Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

Modifikasi Pembangkit Kunci Algoritma Vigenere Cipher Berdasarkan Pembangkit Bilangan Acak CSPRNG Untuk Mengamankan Citra Digital

Menanti Sianturi[*], Taroni Sokhi Zebua

F Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamanganraja No. 338, Medan, Sumatera Utara, Indonesia
E-mail: [1,*]Christian.sianturi1502@gmail.com, [2]taronizeb@gmail.com

Abstrak-Distribusi citra digital pada era digital sekarang sangat pesat. Distribusi citra digital sudah menjadi seperti kebiasaan setiap insan setiap hari, ada yang bersifat komsumsi umum dan juga ada yang bersifat rahasia. Pendistribusian citra digital ini dapat kita lihat pada penggunaan media sosial, toko- toko online, perkantoran, maupun pemerintahan. Tentu setiap orang yang mendistribusikan citra digital, tidak ingin kehilangan makna dari citra digital tersebut karena orang pekerjaan orang- orang yang tidak baik, atau citra digital itu tidak disalah gunakan oleh pihak yang tidak berwewenang atas citra tersebut, sehingga perlu diamankan. Masalah keamanan menjadi isu yang tiada habisnya dibahas sejak dulu hingga sekarang. Informasi yang bersifat rahasia sensitif atau bernilai tinggi dijaga keamanannya agar tidak bisa diakses orang-orang yang tidak memiliki wewenang dengan informasi tersebut. Demikian juga halnya dengan citra digital, harus aman dari orang-orang yang tidak memiliki wewenang terhadap citra tersebut. Citra digital dapat diamankan dengan menggunakan algoritma kriptografi. Penelitian ini membahas bagaimana memodifikasi Vigenere cipher dengan pembangkit kunci CSPRNG berbasis algoritma RSA. Vigenere cipher adalah algoritma kriptografi klasik yang memanfaatkan panjang kunci sebagai kekuatan untuk mengamankan data dan informasi. Semakin panjang kunci yang diterapkan semakin aman enkripsinya, dan kunci yang panjang harus acak dan unik. Pada penelitian ini, kunci yang akan digunakan adalah pembangkit bilangan acak CSPRNG berbasis algoritma RSA. Bilangan acak yang dihasilkan algoritma ini diyakini sangat sulit dikomputasi penyerang. Dengan menerapakan algoritma ini untuk mengenkripsi citra digital diyakini mampu mengamankan citra digital, pola pixel pada citra akan diacak seacak mungkin. Citra digital yang ditrasmisikan akan terdistribusikan dalam pola pixel yang acak dan kelihatatan tidak bermanfaat bagi para penyerang. Penerapan algoritma ini diyakini mampu mempertahankan keamanan citra digital.

Kata Kunci: Kriptografi; Vigenere Cipher; Kunci; CSPRNG; Citra; Matlab 2013

Abstract-The distribution of digital images in the current digital era is very rapid. The distribution of digital images has become a habit for every person every day, some are for public consumption and some are confidential. We can see the distribution of digital images in the use of social media, online shops, offices and government. Of course, everyone who distributes digital images does not want to lose the meaning of the digital image because people do bad work, or the digital image is misused by parties who do not have authority over the image, so it needs to be secured. Security issues have been an issue that has been discussed endlessly since the past until now. Information that is confidential, sensitive or of high value is kept secure so that it cannot be accessed by people who do not have authority over the information. Likewise with digital images, they must be safe from people who do not have authority over the image. Digital images can be secured using cryptographic algorithms. This research discusses how to modify the Vigenere cipher with a CSPRNG key generator based on the RSA algorithm. The Vigenere cipher is a classic cryptographic algorithm that utilizes key length as a strength to secure data and information. The longer the key applied, the more secure the encryption, and long keys must be random and unique. In this research, the key that will be used is a CSPRNG random number generator based on the RSA algorithm. The random numbers generated by this algorithm are believed to be very difficult for attackers to compute. By applying this algorithm to encrypt digital images, it is believed to be able to secure digital images, the pixel pattern in the image will be as random as possible. The transmitted digital image will be distributed in a random pixel pattern and will appear useless to attackers. The application of this algorithm is believed to be able to maintain digital image security.

