Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

Adopsi Generator Kunci Euler Number dan Pembangkit Kunci Blum Blum Shub untuk Meningkatkan Confidentiality Level pada Extended Vigenere

Eka Ardhianto[1] *, Rara Sriartati Redjeki[2], Edy Supriyanto[3], Hari Murti[4], Eko Nur Wahyudi[5]
[1]Program Studi Teknik Informatika, Universitas Stikubank
[2,3,4]Program Studi Sistem Informasi, Universitas Stikubank
[5]Program Studi Manajemen Informatika, Universitas Stikubank
*ekaardhianto@edu.unisbank.ac.id

Abstrak

Algoritma Vigenere merupakan model algoritma enkripsi yang masih dikembangkan dalam bidang keamanan informasi saat ini. Salah satu aspek yang dianggap penting dalam bidang keamanan informasi adalah kerahasiaan. Masalah pencapaian kerahasiaan pesan atau informasi yang tinggi sangat penting dalam bidang keamanan informasi. Extended Vigenere dikenal sebagai evolusi dari Vigenere yang menerapkan lebih banyak set karakter. Salah satu pengembangan algoritma Vigenere adalah dengan memodifikasi generator kunci yang digunakan. Eksperimen ini bertujuan untuk menguji pengaruh kerahasiaan informasi pada penggunaan generator kunci Blum Blum Shub (BBS) dan nomor Euler yang diterapkan pada Extended Vigenere. Metode pembangkitan kunci BBS dan nomor Euler digunakan secara berurutan. Sebagai sampel digunakan percakapan laporan pengamatan astrnomoner singkat yang dikirim melalui telegram dengan ukuran file 1 KB. Percobaan dilakukan dengan menggunakan panjang kunci yang berbeda, yakni kunci 32-bit, dan kunci 64-bit. Sebagai metrik pengukuran, perhitungan entropi dari keluaran Extended Vigenere digunakan. Hasil yang diperoleh berupa peningkatan kerahasiaan informasi yang signifikan dengan nilai entropy achievement lebih dari 79% dari entropy optimum.

Kata kunci : blum blum shub, euler, extended vigenere, generator kunci.

Abstract

The Vigenere algorithm is an encryption model that is still being developed in the field of information security today. One aspect that is considered important in the field of information security is confidentiality. The problem of achieving high message or information thresholds is very important in the field of information security. Extended Vigenere is known as an evolution of Vigenere that implements more character sets. One of Vigenere's development algorithms is to modify the key generator used. This experiment aims to test the effect of information confidentiality on the use of the Blum Blum Shub (BBS) key generator and the Euler number applied to Extended Vigenere. The BBS key generation method and Euler number are used sequentially. As a sample, short astronomical observation conversations sent via telegram with a file size of 1 KB were used. Experiments were carried out using different key lengths, namely 32-bit keys and 64-bit keys. As a measurement metric, the entropy calculation of the Extended Vigenere output is used. The results obtained are a significant increase in information confidentiality with an entropy achievement value of more than 79% of the optimum entropy

Keywords : *blum blum shub, euler, extended vigenere, key generator*

1. Pendahuluan

Vigenere atau dikenal sebagai Vigenere Cipher dipublikasikan pada tahun 1586 oleh Blaise de Vigenere[1]. Vigenere diklasifikasikan sebagai salah satu produk pada bidang Kriptografi. Kriptografi adalah cabang ilmu yang bertujuan untuk mencari cara mengamankan sebuah informasi asli yang disusun acak dan tidak dapat

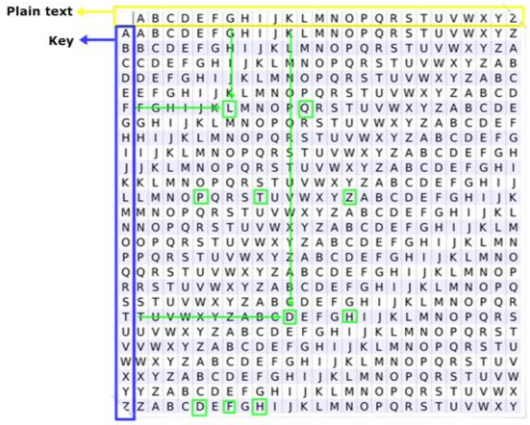
Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

