KOMBINASI VIGENERE-AES 256 DAN FUNGSI HASH DALAM KRIPTOGRAFI APLIKASI CHATTING

Lekso Budi Handoko[1*] dan Chaerul Umam[1]
[1]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bojol 207 Semarang
*Email: handoko@dsn.dinus.ac.id

Abstrak

Aplikasi chatting adalah aplikasi yang memungkinkan pengguna untuk mengirim pesan secara langsung atau real time tanpa jarak dari dunia internet. Berbagai jenis aplikasi perpesanan yang tersedia saat ini belum tentu memiliki keamanan yang baik karena tidak ada aturan baku yang digunakan untuk melindungi pesan dalam aplikasi tersebut. Dalam enkripsi, data atau informasi dilindungi dengan cara menyandikan data tersebut sehingga makna aslinya tidak dapat langsung ditafsirkan oleh pembaca. Vigenere Cipher adalah algoritma enkripsi klasik sederhana yang pengkodeannya menggunakan kotak yang disebut tabel Vigenere. AES (Advanced Encryption Standard) adalah salah satu teknik enkripsi modern yang menggunakan permutasi, permutasi, dan beberapa putaran atau putaran yang diterapkan pada setiap blok yang dienkripsi/didekripsi. Dengan demikian, dalam penelitian ini, kami mengimplementasikan kombinasi password klasik dan modern, yaitu Vigenere Cipher dan AES. Hasil eksperimen membuktikan bahwa kombinasi enkripsi menghasilkan nilai entropi informasi yang tinggi sebesar 4,125937 dan nilai koefisien korelasi mendekati nol sebesar 0,00722057 untuk pesan 1024 byte.

***Kata kunci**: Kriptografi, Vigenere Cipher, AES-256, fungsi hash.*

1. PENDAHULUAN

Terdapat banyak aplikasi yang dapat diunduh secara gratis untuk mengirim dan menerima pesan, tetapi aplikasi perpesanan ini tidak menerapkan keamanan apa pun pada pesan untuk membacanya, jadi kami tidak dapat menjamin keamanan, terutama privasi pengguna aplikasi ini. Berbagai jenis aplikasi perpesanan yang saat ini tersedia di Playstore belum tentu memiliki keamanan yang baik karena tidak ada aturan standar yang digunakan untuk mengamankan pesan dalam aplikasi tersebut. Dengan demikian, diperlukan sebuah aplikasi perpesanan yang menerapkan keamanan dengan mengenkripsi (encrypting) dan mendekripsi (decrypting) pesan.

Secara umum, ada tiga teknik untuk melindungi data: kriptografi (Purnama Reza Dwi Oktaf, 2016; Permana *et al*., 2017; Rasjid *et al*., 2017), steganografi (Chowdhuri, Jana and Giri, 2018; Elkandoz, Alexan and Hussein, 2019), dan watermarking (Singh and Singh, 2017; Soualmi, Alti and Laouamer, 2018; Rachmawanto, Atika Sari and Pradana, 2020). Dalam enkripsi, data atau informasi dilindungi dengan cara menyandikan data tersebut sehingga makna aslinya tidak dapat langsung ditafsirkan oleh pembaca. Data yang diamankan dapat dilihat dengan mata telanjang, tetapi makna sebenarnya menjadi ambigu atau tidak jelas (Maricar and Sastra, 2018). Teknologi steganografi melindungi data asli dengan menyembunyikannya pada objek tertentu sehingga data tersebut tidak dapat dilihat secara visual oleh mata manusia. Teknologi watermarking menjaga keamanan dengan memberikan perlindungan hak cipta gambar dengan menyisipkan tanda air ke dalam gambar digital. Keberadaan kriptografi sudah ada sejak zaman dahulu, namun dengan berkembangnya teknologi kriptografi ini pun ikut berkembang. Perkembangan kriptografi adalah untuk mencegah siapa pun memecahkannya. Seiring dengan perkembangan teknologi informasi, teknologi komunikasi juga berkembang. Dari surat fisik hingga e-mail hingga telepon, bentuk komunikasi yang paling populer hingga saat ini adalah Internet. Internet sangat diminati karena mudah digunakan dan dapat diakses oleh semua orang. Pada saat ini, salah satu contoh perkembangan teknologi dan informasi adalah aplikasi pesan instan, seperti yang dikenal saat ini, aplikasi chatting.

