MATICS : Jurnal Ilmu Komputer dan Teknologi Informasi ISSN : 1978-161X(p); 2477-2550(e)
Volume 11, No. 2 (2019), pp 56-61 DOI : 10.18860/mat.v11i2.8438
Received : October 28th 2019; **Accepted** : November 21th 2019 ; **Avalaible Online** : December 5th 2019

Peningkatan Keamanan Grup Chat Menggunakan Kombinasi Metode RSA, Elgamal Dan Viginere Cipher

Dwi Risky Setiawan[1], Cahyo Crysdian[2], Ajib Hanani[3]

***Abstract*— Along with the development of mobile messenger technology and the many uses of mobile messenger services, the security aspect is very important to consider. Security is the biggest problem for mobile messenger users in a company or enterprise. So we need a mobile messenger application with an encryption system using a combination of RSA, Elgamal, and Viginere Cipher methods that are more difficult to get cracked than using a single method. Using a combination of methods will increase time consumption by 45%, decryption success rate decreases by 46.2%, and message size increases by 80% but security aspects are far more important. Using a combination of methods will increase the brute force looping effort by 73,496,518.7%.**

Keywords*— *Kiptografi; Elgamal; RSA; Viginere Cippher.

***Abstrak*— Seiring dengan perkembangan teknologi telepon seluler yang pesat dan banyaknya penggunaan layanan mobile messenger, maka aspek keamanan menjadi sangat penting untuk dipertimbangkan. Keamanan merupakan masalah terbesar bagi pengguna mobile messenger pada perusahaan atau enterprise. Maka dibutuhkan aplikasi mobile messenger dengan sistem enkripsi menggunakan kombinasi metode RSA, Elgamal, dan Viginere Cipher yang lebih sulit untuk dipecahkan dari pada menggunakan single metode. Penggunaan kombinasi metode akan meningkatkan konsumsi waktu sebanyak 45%, tingkat keberhasilan dideskripsikan kembali menurun sebanyak 46,2%, dan peningkatan size pesan sebanyak 80% namun aspek keamanan jauh lebih penting. Dengan menggunakan kombinasi metode akan meningkatkan usaha perulangan brute force sebesar 73.496.518,7%.**

Kata Kunci*— *Kiptografi; Elgama; RSA; Viginere Cippher.

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi sangat pesat yaitu menciptakan berbagai aplikasi yang memudahkan pengguna khususnya untuk layanan pengiriman yang memanfaatkan jaringan data internet untuk saling berbagi informasi. Konsep awal pengiriman pesan mengginakan media internet adalah konsep *one-to-one* yang menggunakan e-mail, yang mana e-mail dinilai terlalu formal dan kaku sebagai alat komunikasi, dan e-mail dinilai terlalu lama dalam merespons.

terungkapnya kegiatan pengawasan massal oleh badan intelijen, saat ini aplikasi IM(*Instant Messager*) menggabungkan enkripsi *end-to-end* pada aplikasinya, aplikasi IM menambahkan protokol enkripsi untuk melindungi komunikasi menuju server pengiriman pesan. Karenanya menganalisis, menyelidiki protokol-protokol ini, juga termasuk serangan berbasis server. Hal ini bertujuan untuk melindungi konten pesan tunggal dan kekuatan protokol untuk memastikan bahwa pengguna yang tidak termasuk ke grup harus tidak dapat menambahkan diri ke grup atau menerima pesan dari grup tanpa anggota izin [1].

Dalam menjaga kerahasian data diperlukan ilmu kriptografi, yang mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Dengan adanya algoritma kirptografi dapat mencegah terjadinya kebocoran informasi dari pesan yang dikirim dengan membuat pesan agar ter-enskripsi dengan baik dan data pesan pengguna dapat terlindungi sehingga mendapatkan hak privasinya.

