Tur_Adopsi Pembangkit Kunci Blum Blum Shub Dan Bilangan Euler Pada

by WT Handoko

Submission date: 28-Oct-2023 07:45AM (UTC+0700)
Submission ID: 2208737393
File name: opsi_Pembangkit_Kunci_Blum_Blum_Shub_Dan_Bilangan_Euler_Pada.pdf (379.88K)
Word count: 3240
Character count: 20088

Terakreditasi SINTA Peringkat 3
Surat Keputusan Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi Nomor 225/E/KPT/2022
masa berlaku mulai Vol.7 No. 1 tahun 2022 s.d Vol. 11 No. 2 tahun 2026

Terbit online pada laman web jurnal:
http://publishing-widyagama.ac.id/ejournal-v2/index.php/jointecs

JOINTECS
Vol. 8 No. 2 (2023) 41 - 48

JOINTECS
(Journal of Information Technology and Computer Science)
e-ISSN:2541-6448 p-ISSN:2541-3619

Adopsi Pembangkit Kunci Blum Blum Shub Dan Bilangan Euler Pada Algoritma Extended Vigenere

Eka Ardhianto[1*], Widiyanto Tri Handoko[2], Endang Lestariningsih[3], Felix Andreas Sutanto[4]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri,
Universitas Stikubank
[1*]ekaardhianto@edu.unisbank.ac.id, [2]wthandoko@edu.unisbank.ac.id,
[3]endanglestariningsih@edu.unisbank.ac.id, [4]felix@edu.unisbank.ac.id

Abstract

The Vigenere algorithm is an encryption algorithm model which is still being developed in the field of information security today. One aspect that is considered important in the field information security is confidentiality. The problem of achieving high confidentiality of messages or information is critical in the field of information security. Extended Vigenere is known as an evolution of Vigenere which applies a wider number of character sets. One of the developments in the Vigenere algorithm is to modify the key generator used. This experiment aims to examine the effect of confidentiality of information 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 measurement metric, the entropy calculation of the Extended Vigenere output is used. The results obtained are in the form of a significant increase in information confidentiality with an entropy achievement value of more than 79% of the optimum entropy.

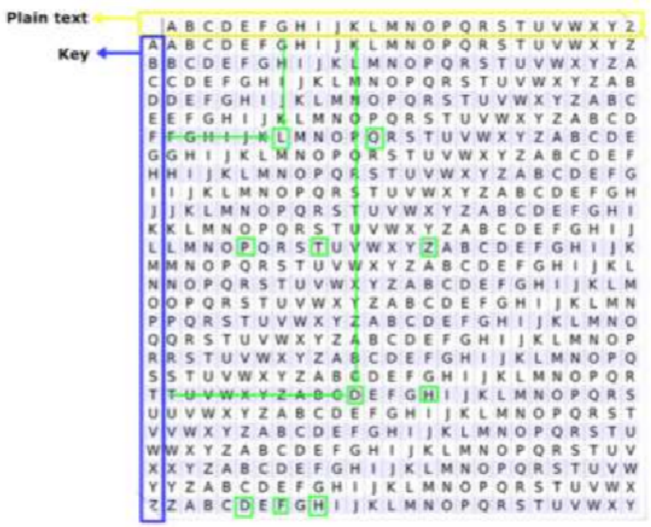
Keywords: Vigenere; BBS; Euler; Key; Extended Vigenere.

Abstrak

Algoritma Vigenere merupakan model algoritma enkripsi yang sampai saat ini masih dikembangkan dalam bidang keamanan infromasi sampai saat ini. Salah satu aspek yang dipandang penting dalam bidang keamanan informasi adalah confidentiality. Permasalahan pencapaian confidentiality pesan atau informasi yang tinggi menjadi sesuatu yang kritis dalam bidang pengamanan informasi. Extended Vigenere dikenal sebagai evolusi Vigenere yang menggaplikasikan jumlah karakter set yang lebih luas. Salah satu pengembangan dalam algoritma Vigenere adalah dengan memodifikasi pembangkit kunci yang digunakan. Eksperimen ini bertujuan untuk melihat pengaruh confidentiality informasi terhadap penggunaan pembangkit kunci Blum Blum Shub (BBS) dan Bilangan Euler yang diaplikasikan pada Extended Vigenere. Metode pembangkit kunci BBS dan Bilangan Euler digunakan secara berurutan. Sebagai metrik pengukuran digunakan perhitungan entropi terhadap output Extended Vigenere. Hasil yang diperoleh ialah berupa peningkatan confidentiality informasi yang signifikan dengan nilai capaian entropi lebih dari 79% terhadap entropi optimum.