Keywords: Cryptography; Vigenere Cipher; Key; CSPRNG; Image; Matlab 2013

1. PENDAHULUAN

Keamanan data merupakan kumpulan piranti yang dirancang untuk melindungi data atau informasi ketika ditransmisikan atau disimpan terhadap ancaman pengaksesan, pengubahan dan penghalangan oleh pihak tidak berwewenang. Keamanan data harus menjamin bahwa data tidak dibaca oleh pihak berhak, data sampai pada tujuan dengan utuh dan juga kebenaran pihak- pihak yang sedang mentrasmisikan. Keamanan data tidak boleh hanya bergantung pada *firewall* dan *instrusion detection system* saja. Ada beberapa teknik kemanan data yang umum digunakan hingga saat ini, diantaranya adalah teknik kriptografi, teknik steganografi, *watermarking* dan lain-lain.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kekuatan kemanan algoritma kriptografi harus bergantung pada kucinya, bukan pada metodenya[1]. Penggunaan kriptografi dalam kehidupan sehari-hari pun semakin meningkat dan terus dikembangkan untuk memberikan kenyamanan dan keamanan bagi pengguna. Teknik kriptografi memiliki berbagai algoritma salah satunya adalah algoritma *vigenere cipher*.

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

Vigenere cipher mengandung sejumlah *caesar cipher* yang dirangkai dengan kunci pergeseran yang berbeda-beda[2]. *Vigenere cipher* menggunakan substitusi dengan fungsi *shift*. Enkripsi dan dekripsi dengan *vigenere cipher* dapat diformulasikan secara matematis, dengan panjang kunci m adalah rangkaian kunci $k^{-}_{1,}$ k_2,k_3.....k_m, *plaintext* adalah p_1,p_2,p_3....p_t maka enkripsi adalah $c_i = (p_i + k_i) \bmod 26$ sedangkan dekripsi adalah $p_i = (c_i - k_i) \bmod 26$. Berdasarkan penelitian terdahulu mengatakan bahwa, salah satu kelemahan dari algoritma *vigenere chipher* adalah bila menggunakan kunci yang pendek. Pemecahan *vigenere cipher* cukup dilakukan dengan menentukan panjang kuncinya. Bila panjang kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditemukan dengan menulis program komputer untuk melakukan *exhaustive key serach.* Semakin panjang kunci, maka semakin besar periode dan akan semakin besar usaha percobaan yang dilakukan[3]. Kelemahan ini dapat diselesaikan dengan melakukan pembangkitan kunci yang lebih acak, sehingga dapat meminimalkan kemudahan pemecahannya.

Beberapa sistem kriptografi memerlukan masukan berupa bilagan acak. Bilangan acak adalah bilangan yang tidak dapat diprediksi kemunculannya, frekunsi kemunculan setiap bilangan harus maksiman satu. Bilangan acak ada dua macam, pertama adalah bilangan acak sejati (*true random numbers*) dan bilangan acak semi-acak (*pseudorandom numbers*).

Tidak semua pembangkit bilangan acak dapat digunakan untuk mengoptimalkan metode kriptografi, pembangkit bilangan acak yang aman digunakan untuk kriptografi disebut *Cryptographically Secure Pseudorandom Generator* (*CSPRNG).* Pembangkit bilanangan acak berbasis *CSPRNG* diformulasikan berdasarkan persoalan matematika yang sulit, pemfaktoran bilangan prima, logaritma diskrit, dan lain-lain. Bilangan acak yang dihasilkan metode ini tahan terhadap serangan yang serius[3]. Berdasarkan keyakinan inilah maka, *CSPRNG* akan digunakan untuk mengoptimalkan kekuatan kunci *vigenere cipher.* Penelitian ini menguraikan proses pembangkitan kunci berdasarkan teknik pembangkit kunci *CSPRNG*. Kunci yang dihasilkan digunakan sebagai kunci untuk melakukan proses enkripsi dan dekripsi data citra *digital* berdasarkan algoritma *vigenere cipher*. Modifikasi yang dilakukan mampu memperkuat kemananan data terhadap tindakan penyerangan.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kata kriptografi berasal dari bahasa Yunani, yaitu *"cryptos"* yang artinya *"secret"* (rahasia), dan *"graphein"* berartinya *"writing"* (tulisan), kriptografi berarti *"secret writing"* (tulisan rahasia). Ada beberapa defenisi kriptografi yang telah dikemukakan di dalam berbagai literature yaitu, ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikan pesan[6][7].