e-ISSN: 2964-2531
DOI : 10.36499/psnst.v12i1.7068 **p-ISSN: 2964-5131**

Manfaatkan layanan Internet untuk menjalankan aplikasi obrolan dengan mudah dan cepat. Aplikasi chatting populer saat ini memiliki banyak fitur seperti password user di menu login, enkripsi dan kurangnya fitur keamanan untuk melindungi pesan yang dikirim dan disimpan di database server aplikasi chatting (Pradipta, 2016; Syahroji and Pradana, 2018). Jika server diretas, konten semua percakapan yang disimpan dalam basis data dapat dibuat dapat dibaca oleh orang yang tidak berwenang, yang mengakibatkan pencurian atau manipulasi data. Oleh karena itu, diperlukan teknologi enkripsi untuk menyimpan pesan dalam database. Menurut (Aulia *et al.*, 2019), mengkodekan obrolan teks melalui Internet ke dalam algoritma kriptografi vigenere berbasis Android. Pekerjaan ini hanya menggunakan satu algoritma untuk melakukan enkripsi, dan algoritma ini masih dapat diselesaikan dengan metode uji Kaski dan analisis frekuensi. Penelitian selanjutnya pada (Syahroji and Pradana, 2018) adalah Vigenere-Affine Cipher untuk keamanan chat berbasis aplikasi Android menggunakan dua algoritma kriptografi klasik sehingga algoritma affincifer dapat diselesaikan dengan metode analisis frekuensi. Kemudian penelitian yang dilakukan oleh (Suryanto, Suhery and Brianorman, 2017) adalah pengembangan aplikasi chat messenger dengan kriptografi AES (Advanced Encryption Standard) yang diterapkan pada smartphone. Penelitian ini diyakini efektif dengan alasan pesan yang dikirimkan dilindungi dengan algoritma enkripsi modern. Namun, aplikasi ini memiliki beberapa kelemahan, terutama karena hanya dapat digunakan untuk mengirim pesan teks dan hanya pesan teks yang dapat dienkripsi.

2. TINJAUAN PUSTAKA

Dalam melengkapi penelitian ini, peneliti menggunakan beberapa penelitian yang terkait. Penelitian yang dilakukan (Aulia *et al.*, 2019) yaitu mengusulkan penyandian texts chat via internet dengan algoritma Vigenere Cipher. Dalam penelitiannya menghasilkan sebuah aplikasi yang mengimplementasikan algoritma kriptografi Vigenere Cipher yang dimana metode ini dapat mengubah pesan menggunakan kombinasi dua puluh enam (26) huruf alfabet. Selanjutnya pada penelitian yang dilakukan oleh (Syahroji and Pradana, 2018) mengusulkan kombinasi Enkripsi Vigenere Cipher dengan Affine Cipher. Dalam penelitiannya menghasilkan sebuah aplikasi chatting yang mengimplementasikan kombinasi dua algoritma kriptografi klasik yaitu Vigenere Cipher dan Affine Cipher. Dan aplikasi tersebut memilik tingkat keberhasilan sebesar 100% karena dapat mengenkripsi dan mendekripsi pesan yang dikirim oleh pengguna. Penelitian terakhir yaitu dilakukan oleh (Suryanto, Suhery and Brianorman, 2017) mengusulkan Enkripsi AES-128. Dalam penelitiannya menghasilkan sebuah aplikasi perpesanan dengan menerapkan teknik kriptografi Advanced Encryption Standard (AES). Penerapan Metode kriptografi dengan algoritma AES dirasa cukup efektif karena pesan yang dikirim sudah diamankan dengan enkripsi algoritma modern.

