ADOPSI PEMBANGKIT KUNCI EXTENDED VIGENERE MENGGUNAKAN FUNGSI RANDOM DAN BLUM BLUM SHUB

by Endang Lestariningsih

Submission date: 05-Jan-2023 09:03AM (UTC+0700)
Submission ID: 1988692750
File name: 1_ADOPSI_PEMBANGKIT_KUNCI_EXTENDED.pdf (1.36M)
Word count: 3373
Character count: 20822

ADOPSI PEMBANGKIT KUNCI EXTENDED VIGENERE MENGGUNAKAN FUNGSI RANDOM DAN BLUM BLUM SHUB

Endang Lestariningsih[1], Eka Ardhianto[2], Widiyanto Tri Handoko[3]

[123,]Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank

Jln. Tri Lomba Juang No.1 Semarang
[1]endanglestariningsih@edu.unisbank.ac.id, [2]ekaardhianto@edu.unisbank.ac.id,
[3]wthandoko@edu.unisbank.ac.id

Abstract

The existence of database technology provides many advantages in exchanging, sending and storing information. However, data stored in the cloud in plain third parties will be easily hacked and read by unauthorized parties. Using cryptographic techniques will help keep the data secret so that it will be more secure. However, many algorithms have been hacked, so it is necessary to modify and develop a cryptographic algorithm. One of the classic algorithms that is still being developed today is vigenere. By choosing the right key, the information that Vigenere says will become stronger. This experiment aims to strengthen vigenere by adopting a layered key selection process. In addition to using the random function, the use of blum blum shub is also added. Entropy is used as a performance metric. The results obtained are an increase in the achievement of information security by more than 80% with a better entropy value than before.

Keywords : *vigenere, key, key selection, entropy.*

Abstrak

Keberadaan teknologi basis data memberikan banyak keuntungan dalam melakukan pertukaran, pengiriman dan penyimpanan informasi. Meskipun demikian, data yang disimpan secara awan ditempat pihak ketiga secara polos akan dengan mudah untuk diretas dan dibaca oleh pihak yang tidak berwenang. Dengan menggunakan teknik kriptografi akan membantu merahasikan data tersebut sehingga akan menjadi lebih aman. Namun banyak algoritma yang telah diretas, sehingga perlu adanya modifikasi dan pengembangan yang dilakukan pada sebuah algoritma kriptografi. Salah satu algoritma klasik yang masih dikembangkan sampai saat ini ialah vigenere. Dengan melakukan pemilihan kunci yang tepat, maka informasi yang diamakan oleh vigenere akan mejadi lebih kuat. Eksperimen ini bertujuan untuk memperkuat vigenere dengan mengadopsi proses pemilihan kunci yang berlapis. Selain menggunaka fungsi random juga ditambahkan penggunaan blum blum shub. Sebagai metrik performasi digunakan entropi. Hasil yang diperoleh ialah peningkatan capaian ketahanan informas hingga lebih dari 80% dengan nilai entropi yang lebih baik dari sebelumnya.

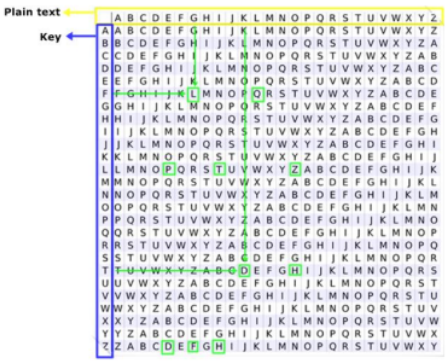
Kata kunci : *vigenere, kunci, pemilihan kunci, entropi.*

1. PENDAHULUAN

Selama lebih dari satu dekade, inovasi teknologi basis data telah banyak membantu dalam penyediaan data yang cepat dan mudah. Data dapat berasal dari perangkat apa saja yang terkoneksi dengan jaringan, seperti pengguna server, perangkat komunikasi, satelit, sensor pada berbagai perangkat IoT dapat disimpan pada sebuah lokasi awan. Keberadaan teknologi ini seperti dua sisi mata pisau, selain memiliki keuntungan didalamnya juga memiliki hal hal yang menjadi kerugiannya. Data yang tersimpan pada perangkat awan memiliki kemungkinan untuk dibuka, dianalisa bahkan diretas oleh orang lain. Oleh karena itu, masalah keamanan data

merupakan tantangan besar karena data disimpan di pihak ketiga dan ancaman terbesar terjadi ketika pengguna menyimpan datanya dalam bentuk yang jelas [1]. Sehingga suatu privasi informasi menjadi pertimbangan penting.