2.2 Vigenere Cipher

Algoritma *vigenere* mengenkripsi dan dekripsi pesan dengan kunci huruf dalam *tabula recta* (bujur sangkar *vigenere*). *Tabula recta* digunakan untuk memperoleh teks kode dengan menggunakan kunci yang sudah ditentukan, bila panjang kunci lebih pendek dari pada panjang *plaintext.* Maka pengulangan kunci akan dilakukan.

Adapun langkah-langkah proses enkripsi dan dekripsi pada algoritma *vigenere cipher*[4], sebagai berikut:

$$Enc(P_{1....}P_i)=(C_1.....C_i) = (P_1+K_1....P_i+K_i) \bmod 26 \quad (1)$$

$$Dec(C_{1....}Ci=(P_1....P_i) = (C_1- K_{1.....}C_i - K_i) \bmod 26 \quad (2)$$

2.3 Cryptografilcally Secure Pseudorandom Generator (CSPRNG)

Pembangkit bilangan acak yang aman untuk kriptografi disebut dengan CSPRNG. Metode ini membangkitkan bilangan acak yang tidak dapat diprediksi kemunculannya. Sebuah *CSPRNG* harus memenuhi syarat[20], yaitu,

a. Secara statistik mempunyai sifat-sifat yang bagus (lolos uji keacakan secara statistik), frekuensi kemunculan kunci yang sama sangat kecil.
b. Tahan terhadap serangan (*attact)* yang serius, serangan ini bertujuan untuk memprediksi bilangan acak yang dihasilkan.

2.4 CSPRNG Berbasis Algoritma RSA

Berikut ini diuraikan langkah-langkah dalam membangkitkan bilangan acak *CSPRNG* berbasis RSA[21].

a. Pilih dua buah bilangan prima rahasia, *p* dan *q* dan bilangan bulat *e* yang relatif prima dengan (*p -1)* (*q-1)*.
b. Kalikan keduanya menjadi n = *pq*.
c. Pilih bilangan bulat acak lain , s sebagai x_0 yang dalam hal ini $2 \leq s \leq n$.
d. Barisan acak dihasilkan dengan melakukan iterasi berikut sepanjang yang diinginkan:
   1. Hitung $x_i = x_i - {}_1^e \bmod n$ dengan $x_0 = s$.
   2. Z_i = bit *LSB* (*Least Signifficant Bit)* dari x_i.
e. Barisan bit acak adalah z_1,z_2,z_3,.....
   Kemanan pembangkit bilangan acak berbasis algoritma RSA terletak pada sulitnya memfaktorkan n, jika n besar, maka pembangkit bilangan acak ini dikatakan aman[3].

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

2.5 Matlab 2013

Matlab 2013 merupakan suatu paket perangkat lunak yang memampukan pengguna untuk melakukan komputasi matematika, menganalisa data, mengembangkan algoritma, melakukan simulasi dan pemodelan, menghasilkan tampilan grafik dan antar muka grafikal[11]. Karena objek yang diteliti adalah citra maka Matlab 2013 akan digunakan untuk simulasi dan pengujian.