Tabel 1. ***State of The Art***

Penelitian	Metode	Masalah	Hasil Penelitian	Kekurangan
(Aulia et al., 2019)	Vigenere cipher	Aplikasi chatting yang belum memiliki pengamanan pesan	Terciptanya sebuah aplikasi yang mengimplementasikan algoritma kriptografi Vigenere Cipher	Proses evaluasi hasil hanya dalam bentuk behavior aplikasi, belum dari sisi perhitungan matematis misalnya pada ranah robustness
(Syahroji and Pradana, 2018)	Vigenere cipher, affine cipher	Vigenere cipher yang masih dapat dipecahkan dengan metode analisis frekuensi dan kasiski test	Terciptanya sebuah aplikasi Chatting yang menggunakan 2 (dua) metode kriptografi yaitu, Vigenere Cipher dan Affine Cipher dapat mengamankan pesan. Mempunyai keberhasilan sebesar 100% karena dapat mengenkripsi dan mendekripsi pesan yang dikirim oleh pengguna.	
(Suryanto, Suhery and Brianorman, 2017)	Eadvanced Encryption Standard (AES)	Penerapan pengamanan pesan pada aplikasi chatting yang masih menggunakan teknik kriptografi klasik	Terciptanya sebuah aplikasi chatting dengan pengamanan menggunakan metode kriptografi Advanced Encryption Standard (AES)	

Dalam penelitian ini, pengamanan pesan pada aplikasi chatting akan menggunakan kombinasi kriptografi klasik dan modern yaitu Vigenere Cipher dan Advanced Encryption Standard (AES). Dengan menggabungkan dua teknik kriptografi klasik dan modern tersebut maka akan menghasilkan sebuah aplikasi chatting yang lebih aman dari pada hanya menggunakan satu algoritma kriptografi klasik.

3. METODE

3.1. Algoritma Vigenere

Vigenere cipher merupkaan salah satu bentuk *polygram cipher* substitusi pengembanga dari Caesar Cipher. *Vigenere* dapat diimplementasikan dengan *tabula recta* maupun perhitungan *modulo*. Untuk pesan teks abjad dapat menggunakan modulo 26, sedangkan untuk pesan teks ASCII atau pesan gambar dapat menggunakan modulo 256 (Mulyono *et al.*, 2018). Saat mengkodekan algoritma *Vigenere*, kami menggunakan kotak yang disebut tabel Vigenere. Karena tabel *Vigenere* berisi 26 abjad, tabel ini menghasilkan 26 kemungkinan enkripsi. Kolom paling kiri adalah kata kunci dan kolom paling atas adalah teks atau pesan biasa untuk dilindungi. Proses enkripsi dilakukan dengan menggunakan rumus (1). Penjelasan rumus: P adalah plainteks, K adalah kunci, C adalah cipherteks. Dan huruf i adalah variabel indeks yang menunjukan lokasi huruf pada kalimat pesan. Proses dekripsi dilakukan menggunakan rumus (2).

$$C = (P + K) \bmod 26 \quad (1)$$

$$P = (C - K) \bmod 26 \quad (2)$$

3.2. Algoritma AES

AES (Advanced Encryption Standard) memiliki nama lain Rijndael dan merupakan algoritma enkripsi berbasis block cipher. AES merupakan pengembangan dari Data Encryption Standard (DES). Algoritma AES kunci menggunakan permutasi, permutasi, dan beberapa putaran atau putaran yang diterapkan pada setiap blok yang dienkripsi/didekripsi. Dalam setiap putaran, AES menggunakan kunci berbeda sehingga AES dinilai lebih aman disbanding DES maupun algoritma substitusi lain. AES bekerja dalam arah byte, sehingga algoritmanya efisien ketika diimplementasikan dalam perangkat lunak dan perangkat keras (Sangeeta and Kaur, 2017; Sharma, Prabhjot and Kaur, 2017). AES adalah algoritma enkripsi block cipher yang menggunakan sistem permutasi dan substitusi (P-Box dan S-Box). AES dibagi menjadi tiga jenis: AES-128, AES-192, dan AES-256. Perbedaannya terletak pada panjang kunci yang digunakan. Angka setelah AES menunjukkan panjang kunci yang digunakan. Selain perbedaan panjang kunci, ada perbedaan jumlah putaran yang digunakan. AES-128 menggunakan 10 putaran, AES-192 menggunakan 12 putaran, dan AES-256 menggunakan 14 putaran. Tabel 1 menunjukkan berbagai jenis AES. Kunci pada Tabel 1 didefinisikan sebagai 32 byte, jadi AES-128 memiliki nomor kunci 4x32 = 128 byte, ukuran blok 4x32 = 128 byte, dan jumlah putaran 10. Mirip dengan AES-192 dan AES-256 , yang memiliki ukuran blok yang sama dengan AES-128, perbedaan dari AES-192 adalah memiliki kunci 192-byte dan 12 putaran, mirip dengan AES-256. Jumlah kunci 256 byte dan jumlah putaran putaran 14 putaran. Cara kerja enkripsi pada AES-256 [15]:

