Universitas Maritim Raja Ali Haji
Student Online Journal
Online ISSN 2746-8461

IMPLEMENTASI KRIPTOGRAFI HYBRID MENGGUNAKAN ALGORITMA AES-128 DAN ALGORITMA RABIN UNTUK MENGAMANKAN DATA DALAM DATABASE

Natanael Sijabat[1], Nurul Hayaty[2], Eka Suswaini[3]
Naellabit@gmail.com
Program studi Informatika, Fakultas Teknik., Universitas Maritim Raja Ali Haji

Abstract

Along with the development of time and the rapid advancement of technology, then many new techniques are used to retrieve data. With the advent of these new techniques, it is feared that the data taken could be misused by irresponsible parties, thus threatening the data- confidential data or messages. Because of this, many developments have been carried out in the field of data security, such as cryptographic techniques. In this study, security techniques were used, namely AES-128 for symmetric cryptography and Rabin for asymmetric cryptography. thus making the percentage of data security greater and not easily cracked by unauthorized parties. Data security in the database using AES-128 and Rabin methods has been successfully implemented to make confidential data more secure.
Kata kunci: *cryptography, symmetric cryptography, asymmetric cryptography, AES-128, Rabin.*

I. Pendahuluan

Keamanan sebuah data merupakan suatu hal yang harus diperhatikan, hal ini dikarenakan jika sebuah data dapat diakses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka data tersebut dapat disalahgunakan. Data yang seharusnya bersifat rahasia menjadi rentan untuk dicuri ataupun diakses oleh orang yang tak bertanggung jawab. Salah satunya dengan cara mengakses secara langsung pada database. Melihat kondisi diatas, maka keamanan data menjadi suatu hal yang sangat penting. Untuk itu perlu teknik khusus untuk mengamankan data dalam database sistem informasi. Salah satu mekanisme untuk meningkatkan keamanan data dalam database adalah dengan menggunakan teknologi enkripsi.

Data-data yang disimpan dalam database diubah sedemikian rupa sehingga tidak mudah dibaca. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data (yang disebut *plaintext*) menjadi data yang tersembunyi (disebut *ciphertext*).Pengetahuan yang mempelajari tentang enkripsi adalah kriptografi. Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Manezes dkk, 1966).

Berdasarkan kunci kriptografi dibedakan menjadi dua buah yaitu kriptografi simetris dan kriptografi asimetris. Kedua kriptografi tersebut memiliki kelemahan dan kekurangan tergantung dari jenis algoritma yang digunakan. *Hybrid Cryptosystem* merupakan gabungan dari kriptografi asimetris dan kriptografi simetris dengan memanfaatkan kelebihan masing-masing chipper (Tyagi dkk, 2017). Dalam hal ini, algoritma yang akan digunakan ialah algoritma AES dan algoritma Rabin.

Advanced Encryption Standar (AES) adalah salah satu algoritma enkripsi simetris yang dapat mengenkripsi dan deskripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit(Asri & Nyoman, 2018). Pada tahun 2000, National institute of standards and technology (NIST) sebagai agensi departemen perdagangan AS menetapkan sebuah standard kriptografi yang baru yaitu Algoritma Rijandel dan ditetapkan sebagai Advanced Encryption Standard (AES) (Munir, 2006). Selain itu AES lebih efisien dari segi biaya dan lebih mudah diimplementasikan pada memori berukuran kecil(Sadikin,2012).

Algoritma Rabin adalah salah satu algoritma kriptografi kunci asimetris, yang keamanannya seperti *RSA((Rivest Shamir Adleman),* namun memiliki kelemahan yaitu menghasilkan ciphertext yang beberapa kali lebih panjang dari plaintext. Seperti semua kriptografi kunci asimetris, algoritma Rabin menggunakan satu pasang kunci : kunci public untuk enkripsi dan kunci privat untuk deskripsi. Pada proses dekripsi, algoritma Rabin menghasilkan 4 buah *plaintext*, sehingga dibutuhkan proses yang lebih kompleks untuk mengetahui mana yang merupakan *plaintext* yang asli. Selain itu waktu eksekusi algoritma Rabin lebih cepat jika dibandingkan dengan algoritma Elliptic Curve Cryptography dan algoritma RSA(Selvi dan Vaishnavi,2012).Manfaat dari penelitian ini,yaitu membuat sistem yang bisa mengamankan data pada database dari pihak yang tidak bertanggung jawab.