II. LANDASAN TEORI

Penelitian sejenis yang pernah dilakukan yaitu pada penelitian yang membahas tingkat keamanan pada networ layer seperti firewall dan antivirus tidak cukup dalam mengamankan data maka pada tingkat aplikasi dibutuhkan keamanan tambahan yaitu berupa eksripsi. Pada sistem group based enskripsi hanya dibutuhkan satu kali kemudian dekripsi dilakukan secara tersendiri [2]. Penelitian sejenis yang lain yaitu penyerangan ketahanan Algoritma RSA terhadap penyerangan Brute Force jika ada waktu untuk melakukannya, semakin besar kunci yang digunakan semakin lama pula waktu yang diperlukan, untuk kunci sebesar 56 bit, maka dibutuhkan waktu 1142 tahun untuk memecahkan pesan yang dienskripsinya [3]. Penelitian sejenis yang lain ElGAmal mempunyai kemamuan yang baik dalam pendistribusian kunci, ini dikarenakan saat pembentukan kunci sang penerima pesan membuat 2

Dwi Risky Setiawan is with the Informatic Engineering Departement of Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia, (email dwiriskysetiawan1996@gmail.com).

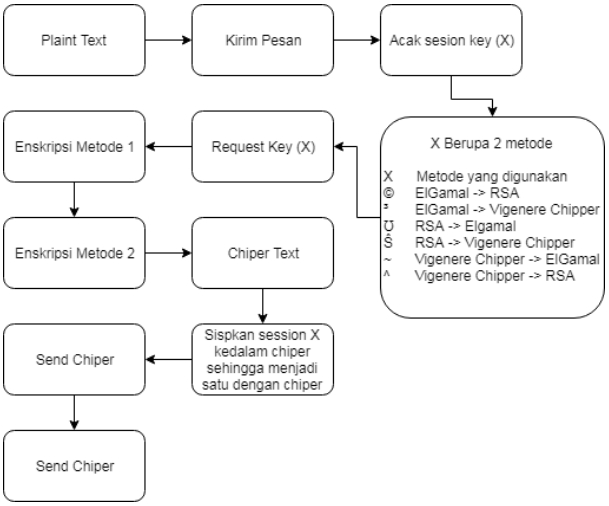
Cahyo Crysdian., is with the Informatic Engineering Departement of Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia.

Ajib Hanani is is the Informatic Engineering Departement of Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia.

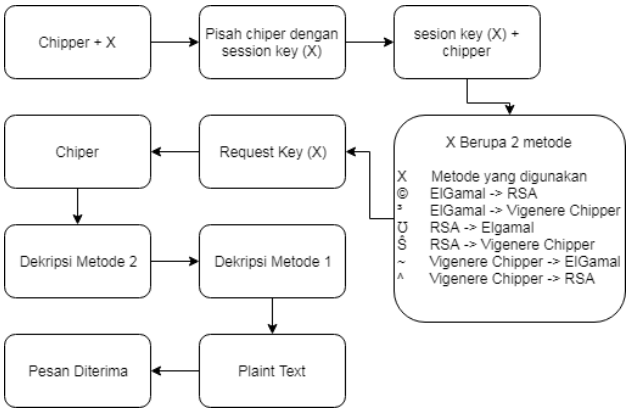
kunci yaitu kunci public dan kunci private, kunci public akan diserahkan ke orang lain yang akan digunakan untuk mengamankan pesan yang akan dikirim sedangkan kunci private tetap di pengang oleh pembuat kunci saja, algoritma ini mempunyai kelebihan yaitu pada proses enskripsi akan menghasilkan chipper yang berbeda-beda, namun pada proses dekripsi akan menghasilakan plaint text yang sama [4].

III. PERANCANGAN SISTEM

A. Blok Diagram Penelitian



Gambar 1. Diagram Blok Krim pesan



Gambar 2. Diagram Blok Terima pesan

Peningkatan keamanan dilakukan dengan cara kombinasi metode RSA, *Elgamal*, dan *Vigenere Cipher* dilakukan dengan teknik Sistem *Hybrid.* System ini menggabungkan dua atau metode kiptografi guna untuk meningkatkan keamanan data. Proses ini dilakukan dengan cara menegosiasikan penggunaan metode diantara pihak penerima dengan pihak pengirim pesan, ke dua belah pihak diharuskan setuju dengan metode yang dipakai.