1. AddRoundKey: menggunakan operasi XOR pada state awal (plainteks) dengan cipherkey. Pada tahap ini biasa disebut juga initial round.
2. Putaran sebanyak Nr – 1 kali atau Total r – 1. Terdapat empat proses yang akan dilakukan pada tiap putarannya, yaitu:
   a. SubBytes: melakukan substitusi byte dengan Sbox atau table substitusi.
   b. ShiftRows: melakukan penggeseran baris array state secara wrapping.
   c. MixColumns: mengacak data pada masing-masing kolom array state.
   d. AddRoundKey: melakukan operasi XOR antara state sekarang round key.
3. Final round yaitu proses untuk putaran terakhir, perbedaanya dengan menghilangkan proses MixColumns.

Proses dekripsi AES dilakukan dengan ciphertext dibalik. Transformasi kriptografi dilakukan dengan arah yang berlawanan dengan proses enkripsi untuk menghasilkan reverse password. Transformasi byte

e-ISSN: 2964-2531
DOI : 10.36499/psnst.v12i1.7068
p-ISSN: 2964-5131

yang digunakan untuk kata sandi terbalik adalah *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*.

Tabel 1. Perbandingan Jumlah Key dan Round

Jenis AES	Jumlah Key	Ukuran Blok	Jumlah Round
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

3.3. *Hash SHA*

SHA (Secure Hashing Algorithm) adalah algoritma yang digunakan untuk mengubah teks menjadi karakter arbitrer dengan panjang sesuai dengan nama SHA itu sendiri. SHA dibuat oleh Badan Keamanan Nasional AS dan diumumkan pada tahun 2001. SHA juga dikenal sebagai enkripsi tanpa kunci.

3.4. Analisis Statistik

Koefisien korelasi biasanya digunakan untuk menentukan hubungan antara dua variabel. Misalnya, kedua variabel tersebut adalah plaintext dan ciphertext. Jika nilai koefisien korelasi mendekati 1, berarti kedua variabel tersebut saling berhubungan, dan dapat dikatakan bahwa proses enkripsi tidak berjalan dengan baik. Namun, nilai modulus yang mendekati -1 menunjukkan bahwa plaintext menyerupai ciphertext negatif. Kriteria kata sandi yang baik yaitu harus menghasilkan nilai koefisien korelasi mendekati nol. Perhitungan nilai korelasi dilakukan dengan menggunakan rumus (3).

$$KK(x,y) = \frac{\sum_{i=1}^{n}(x_i-\mu(x))(y_i-\mu(y))}{\sigma(x)\sigma(y)} \quad (3)$$

dengan :

$\mu(x) = \frac{1}{n}\sum_{i=1}^{n} x_i$ dan $\mu(y) = \frac{1}{n}\sum_{i=1}^{n} y_i$

$\sigma(x) = \sqrt{\sum_{i=1}^{n}(x_i} - \mu(x))^2$ dan $\sigma(y) = \sqrt{\sum_{i=1}^{n}(y_i} - \mu(y))^2$