2.6 Tahapan Penelitian

Adapun tahapan penelitian yang digunakan untuk melakukan penelitian ini adalah:

a. Studi Pustaka
   Merupakan metode pengumpulan data dengan cara mempelajari literatur yang mendukung penelitian.
b. Analisis
   Menganalisa bagaimana modifikasi vigenere cipher dan CSPRNG berbasis algoritma RSA
c. Implementasi
   Implementasi merupakan tahap untuk menerapkan modifikasi vigenere cipher dan CSPRNG pada citra digital berformat jpg.
d. Dokumentasi
   Membuat dokumentasi seluruh kegiatan penelitian yang dimulai dari awal hingga akhir.

3. HASIL DAN PEMBAHASAN

3.1 Analiasa Masalah

Algoritma vigenere cipher termasuk pada algoritma kriptografi klasik, yang menggunakan metode substitusi untuk mengamankan data. Teknik substitusi vigenere cipher rentan terhadap serangan, kelemahan metode ini terdapat pada kunci. Umumnya user mengggunakan kata-kata yang bermakna atau kunci yang pendek supaya mudah diingat dan inilah salah satu yang menjadi kelemahan kunci metode ini.

Salah satu upaya yang dapat dilakukan untuk meningkatkan keamanan kunci pada algoritma vegenere cipher adalah melakukan modifikasi pada pembangkitan kuncinya, sehingga keamanan kunci dan pesan yang diamankan lebih optimal.

Bila vigenere cipher menggunakan kunci yang pendek maka, vigenere cipher mudah diserang, metode kasiski akan mencari kemungkinan panjang kunci dan analisis frekuensi untuk mendetaksi karakter-karakter yang dominan. Kelemahan ini muncul pada teks berukuran panjang, karena teks yang panjang pada umumnya menggunakan kata-kata yang berulang dan adanya karakter-karakter tertentu yang dominan digunakan dibanding dengan karakter lain, seperti huruf “A, I, E, N, T” sangat dominan dibanding karakter lain, dan diantara huruf itu, karakter “A” adalah karakter paling dominan dan jauh meninggalkan kemunculan karakter lain. Itu sebabnya vigere cipher harus diberikan kunci yang panjang dan acak agar frekuensi kemunculan dapat diminimalis dan panjang kunci tidak mudah dideteksi.

Menggunakan kunci panjang tidak efektif bila diberikan secara manual, untuk lebih efisien maka sebaiknya menggunakan generator pembangkit bilangan acak. Adapun generator pembangkit bilangan acak yang akan digunakan dalam penelitian ini adalah CSPRNG berbasis RSA.

Berikut ini akan diterapkan modifikasi pembangkit kunci *vigenere cipher* dengan menggunakan CSPRG berbasis RSA, dimana data yang diuji adalah citra *grayscale*.

a. Defenisikan Citra yang akan amankan

Objek yang diteliti adalah citra *grayscale* berformat .jpg dengan resolusi 256 x 256 *pixel.*. Berikut ini adalah citra yang akan diamankan yang ditampilkan dengan *Matlab* 2013.

img=*imread* (‘masker.jpg’);% membaca nama file citra
figure, imshow(gray_img);%menampilkan citra *grayscale* ke window

Gambar 1. Sampel masker.jpg

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

Tabel 1. Nilai *pixel* 16 x 16

Pixel ke-i	0	1	2	3	4	5	6	7	8	9	10	11
0	244	242	241	243	244	244	244	244	243	244	245	244
1	239	235	234	235	236	236	236	237	235	237	238	239
2	233	229	227	228	228	229	229	230	230	231	232	231
3	230	226	224	224	224	225	225	226	226	227	228	229
4	232	228	226	226	225	227	226	228	227	229	232	232
5	231	227	226	227	225	226	226	228	229	231	233	233
6	231	228	226	227	226	227	227	228	230	231	232	232
7	231	228	225	227	226	227	227	228	228	230	230	229
8	232	227	228	228	229	228	228	229	230	230	230	230
9	232	228	228	229	229	228	228	229	230	230	230	230
10	232	228	228	229	230	229	230	231	229	229	229	229
11	232	228	228	228	229	228	228	228	229	229	229	229
12	232	229	228	229	229	228	228	229	229	229	229	229
13	232	229	228	229	229	228	229	229	229	229	229	229
14	232	229	227	229	229	228	229	229	229	229	229	229
15	232	229	228	229	229	229	229	229	229	229	229	229