Proses negosiasi dimulai dari pihak pengirim pesan dimana pihak pengirim pesan mengirim *session key* yang disipkan ke dalam chipper text yang kemudian chipper text tersebut dikirim ke pihak penerima. Suatu *session key* hanya dipakai sekali sesi atau sekali pengiriman pesan. Untuk sesi selanjutnya *session key* harus dibuat kembali secara acak sesuai dengan tabel. *Session key* tersebut berisi urutan penggunaan metode yang dipakai dalam proses enkripsi pesan.

Tabel 1. *Session Key*

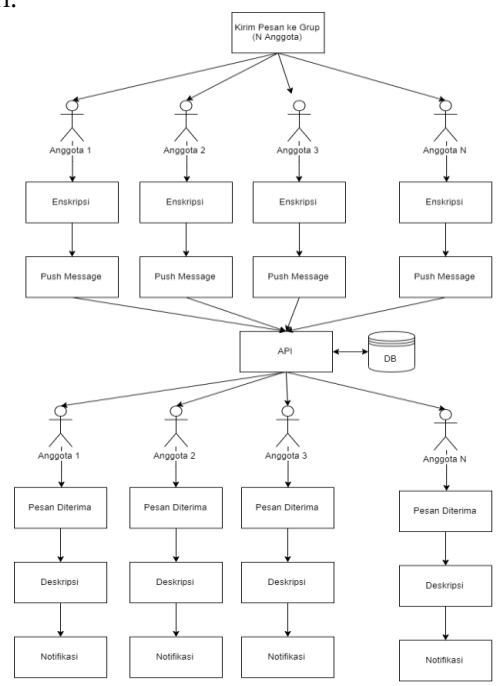
session key	metode yang digunakan
©	ElGamal -> RSA
³	ElGamal -> Vigenere Chipper
Ʊ	RSA -> ElGamal
Ŝ	RSA -> Vigenere Chipper
~	Vigenere Chipper -> ElGamal
^	Vigenere Chipper -> RSA

.

B. Arsitektur grup Chat

Aplikasi chat yang tidak di enkripsi biasanya menggunakan “server-side fan-out” untuk pesan grup. Seorang klien yang ingin mengirim pesan ke sekelompok pengguna mentransmisikan satu pesan, yang kemudian didistribusikan N kali ke N anggota grup yang berbeda oleh server.

Berbeda dengan aplikasi chat tanpa enkripsi pada aplikasi chat yang menggunakan enkripsi menggunakan "client-side fan-out" di mana klien akan mengirimkan satu pesan N kali ke N anggota grup yang berbeda itu sendiri.



Gambar 3. Arsitektur Grup Chat

C. Elgammal

Elgamal merupakan kiptografi asimetris yang memiliki dua kunci yaitu kunci publik, dan kunci privat yang digunakan dalam proses enkripsi dan dekripsi pesan. untuk memperoleh sepasang kunci tersebut sistem melakukan proses pembentukan kunci yang kemudian terbentuk kunci publik yang akan di bagikan kepada user lain, dan kunci private yang hanya akan disimpan dalam internal *device* itu saja. Proses generate kunci adalah sebagai berikut.

$$y = g^x \bmod p \qquad (1)$$

Proses ini membutuhkan sebuah bilangan prima p dan dua buah bilangan acak g dan x dengan syarat $g < p$ dan $x < p$. proses enkripsi adalah sebagai berikut.

k = nilai random
m = ASCII
$a = g^k \bmod p$

Untuk dapat membaca pesan dalam bentuk Cipher text perlu dilakukan proses dekripsi pesan, dengan cara :

$$m = b * a^{(p-1-x)} \bmod p \qquad (2)$$

D.RSA

Proses pembentukan kunci adalah sebagai berikut

- $b = y^x m \bmod p$ Generate bilangan prima p dan q
- $n=p*q$
- $m=(p-1)*(q-1)$
- Pilih d yang relative prima terhadap m, e relative prima terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut $gcd(e,m) = 1$.
- Cari d, sehingga $e*d = 1 \bmod (m)$, atau $d = (1+nm)/e$.