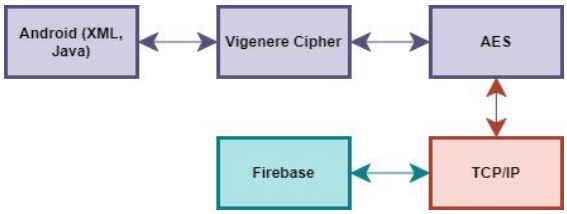
Entropi informasi digunakan untuk menunjukkan tingkat ketidakpastian informasi. Oleh karena itu, semakin tinggi nilai entropi, semakin tidak pasti informasinya. Dan dalam kriptografi, nilai entropi yang lebih tinggi berarti ciphertext tidak diketahui, dan nilai entropi yang lebih tinggi berarti algoritma kriptografi yang lebih baik [12]. Perhitungan nilai entropi informasi dilakukan dengan menggunakan rumus (4), dimana X adalah pesan, S_i adalah simbol ke-i dalam pesan, $p(S_i)$ adalah peluang kemunculan S_i dan a_i adalah jumlah kemunculan S_i.

$$H(X) = -\sum_{i=1}^{n} {a_i}^2 \, log(p(S_i)) \quad (4)$$

3.5. Metode yang Diusulkan

Berdasarkan Gambar 1, pengguna membuka aplikasi chatting yang telah diinstall pada perangkat androidnya. Apabila pengguna belum memiliki akun pada aplikasi ini, maka pengguna membuat akun baru. Pengguna mengisi data nama, email, dan password. Apabila pengguna sudah mendaftar, maka pengguna dapat melakukan *login* dengan menggunakan email dan password yang didaftarkan sebelumnya. Setelah *login* dan berhasil masuk. Pengguna masuk pada dashboard atau menu utama yang terdiri dari dua menu yaitu chat dan teman lainnya. Untuk melakukan chat pengguna harus memilih salah satu dari teman yang terdaftar pada aplikasi tersebut. Setelah memilih teman maka pengguna mengirimkan pesan yang ingin dikirimkan ke penerima. Pada saat pesan dikirim, aplikasi akan melakukan proses enkripsi terlebih dahulu sebelum dikirim ke *Database Firebase*. Pesan yang dikirim akan diubah menjadi *ciphertext* sesuai dengan kunci yang diterapkan pada system. Setelah proses

enkripsi selesai, selanjutnya pesan yang sudah dirubah menjadi *ciphertext* akan dikirim ke *Database Firebase*. Penerima akan menerima pesan ciphertext dari Database Firebase dan aplikasi akan otomatis melakukan dekripsi pesan sehingga pesan kembali seperti bentuk aslinya.



Gambar 1. Perancangan Sistem

4. HASIL DAN IMPLEMENTASI

Kata sandi Vigenere dan sistem enkripsi AES dibangun ke dalam aplikasi obrolan dan sistem enkripsi Vigenere dan AES dibangun menggunakan bahasa pemrograman Java. Proses enkripsi dan dekripsi dilakukan dalam aplikasi smartphone (enkripsi end-to-end), sehingga saat mentransfer data ke Firebase, pesan yang dikirim dalam format ciphertext, sehingga tidak dapat dibaca dan karenanya aman. Kata sandi vigenere adalah cara untuk menggunakan tabel yaitu tabel vigenere. Namun, aplikasi dalam sistem berbasis digital tidak memungkinkan penggunaan tabel vigenere. Namun, ia menggunakan sistem matematika untuk melakukan enkripsi dan dekripsi. Proses enkripsi dan dekripsi menggunakan algoritma kriptografi Vigenere. Artinya, enkripsi menggunakan persamaan (1) dan (2).

4.1. Proses Enkripsi

Dapat dilakukan pengiriman pesan dengan kombinasi abjad, angka, emoji, dan simbol pesan, serta mengenkripsi dan mendekripsi dengan tepat berdasarkan hasil pengujian. Pesan yang dikirim dienkripsi menggunakan kunci untuk vigenere yaitu 'tngekriptpaketklasiktoktoktjuga' dan dienkripsi menggunakan AES dengan kunci 'modernlehughanich' dan disimpan dalam database dan proses dekripsi pesan dikirim ke server terjadi segera setelah disimpan. basis data. Hasil pengujian dapat dilihat pada Tabel 2.