dipahami selain entitas yang berhak menerimanya [2],[3],[4],[5]. Vigenere termasuk sebagai algoritma kriptografi kunci simetris, karena vigenere menggunakan kunci (key) yang sama pada proses enkripsi dan dekripsi [6], [7]. Enkripsi adalah cara untuk membuat data yang terbaca menjadi sulit dikenali, sedangkan dekripsi adalah cara untuk merubah data terenkripsi supaya dapat dibaca dengan mudah [8]. Pesan atau informasi rahasia dalam kriptografi dikenal sebagai plainteks, sedangkan pesan yang telah dirahasiakan dikenal sebagai ciphertetks [9].

Vigenere juga digolongkan sebagai algoritma substitusi polialfabet yang menggunakan pemetaan posisi karakter, dimana setiap karakter ditransformasikan oleh salah satu dari beberapa cipher-shift yang ditentukan dengan kunci (key) [10]. Vigenere pada secara umum digunakan untuk memproses informasi teks, baik dalam pesan yang akan dirahasiakan juga penggunaan kuncinya. Kunci dalam vigenere jika memiliki panjang kurang dari pesan yang akan dirposes, maka kunci tersebut akan digunakan secara berulang sampai teks pesan terproses seluruhnya. Dalam penggunaannya Vigenere mirip seperti penggunaan Caesar dengan mengikuti pergeseran kunci yang disesuaikan untuk mendapatkan karakter cipher. Gambar 1 memperlihatkan tabel Vigenere versi 26 x 26 karakter. Sebagai contoh plainteks: ILIKEGOOGLE, dan kunci: ZFLT. cipherteks yang terbentuk adalah: HQTDDLZHFQP, proses ini diperlihatkan pada tabel 1.



Gambar 1. Contoh ilustrasi proses enkripsi vigenere.

Tabel 1. Contoh Proses Enkripsi Vigenere

Simbol	Urutan Simbol										
	1	2	3	4	5	6	7	8	9	10	11
Plainteks	I	L	I	K	E	G	O	O	G	L	E
Key	Z	F	L	T	Z	F	L	T	Z	F	L
Cipherteks	H	Q	T	D	D	L	Z	H	F	Q	P

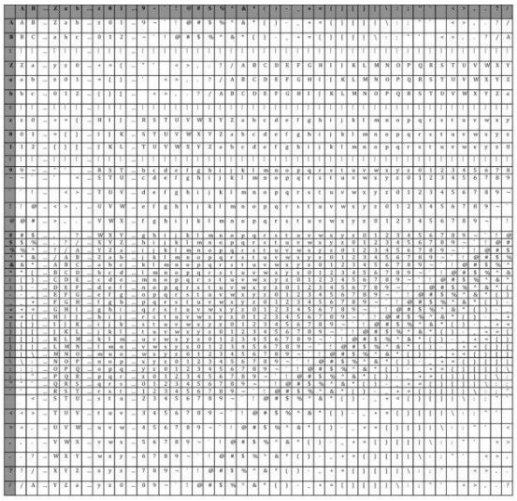
Peningkatan ketahanan algoritma dilakukan dengan memodifikasi dan menggabungkan beberapa algoritma untuk mengamankan pesan. Salah satu bentuk pengembangan Vigenere adalah menambahkan karakter set, dan penggunan teknik pembangkit kunci. Penggunaan tabel vigenere 95 x 95 diperlihatkan pada gambar 2, mampu meningkatkan ketahanan vigenere terhadap percobaan pembobolan. Model Vigenere ini dikenal sebagai Extended Vigenere. Penggunaan tabel yang lebih besar ini mampu menampung jumlah karakter yang lebih banyak dan dapat diaplikasikan secara lebih luas,