Proses enskripsi adalah sebagai berikut

- kunci publik (e dan n).
- P = ASCII blok-blok karakter dari Plaint Text
- $C = P^e \bmod n$

Proses deskripsi adalah sebagai berikut

- kunci privat d dan dan kunci publik n
- C = ASCII blok-blok karakter dari Cipher Text
- $P = C^d \bmod n$
- P = Plaint Text

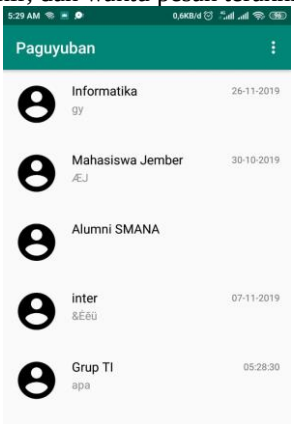
E. Vigenere Cipher

Vigenere Chiper merupakan kiptografi yang memiliki proses enkripsi dan dekripsi menggunakan teknik subtitusi yaitu dengan menggeser setiap huruf dengan jumlah yang berbeda-beda disetiap hurufnya. Untuk Generate key dengan karakter dan panjang karakter secara acak.

IV. PEMBAHASAN

A. Antarmuka Aplikasi

Tampilan Beranda Aplikasi adalah sebuah list grup dimana user menjadi anggotanya yang berisi nama grup, isi pesan terakhir, dan waktu pesan terakhir.

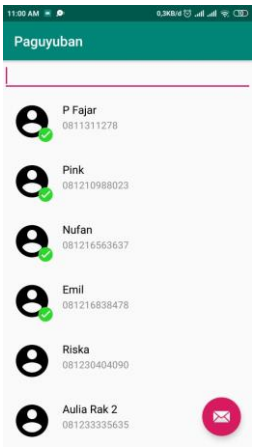


Gambar 4. Tampilan Beranda

Tampilan Chating merupakan tampilan dimana user dapat mengirim dan menerima pesan yang mana pesan tersebut sudah diamankan oleh enskripsi. Tampilan chating terdapat nama grup, isi pesan, pengirim pesan, dan waktu dari pesan terrkirim.

Gambar 5. Chating

Buat Grup merupakan tampilan untuk membuat grup dengan cara menambahkan anggota pada list kontak.



Gambar 6. Buat Grup

B. Uji Coba

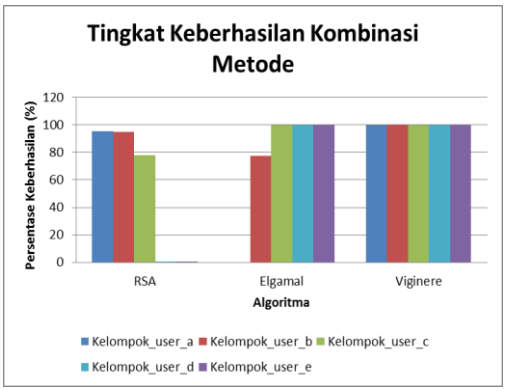
Untuk uji coba sistem penguji membuat 5000 user dummy yang memiliki kunci public dan kunci private yang berbeda-beda, kunci tersebut user dummy ini akan dijadikan sebagai objek testing.

Tabel 2 Hasil Validasi

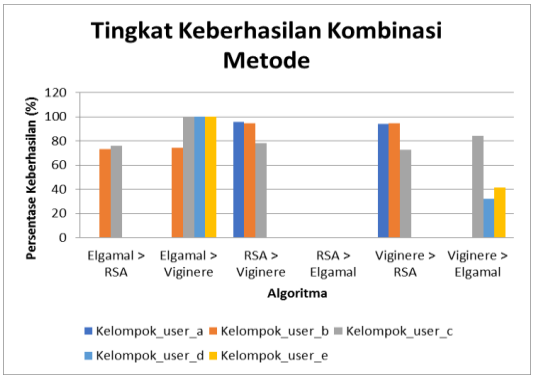
Kelompok User	Range key (RSA & ElGamal)	Jenis Kunci (Vigenere Cipher)	Banyak
Kelompok_user_a	10 - 100	Huruf (low case)	1000 users
Kelompok_user_b	100 - 200	Huruf (low case + Uppercase)	1000 users
Kelompok_user_c	200 - 300	Huruf (low case + Uppercase) + angka	1000 users
Kelompok_user_d	300 - 400	Huruf (low case + Uppercase) + angka + simbol unik	1000 users
Kelompok_user_e	400 - 500	Huruf (low case + Uppercase) + angka + simbol unik	1000 users