II. Metode Penelitian

2.1 Metode AES-128

Algoritma AES adalah algortima kriptografi yang sifatnya simetris dan *cipher block*. Algoritma ini menggunakan kunci yang sama saat melakukan enkripsi maupun dekripsi. Algoritma AES memiliki ukuran blok dan kunci yang tetap yaitu sebesar 128 bit, 192 bit, 256 bit. Berikut perbandingan jumlah proses panjang kunci yang dilalui untuk masing-masing masukan bit (Rahmawati & Rahardjo, 2016).

Table **1.** Perbandingan Panjang Kunci AES

Tipe	Jumlah key (Nk)	Besar Blok (Nb)	Jumlah round (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

1. Enkripsi AES-128

Secara umum, proses enkripsi algoritma AES mempunyai beberapa tahapan yaitu :

1. *AddRoundKey* yaitu, proses melakukan XOR antara state awal (plaintext) dan cipherkey. Tahap ini disebut juga dengan initial round.
2. *Round*: yaitu, putaran sebanyak NR – 1 kali. Pada setiap putaran atau ronde memiliki beberapa proses, diantaranya adalah :
   a. *SubBytes* : yaitu, mensubstitusikan byte dengan menggunakan tabel S-Box (tabel substitusi) .
   b. *Shiftrows* : yaitu, melakukan pergeseran tiap baris array state secara wrapping.
   c. *MixColumns* : yaitu, mengacak data pada tiap kolom array state dengan melakukan perkalian matriks state dengan matriks yang sudah ditentukan.
   d. *AddRoundKey* : yaitu, melakukan XOR antara hasil state sekarang dengan kunci hasil proses expand key.
3. Final Round: yaitu, proses untuk putaran atau ronde terakhir :
   a. *SubBytes*
   b. *Shiftrows*
   c. *AddRoundKey*

2. Dekripsi AES-128

Sedangkan untuk proses dekripsi pada algoritma AES merupakan kebalikan dari proses enkripsi algoritma AES dengan menggunakan transformasi *Invers.*

2.2 Metode Rabin

Algoritma Rabin merupakan salah satu algoritma kriptografi kunci-publik. Algoritma ini menggunakan satu pasang kunci yaitu kunci publik dan kunci privat. Kunci publik digunakan dalam proses enkripsi sedangkan kunci privat digunakan dalam proses dekripsi. Pada proses dekripsi, algoritma rabin menghasilkan 4 buah plaintext. Oleh karena itu, diperlukan modifikasi dalam proses dekripsi untuk menentukan plaintext yang sebenarnya.

1. Pembangkitan Kunci Rabin

Berikut ini adalah algoritma proses pembangkitan kunci pada algoritma Rabin Public Key:

1. Pilih dua bilangan prima besar sembarang, *p* dan *q*, dimana keduanya kongruen terhadap 3 mod 4. Atau dengan kata lain, jika *p* dan *q* dimodulokan 4 akan menghasilkan 3 dapat dilihat pada persamaan (1)

$$p \equiv q \equiv 3 \pmod 4 \qquad (1)$$

2. *n* merupakan kunci publik yang diperoleh dengan rumus seperti yang ditunjukan pada persamaan (2).

$$n = p.q \qquad (2)$$

3. Simpan dan rahasiakan nilai *p* dan *q* (private key), sedangkan nilai *n* (public key) dapat disebarkan seluas-luasnya.

2. Enkripsi Rabin

Proses enkripsi pada algoritma Rabin Public Key menggunakan kunci publik *n*. Untuk melakukan enkripsi pesan (*m*), *m* harus lebih kecil dari *n*. Berikut adalah rumus untuk melakukan enkripsi pada algoritma Rabin Public Key (Schneier, 1996) dapat dilihat pada persamaan *(3)*.

$$c = m^2 \ mod \ n \qquad (3)$$

Dimana:
c = ciphertext
m = plaintext/message
n = kunci public

Berikut langkah–langkah proses enkripsi pesan rahasia menggunakan algoritma Rabin Public Key:

1. Ubah nilai *plaintext m* menjadi nilai biner, kemudian gandakan nilai biner *m* itu sehingga nilai biner lebih panjang.
2. Ubah hasil penggandaan nilai biner *plaintext* tersebut menjadi nilai desimalnya.
3. Hitung nilai *ciphertext c* dengan menggunakan rumus seperti yang ditunjukan pada persamaan (*3*).