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

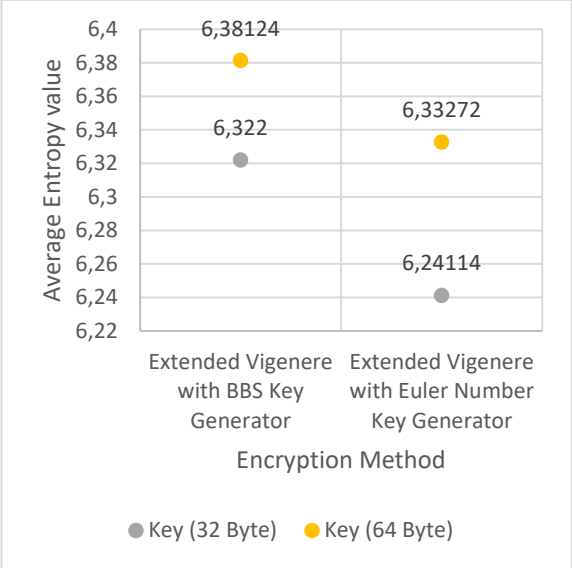
DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

sehingga tidak terbatas hanya pada penggunaan karakter kapital. Pada tabel 95 x 95, susunan karakter dibuat acak tidak berurutan selayaknya kode ASCII, hal ini akan mempersulit pihak yang tidak berhak dalam mengakses pesan tereknripsi.



Gambar 2. Tabel enkripsi extended vigenere.

Kunci vigenere yang lebih pendek dari plainteksnya akan digunakan secara berulang, ini dipandang sebagai suatu kerentanan pada informasi yang diamankan. Beberapa penelitian terkait dengan penerbitan kunci vigenere diantaranya pemanfaatan Bilangan Euler sebagai pembangkit kunci [11]. Bilangan euler yang memiliki untaian unik dimanfaatkan sebagai kunci pada vigenere, sehingga memberikan keacakan informasi dan akan menyulitkan kriptanalis. Pembangkit kunci Blum Blum Shub (BBS) juga diadopsi sebagai pembangkit kunci pada vigenere [12]. Penggunaan penerbitan kunci secara berlapis menghasilkan ketahanan algoritma vigenere yang lebih baik.



Gambar 3. Nilai entropi extended vigenere dengan pembangkit kunci euler, dan pembangkit kunci BBS.

Sebagai preliminari eksperimen, Gambar 3 memperlihatkan hasil eksperimen awal dalam algoritma extended vigenere menggunakan pembangkit kunci BBS , dan extended vigenere menggunakan pembangkit kunci berbasis Bilangan Euler. Sebagai sampel digunakan percakapan laporan pengamatan astrnomoner singkat yang dikirim melalui telegram dengan ukuran file 1 KB. Percobaan dilakukan dengan menggunakan panjang kunci yang berbeda, yakni kunci 32-bit, dan kunci 64-bit. Percobaan dilakukan sebanyak 25 kali untuk setiap model penerbitan kunci dengan sampel yang sama. Dari gambar 3 dapat dijelaskan bahwa penggunaan teknik penerbitan kunci yang berbeda pada extended vigenere akan berimbas pada tingkat keacakan cipherteks. Pada preliminary experiment, diperoleh nilai entropi paling tinggi

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

ialah dengan menggunakan kunci 32-bit dengan entropi 6,38124. Dengan demikian dengan memilih teknik penerbitan kunci yang tepat maka akan berimbas pada meningkatnya keamanan dari ciphertext. Penggunaan mekanisme penerbitan kunci secara berlapis mampu meningkatkan ketahanan algoritma vigenere. Pengukuran ketahanan algoritma vigenere dilakukan dengan menghitung nilai entropi pada cipherteks yang dihasilkan. Entropi merepresentasikan keacakan informasi sebagai pencerminan ketahanan algoritma [13], [14]. Semakin tinggi nilai entropi, maka akan semakin acak informasinya. Sehingga dapat berpengaruh pada ketahanan algoritma.

Berdasarkan preliminari eksperimen yang dilakukan, maka sebagai pertanyaan riset ialah bagaimana pengaruh ketahanan algoritma vigenere dengan menggunakan proses penerbitan kunci berbasis BBS dan Bilangan Euler. Penelitian ini memanfaatkan hasil perhitungan pada pembangkit kunci BBS yang digabungkan dengan pembangkit kunci berbasis Bilangan Euler digunakan sebagai kunci pada vigenere sehingga memberikan ketahanan terhadap informasi yang dirahasiakan.

Artikel ini terbagi menjadi beberapa bagian, pendahuluan disajikan pada bagian awal, bagian kedua berisi tinjauan pustaka, bagian ketiga menjelaskan metode penelitian, hasil dan pembahasan pada seksion 4, dan pada akhir artikel berisi simpulan.