Kriptografi dikenal sebagai sebuah bidang ilmu yang berkaitan dengan pengamanan suatu data penting [2]. Kriptografi berasal dari kata Yunani, *kryptos* yang bermakna rahasia dan *graphien* yang bermakna tulisan [3]. Tujuan kriptografi ialah membuat data menjadi rahasia dan hanya dapat dibaca oleh orang tertentu saja [4]–[7]. Teknik kriptografi dikenal sebagai enkripsi dan dekripsi. 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]–[11].

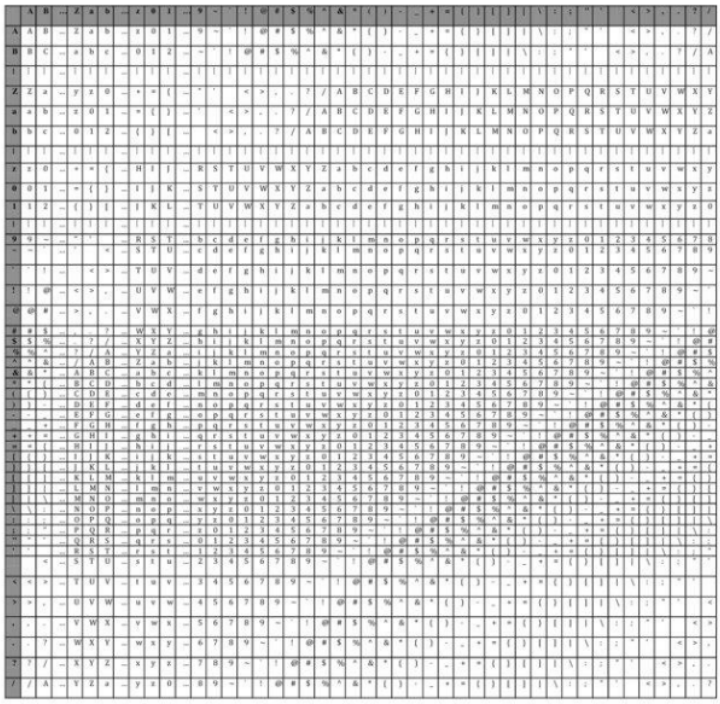


Gambar 1. Proses Enkripsi Vigenere.

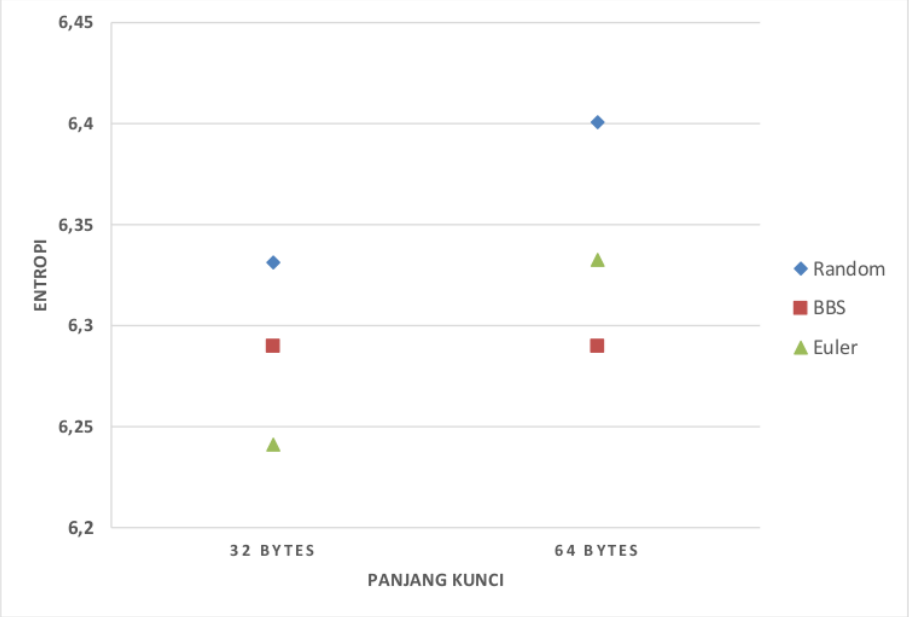
Sebuah teknik enkripsi klasik yang masih dikembangkan sampai saat ini ialah algoritma vigenere [12]. Vigenere dikenalkan pada abad ke-15 yang pada mulanya digunakan utnuk mengamankan data berbasis teks. [13] Vigenere merupakan cipher substitusi polialfabet yang menggunakan pemetaan posisi simbol karakter, dimana setiap simbol ditransformasikan oleh salah satu dari beberapa *cipher-shift* yang ditentukan dengan kunci (*key*) [14]. Penggunaan kunci pada vigenere dilakukan secara berulang hingga karakter akhir dienkripsi. Penggunaan ini sama seperti cipher Caesar dengan pergeseran simbol yang beberda seperti diilustrasikan pada gambar 1. Sebagai plainteks: ILIKEGOOGLE, sebagai kunci: ZFLT dan hasil cipherteks diperolah: HQTDDLZHFQP.