3. Dekripsi Rabin

Proses dekripsi pada algoritma Rabin Public Key menggunakan kunci privat *p* dan *q*. Berikut langkah–langkah proses dekripsi dengan menggunakan algoritma Rabin Public Key yang telah dimodifikasi (Menezes, et al, 1996) :

1. Tentukan nilai *a* dan *b* yang merupakan pembagi GCD (Greatest Common Divisor) dari *p* dan *q* dengan menggunakan *Extended Euclidean.*

$$a^*p + b^*q = 1 \quad (4)$$

2. Hitung nilai akar kuadrat dari ciphertext terhadap p dan q yang merupakan private key dengan rumus pada persamaan (5) :

$$m_p = c^{\left(\frac{p+1}{4}\right)} mod\ p$$

$$m_q = c^{\left(\frac{q+1}{4}\right)} mod\ q \quad (5)$$

dengan m_p adalah akar kuadrat dari *ciphertext* terhadap p dan m_q adalah akar kuadrat dari *ciphertext* terhadap q.

3. Hitung nilai x dan y dengan menggunakan *Chinese Remainder Theorem*, dengan persamaan (6) :

$$x = \left(a^*p^*m_q + b^*q^*m_p\right) mod\ n$$

$$y = \left(a^*p^*m_q - b^*q^*m_p\right) mod\ n \quad (6)$$

4. Hitung empat kemungkinan hasil nilai m sedemikian dengan persamaan (7) :

$$m_1 = x\ mod\ n$$
$$m_2 = -x\ mod\ n$$
$$m_3 = y\ mod\ n$$
$$m_4 = -y\ mod\ n \quad (7)$$

5. Ubah nilai desimal m_1, m_2, m_3, dan m_4 ke dalam bentuk biner. Kemudian nilai biner m_1, m_2, m_3, dan m_4 dibagi menjadi dua bagian. Jika kedua bagian nilai biner tersebut memiliki bentuk biner yang sama, maka didapatlah hasil dekripsi *ciphertext c* dengan mengubah bentuk biner salah satu bagian ke dalam nilai desimal.

III. Hasil dan Pembahasan

3.1 Hasil Penelitian

Data yang akan digunakan diambil dari database dalam bentuk tabel yang berisi 4 *fields*. Adapun 4 *fields* tersebut adalah nama, alamat, no hp dan email. Data akan diuji per metode dan hasilnya seperti terlihat pada tabel

Table **2.** Pengujian Metode AES-128

No	Rows	Kunci	Waktu proses enkripsi(detik)	Waktu proses deskripsi (detik)	Berhasil Dekripsi ?
1	100	INFORMATIKAUMRAH	6.59	7.13	Ya
2	50	algoritmaaes-128	3.51	4.18	Ya
3	10	natanaelsijabat1	0.63	0.88	Ya
4	200	TANJUNGPINANGBT9	12.28	13.12	Ya

Berdasarkan Tabel 2, semua data yang digunakan untuk pengujian berhasil dienkripsi dan dekripsi.

Table **3.** Pengujian Metode Rabin

No	Plainkey	Kunci Private (p,q)	Kunci Publik (n)	Waktu proses enkripsi (detik)	Waktu proses dekripsi (detik)	Berhasil dekripsi

1	INFORMATIKAUMRAH	139,223	30997	0.99	0.01	Ya
2	algoritmaaes-128	523,647	338381	1	0.01	Ya
3	natanaelsijabat1	311,419	130309	1.02	0.01	Ya
4	TANJUNGPINANGBT9	239,127	30353	0.86	0.11	Ya

Berdasarkan Tabel 3, semua plainkey yang digunakan untuk pengujian berhasil dienkripsi dan dekripsi.

