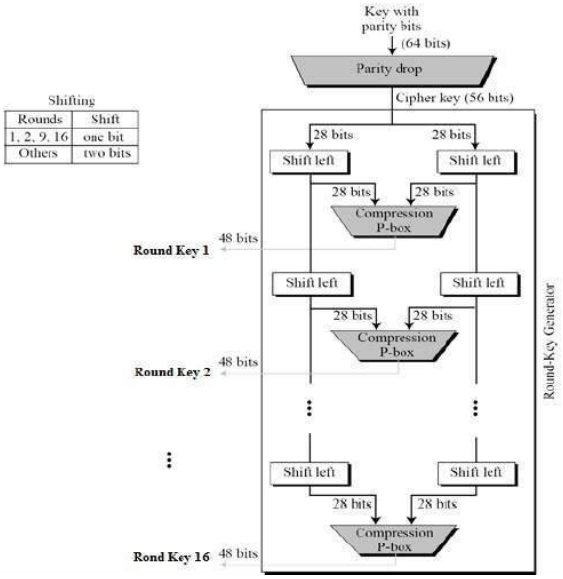


Fig. 7. Metode Pembangkitan Kunci DES

(sumber:https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm)

III. PEMBAHASAN

Pada pembahasan, akan membandingkan diagram alir dari AES dan DES sebagai analisis terkait mengapa AES tergantikan oleh DES sebagai sistem keamanan pada sistem perbankan.

Sebelumnya, perhatikan terlebih dahulu *flow chart* dari algoritma DES.

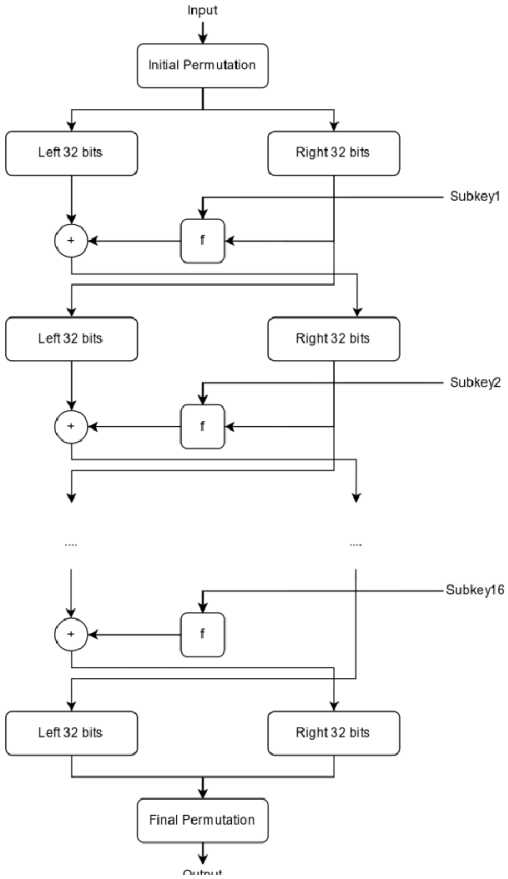


Fig. 8. Diagram Alir DES

(sumber: https://www.researchgate.net/figure/DES-algorithm-flowchart_fig1_343124563)

Dapat dilihat pada diagram alir tersebut, proses enkripsi dengan menggunakan DES hanya menggunakan fungsi DES ditambah dengan metode XOR yang ditandai dengan "+". Hal ini membuat peretasan pada data yang dienkripsi dengan DES menjadi lebih mudah dilakukan. Selain itu, jumlah bit yang hanya 32 bit membuat DES lebih mudah didekripsi oleh para peretas.

Terdapat pengembangan dari algoritma DES, yaitu Triple DES. Perhatikan terlebih dahulu diagram alir dari Triple DES.

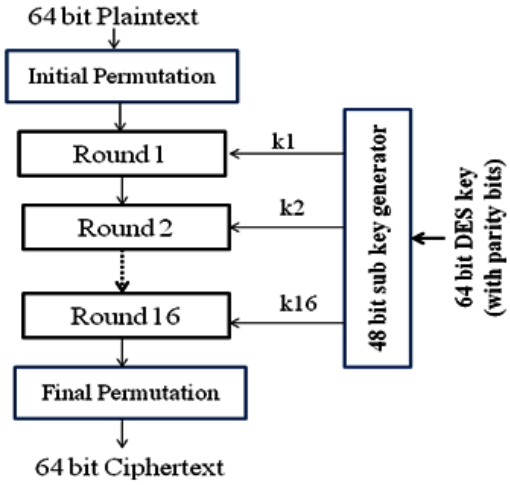


Fig. 9. Diagram Alir Triple DES

(sumber:https://www.researchgate.net/figure/Overall-schematic-diagram-of-DES-Triple-DES-3-DES-is-a-modification-of-simple-DES_fig1_261421877)

Modifikasi yang dilakukan pada Triple DES hanya pada penambahan jumlah bit yang dienkripsi menjadi 64. Selain itu terdapat perubahan pada fungsi yang digunakan. Namun, proses enkripsi masih sama dengan DES sebelumnya. Hal ini tentu masih dalam tingkatan yang lebih mudah diretas dibandingkan dengan AES.

Untuk pembanding terakhir, perhatikan diagram alir dari algoritma AES.