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Berikut merupakan penelitian-penelitian sebelumnya yang terkait dengan penelitian yang diambil oleh peneliti:

- Beberpa penelitian menyebutkan pembangkit blumblum shub memberikan dampak positif dalam pengamanan informasi. Pengamanan objek citra menggunakan algoritma beaufort menjadi lebih optimal saat mengadopsi pembangkit kunci Blum Blum Shub [14], [15]. Blum blum shub juga digunakan sebagai pembangkit kunci pada algoritma RSA yang memberikan dampak keacakan yang lebih rumit sehingga hasil enkripsi lebih sulit untuk ditembus serta memerlukan waktu yang lebih lama [16]. Nihilist cipher yang dipadukan dengan pembangkit kunci BBS memberikan hasil yang lebih kuat pada keacakan sandi, menyembunyikan pola, dan mempersulit penebak melalui proses pemfaktoran [17]. Blum blum shub dimanfaatkan sebagai generator acak pada pengamanan file audio dalam teknik steganografi [18]. Blum blum shub juga digunakan sebagai pembangkit nilai acak pada proses transposisi pesan dalam steganografi audio [19].
- Penelitian terkait pemanfaatan bilangan euler sebagai pembangkit kunci pada pengamanan

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

informasi diterapkan pada algoritma Caesar dengan pembangkit kunci berbasis bilangan euler [20]. Hasil yang diperoleh adalah adanya peningkatan keamanan pesan terhadap teknik analisis frekuensi. Hasil fungsi pembangkit bilangan acak berbasis euler juga digunakan sebagai nilai modulo pada proses enkripsi, hal ini euler dipandang sebagai modul yang mampu menghasilkan angka acak yang unik yang mampu membantu menghasilkan cipherteks yang lebih acak. Euler juga dimanfaatkan pada model enkripsi AES untuk menghasilkan kunci enkripsi, hasil yang diperoleh adalah bentuk keacakan yang lebih sulit ditembus oleh peretas.

- Berdasarkan penelitian sebelumnya, penggunaan bilangan euler dan teknik blum blum shub memberikan dampak yang lebih baik terhadap data yang dirahasiakan. Sehingga dalam artikel ini dilakukan eksperimen untuk menggabungkan keduanya dan melihat dampak yang dihasilkan dari nilai kunci yang dihasilkan terhadap keamanan informasi yang diamankan

2.2. Landasan Teori

1. Keamanan Komputer

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer [21]. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap beberapa aspek keamanan komputer, di antaranya ialah sebagai: 1) Authentication : memastikan bahwa informasi benar-benar asli berasal dari pihak yang dikehendaki. 2) Integrity : memastikan bahwa informasi yang dikirim benar-benar original (tidak dimodifikasi). 3) Confidentiality : merupakan usaha untuk menjaga kerahasiaan informasi. 4) Availability : memastikan ketersediaan informasi.

2. Kriptografi

Kriptografi diartikan sebagai merupakan sebuah cara untuk mengamankan sebuah informasi asli yang disusun acak dan tidak dapat dipahami selain entitas yang berhak menerimanya. Kriptografi melakukan pengamanan data dengan mengubah data menjadi bentuk lain yang tidak ada artinya. Kriptografi dikenal sebagai sebuah bidang ilmu yang berkaitan dengan pengamanan suatu data penting. Kriptografi berasal dari kata Yunani, kryptosyang bermakna rahasia dan graphienyang bermakna tulisan.Tujuan kriptografi ialah membuat data menjadi rahasia dan hanya dapat dibaca oleh orang tertentu saja.

Teknik kriptografi dikenal sebagai enkripsi dan dekripsi. Enkripsi adalah cara untuk membuat data yang terbaca menjadi sulit dikenali, sedangkan dekripsi adalah cara untuk merubah

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

data terenkripsi supaya dapat dibaca dengan mudah.

3. Algoritma Vigenere

Vigenere digolongkan pada cipher substitusi polialphabetik yang dikenalkan oleh Blaise de Vigenere pada tahun 1500 an. Vigenere Cipher adalah metode menyandikan pesan alfabet dengan menggunakan untaianCaesar cipher berdasarkan huruf-huruf pada kata kuncinya.