Kata kunci: Vigenere; BBS; Euler; Kunci; Extended Vigenere.

Diterima Redaksi : 22-12-2022 | Selesai Revisi : 11-06-2023 | Diterbitkan Online : 01-07-2023



Gambar 1. Tabel Enkripsi Vigenere 26 x 26.

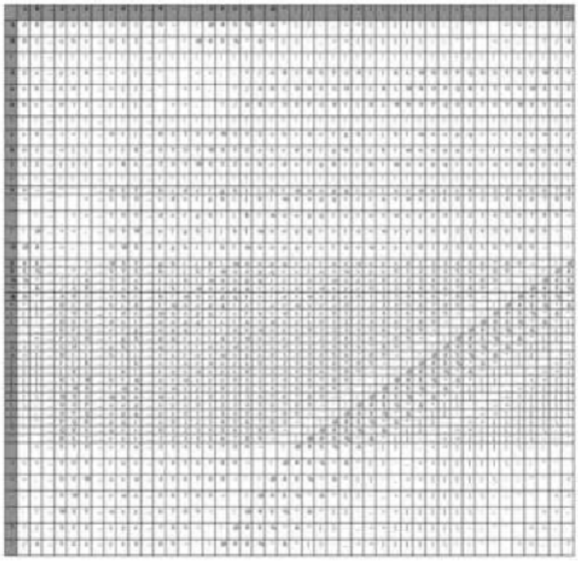
1. Pendahuluan

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 dipahami selain entitas yang berhak menerimanya [2]–[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 [1]. Kunci dalam vigenere jika memiliki panjang kurang dari pesan yang akan dirposes, maka kunci tersebut akan digunakan secara berulang sampai teks pesan terproses seluruhnya [1]. 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.

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 [7]. Penggunaan tabel vigenere 95 x 95 diperlihatkan pada Gambar 2, mampu meningkatkan ketahanan vigenere terhadap percobaan pembobolan [2]. 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, 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.

Kunci vigenere yang lebih pendek dari plainteksnya akan digunakan secara berulang, ini dipandang sebagai suatu kerentanan pada informasi yang diamankan [7]. 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 [8]. Sebagai preliminari eksperimen, Gambar 3 memperlihatkan hasil eksperimen awal dalam algoritma



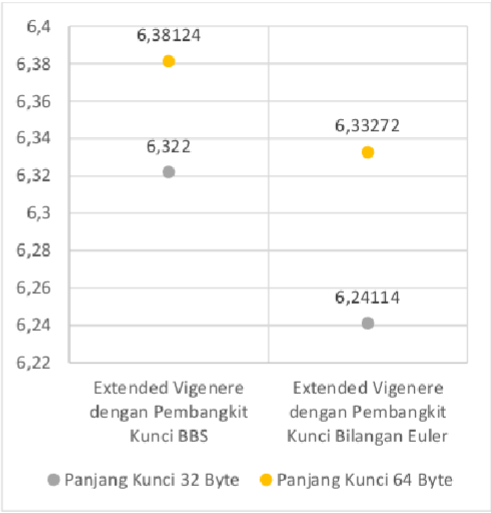
Gambar 2. Tabel Extended Vigenere 95 x 95.

extended vigenere menggunakan pembangkit kunci BBS [12], dan extended vigenere menggunakan pembangkit kunci berbasis Bilangan Euler [11]. 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 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.