Pengembangan sebuah algoritma enkripsi bertujuan untuk memperkuat algoritma dari serangan peretas data yang diamankan menggunakan algoritma tersebut. Salah satu pengembangan algoritma vigenere yaitu dengan memodifikasi cara penerbitan kunci dan menambah jumlah karakter set [12]. Penambahan karakter set pada vigenere dikenalkan olah Nahar dan Chakraborty [15]. Versi vigenere ini dikenal sebagai Extended Vigere. Vigenere versi ini menggunakan tabel karakter berukuran 95 x 95 seperti terlihat pada gambar 2, tabel ini lebih besar dari versi vigenere awal yang menggunakan ukuran 26 x 26. Penggunaan karakter set dengan jumlah yang lebih banyak ini akan membuat penggunaan vigenere secara luas dan dapat diaplikasikan pada banyak tipe data, karakter upper case, lower case, numerik, tanda baca serta penggunaan karakter khusus. Pada tabel 95 x 95, susunan karakter tidak dibuat sesuai dengan urutan kode ASCII, hal ini juga menjadi pertimbangan untuk mempersulit kriptanalis dalam memecahkan data yang diamankan [15].

Penentuan nilai kunci pada algoritma kriptografi menjadi penentu tingkat keamanan data yang diamankan, sehingga kunci akan memegang peranan penting dalam keamanan informasi [16]. Kunci vigenere yang lebih pendek dari plainteksnya akan digunakan secara berulang, ini dipandang sebagai suatu kerentanan pada informasi yang diamankan [12]. Beberapa penelitian terkait dengan penerbitan kunci vigenere diantaranya pemanfaatan Bilangan Euler sebagai pembangkit kunci [5]. 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 [17]. Penelitian ini memanfaatkan hasil perhitungan pada pembangkit kunci BBS digunakan sebagai kunci pada vigenere sehingga memberikan bentuk keacakan pada informasi terenkripsi.



Gambar 2. Tabel Extended Vigenere.



Gambar 3. Nilai Entropi Hasil *Preliminary Experiment*

Sebagai *preliminary experiment*, dilakukan pengukuran nilai entropi terhadap extended vigenere yang mengadopsi penerbitan kunci dengan teknik: random, pembangkit kunci BBS [17] dan penggunaan bilangan Euler [5]. Gambar 3 memperlihatkan nilai entropi yang diperoleh. Eksperimen awal ini menggunakan data sampel dengan ukuran 1 KB. Sampel yang digunakan diambil dari dataset informasi pengamatan astonomi yang dikirimkan melalui telegram. 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 cipherteksnya. Pada preliminary experiment, diperoleh nilai entropi paling tinggi ialah dengan menggunakan kunci 64-bit dengan entropi 6,4. Dengan demikian dengan memilih teknik penerbitan kunci yang tepat maka akan berimbas pada meningkatknya keamanan dari ciphertext. Penggunaan kunci vigerene secara umum memiliki sifat yang pendek dan digunakan secara berulang [18] selain itu pemilihan kunci juga dilakukan secara manual [19], ini akan menjadikan kerapuhan pada algoritma vigenere. Berdasarkan eksperimen awal yang dilakukan maka sebagai pertanyaan riset ialah: bagaimana pengaruh pemilihan kunci pada extended vigenere terhadap informasi yang diamankannya jika dilakukan proses penerbitan secara berlapis.

