TIN: Terapan Informatika Nusantara
Vol 3, No 1, June 2022, page 1-4
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v3i1.1699

Modifikasi Metode One-Time Pad Dan Chaostic Function Untuk Mengamankan Pesan

Nyata Manalu

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budidarma, Medan, Indonesia
Email: nyatamanalu11@gmail.com
Email Penulis Korespondensi: nyatamanalu11@gmail.com

Abstrak−Informasi merupakan kumpulan data yang berupa teks yang telah disatukan yang bersifat publik atau rahasia. Data rahasia merupakan data yang berisi tentang sesutau atau yang tidak untuk dipublikasikan, sebab data tersebut merupakan dat penting. Untuk itu, data tersebut perlu diamankan. Salah satu cara untuk mengamankan data tersebut adalah dengan memanfaatkan kriptografi. Kriptografi merupakan salah satu ilmu yang yang berperan penting dalam bidang pengamanan informasi. Kriptografi memiliki teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentikasi. Algoritma di dalam kriptografi terbagi menjadi dua, yaitu algoritma kunci simetri dan algoritma kunci asimetri. Salah satu yang termasuk dalam algoritma kunci simetri adalah one time pad. One Time Pad merupakan algoritma kunci simetri yang menggunakan subtitusi abjad dengan menggunakan huruf tersebut sebagai plaintext dan huruf kunci yang memiliki posisi sebanding. Namun seiring dengan perkembangan ilmu pengetahuan manusia, kelemahan dari one time pad berhasil ditemukan.. Salah satu cara yang dapat dilakukan untuk mengatasi kelemahan one time pad di atas adalah dengan melakukan pembangkitan kunci yang lebih acak Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk memodifikasi pembangkitan kunci yang digunakan pada algoritma one time pad. pembangkitan kunci dilakukan berdasarkan pembangkit kunci blum blum shub, artinya kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang dibangkitkan berdasarkan pembangkit kunci chaostic function, sehingga proses modifikasi yang dilakukan dalam pembangkitan kunci tersebut dapat meminimalkan tindakan pemecahan kunci yang dilakukan pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan data.

Kata Kunci: Kriptografi; Algoritma One Time Pad; Pembangkit Kunci Chaostic Function

Abstract−Information is a collection of data in the form of unified text that is public or confidential. Confidential data is data that contains something or not to be published, because the data is important data. For that, the data needs to be secured. One way to secure the data is to use cryptography. Cryptography is a science that plays an important role in the field of information security. Cryptography has mathematical techniques related to information security aspects, such as data confidentiality and integrity, and authentication. Algorithms in cryptography are divided into two, namely symmetric key algorithms and asymmetric key algorithms. One that is included in the symmetric key algorithm is the one time pad. One Time Pad is a symmetric key algorithm that uses alphabetic substitution by using these letters as plaintext and key letters that have comparable positions. However, along with the development of human science, the weaknesses of the one time pad were found. One way to overcome the weaknesses of the one time pad above is to generate a more random key This study describes how the procedure is carried out to modify the key generation used in the one time pad algorithm. Key generation is done based on the Blum Blum Shub key generator, meaning that the key used in the encryption and decryption process is the key generated based on the chaostic function key generator. can be more optimal in securing data.

Keywords: Cryptography; One Time Pad Algorithm; Chaostic Function Key Generation

1. PENDAHULUAN

Ada beberapa bentuk ancaman terhadap pertukaran informasi seperti penyadapan, pencurian dan pemalsuan informasi.Yang mana jika hal itu terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirimi pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Keterpaduan antara perkembangan teknologi informasi dengan media dan telekomunikasi ini telah mengakibatkan semakin beragamnya aneka jasa dan produk layanan sistem informasi dan komukasi yang ada. Informasi tersebut dapat berupa data pribadi yang tidak dibuat umtuk dipublikasikan, data perusahaan penting dan berbagai informasi lain yang bersifat rahasia. Salah satu cara yang dilakukan untuk mengamankan informasi tersebut adalah dengan cara menggunakan metode kriptografi. Kriptograafi merupakan salah satu ilmu yang berperan penting dalam biddang pengamanan informasi. Kriptografi memiliki teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentifikasi. Kuat lemahnya kriptografi tidak terletak dari hasil *enkripsi* atau *ciphertext*, melainkan terletak pada kunci yang digunakan.

Algoritma *One Time Pad* (OTP) adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Algoritma memilki kelemahan yang dapat mengancam keamanan data(Harahap & Khairina, 2017)(Dakhi et al., 2020)(Sulaiman et al., 2020). Salah satunya adalah kuncinya yang terlalu panjang dan masih menggunakan jenis karakter saja yaitu abjad. Penelitian ini menguraikan bagaimana prosedur yang dilakukukan untuk memodifikasi pembangkit kunci yang digunakan pada algoritma *one time pad*. Proses pembangkit kunci yang digunakan berdasarkan pembangkit kunci *chaostic function*, artinya kunci yang digunakan pada proses enkripsi dan deskripsi adalah kunci yang dibangkitkan berdasarkan pembangkitkan kunci *chaostic function*, sehingga proses modifikasi yang dilakukan dalam pembangkit kunci tersebut dapat meminimalkan tindakan pemcahan kunci yang dilakukan oleh pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan pesan.