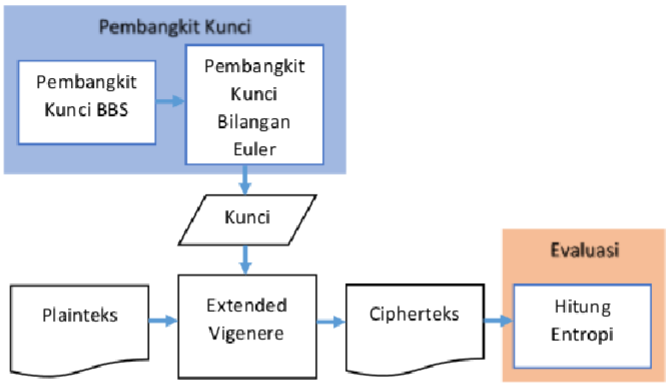
Penggunaan mekanisme penerbitan kunci secara berlapis mampu meningkatkan ketahanan algoritma vigenere. Pengukuran ketahanan algoritma vigenere dilakukan dengan menghitung nilai entropi pada cipherteks yang dihasilkan. Entropi merepresentasikan keacakan informasi sebagai pencerminan ketahanan algoritma [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. Tujuan penelitian ini adalah untuk melihat pengaruh *confidentiality* informasi terhadap penggunaan pembangkit kunci Blum Blum Shub (BBS) dan Bilangan Euler yang diaplikasikan pada Extended Vigenere secara berurutan.

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.



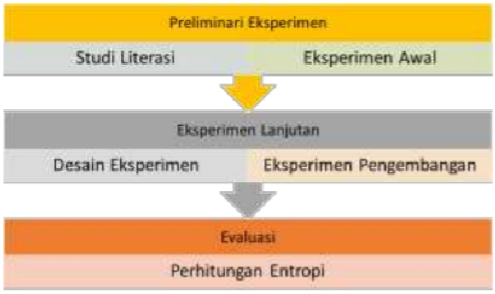
Gambar 3. Nilai Entropi rata rata preliminary eksperimen.



Gambar 5. Desain Penelitian Algoritma Extended Vigenere dengan Pembangkit Kunci BBS dan Bilangan Euler.

2. Metode Penelitian

Bagian ini menjelaskan kerangka penelitian eksperimental penggunaan pembangkit kunci berbasis BBS dan Bilangan Euler pada algoritma Extended Vigenere, dan dasar teori kriptografi, algoritma vigenere, pembangkit kunci BBS, Bilangan Euler, dan entropi. Kerangka penelitian diperlihatkan pada Gambar 4.

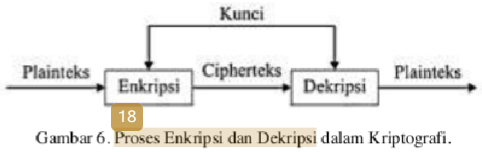


Gambar 4. Kerangka Penelitian.

Penelitian yang dilakukan terbagi dalam tiga tahap yaitu: 1) Preliminari Eksperimen, 2) Eksperimen Lanjutan, dan 3) Evaluasi. Tahap preliminary eksperimen dilakukan studi literasi mengenai pembangkit kunci Blum Blum Sub dan Bilangan Euler, dan melakukan percobaan awal untuk mendapatkan pemahaman dan bentuk ketahanan algoritma Extended Vigenere. Pada eksperimen lanjutan dilakukan pembuatan desain penelitian dengan memodifikasi algoritma extended vigenere dengan pembangkit kunci berbasis BBS dan Bilangan Euler. Pada eksperimen lanjutan dilakukan percobaan dengan sampel teks yang sama pada saat melakukan eksperimen awal. Gambar 5 memperlihatkan desain extended vigenere dengan pembangkit kunci berbasis BBS dan Bilangan Euler. Jumlah eksperimen lanjutkan dilakukan sebanyak 25 kali untuk setiap sampel. Pada bagian Evaluasi dilakukan perhitungan nilai entropi rata rata dari cipherteks yang dihasilkan.