Penelitian ini bertujuan untuk melihat pengaruh penggunaan teknik berlapis pada penerbitan kunci yang diadopsikan pada extended vigenere. Teknik yang digunakan untuk penerbitak kunci digunakan fungsi random sebagai pembangkit awal dan dilanjutkan dengan pembangkt kunci Blum Blum Shub. Hasil yang diperoleh selanjutnya akan dihitung nilai entropinya dan dibandingkan dengan penelitian sebelumnya.

2. TINJAUAN PUSTAKA DAN TEORI

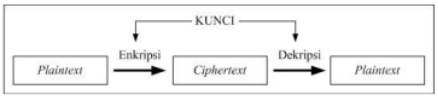
2.1. Algoritma Enkripsi Simetris

Algoritma enkripsi simetri ialah algoritma kriptografi klasik yang kuncinya sama untuk pada proses enkripsi dan deskripsi, seperti terlihat pada gambar 4. Suatu plainteks dienkripsi menggunakan suatu kunci menghasilkan suatu cipher teks. Cipher teks didekripsi menggunakan kunci yang sama untuk menghasilkan plain teks. 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).

2.2. 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



Gambar 2. Algoritma Simetris.

dengan menggunakan untaian Caesar cipher berdasarkan huruf-huruf pada kata kuncinya [12], [20], [21] .

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 [15].

2.3. Algoritma Vigenere dengan Kunci Blum Blum Shub

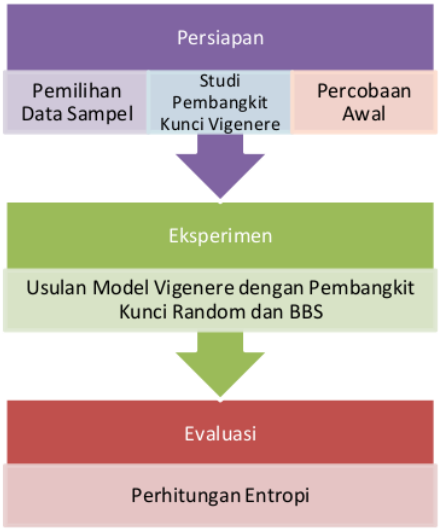
Pembangkit bilangan Blum Blum Shub (BBS) adalah cryptographically secure pseudo random number generato (CSPRNG) yang paling sederhana dan paling mangkus (secara kompleksitas teoritis). BBS dibuat pada tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub [17]. Persamaan yang digunakan pada BBS ialah sebagai berikut:

$$X_{i+1} = X_i^2 \text{ Mod } M \quad (1)$$

Pada penelitian ini telah melakukan eksperimen awal yang dilakukan pada extended vigenere menggunakan fungsi random [15]dan extended vigenere menggunakan pembangkit kunci BBS [17] sebagai *state of the art*, untuk mencapai tingkat keamanan yang lebih baik, pembangkit kunci yang digunakan ialah kombinasi dari fungsi random dan pembangkit bilangan BBS.

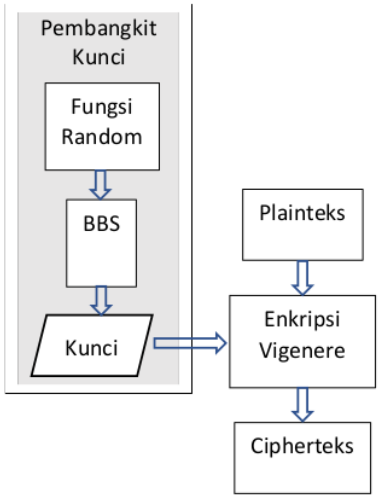
3. METODE

3.1. Kerangka Penelitian



Penelitian yang dilakukan terbagi menjadi tiga tahap, yaitu: 1) Pesiapan, 2) Eksperimen, dan 3) Evaluasi. Gambar 5 memperlihatkan kerangka penelitian yang dilakukan. Pada tahap persiapan dilakukan pemilihan data sampel, studi tentang pembangkit kunci yang telah di aplikasikan pada model vigenere, dan melakukan kegiatan eksperimen awal (*prelimirary experiment*). Sebagai data sampel digunakan data percakapan laporan pengamatan astronomi dari *astronom dataset*. Sampel yang digunakan berukuran 1 KB.