Vigenere Cipher standar dengan karakter berisi alfabet yang ditulis dalam tabel 26x26, masing-masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi Caesar setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang seperti pada gambar 1. Rumus dari enkripsi dan dekripsi data vigenere cipher adalah:

Enkripsi: Ci = (Pi + Ki) mod 26

Dekripsi: Pi = (Ci –Ki) mod 26; untuk Ci ≥ Ki

Pi = (Ci+ 26 –Ki) mod 26; untuk Ci ≤ Ki

Dalam perkembangannya jumlah karakter set vigenere saat ini diformulasikan untuk mengadopsi jenis karakter yang lebih banyak sesuai dengan karakter yang terkandung pada kode ASCII. Pengembangan ini dikenal sebagai extended vigenere.

4. Pembangkit Kunci Blum Blum Shub

Pembangkit bilangan Blum Blum Shub (BBS) adalah *cryptographically secure pseudorandom number generator* (CSPRNG) yang paling sederhana dan paling mangkus (secara kompleksitas teoritis). BBS dibuat pada tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub .

5. Entropi

Dalam bidang teori informasi, nilai entropi yang tinggi merepresentasikan keacakan yang sebenarnya. Masalah keamanan data yang muncul dari pengaruh entropi yang tidak mencukupi menunjukkan bahwa keacakan yang memadai penting untuk keamanan. Entropi digunakan sebagai ukuran dalam keacakan informasi yang merefelsikan kekuatan sebuah algoritma kriptografi. Semakin tinggi nilai entropi, maka akan semakin acak informasinya. Sehingga dapat berpengaruh pada ketahanan algoritma dari serangan peretas. Untuk mengkalkulasi entropi digunakan persamaan (1).

$$H_m = \sum_{i=0}^{2^n-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (1)$$

3. Metode Penelitian

Pada bagian ini akan dijelaskan research framework (kerangka penelitian), dan usulan model pengembangan extended vigenere dengan adopsi pembangkit kunci blum blum shub dan euler number.

3.1. Kerangka Penelitian

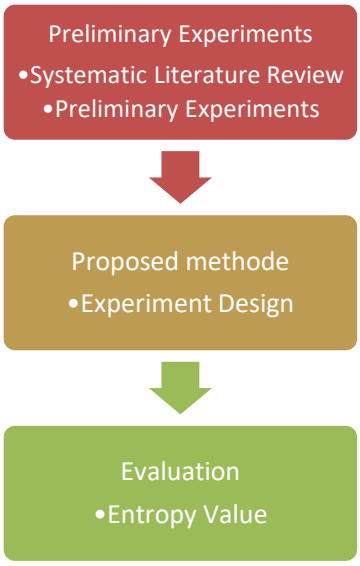
Bagian ini menjelaskan kerangka penelitian eksperimental penggunaan pembangkit kunci berbasis BBS dan Bilangan Euler pada algoritma Extended Vigenere, dan dasar teori kriptografi,

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

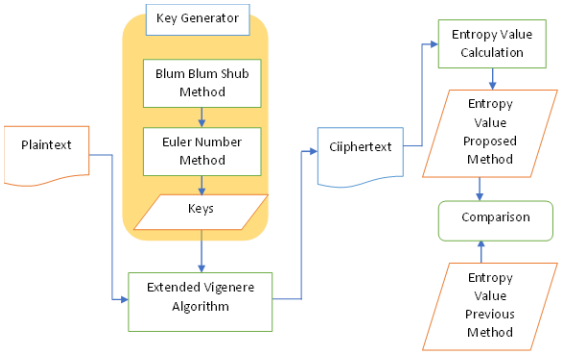
algoritma vigenere, pembangkit kunci BBS, Bilangan Euler, dan entropi. Kerangka penelitian diperlihatkan pada gambar 4. Penelitian yang dilakukan terbagi dalam tiga tahap yaitu: 1) Preliminari Eksperimen, 2) Proposed Method, dan 3) Evaluasi. Tahap preliminary eksperimen dilakukan studi literasi mengenai pembangkit kunci Blum Blum Sub (BBS) dan Bilangan Euler, dan melakukan percobaan awal untuk mendapatkan pemahaman dan bentuk ketahanan algoritma Extended Vigenere.



Gambar 4. Kerangka Penelitian.