b. Pembangkitan kunci

1. Pilih dua buah bilangan prima rahasia, *p* dan *q*, dimisalkan nilai yang dipilih adalah :
   p = 23 dan q = 251
2. Pilih bilangan bulat e yang relatif prima dengan (p-1)(q-1)
   (p-1)(q-1) = (23 – 1) (251 – 1) = 5500
   Faktor pembagi dari 5500 adalah 1, 2, 4, 5, 10, 20, 22, 25,.....2750.
   e = 21
   Faktor pembagi dari 21 adalah 1, 3, 7, 21
   Berdasarkan uraian di atas bahwa FPB(5500, 21) = 1, adalah memenuhi syarat sebagai bilangan yang relatif prima, sehingga e = 21 adalah memenuhi syarat.
3. Kalikan keduanya menjadi n = p * q
   n = p * q
   n = 23 * 251
   n = 5773
4. Pilih bilangan bulat acak lain, s sebagai x_0 dimana, $2 \leq s \leq n$, s = 5771
5. Barisan *bit* acak dihasil dengan iterasi sebagai berikut:
   $x_i = x_{i-1}^{e} \bmod n$, dimana $x_0 = s$
   z_i = *bit* LSB (*Least Significant Bit*) dari x_i
6. Membangkitkan kunci 256 x 256 dengan Matlab 2013

```
for x=1:baris
    for y=1:kolom
        kunci(x,y)=mod((s^e),n);
        s=kunci(x,y);
    end
end
```

Perhitungan pada LSB kunci(x,y) tidak dilakukan dalam penelitian ini, hal karena berkaitan dengan syarat kunci keamanan metode *vigenere cipher* yaitu kunci panjang, acak dan unik. Bila perhitungan LSB dilanjutkan maka, hanya akan menghasilkan bilangan acak 0 atau 1, kunci memang panjang, tetapi tidak unik, karena kunci akan sering muncul. Selain itu bila hanya menggunakan *bit* 0 atau 1 maka, citra yang dienkripsi justru tidak akan mengalami perubahan yang signifikan, sebab perubahan pada nilai *pixel* hanya antar 1 atau tidak berubah sama sekali. Berdasarkan keyakinan inilah peneliti tidak menggunakan *bit* LSB sebagai kunci. Adapun deret kunci yang dibangkitkan berdasarkan *script* tersebut diperoleh matriks kunci(x,y). Nilai setiap kunci(x,y) dapat dilihat dengan menggunakan Matlab 2013 pada tabel berikut.

Tabel 2. Kunci(x,y)

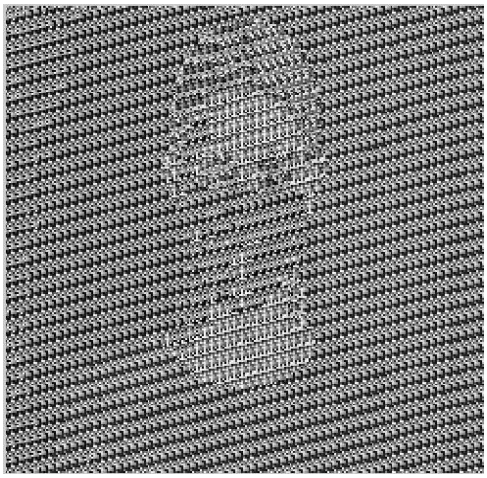
Kunci ke-i	0	1	2	3	4	5	6	7	8	9	10	11
0	2232	201	631	5590	1311	3243	4251	698	2169	1528	3653	645
1	1792	855	4484	1659	2488	1665	1796	2212	54	1780	3888	1428
2	2488	1665	1796	2212	54	1780	3888	1428	3472	4277	1013	4325
3	54	1780	3888	1428	3472	4277	1013	4325	1179	3867	556	3561
4	3472	4277	1013	4325	1179	3867	556	3561	5579	3500	3610	5321
5	1179	3867	556	3561	5579	3500	3610	5321	5285	664	3374	1111