Pada tahap eksperimen dilakukan adopsi pembangkit kunci yang baru sesuai desain pada gambar 6, yang kemudian hasil kunci yang diperoleh digunakan sebagai kunci pada model vigenere. Sebagai evaluasi dilakukan pengukuran



Gambar 6. Desain Pembangkit Kunci.

nilai entropi dari model yang diusulkan dengan model yang telah dikembangkan pada penelitian terdahulu.

3.2. Desain Modifikasi Pembangkit Kunci

Eksperimen mengusulkan pembangkitan kunci berlapis dengan menggunakan fungsi random dan Blum Blum Shub sebagai penerbit kunci yang diadopsikan pada extended vigenere. Gambar 6 memperlihatkan desain adopsi pembangkit kunci untuk extended vigenere menggunakan fungsi random dan pembangkit BBS.

Pembangkitan kunci yang diusulkan dilakukan dengan menggunakan fungsi random dan BBS yang proses secara berurutan (sekuensial). Penggunaan fungsi random memanfaatkan hasil penelitian [15], sedangkan pembangkit BBS menggunakan penelitian [17]. Hasil yang diperoleh dari penggabungan kedua pembangkit kunci tersebut digunakan sebagai kunci pada proses enkripsi vigenere. Sebagai data sampel digunakan dataset informasi pengamatan astonomi yang dikirimkan melalui telegram dengan ukuran 1 KB. Hasil proses enkripsi dihitung nilai entropi sebagai matrik performasi.

3.3. Entropi

Dalam teori informasi, entropi tinggi merepresentasikan keacakan yang sebenarnya. Masalah keamanan data yang muncul dari pengaruh entropi yang tidak mencukupi menunjukkan bahwa keacakan yang memadai penting untuk keamanan [22]. Entropi digunakan sebagai ukuran dalam keacakan informasi yang merefelsikan kekuatan sebuah algoritma kriptografi [23], [24]. Semakin tinggi nilai entropi, maka akan semakin acak informasinya. Sehingga dapat berpengaruh pada ketahanan algoritma dari serangan peretas. Untuk mengkalkulasi entropi digunakan persamaan sebagai berikut :

Gambar 5. Kerangka Penelitian.

$$H(m) = \sum_{i=0}^{2^n-1} P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (1)$$

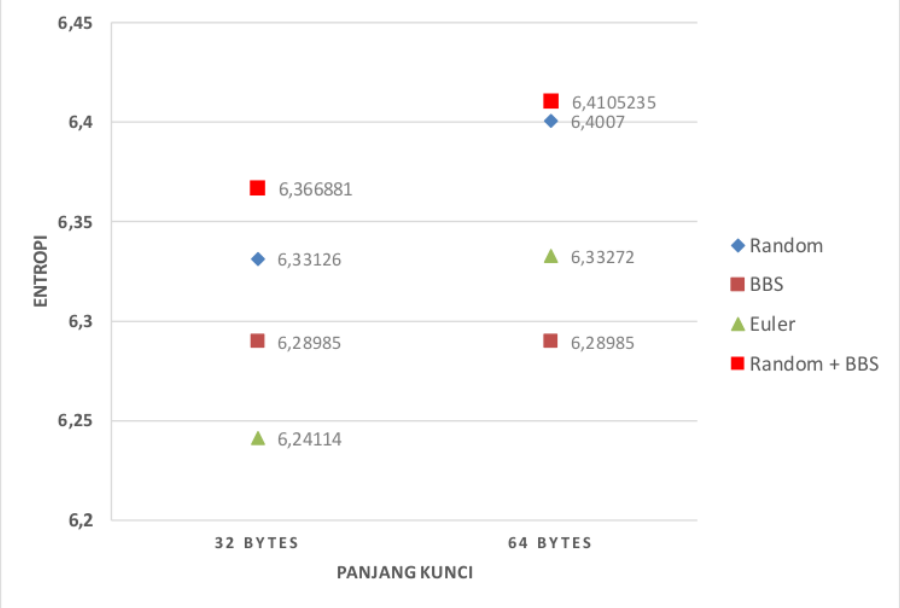
4. HASIL DAN PEMBAHASAN

Gambar 7 memperlihatkan hasil eksperimen yang diperoleh. Penggunaan pembangkit kunci secara berlapis yang diadopsikan pada algoritma extended vigenere memberikan perbaikan nilai entropi. Pada kunci dengan panjang 32 Bit, nilai entropi yang diperoleh sebesar 6,367. Sedangkan, dengan metode yang lain mendapatkan 6,29 dan 6,33. Pada ekperimen dengan panjang kunci 64 Bit didapatkan nilai entropi 6,41. Dibandingkan penggunaan pembangkit kunci sebelumnya 6,29 dan 6,40. Dengan peningkatan nilai entropi ini, dapat diartikan bahwa penggunaan pembangkit kunci yang dilakukan secara berlapis memberikan dampak pada keacakan informasi hasil enkripsi, sehingga cipherteks akan semakin sulit dibaca dan dikenali.