3.2. Usulan Model Pembangkit Kunci Baru

Perbedaan model enkripsi extgended vigenere pada proposed model ini adalah penggunaan kunci generator yang menggunakan gabungan metode blum blum shub dan euler number terlihat pada gambar 5. Inputan yang diperlukan pada extended vigenere adalah plainteks dan kunci. Sebagai plainteks digunakan sample dari dataset telegram dataset astronom yang berisi laporan pengamatan astronomi singkat melalui telegram. Sampel yang digunakan berukuran 1KB. Percobaan dilakukan menggunakan 2 kunci yaitu kunci 32 bytes dan kunci 64 bytes. Setiap kunci di cobakan terhadap sampel sebanyak 25 kali. Pembangkitann kunci dilakukan dengan menggunakan metode blum blum shub dan euler number secara berurutan. Proses enkripsi dilakukan menggunakan algoritma extended vigenere. Output yang diperoleh adalah berupa cipherteks. Perhitungan nilai entropi digunakan sebagai metrik performasi dari proposed method. Nilai entropi yang diperoleh dibandingkan dengan nilai entropi pada preliminary eksperimen.



Gambar 5. Usulan Metode Pembangkit Kunci BBS dan Euler Number Extended Vigenere.

4. Hasil dan Pembahasan

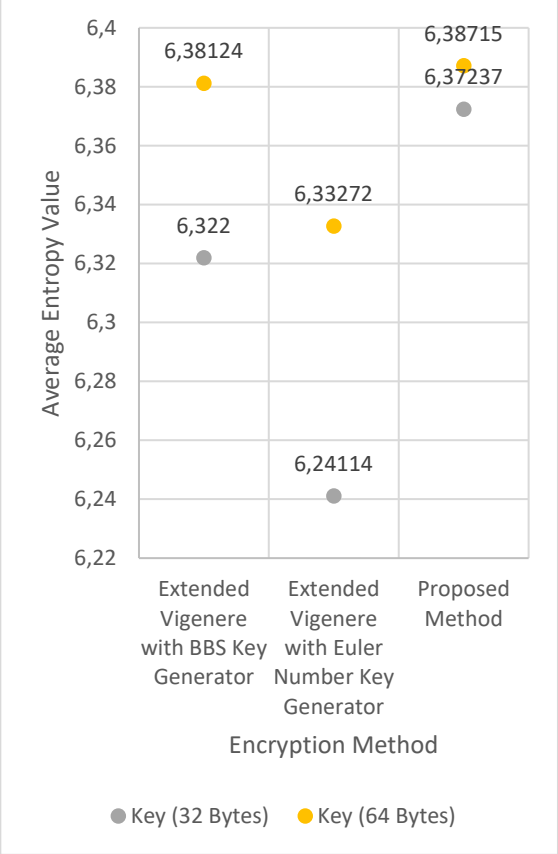
Sebagai sampel plainteks digunakan sampel yang sama seperti pada preliminary eksperimen. Plainteks menggunakan percakapan laporan singkat pengamatan astronomi yang dikirimkan melalui telegram dengan ukuran 1 KB. Percobaan dilakukan sebanyak 25 kali untuk setiap panjang

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

kunci. Dengan demikian terdapat 25 bentuk cipherteks yang dihitung rata rata nilai entropi. Gambar 6 memperlihatkan hasil perhitungan nilai entropi rata rata eksperimen yang dibandingkan dengan nilai rata rata entropi pada preliminary eksperimen.



Gambar 6. Nilai Entropi Hasil Eksperimen.

Gambar 6 memperlihatkan hasil eksperimen pada Extended Vigenere dengan pembangkit kunci BBS dan Bilangan Euler menunjukkan peningkatan nilai rata rata entropi yaitu 6,38715 untuk penggunaan panjang kunci 64 byte, dan 6,37237 untuk panjang kunci 32 byte. Jika dibandingkan dengan eksperimen sebelumnya, Extended vigenere dengan pembangkit kunci bilangan euler menunjukkan nilai rata rata entropi 6,33272 dan 6,24114 untuk panjang kunci 64-byte dan 32-byte. Sedangkan Extended Vigenere dengan pembangkit kunci BBS menunjukkan nilai rata rata entropi 6,38124 dan 6,322 untuk panjang kunci 64-byte dan 32-byte.

Tabel 2. Capaian entropi hasil eksperimen.