C. Uji Coba Pertama

Pada uji coba pertama penulis akan menguj kesesuaian data setelah melewati proses enkripsi dan deskripsi. Parameter yang menjadi ukuran dalam pengujian ini adalah metode kiptografi yang digunakkan, besaran kunci yang digunakan. Pada uji coba ini penulis mengelompokkan berdasarkan algoritma yang digunakan terlebih dahulu, setelah itu penulis akan menguji berdasarkan besaran kunci.



Gambar 7. Tingkat Keberhasilan Enskripsi Dekripsi Single Metode



Gambar 8. Tingkat Keberhasilan Enskripsi Dekripsi Single Metode

D. Uji Coba Kedua

Pada uji coba kedua penulis akan menguji seberapa besar pembengkakan ukuran data dari plaint text ke chipper text. Pembengkakan data dilihat berdasarkan perbandingan plaint text dengan chipper text. Parameter yang menjadi ukuran dalam pengujian ini adalah size pesan dan metode kiptografi yang digunakkan.

Tabel 3. Peningkatan Size Single Metode

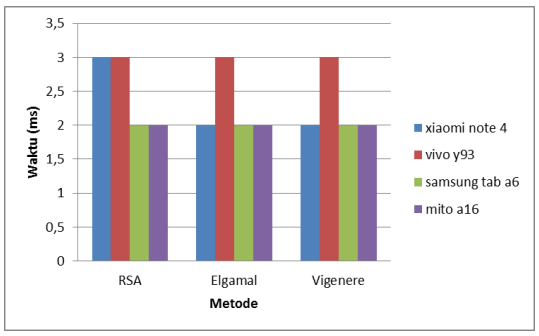
No	Metode	size awal	size akhir	Peningkatan %
1	RSA	10	10	100
2		20	20	
3		40	40	
4		80	80	
5		160	160	
6	Elgamal	10	20	200
7		20	40	
8		40	80	
9		80	160	
10		160	320	
11	Vigenere	10	10	100
12		20	20	
13		40	40	
14		80	80	
15		160	160	

Tabel 4. Peningkatan Size Kombinasi Metode

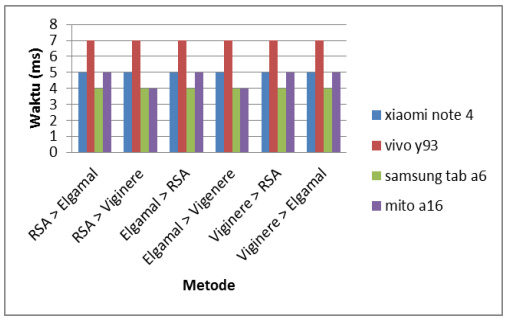
No	Metode	size awal	size akhir	Peningkatan %
1	RSA > Elgamal	10	20	200
2		20	40	
3		40	80	
4		80	160	
5		160	320	
6	RSA > Viginere	10	10	100
7		20	20	
8		40	40	
9		80	80	
10		160	160	
11	Elgamal > RSA	10	20	200
12		20	40	
13		40	80	
14		80	160	
15		160	320	
16	Elgamal > Vigenere	10	20	200
17		20	40	
18		40	80	
19		80	160	
20		160	320	
21	Viginere > RSA	10	10	100
22		20	20	
23		40	40	
24		80	80	
25		160	160	
26	Viginere > Elgamal	10	20	200
27		20	40	
28		40	80	
29		80	160	
30		160	320	

E. Uji Coba Ketiga

Pada uji coba ketiga penulis akan menguji seberapa lama waktu yang digunakan untuk pengirim dalam proses mengenkripsi pesan, dan seberapa lama waktu yang digunakan penerima dalam proses mendeskripsikan pesan, waktu dihitung sejak pesan masuk sampai dengan pesan selesai didekripsikan