Jika dibandingkan dengan nilai entropi optimum 8, maka akan terlihat peningkatan capaian nilai entropi hasik eksperimen. Tabel 1 menunjukkan capaian nilai entropi yang didapatkan. Hasil yang diperoleh untuk capaian entropi laiah 79,59 % pada panjang kunci 32 Bit dan 80,13 % pada panjang kunci 64 Bit. Ini terjadi peningkatan dari eksperimen sebelumnya yang menunjukkan capaian 79,14 % dan 78,63 % pada penggunaan fungsi random dan BBS dengan panjang kunci 32 Bit dan 80% dan 78,61 % dengan penggunaan panjang kunci 64 Bit. Dengan peningkatan ini, dapat diartiken bahwa terdapat peningkatan ketahanan algoritma extended vigenere yang mengadopsi penggunaan pembangkit kunci secara berlapis, fungsi random dan BBS. Dengan demikian algoritma extended vigenere menjadi semakin kuat dan tangguh dari serangan terhadap informasi yang diamankannya.

TABEL I. PERBANDINGAN CAPAIAN NILAI ENTROPI

Metode Pembangkit Kunci	Panjang Kunci	
	32 Bit	64 Bit
Fungsi Random	79,14 %	80 %
BBS	78,63 %	78,61 %
Fungsi Random + BBS	79,59 %	80,13 %



Gambar 7. Perbandingan Entropi Extended Vigenere dengan Pembangkit Kunci yang berbeda

5. Kesimpulan dan Saran

Berdasarkan eksperimen yang dilakukan dan hasil yang diperoleh, maka dapat disimpulkan bahwa pengambilan pemilihan kunci akan mempengaruhi tingkat kemanan informasi. Dengan menerapkan penggunaan pembangkit kunci secara berlapis akan mampu meningkatkan keacakan informasi rahasia, sehingga akan lebih sulit untuk ditebak dan diretas oleh pihak yang tidak berwenang. Meskipun demikan, sebagai eksperimen lanjutan kedepan perlu dilakukan pendalaman eksploratif pada eksperimen lebih lanjut mengenai pengaruh panjang kunci yang digunakan untuk memperkuat algoritma extended vigenere.

6. Ucapan Terimakasih

Terimakasih kepada Direktorat Penelitian, Pengabdian Masyarakat, dan Publikasi Universitas Stikubank (Unisbank) atas dukungan pendanaan atas penelitian ini.

Daftar Pustaka:

[1] M. S. Abbas, S. S. Mahdi, and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," in *2020 International Conference on Computer Science and Software Engineering (CSASE)*, Apr. 2020, pp. 123–127. doi: 10.1109/CSASE48920.2020.9142072.

[2] E. Ardhianto, H. Murti, E. Supriyanto, and E. Lestariningsih, "Modifikasi Model Enkripsi Encryption With Covertext and Reordering menggunakan Fungsi Random dan Tabel Permutasi," *Jurnal Informatika Upgris*, vol. 8, no. 1, Jul. 2022, doi: 10.26877/jiu.v8i1.9758.

[3] E. Ardhianto, "Improvement of Steganography Technique: A Survey," in *1st International Multidisciplinary Conference on Education, Technology, and Engineering*

(IMCETE 2019), 2020, pp. 289–292. [Online]. Available: www.scimagojr.com.

[4] A. AminSoofi, M. Irfan Khan, and F.-A. Fazal-e-Amin, "A Review on Data Security in Cloud Computing," *Int J Comput Appl*, vol. 94, no. 5, pp. 12–20, May 2014, doi: 10.5120/16338-5625.

[5] 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.

[6] A. Permana, T. Tulus, and Z. Situmorang, "Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY," Jan. 2020. doi: 10.4108/eai.3-8-2019.2290723.