Performansi	Kunci 32 Byte		Kunci 64 Byte	
	Entropi	%	Entropi	%
Extended Vigenere dengan pembangkit Kunci BBS	6,322	79,03%	6,38124	79,77%
Extended Vigenere dengan pembangkit Kunci Euler Number	6,24114	78,01%	6,33272	79,77%
Usulan Pembangkit Kunci Baru (hasil eksperimen)	6,37237	79,65%	6,38715	79,84%

Tabel 2 memperlihatkan grafik capaian nilai entropi rata rata terhadap nilai entropi optimum. Tabel 2 menunjukkan nilai capaian rata rata entropi pada Extended Vigenere dengan pembangkit kunci BBS dan Euler sebesar 79,65% dan 79,84%. Eksperimen sebelumnya yaitu Extended Vigenere dengan pembangkit kunci bilangan euler memiliki capaian rata rata entropi sebesar 78,01% dan 79,77%, dan Extenden Vigenere dengan pembangkit kunci BBS

Infotek : Jurnal Informatika dan Teknologi
Vol. 7 No. 1, Januari 2024
Hal.1-11

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

menunjukkan nilai capaian rata rata entropi sebesar 79,03% dan 79,77%.

Capaian dari model Extended Vigenere dengan pembangkit kunci BBS dan Euler secara kuantitatif menunjukkan peningkatan yang berarti. Perhitungan secara statistic dilakukan menggunakan metode Mann Withney menunjukkan hasil yang siginfikan antara Extended Vigenere dalam enksperimen ini dibandingkan Extended Vigenere dengan eksperimen sebelumnya. Pengujian menunjukkan nilai-z adalah -5.39649 < dari nilai-p yaitu 0.00001 dengan tingkat signifikansi 0.05.

Berdasarkan hasil eksperimen terhadap algoritma extended vigenere dan pengujian signifikansi yang diperoleh, maka penggunaan pembangkit kunci BBS dan Euler memberikan peningkatan ketahanan algoritma Extended Vigenere sehingga informasi yang diamankan menjadi lebih sulit untuk diretas

5. Kesimpulan

Berdasar hasil eksperimen dan pembahasan pada bagian sebelumnya, maka dapat disimpulkan bahwa ketahanan algoritma Extended Vigenere mejadi lebih kuat dengan menggunakan proses penerbitan kunci berbasis BBS dan Bilangan Euler dibandingkan dengan menggunakan penerbitan kunci yang dilakukan menggunakan BBS atau Bilangan Euler saja. Dengan peningkatan nilai entropi sebesar 6,38715 dengan capaian 79,84% pada panjang kunci 64-byte, dan nilai entropi sebesar 6,37237 dengan capaian 79,65%.

Sebagai eksperimen lebih lanjut, perlu adanya pendalaman lebih lanjut mengenai pencarian model pembangkitan kunci yang sesuai supaya ketahanan Algoritma Extended Vigenere memiliki ketahanan yang lebih baik

6. Daftar Pustaka

[1] D. Rachmawati, A. Sharif, and R. Sianipar, “A combination of vigenere algorithm and one time pad algorithm in the three-pass protocol,” in *The 3rd Annual Applied Science and Engineering Conference (AASEC 2018)*, A. G. Abdullah and A. B. D. Nandiyanto, Eds., MATEC Web Conf, Sep. 2018, pp. 1–4. doi: 10.1051/matecconf/201819703008.

[2] K. Nahar and P. Chakraborty, “A Modified Version of Vigenere Cipher using 95×95 Table,” *International Journal of Engineering & Advanced Technology (IJEAT)*, vol. 9, no. 5, pp. 1144–1148, 2020, doi: 10.35940/ijeat.E9941.069520.

[3] K. Limniotis, “Cryptography as the Means to Protect Fundamental Human Rights,” *Cryptography*, vol. 5, no. 4, p. 34, Nov. 2021, doi: 10.3390/cryptography5040034.

[4] S. Rubinstein-Salzedo, “The Vigenère Cipher,” in *Cryptography*, Springer, Cham, 2018, pp. 41–54. doi: 10.1007/978-3-319-94818-8_5.

[5] E. Ardhianto, A. Trisetyarso, W. Suparta, B. S. Abbas, and C. H. Kang, “Design Securing Online Payment Transactions Using Stegblock Through Network Layers,” *IOP Conf Ser Mater Sci Eng*, vol. 879, no. 1, p. 012027, Jul. 2020, doi: 10.1088/1757-899X/879/1/012027.