Tabel 2. Contoh Hasil Enkripsi dan Dekripsi

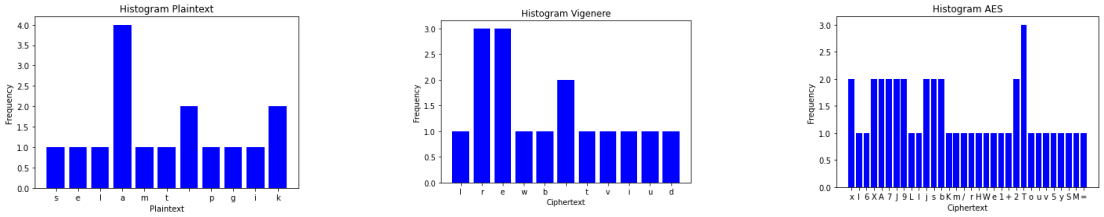
Pesan Terkirim	Ciphertext Vigenere	Ciphertext AES	Pesan Di Database	Pesan Terbaca
halooo	anrsyf	N5koVJJE/JsOQmlsk6cECQ==	N5koVJJE/JsOQmlsk6cECQ==	halooo
selamat pagi kak	lrrewrb etvi ued	xI6XAx7JA9LljsbKm/rJHWe1+292Tsouv5TjTySb7XM=	xI6XAx7JA9LljsbKm/rJHWe1+292Tsouv5TjTySb7XM=	selamat pagi kak
ketiduran 😅	drzmnlzpg 😅	PL6j51S3uTZbTatlOHlXRw==	PL6j51S3uTZbTatlOHlXRw==	ketiduran 😅
tgl 14 ultah ya ?	mtr 14 yvkiw rp?	zcWt3alYbGiktOAzmf1HCUOMg5DsAoMBEX23CWGvxVI=	zcWt3alYbGiktOAzmf1HCUOMg5DsAoMBEX23CWGvxVI=	tgl 14 ultah ya ?
	agztc://wqgxqacildzrsoo.zcyzuygpbf.isw/m0/j/raptkilftgwvoks.kiymvom.puq/y/dmhlpgow_bwlgw%2n-wctuun6hhvtt_eezsvx.ceg?kpm=wpdai&dhyog=4566oxh2-6c37-4096-8868-1y1p23h754f2	Cv0pAgefAo6anCxzS5mc6Qfbg8bka0aI029pd37ptR0euRkaJyOFF6tA+SzdkoPZT1/NWBrQ9ABZAz1CZBZL6E8gTZtW2SXc23hcgusVE8ELPJs73gX7eFLcbOEjxAD0fiMF6/KpDNouN3/+rmWKnFUQ/wK0qJevZ04tnwiH6nbJLRusmxjUwVZv5/L0E7nIb0E8+ulHGd/5KKXPHb1vv+s+cU6rEHK0H62IqIE7aco=	Cv0pAgefAo6anCxzS5mc6Qfbg8bka0aI029pd37ptR0euRkaJyOFF6tA+SzdkoPZT1/NWBrQ9ABZAz1CZBZL6E8gTZtW2SXc23hcgusVE8ELPJs73gX7eFLcbOEjxAD0fiMF6/KpDNouN3/+rmWKnFUQ/wK0qJevZ04tnwiH6nbJLRusmxjUwVZv5/L0E7nIb0E8+ulHGd/5KKXPHb1vv+s+cU6rEHK0H62IqIE7aco=	

Berikut perbandingan frekuensi karakter pada contoh kata “selamat pagi kak” yang ditampilkan dalam bentuk histogram. Pada histogram di atas, dapat disimpulkan bahwa kombinasi enkripsi Vigenere Cipher dan AES-256 cukup baik karena terdapat perbedaan yang signifikan dalam jumlah karakter, modifikasi karakter, transformasi karakter plaintext dan AES-256.