[7] E. Ardhianto, W. Budiharto, Y. Heryadi, and L. A. Wulandhari, "A Comparative Experiment of Document Security Level on Parallel Encryption With Digit Arithmetic of Covertext and Parallel Encryption using Covertext," in *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, Nov. 2021, pp. 163–167. doi: 10.1109/SCOReD53546.2021.9652746.

[8] E. Ardhianto, W. T. Handoko, H. Murti, and R. S. A. Redjeki, "Encryption with Covertext and Reordering using Permutated Table and Random Function," in *2021 2nd International Conference on Innovative and Creative Information Technology (ICITech)*, Sep. 2021, pp. 90–93. doi: 10.1109/ICITech50181.2021.9590171.

[9] R. Shukla, H. O. Prakash, R. P. Bhushan, S. Venkataraman, and G. Varadan, "Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem," in *2013 International Conference on Machine Intelligence and Research Advancement*, Dec. 2013, pp. 174–178. doi: 10.1109/ICMIRA.2013.40.

[10] F. Al-Haidari, A. Gutub, K. Al-Kahsah, and J. Hamodi, "Improving security and capacity for Arabic text steganography using Kashida extensions," in *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 2009, pp. 396–399. doi: 10.1109/AICCSA.2009.5069355.

[11] Y. Wu and X. Dai, "Encryption of accounting data using DES algorithm in computing environment," *Journal of Intelligent and Fuzzy Systems*, vol. 39, no. 4, pp. 5085–5095, 2020, doi: 10.3233/JIFS-179994.

[12] 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.

[13] E. Supriyanto, W. T. Handoko, S. A. Wibowo*, and E. Ardhianto, "Peningkatan Ketahanan Algoritma Vigenere menggunakan Generator kunci Tiga Lapis," *JURNAL MAHAJANA INFORMASI*, vol. 7, no. 1, pp. 24–33, Jun. 2022, doi: 10.51544/jurnalmi.v7i1.2894.

[14] 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.

[15] 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.

[16] N. Uniyal, G. Dobhal, A. Rawat, and A. Sikander, "A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication," *Wirel Pers Commun*, vol. 119, no. 2, pp. 1577–1587, Jul. 2021, doi: 10.1007/s11277-021-08295-5.

[17] 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.

[18] Z. Qowi and N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," in *Journal of Physics: Conference Series*, Jun. 2021, vol. 1918, no. 4, pp. 1–6. doi: 10.1088/1742-6596/1918/4/042009.

[19] A. P. Sidik, "Improve The Security of The Vigenère Cypher Algorithm by Modifying the Encoding Table and Key," *International Journal of Basic and Applied Science*, vol. 10, no. 2, pp. 42–50, 2021, [Online]. Available: www.ijobas.pelnus.ac.id

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

[21] I. Mu'alimin Arrijal, R. Efendi, and B. Susilo, "PENERAPAN ALGORITMA KRIPTOGRAFI KUNCI SIMETRIS DENGAN MODIFIKASI VIGENERE CIPHER DALAM APLIKASI KRIPTOGRAFI TEKS," *Jurnal Pseudocode*, vol. 1, 2016, [Online]. Available: www.ejournal.unib.ac.id

[22] 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.

[23] 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.

[24] 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.

ADOPSI PEMBANGKIT KUNCI EXTENDED VIGENERE MENGGUNAKAN FUNGSI RANDOM DAN BLUM BLUM SHUB

ORIGINALITY REPORT

16%	12%	11%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	openjournal.unpam.ac.id Internet Source	5%
2	Ahmad Tantoni, Mohammad Taufan Asri Zaen. "MANAJEMEN WIRELESS DENGAN MAPPING SSID ACCESS POINT PADA STMIK LOMBOK", Jurnal Informatika dan Rekayasa Elektronik, 2019 Publication	2%
3	ejournal.unib.ac.id Internet Source	1%
4	id.123dok.com Internet Source	1%
5	123dok.com Internet Source	1%
6	Submitted to University of Thessaly Student Paper	1%
7	prosiding.konik.id Internet Source	1%

8	www.i-scholar.in Internet Source	1 %
9	Submitted to Royal Holloway and Bedford New College Student Paper	1 %
10	ojs.htp.ac.id Internet Source	1 %
11	Submitted to University of Liverpool Student Paper	1 %
12	Submitted to itera Student Paper	1 %
13	Submitted to Georgia Southern University Student Paper	1 %

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		