Table **4.** Pengujian Metode Rabin dengan panjang kunci berbeda

No	Plainkey	Kunci Private (p,q)	Kunci Publik (n)	Berhasil Enkripsi ?	Berhasil Dekripsi ?
1	INFORMATIKAUMRAH	99,95	9405	Tidak	Tidak
2	INFORMATIKAUMRAH	139,223	30997	Ya	Ya
3	INFORMATIKAUMRAH	1043,1323	1379889	Ya	Tidak

Berdasarkan Tabel 4, plainkey 1 dengan menggunakan panjang kunci private 2 digit tidak bisa dienkripsi dan dekripsi karena nilai desimal dari replikasi biner lebih besar dari nilai desimal kunci publik. Sedangkan pada plainkey 3 dengan menggunakan panjang kunci private 4 digit tidak bisa didekripsi tapi bisa dienkripsi karena nilai biner dari m1-m4 setelah dibagi menjadi 2 bagian tidak memiliki bentuk yang sama.

Table **5.** Pengujian Metode AES-128 dan Rabin

No	Nama Tabel	Waktu proses enkripsi (detik)	Waktu proses dekripsi (detik)	Berhasil dekripsi ?
1	Datatesting	5.72	6.11	Ya
2	Datatesting1	4.12	2.91	Ya
3	Datatesting2	1.49	0.89	Ya
4	Datatesting3	12.47	11.83	Ya

Berdasarkan Tabel 5, ketika kedua metode digabungkan, data semuanya berhasil dikembalikan.

IV. Kesimpulan

Dari hasil penelitian, penulis menyimpulkan bahwa metode AES-128 dan Rabin berhasil diimplementasikan ketika digabungkan dengan syarat nilai desimal dari replikasi biner panjang kunci private rabin lebih besar dari nilai desimal kunci publik rabin.

V. Daftar Pustaka

Akbar, F., dan Waluyo, S., 2018, Sistem Keamanan Database menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus : Red Aveneu Indonesia, *Skanika*, 1(2), 821-828.

Erlangga, T., dan Kusumaningsih, D., 2018, Implementasi Algoritma Advanced Encryption Standard-128(AES-128) untuk pengamanan Database Berbasis Desktop pada Icaltoys, *Skanika*, 1(2), 565-569.

Mustika, L., 2020, Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web, *Jurikom (Jurnal Riset Komputer)*, 7(1), 148-155.

Nopianto, F. R., dan Ferdiansyah., 2018, Aplikasi Enkripsi Data Penilaian Siswa pada Database menggunakan Algoritma Kriptografi (AES-128) Berbasis Web, *Skanika*, 1(2), 669-675.
Pudoli, A., dan Kusumaningsih, D., 2017, Penggunaan Hybrid Cryptosystem Untuk Enkripsi Dan Dekripsi Pesan Messanger Menggunakan Algoritma Rivest Shamir Adleman (RSA) Dan Advanced Encryption Standard (AES) Dengan Firebase Pada Android, *Jurnal TELEMATIKA MKOM*, 9(3), 125-131.
Rahmadhiyanti, S., 2019, Implementasi Kriptografi RSA untuk peningkatan keamanan Database E-Commerce, *Jurnal Pelita Informatika*, 8(2), 288-291.
Santoso, K. I., dan Priyoatmoko, W., 2016, Pengamanan Data MySQL pada E-Commerce dengan Algoritma 256, *Seminar Nasional Sistem Informasi Indonesia*, 119-126.
Saputra, D. A., dan Kusumaningsih, D., 2018, Implementasi Keamanan Database Menggunakan Algoritma AES-192 Pada PT GURITA LINTAS SAMUDERA Berbasis Android, *Skanika*, 1(3), 884-888.
Sumarno., Gunawan, I., Tambunan, H. S., dan Irawan, E., 2018, Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (Md5), Rivest Shamir Adleman (Rsa) Dan Rivest Cipher 4 (Rc4) Pada Keamanan E-Dokumen, *JUSIKOM PRIMA (Junal Sistem Informasi Ilmu Komputer Prima)*, *2*(1), 41–48.
Tyagi, N., Agarwal, A., Katiyar, A., Garg, S., dan Yadav, S., Hybrid Key Cryptography: A Tool for Security, International *Journal of Innovative Research in Science, Engineering and Technology*, Vol. 6, Issue 3, 2017. ISSN: 2347-6710.