DOI : 10.36499/psnst.v12i1.7068
e-ISSN: 2964-2531
p-ISSN: 2964-5131

Tabel 3. Tabel hasil Histogram

Keterangan	Jumlah Karakter	Perubahan Karakter	Variasi Karakter
Plaintext	16	{selamt pgik}	11
Vigenere Cipher	16	{lrewb tviud}	11
AES-256	44	{xI6XA7J9LljsbKm/rHWel+2Touv5ySM=}	32

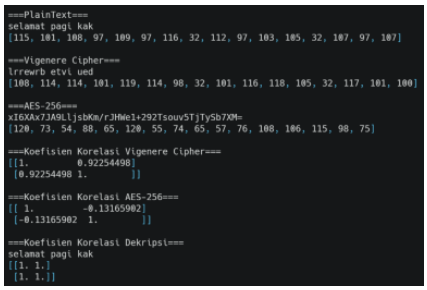


(a) *Histogram Plaintext* **(b) *Histogram Vigenere*** **(c) *Histogram AES***

Gambar 3. Hasil Histogram

4.2. Koefisien Korelasi

Berikut hasil pengujian koefisien korelasi terhadap kata “selamat pagi kak” yang dienkripsi menggunakan vigenere cipher dan AES-256. Pada AES-256 akan ditetapkan threshold sesuai dengan panjang dari plaintext agar dapat dilakukan pengujian koefisien korelasi. Didapatkan hasil koefisien korelasi Vigenere Cipher yaitu 0,92254498 yang berarti nilai mendekati 1 yang berarti enkripsi kurang baik, sehingga perlu dienkripsi lagi menggunakan AES-256 dan mendapatkan hasil -0,13165902 yaitu nilai yang mendekati 0 dapat dikatakan plaintext dan ciphertext berbeda dan enkripsi bekerja dengan baik, dan pada hasil dekripsi mendapatkan nilai 1 dimana proses enkripsi-dekripsi berhasil yaitu plaintext dan decrypttext mirip.



Gambar 4. Koefisien Korelasi

4.3. Hasil Uji Coba

Berdasarkan hasil uji coba dengan menggunakan pesan yang memiliki panjang 1024 byte, 2048 byte, 4096 byte yang dilakukan enkripsi dan dekripsi pada vigenere cipher dan AES-256 dapat disimpulkan proses enkripsi dan dekripsi bekerja dengan baik, dengan running time yang rendah dan tingkat kerumitan ciphertext yang baik yang dapat dilihat berdasarkan koefisien korelasi dan entropi informasi. Hasil ujicoba kriptografi dapat dilihat pada Tabel 4.

Tabel 4. Hasil Uji Coba Kriptografi

Pesan	Panjang Pesan (byte)	Running Time				Koefisien Korelasi				Entropi Informasi	
		Vigenere (ms)	AES (ms)	Vigenere & AES (ms)	Stored to DB (ms)	Vigenere	AES	Vigenere & AES	Stored to DB	Plaintext	Ciphertext
Pesan 1	1024	6	1	7	325	0,932	0,018	0,007	1	2,927277	4,125937
Pesan 2	2048	15	2	17	730	0,933	0,022	0,006	1	2,919730	4,142654
Pesan 3	4096	68	4	72	221 m	0,012	0,012	0,012	1	2,943429	4,150892

5. KESIMPULAN

Pada sistem enkripsi dan dekripsi pada AES diperlukan algortima pendukung yaitu base64 yang berfungsi untuk standarisasi pesan yaitu pesan diubah menjadi *hexadesimal* agar pesan yang dienkripsi (kirim) dan didekripsi (terima) sama persis. Fungsi *Hash SHA-256* yang digunakan untuk *generate* kunci agar menjadi standar kunci dari AES-256 berkerja dengan baik. Penerapan *Vigenere Cipher* dan AES-256 pada aplikasi chatting dengan realtime database firebase bekerja dengan baik, dibuktikan dengan dengan *running-time* yang cepat dan teks pesan yang berhasil diamankan dengan kriptografi tersebut. Pada penelitian selanjutnya diharapkan metode kombinasi dapat diimplementasikan pada kriptografi asimetris sehingga kunci lebih aman. Pengujian mengenai keamanan yang sudah dicapai dapat di analisa menggunakan teknik *Avalache Effect*.