2.1. Kriptografi Kunci Simetris

Algoritma enkripsi simetri adalah algoritma kriptografi klasik yang kuncinya sama untuk pada proses enkripsi dan deskripsi, seperti terlihat pada Gambar 6. Suatu plainteks dienkripsi menggunakan suatu kunci menghasilkan suatu cipherteks. Cipherteks didekripsi menggunakan kunci yang sama untuk menghasilkan plainteks. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Dimana pada algoritma aliran, proses penyandiannya akan beriorientasi pada satu bit/byte data. Sedangkan pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit/byte data (per blok).



Gambar 6. Proses Enkripsi dan Dekripsi dalam Kriptografi.

2.2. Algoritma Vigenere

Vigenere digolongkan pada cipher substitusi polialphabetik yang dikenalkan oleh Blaise de Vigenere pada tahun 1500-an [15]. Vigenere Cipher adalah metode penyandian pesan alfabet dengan menggunakan untaian Caesar cipher berdasarkan huruf-huruf pada kata kuncinya seperti pada Gambar 1.

Vigenere Cipher versi standar menggunakan karakter isi 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 seperti persamaan (1), (2), dan (3). *Ci*

Gambar 7. Entropi rata rata Extended Vigenere dengan pembangkit kunci BBS dan Bilangan Euler.

adalah cipherteks, plainteks dilambangkan dengan **Pi**, dan kunci yang digunakan adalah sebagai ***Ki***. Operasi modulo dilambangkan dengan *mod*.

Proses Enkripsi:

$$Ci = (Pi + Ki)\ mod\ 26 \quad (1)$$

Proses Dekripsi:

$$Pi = (Ci - Ki)\ mod\ 26;\ untuk\ Ci \geq Ki \quad (2)$$

$$Pi = (Ci + 26 - Ki)\ mod\ 26;\ untuk\ Ci \leq Ki \quad (3)$$

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

2.3. Pembangkit Kunci Blum Blum Shub

Pembangkit bilangan Blum Blum Shub (BBS) adalah yptographically Secure Pseudorandom Number enerator (CSPRNG) yang paling sederhana dan ling mangkus (secara kompleksitas teoritis). BBS dibuat pada tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub [8], [12]. Persamaan (4) yang digunakan pada BBS.

$$Xi + 1 = Xi2\ Mod\ M \quad (4)$$

2.4. 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 [16]. Entropi digunakan sebagai ukuran dalam keacakan informasi yang merefleksikan kekuatan sebuah algoritma kriptografi [13], [14], [16]. Semakin tinggi nilai entropi, maka akan semakin acak informasinya. Sehingga dapat berpengaruh pada ketahanan algoritma dari serangan peretas. Untuk mengkalkulasi entropi digunakan persamaan (5).

$$H_m = \sum_{i=0}^{2^n-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (5)$$

3. 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 kunci. Dengan demikian terdapat 25 bentuk cipherteks yang dihitung rata rata nilai entropi. Gambar 7 memperlihatkan hasil perhitungan nilai entropi rata rata eksperimen yang dibandingkan dengan nilai rata rata entropi pada preliminary eksperimen.

Tabel 1. Capaian Nilai Rata-rata Entropi terhadap Nilali Entropi Optimal.

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

Pada eksperimen awal (*preliminary experiment*), eksperimen dilakukan dengan membandingkan penggunaan Extended Vigenere menggunakan pembangkit kunci BBS, dan Extended Vigenere menggunakan pembangkit kunci Bilangan Euler. Pada Extended Vigenere menggunakan pembangkit kunci BBS diperoleh nilai rata-rata entopi 6,322 untuk panjang kunci 32-byte, dan 6,38124 untuk penjang kunci 64-byte. Pada eksperimen Extended Vigenere yang menggunakan pembangkit kunci Bilangan Euler memperlihatkan nilai rata-rata entropi 6,24114 untuk panjang kunci 32-byte, dan 6,33272 untuk panjang kunci 64-byte.

Eksperimen lanjutan 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 1 memperlihatkan 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 menunjukkan nilai capaian rata rata entropi sebesar79,03% 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. Dengan demikian penggunaan pembangkit kunci BBS dan Euler memberikan peningkatan ketahanan algoritma Extended Vigenere sehingga informasi yang diamankan menjadi lebih hsulit untuk diretas.

4. 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.