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

6	5579	3500	3610	5321	5285	664	3374	1111	539	1864	4394	928
7	5285	664	3374	1111	539	1864	4394	928	3136	45	299	3854
8	539	1864	4394	928	3136	45	299	3854	1792	855	4484	1659
9	3136	45	299	3854	1792	855	4484	1659	2488	1665	1796	2212
10	1792	855	4484	1659	2488	1665	1796	2212	54	1780	3888	1428
11	2488	1665	1796	2212	54	1780	3888	1428	3472	4277	1013	4325
12	54	1780	3888	1428	3472	4277	1013	4325	1179	3867	556	3561
13	3472	4277	1013	4325	1179	3867	556	3561	5579	3500	3610	5321
14	1179	3867	556	3561	5579	3500	3610	5321	5285	664	3374	1111
15	5579	3500	3610	5321	5285	664	3374	1111	539	1864	4394	928

c. Proses enkripsi dengan Matlab 2013

```
pi=double(gray_img); % Mengambil nilai desimal pixel citra
ci=mod((kunci(x,y)+pi),256); %proses enkripsi
ci=uint8(ci);                % Mengubah nilai decimal ke format warna
figure,imshow(ci);           % Menampilkan cipherimage ke window
```



Gambar 2. citra hasil enkripsi.

d. Proses dekripsi dengan matlab 2013

```
pi=double(gray_img); % Mengambil nilai desimal pixel citra
ci=mod((kunci(x,y)-pi),256); %proses dekripsi
ci=uint8(ci);                % Mengubah nilai decimal ke format warna
figure,imshow(ci);           % Menampilkan cipherimage ke window
```

Gambar 3. Citra hasil dekripsi

3.2 Analisa Ketahanan Kunci

Untuk membuktikan ketahanan kunci, maka akan dibagkitkan sejumlah 50 bilangan dengan menggunakan parameter yang telah diteliti pada kasus di atas, yaitu:
p= 23, q= 251, s=5771, e=21.

Adapun perintah *matlab* 2013 untuk membangkitkan bilangan acak sebanyak 50 buah adalah:

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

for x=1: 50
kunci (x)=mod((s^e),n);
s=kunci(x);
end.

Sehingga diperoleh bilangan acak sebagai berikut:

Kunci ke-i	Kunci ke-i	Kunci ke-i	Kunci ke-i	Kunci ke-i
2232,frekuensi=1	3653,	3089,	2513,	960,frekuensi=1
201,frekuensi=1	frekuensi=1	frekuensi=1	frekuensi=1	2531,frekuensi=1
631,frekuensi=1	645, frekuensi=1	356, frekuensi=1	5724,	5260,frekuensi=1
5590,	1466,	5619,	frekuensi=1	1480,
frekuensi=1	frekuensi=1	frekuensi=1	1009,	frekuensi=1
1311,	3643,	2629,	frekuensi=1	5650,frekuensi=1
frekuensi=1	frekuensi=1	frekuensi=1	892, frekuensi=1	1207,frekuensi=1
3243,	1588,	135, frekuensi=1	3894,	3166,
frekuensi=1	frekuensi=1	157, frekuensi=1	frekuensi=1	frekuensi=1
4251,	3795,	3832,	3917,	4175,
frekuensi=1	frekuensi=1	frekuensi=1	frekuensi=1	frekuensi=1
698, frekuensi=1	3289,	339, frekuensi=1	932, frekuensi=1	5442,
2169,	frekuensi=1	779, frekuensi=1	2486,	frekuensi=1
frekuensi=1	5293,	2766,	frekuensi=1	3559,frekuensi=1
1528,	frekuensi=1	frekuensi=1	2302,	
frekuensi=1	2326,		frekuensi=1	
	frekuensi=1		1640,	
	497, frekuensi=1		frekuensi=1	