DAFTAR PUSTAKA

Aulia, R. *et al.* (2019) 'Penyandian Texts Chat Via Internet Dengan Algoritma Vigenere Cipher', *JSIK (Jurnal Sistem Informasi Kaputama)*, 3(2), pp. 28–34.

Chowdhuri, P., Jana, B. and Giri, D. (2018) 'Secured steganographic scheme for highly compressed color image using weighted matrix through DCT', *International Journal of Computers and Applications*, 7074, pp. 1–12. doi: 10.1080/1206212X.2018.1505024.

Elkandoz, M. T., Alexan, W. and Hussein, H. H. (2019) 'Double-Layer Image Security Scheme with Aggregated Mathematical Sequences', in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, pp. 1–7. doi: 10.1109/COMMNET.2019.8742370.

Maricar, M. A. and Sastra, N. P. (2018) 'Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi', *Majalah Ilmiah Teknologi Elektro*, 17(1), p. 59. doi: 10.24843/mite.2018.v17i01.p08.

Mulyono, I. U. W. *et al.* (2018) 'Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit)', *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 4(1), pp. 63–74. doi: 10.22219/kinetik.v4i1.701.

Permana, T. S. *et al.* (2017) 'Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher', *Techno.Com*, 16(4), pp. 337–347. doi: 10.33633/tc.v16i4.1267.

Pradipta, G. A. (2016) 'Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting', *Jurnal Sistem dan Informatika*, 10(2), pp. 119–127.

Purnama Reza Dwi Oktaf, L. H. (2016) 'Pengamanan Dokumen Teks Menggunakan Algoritma Kriptografi Mode Operasi Cipher Block Chaining (Cbc) Dan Steganografi Metode End of File (Eof)', *Techno.COM*, 15(1), pp. 22–31.

Rachmawanto, E. H., Atika Sari, C. and Pradana, R. P. (2020) 'DWT-SVD Combination Method for Copyrights Protection', *Scientific Journal of Informatics*, 7(1), pp. 113–124. doi: 10.15294/sji.v7i1.21050.

Rasjid, Z. E. *et al.* (2017) 'A review of collisions in cryptographic hash function used in digital forensic tools', *Procedia Computer Science*. Elsevier B.V., 116, pp. 381–392. doi: 10.1016/j.procs.2017.10.072.

Sangeeta and Kaur, E. A. (2017) 'A Review on Symmetric Key Cryptography Algorithms', *International Journal of Advanced Research in Computer Science*, 8(4), pp. 358–362.

Sharma, N., Prabhjot and Kaur, H. (2017) 'A Review of Information Security using Cryptography Technique.', *International Journal of Advanced Research in Computer Science*, 8(4), pp. 323–326. Available at: http://web.a.ebscohost.com/ehost/detail/detail?vid=0&sid=852854fe-f74a-47d8-b2c5-36c892e545ea%40sessionmgr4006&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=123430611&db=aci.

Singh, D. and Singh, S. K. (2017) 'DWT-SVD and DCT based Robust and Blind Watermarking Scheme

e-ISSN: 2964-2531
DOI : 10.36499/psnst.v12i1.7068 **p-ISSN: 2964-5131**

for Copyright Protection', *Multimedia Tools and Applications*. Multimedia Tools and Applications, 76(11), pp. 13001–13024. doi: 10.1007/s11042-016-3706-6.

Soualmi, A., Alti, A. and Laouamer, L. (2018) 'A New Blind Medical Image Watermarking Based on Weber Descriptors and Arnold Chaotic Map', *Arabian Journal for Science and Engineering*. Springer Berlin Heidelberg, 43(12), pp. 7893–7905. doi: 10.1007/s13369-018-3246-7.

Suryanto, I., Suhery, C. and Brianorman, Y. (2017) 'Pengembangan Aplikasi Chat Messenger dengan Metode Advanced Encryption Standard (AES) pada Smartphone', *Jurnal Coding Sistem Komputer Untan*, 03(2), pp. 1–10.

Syahroji, A. and Pradana, R. (2018) 'Vigenere Cipher dan Affine Cipher untuk Pengamanan Chatting Berbasis Android', *Skanika*, 1(3), pp. 1168–1175. Available at: https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2542.