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), Sep. 2018, pp. 1–4. doi: 10.1051/matecconf/201819703008.

[2] Nahar and P. Chakraborty, "A Modified ersion of Vigenere Cipher using 95×95 Table," International Journal of Engineering & Advanced echnology (IJEAT), vol. 9, no. 5, pp. 1144–48, 2020, doi: 10.35940/ijeat.E9941.069520.

[3] K. Limniotis, "Cryptography as the Means to otect 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," in IOP Conference Series: Materials Science and Engineering, Aug. 2020, vol. 879, no. 1. 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 Caesar Cipher," in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 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. 21 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] 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] B. Barmawi, M. Mira, R. Budiharjo and K. Ramdani, "Implementation of Vigenere Cipher with Euler Key Generator to Secure Text Document," Faculty of Industrial Technology International Congress International Conference, Oct. 2018, pp 9-11.

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

[13] E. Simon, "Entropy and Randomness: Form Analogic to Quantum World", IEEE Access, vol 8, pp. 74553-74561, Apr. 2020, doi: 1109/ACCESS.2020.2988658.

[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] E. Vidya and R. Rathipriya, Key Generation for DNA Cryptography Using Genetic Operators and Diffie-Helman Key Exchange Algorithm", International Journal of Mathematic Computer Science, vol. 15, no. 4, pp. 1109-1115, 2020.

[16] F. Grasseli, G. Murta, H. Kampermann and D. Brub, "Entropy Bounds for Multiparty Device-Independent Cryptography", PRX Quantum, vol. 2, pp. 010308(1) - 010308(36), 2021, doi. 10.1103/PRXQuantum.2.010308.

Halaman ini sengaja dikosongkan

Tur_Adopsi Pembangkit Kunci Blum Blum Shub Dan Bilangan Euler Pada

ORIGINALITY REPORT

19%	17%	12%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pdfs.semanticscholar.org Internet Source	7%
2	ojs.htp.ac.id Internet Source	3%
3	www.researchgate.net Internet Source	1%
4	docplayer.info Internet Source	1%
5	ejournal.unib.ac.id Internet Source	1%
6	www.unisbank.ac.id Internet Source	1%
7	Muon Ha, Duc-Manh Tran, Yulia Shichkina. "Model of Message Transmission across Parallel Route Groups with Dynamic Alternation of These Groups in a Multichannel Steganographic System", Electronics, 2023 Publication	1%

8	journal.uniku.ac.id Internet Source	1%
9	Paulo Henrique Alves, Fernando Correia, Isabella Frajhof, Clarisse Sieckenius De Souza, Helio Lopes. "Designing Intelligent Agents in Normative Systems Toward Data Regulation Representation", IEEE Access, 2023 Publication	<1%
10	eprints.polsri.ac.id Internet Source	<1%
11	Antonius Cahya Prihandoko, Dafik Dafik, Ika Hesti Agustin. "Stream-keys generation based on graph labeling for strengthening Vigenere encryption", International Journal of Electrical and Computer Engineering (IJECE), 2022 Publication	<1%
12	pen.ius.edu.ba Internet Source	<1%
13	Rahma Isnaini Masya, Rizal Fathoni Aji, Setiadi Yazid. "Comparison of Vigenere Cipher and Affine Cipher in Three-pass Protocol for Securing Image", 2020 6th International Conference on Science and Technology (ICST), 2020 Publication	<1%
14	etd.repository.ugm.ac.id Internet Source	<1%

15	mafiadoc.com Internet Source	<1%
16	wrap.warwick.ac.uk Internet Source	<1%
17	www.scribd.com Internet Source	<1%
18	Submitted to Universitas Brawijaya Student Paper	<1%
19	ejournal.akakom.ac.id Internet Source	<1%
20	ejournal.gunadarma.ac.id Internet Source	<1%
21	www.ejurnal.stmik-budidarma.ac.id Internet Source	<1%
22	Aso Ahmed Majeed, Banaz Anwer Qader. "An improved vigener algorithm based on circular-left-shift key and MSB binary for data security", Indonesian Journal of Electrical Engineering and Computer Science, 2021 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		