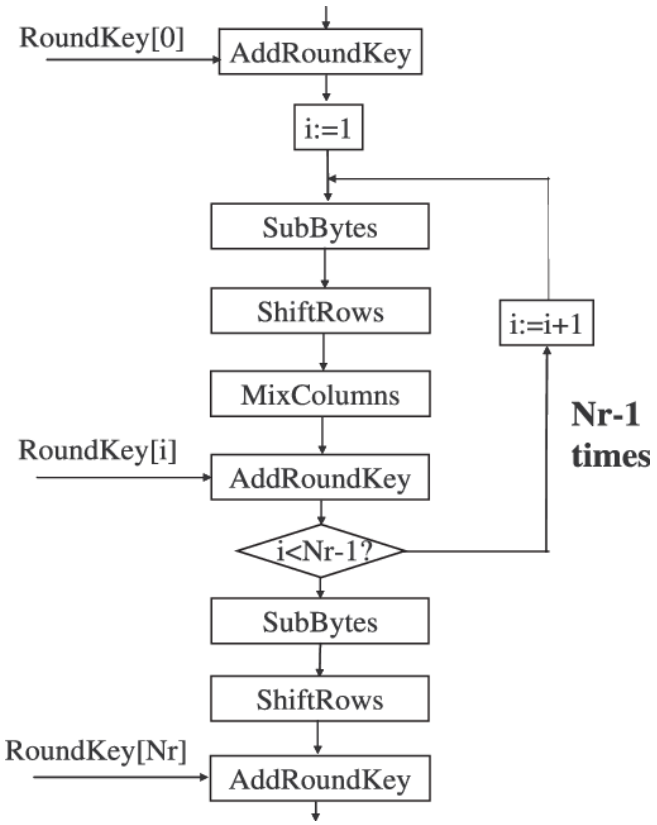


Fig. 10. Diagram Alir AES

(sumber: https://www.researchgate.net/figure/AES-encryption-flowchart_fig3_227063109)

Pada AES, dapat dilihat bahwa jumlah bit bertambah hingga 128 dan proses yang dilakukan untuk melakukan enkripsi dilakukan pada setiap elemen yang terdapat pada teks. Hal ini tentu menambah tingkat keamanan dari penggunaan AES. Selain itu, jumlah bit 128 membuat kunci yang harus diretas menjadi semakin sulit dilakukan.

Penggunaan AES sebagai metode sistem keamanan pada sistem perbankan sangat sulit untuk diretas dan hampir tidak mungkin. Hal ini sangat berguna untuk melakukan pengamanan pada transaksi digital yang dipercaya memiliki tingkat keamanan yang rendah. Dengan implementasi dari algoritma ini, kemungkinan peretasan pada transaksi digital, khususnya transaksi perbankan menjadi semakin sulit dilakukan

IV. Kesimpulan

Kesimpulan dari mengapa AES digunakan pada sistem perbankan adalah tingkat keamanan dan kesulitan yang terdapat pada setiap langkah-langkah dari proses enkripsi teks. Selain itu, algoritma DES berhasil dipecahkan dengan mudah karena jumlah bit yang sedikit dan proses yang mudah untuk diretas. Fungsi DES sendiri memiliki tingkat pemecahan yang cukup tinggi untuk para peretas. Sebagai bayangan lebih lanjut, terdapat beberapa poin kesimpulan dari penggunaan AES dibandingkan dengan DES.

1. Kunci AES besarnya 128/192/256 bit dan membuat AES sulit diretas dibandingkan besar kunci DES sebesar 56 bit
2. Besar blok dari AES 128 bit membuat peretas harus melakukan kombinasi varian dari blok yang lebih banyak dibandingkan jumlah blok DES yaitu 64 bit
3. Proses enkripsi DES lebih lambat dibandingkan AES
4. Proses dekripsi DES lebih mudah dibandingkan AES

Ucapan Terima Kasih

Saya mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas karunia-Nya saya dapat menyelesaikan makalah tugas terakhir ini dengan baik. Saya juga mengucapkan terima kasih kepada Bapak Rinaldi Munir selaku dosen yang sudah mengajarkan dan membimbing saya masuk ke dalam dunia kriptografi. Saya juga berterima kasih kepada komputer dan jaringan internet saya yang tidak menghambat saya dalam menyelesaikan makalah ini. Selain itu, saya juga berterima kasih kepada seluruh teman sekelas seperjuangan saya yang bersama-sama berjuang pada mata kuliah ini. Terima kasih sebesar-besarnya kepada II4031 Kriptografi dan Koding yang sudah memberikan kesempatan berharga untuk mempelajari kriptografi secara baik.

REFERENSI

[1] Reynolds, J. (2021, December 12). Cryptography and Security in Banking - Joshua Reynolds. Medium. https://medium.com/@joshuareynolds/cryptography-and-security-in-banking-2cce7691e70fJ. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] How safe is the 256-bit encryption used in bank transactions? (2012, April 10). Information Security Stack Exchange. https://security.stackexchange.com/questions/13624/how-safe-is-the-256-bit-encryption-used-in-bank-transactions

[3] *How safe is the 256-bit encryption used in bank transactions?* (2020, May). Quora. https://www.quora.com/How-safe-is-the-256-bit-encryption-used-in-bank-transactions

[4] *Improve Customer Satisfaction with Digital Transactions*. (2017, August 30). DocuSign. https://www.docusign.com/learn/digital-transactions

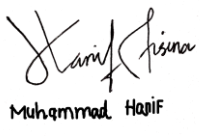
[5] Summe, M. (2015, August 7). *Have Online Payments Become Safer Than Offline?* WIRED. https://www.wired.com/insights/2014/12/have-online-payments-become-safer-than-offline/

[6] *Advanced Encryption Standard*. (n.d.). Tutorials Point. https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 April 2021



Muhammad Hanif A. Nasution - 18219077