Gambar 9. *Banyak Waktu Enskripsi Menggunakan Single Metode*



Gambar 10. *Banyak Waktu Enskripsi Menggunakan Kombinasi Metode*

F. Uji Coba Keempat

Pada langkah keempat penulis akan menguji kekuatan chipper untuk didekripsikan kembali oleh penyerang untuk mengetahui probabilitas ditemukannya text asli. Pengujian dilakukan dalam berbagai skenario, yaitu. probalitas ditebaknya metode yang digunakan oleh responden dan probabilitas dipecahkannya cipher dengan *brute force*

Tabel 5. Banyak Percobaan Dipecahkannya Cipher Text Single Metode

Metode	Range	kunci yang dibutuhkan	total kemungkinan
RSA	10-200	Angka prima p (42 kemungkinan) Angka prima q (42 kemungkinan) Angka prima m (42 kemungkinan)	74.088
Elgamal	200-500	Angka prima p (49 kemungkinan) Angka Desiamal g (300 kemungkinan) Angka Desiamal x (300 kemungkinan)	4.410.000
Vigenere	Huruf (low case + Uppercase) + angka + simbol unik	key (65276 kemungkinan)	1.044.416
Rata-rata banyak percobaan dipecahkannya Cipher text			2.727.208

Tabel 6. Banyak Percobaan Dipecahkannya Cipher Text Single Metode

Kombinasi metode	banyak kemungkinan percobaan (metode 1 * metode 2)	jumlah percobaan metode 1 * metode 2
ElGamal -> RSA	4.410.000 * 74.088	326.728.080.000
ElGamal -> Vigenere Chipper	4.410.000 * 1.044.416	4.605.874.560.000
RSA -> Elgamal	74.088 * 4.410.000	326.728.080.000
RSA -> Vigenere Chipper	74.088 * 1.044.416	77.378.692.608
Vigenere Chipper -> ElGamal	1.044.416 * 4.410.000	4.605.874.560.000
Vigenere Chipper -> RSA	1.044.416 * 74.088	77.378.692.608
Rata-rata banyak percobaan dipecahkannya Cipher text		1.669.993.777.536

V. KESIMPULAN

Setelah dilakukan penelitihan mengenai peningkatan keamanan grup chat menggunakan kombinasi metode RSA, *Elgamal*, dan *Vigener Cipher* untuk mencari perbandingan peningkatan keamanan antara single metode dengan kombinasi metode, maka dapat diambil kesimpulan sebagai berikut: Terjadi penurunan tingkat keberhasilan dideskripsikannya pesan kembasi sebesar 30.867 pesan berhasil di deskripsikan dari 45.000 percobaan menurun sebesar 28.628 pesan berhasil di deskripsikan dari 90.000 percobaan, Sehingga terjadi penurunan tingkat keberhasilan sebanyak sebanyak 46,2%. Peningkatan konsumsi waktu rata-rata sebesar 2,3 ms oleh single metode meningkat sebesar 5,1 ms oleh kombinasi metode, Sehingga terjadi peningkatan konsumsi waktu sebanyak 45%. Terjadi peningkatan size pesan dari size text asli rata-rata sebesar 62 bit mengingkat rata-rata sebesar 82.6 bit dan meningkat rata-rata sebesar 133.3 bit untuk kombinasi metode, Sehingga terjadi peningkatan size sebesar 80%. Terjadi penurunan probabilitas tertebaknya metode yang digunakan oleh responden sebesar 22 metode tertebak dari 60 percobaan untuk single metode, menuruun sebesar 2 metode tertebak dari 30 percobaan untuk kombinasi metode, dengan nilai tersebut terjadi penurunan probabilitas ditebaknya.

REFERENSI

[1] Moran, E.. End To End Encryption an Answer To Security Concerns in Private Sector, 2016.

[2] Bing, H., Bo, W., & Hui, Z. (2014). A design and realization of digital signature of e-government management website group based on Elgamal cipher system. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.

[3] Wicaksono, L.. Ketahanan Algoritma RSA Terhadap Brute Force Attack. Jurnal Teknologi, 1(1), 69–73. https://doi.org/10.11113/jt.v56.60, 2013.

[4] Rizal, M. S. Implementasi Algoritma Kriptografi Kunci-Publik ElGamal Entuk Keamanan Pengiriman Email, 2010.