Berdasarkan statistik di atas jelas terlihat bahwa frekuensi kemunculan setiap angka adalah sama yaitu 1 artinya tidak ada angka yang berulang, dengan demikian memenuhi untuk point nomor 1. Sekarang untuk menguji poin nomor 2, maka akan diuji dengan mengalisa selisih (hubungan K_i dengan K_{i+1}) setiap kunci, apakah membentuk pola atau tidak. Untuk memprediksi kemunculan angka berikutnya dari bilangan acak yang dibangkitkan, pada umumnya yang dilakukan adalah menghitung jarak antar bilangan acak yang dibangkitkan, kemudian memprediksi relasi antar bilangan, apakah membentuk pola tertentu yang dapat ditulis secara matematika, berikut uraiannya.

3472-4277= naik sejauh 805
4277- 1013= turun sejauh 3264
1013- 4325= naik sejauh 3312
4325-1179= turun sejauh 3146
1179-3867= naik sejauh 2688
3867-556= turun sejauh 3311
556-3561= naik sejauh 3005
3561-5579= naik sejauh 2018
5579-3500= turun sejauh 2079
3500-3610= naik sejauh 110
3610-5321= turun sejauh 1711

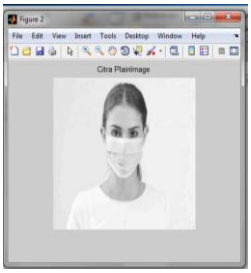
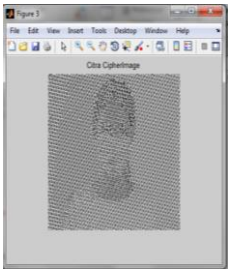
Bila diperhatikan jarak setiap kunci, jelas tidak ada yang sama, selain itu jarak antar kunci juga naik atau turun pada pada periode tertentu dengan jarak yang bervariasi, artinya jarak antar bilangan tidak membentuk pola tertentu, masih sangat sulit mendefeniskan secara matematika, hal ini menunjukkan bahwa masih sangat sulit memprediksi angka-angka selanjutnya, dengan demikian metode ini memenuhi untuk syarat yang kedua. Naik dan turun hubungan antar kunci sama sekali tidak membentuk satu pola.

Pengujian juga dilakukan untuk mendapatkan perbedaan *cipherimage* yang dihasilkan dari proses enkripsi berdasarkan *vegenere cipher* dan modifikasinya, sehingga hasil pengujian sebagai berikut :

Tabel 3. Hasil Pengujian Proses Enkripsi *Vigenere Cipher* dan Modifikasinya

PlainImage	Kunci	*CipherImage*	*MSE*	*PSNR (dB)*	Waktu Proses
Berdasarkan *Vigenere Cipher*					
	kriptografiadalahteknikkeamandatamenerapkanpersamaanmatematika		25281	8,2057	0,324361

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 4, September 2023, Hal 145-151
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i4.4792
Website https://ejurnal.seminar-id.com/index.php/jussi

Size =256 x 256 Berdasarkan Modifikasi *Vigenere Cipher*		*size* = 256 x 256			
	P=59 Q=751 E=61 S=7		63504	0,2056	0, 80746
Size=256 x 256		*Size*= 256 x 256			

Berdasarkan hasil uji coba pada citra yang sama tetapi menggunakan kunci yang berbeda , maka nilai *MSE* dan *PSNR* juga berbeda. Berdasarkan nilai *MSE*, menggunakan nilai p dan q yang lebih besar pada modifikasi *vigenere cipher* terbukti lebih optimal dalam mengamankan citra karena nilasi *MSE* pada modifikasi *vigenere cipher* yaitu 63.504 lebih besar dari pada *MSE vigenere cipher* yaitu 25.281. Sedangkan berdasarkan nilai *PSNR* menggunakan nilai p dan q yang lebih besar pada modifikasi *vigenere cipher* juga lebih optimal dalam mengamankan citra, karena nilai *PSNR* pada modifikasi *vigenere cipher* yaitu 0,2056 lebih kecil dari pada *vigenere cipher* yaitu 8,2057. Tetapi menggunakan nilai p dan q yang lebih besar ternyata membuat waktu proses lebih lama bila dibanding dengan menggunakan nilai p dan q yang lebih kecil