[6] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, “An Enhanced Cipher Technique Using Vigenere and Modified

e-ISSN 2614-8773
DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

Caesar Cipher," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India: IEEE, May 2018, pp. 1–9. doi: 10.1109/ICOEI.2018.8553910.

[7] E. Ardhianto, W. T. Handoko, E. Supriyanto, and H. Murti, "Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi," *JURNAL INFORMATIKA UPGRIS*, vol. 7, no. 2, pp. 23–27, 2021.

[8] E. Lestariningsih, E. Ardhianto, W. Tri Handoko, and J. Tri Lomba Juang No, "ADOPSI PEMBANGKIT KUNCI EXTENDED VIGENERE MENGGUNAKAN FUNGSI RANDOM DAN BLUM BLUM SHUB," *Jurnal Informatika & Rekayasa Elektronika)*, vol. 5, no. 2, pp. 263–271, 2022, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

[9] J. Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *International Journal of Information System & Technology Akreditasi*, vol. 4, no. 1, pp. 471–481, 2020.

[10] S. Park, J. Kim, K. Cho, and D. H. Yum, "Finding the key length of a Vigenère cipher: How to improve the twist algorithm," *Cryptologia*, vol. 44, no. 3, pp. 197–204, May 2020, doi: 10.1080/01611194.2019.1657202.

[11] N. Nofiyanto, hamzah Hamzah, and H. Surbakti, "SHORT MESSAGE ENCRYPTION APPLICATION DEVELOPMENT USING VIGENERE ALGORITHM UTILIZING EULER'S NUMBER ON ANDROID SMARTPHONE," *Jurnal Teknologi Informasi* , vol. 9, no. 27, pp. 81–92, 2014.

[12] F. Telaumbanua and T. Zebua, "Modifikasi Vigenere Cipher Dengan Pembangkit Kunci Blum Blum Shub," *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 4, no. 1, 2020, doi: 10.30865/komik.v4i1.2646.

[13] K. Chanda, "Password Security: An Analysis of Password Strengths and Vulnerabilities," *International Journal of Computer Network and Information Security*, vol. 8, no. 7, pp. 23–30, Jul. 2016, doi: 10.5815/ijcnis.2016.07.04.

[14] P. Patil, P. Narayankar, Narayan D.G., and Meena S.M., "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput Sci*, vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[15] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *Journal of the Operations Research Society of China*, 2020, doi: 10.1007/s40305-020-00320-x.

[16] A. Vassilev and R. Staples, "Entropy as a Service: Unlocking Cryptography's Full Potential," *Computer (Long Beach Calif)*, vol. 49, no. 9, pp. 98–102, Sep. 2016, doi: 10.1109/MC.2016.275.

[17] A. J. P. Delima and J. C. T. Arroyo, "An Enhanced Nihilist Cipher Using Blum Blum Shub Algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 3270–3274, 2020.

[18] E. W. Abood, Z. A. Abduljabbar, M. A. Al Sibahee, M. A. Hussain, and Z. A. Hussien, "Securing audio transmission based on encoding and steganography," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 3, pp. 1777–1786, 2021.

[19] M. T. Elkandoz and W. Alexan, "Logistic Tan Map Based Audio Steganography," in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, IEEE, Nov. 2019, pp. 1–5. doi: 10.1109/ICECTA48151.2019.8959683.

[20] R. Mishra and Dr. J. K. Mantri, "An Enhancement to Caesar Cipher using Euler Totient Function," *Int J Eng Adv Technol*, vol. 11, no. 3, pp. 46–50, Feb. 2022, doi: 10.35940/ijeat.C3363.0211322.

e-ISSN 2614-8773

DOI : 10.29408/jit.v7i1.21512 Link : https://dx.doi.org/10.29408/jit.v7i1.21512

[21] Muh. A. J. Hidayat and H. M. Putra, "Sistem Keamanan Server Linux CentOS Dengan Metode Port Knock dan RST Cookies," *Infotek : Jurnal Informatika dan Teknologi*, vol. 6, no. 2, pp. 411–420, Jul. 2023, doi: 10.29408/jit.v6i2.17500.