4. KESIMPULAN

Berdasarkan uraian di atas dan juga berdasarkan pengamatan penulis, maka penulis merumuskan kesimpulan penelitian dimana, Penggunaan kunci yang pendek dan karakter yang berulang pada algoritma *vigenere cipher* sangat lemah dan mudah dipecahkan, sehingga masih belum optimal dalam mengamankan data rahasia. Kunci algoritma *vegenere cipher* yang dibangkitkan berdasarkan *CSPRNG* berbasis *RSA* sangat bergantung pada besarnya faktor pembagi (n=p*q) dan sulitnya memfaktor n menjadi p dan q karena p dan q bila difaktorkan harus bilangan prima sehingga sangat sulit dan membutuhkan waktu yang sangat lama untuk dipecahkan. Kunci yang dihasilkan *CSPRNG* berbasis *RSA* sangat acak dan unik khususnya bila panjang kunci sama dengan panjang *plaintext.* Kunci yang dibangkitkan dengan *CSPRNG* berbasis *RSA* tidak memperlihatkan pola antara kunci ke-i dengan kunci ke-i+1 bila diamati dengan persamaan-persamaan deret bilangan yang sederhana. Semakin panjang kunci yang digunakan semakin sulit diserang. *CSPRNG* berbasis *RSA* mampu mengoptimalkan *vigenere cipher* dalam mengamankan citra *digital*, karena *cipherimage* yang dihasilkan sangat berbeda dengan *plainimage.* Sebaiknya digunakan untuk mengamankan data rasio kecil hingga sedang karena perhitungan pembangkit kunci menggunakan angka-angka besar dan memerlukan komputasi yang lebih kompleks.

REFERENCES

[1] Dony Arius. Pengantar Ilmu Kriptografi Teori Analisis Dan Implementasi. Yogyakarta. Penerbit Andi. 2008.
[2] Janner Simarmata dkk. Kriptografi Teknik Keamanan Data Dan Informasi. Yogyakarta. Penerbit Andi. 2019.
[3] Rinaldi Munir.Kriptografi. Bandung. Penerbit Informatika. 2019.
[4] Rifki Sadikin. Kriptografi Untuk Kemanan Jaringan. Yogyakarta. Penerbit Andi. 2012.
[5] T. Zebua, "Encoding the Record Database of Computer Based Test Exam Based on Spritz Algorithm," Lontar Komput. J. Ilm. Teknol. Inf., vol. 9, no. 1, p. 52, 2018.
[6] Efrandi, Asnawati, Yupiyanti. Aplikasi Kriptografi Menggunakan Algoritma Vigenere Cipher. Jurnal Media Infotama Vol.10. 2014.
[7] Irham Mu'alimin, Rusdi Effendi, Boko Susilo. Penerepan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode, Volume III Nomor 1, 2016.
[8] Muhammad Khoiruddin Harahap. Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad. Jurnal Nasional Informatika dan Teknologi Jaringan. E-ISSN:2540-7600.
[9] Mahadi Winafil, Sinar Sinurat, Taronisokhi Zebua. Implementasi Algoritma Advanced Encryption Standart Dan Triple Data Encryption Standart Untuk Mengamankan Citra Digital. Komik. Volume 2, Nomor 1, 2018.
[10] Fadhillah Azmi, Rina Anugrahwaty. Analisis Matriks 5x7 Kriptografi Playfair Cihper. Jurnal dan Penelitian Teknik Informatika, Volume 1 nomor 2. 2017.
[11] Marwan St, Belajar Mudah Matlab Beserta Aplikasinya. Yogyakarta.CV ANDI OFFSET. 2017.