TIN: Terapan Informatika Nusantara
Vol 3, No 1, June 2022, page 1-4
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v3i1.1699

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu "*cryptos*" artinya "*secret*" yang berarti rahasia, sedangkan "*graphein*" artinya "*writing*" yang berarti tulisan rahasia(Ii, 2010). Umumnya kriptografi digunakan oleh kalangan militer pada perang dunia II untuk menyampaikan informasi mengenai strategi atau langkah yang harus mereka hadapi untuk melawan musuh(Fadillah et al., 2022)(Yusfrizal, 2019)(Suhandinata et al., 2019).

2.2 Algortima One Time Pad

One time pad ditemukan pada tahun 1917 oleh Mayor Yoseph Mouborgnedan Gilbert Vernam pada perang dunia ke dua. Penggunaan algoritma OTP dalam kriptografi adalah sebagai dasar untuk mengaburkan suatu informasi yang ingin dirahasiakan dengan cara mengacak informasi tersebut sehingga menjadi suatu informasi yang tidak dapat dipahami oleh orang lain(Utomo & Zarlis, 2017)(Maghfiroh, 2022)(Zakti et al., 2022). Berikut adalah tahapan penggunaan *onte time pad* (Fitriyansyah & Hazri, 2020)(Ramadhani et al., 2020):

Tahapan enkripsi dalam algoritma *one time pad* adalah:

1. Ubah plaintext kedalam bentuk biner.
2. Bangkitkan kunci acak dan panjang kunci acak harus sama denganplaintext yang akan di enkripsi.
3. Lakukan proses XOR terhadap plaintext dengan kunci yang telah dibangkitkan sebelumnya.
4. Chipertext dihasilkan.

Sedangkan pada tahapan deskripsi algoritma *one time pad* adaalah :

1. Ubah chipertext kedalam bentuk biner
2. Ambil kunci yang digunakan pada proses enkripsi
3. Lakukan proses operasi XOR terhadap plaintext dengan kunci yang telah dipilih Plaintext dihasilkan

2.3 Algortima Chaostic Function

Salah satu dari dua prinsip Shannon yang dijadikan panduan dalam perancangan algoritma kriptografi adalah difusi (diffusion), yang artinya adalah menyebarkan pengaruh 1 bit (atau digit) plaintext keseluruh bit (digit) ciphertext dengan maksud untuk menyembunyikan hubungan statistik antara plaintext dengan ciphertext(Dharmaadi et al., n.d.)(Aminudin & Hariyady, 2021). Logistic map berupa persamaan iterative yang dijabarkan sebagai berikut:(Wijaya, 2022)

$$X_i + 1 = rx_{i\ (1\ -\ x_{i)\ 1)}} \quad (1)$$

3. HASIL DAN PEMBAHASAN

Ada beberapa bentuk ancaman terhadap pertukaran informasi seperti penyadapan, pencurian dan pemalsuan informasi.Yang mana jika hal itu terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirimi pesan, maupun organisasinya. Keterpaduan antara perkembangan teknologi informasi dengan media dan telekomunikasi ini telah mengakibatkan semakin beragamnya aneka jasa dan produk layanan sistem informasi dan komukasi yang ada. Informasi tersebut dapat berupa data pribadi yang tidak dibuat umtuk dipublikasikan, data perusahaan penting dan berbagai informasi lain yang bersifat rahasia. Kriptograafi merupakan salah satu ilmu yang berperan penting dalam biddang pengamanan informasi. Kriptografi memiliki teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi misalnya kerahasiaan dan integritas data, serta otentifikasi. Kuat lemahnya kriptografi tidak terletak dari hasil *enkripsi* atau *ciphertext*, melainkan terletak pada kunci yang digunakan. Algoritma *One Time Pad* (OTP) adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Proses pembangkit kunci yang digunakan berdasarkan pembangkit kunci *chaostic function*, artinya kunci yang digunakan pada proses enkripsi dan deskripsi adalah kunci yang dibangkitkan berdasarkan pembangkitkan kunci *chaostic function*, sehingga proses modifikasi yang dilakukan dalam pembangkit kunci tersebut dapat meminimalkan tindakan pemcahan kunci yang dilakukan oleh pihak lain serta algoritma ini dapat lebih optimal dalam mengamankan pesan.

3.1 Penerapan Algortima One Time Pad

Modifikasi *one time pad* menggunakan pembangkit kunci *chaostic function* seperti di bawah ini.
Dimisalkan *plaintext* yang digunakan adalah **Hidup senang**
Terdapat *plaintext* yang akan dilakukan enkripsi sebagai berikut : Enkripsi : Hidup senang

a. Tiap huruf pada *plaintext* akan diubah menjadi sesuai urutannya pada tabel ASCII sehingga didapat seperti tabe dibawah ini :

Tabel 1. Nilai ASCII

Huruf	ASCII
H	72

TIN: Terapan Informatika Nusantara
Vol 3, No 1, June 2022, page 1-4
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v3i1.1699

Huruf	ASCII
i	105
d	100
u	117
P	112
Spasi	32
s	115
e	101
n	110
a	97
n	110
g	67

b. Proses pembangkitan kunci berdasakan algoritma *one time pad* bahwa jumlah kunci yang digunakan pada proses enkripsi dan dekripsi harus sama dengan jumlah karakter *plaintext*. Jumlah *plaintext* pada contoh di atas adalah 12 karakter, oleh karena itu akan dibangkitkan 12 karakter kunci berdasarkan pembangkit kunci *chaostic function*. Langkah-langkah yang dilakukan adalah :
   1. Pilih umpan : 6341
   2. Untuk menetukan X_0, nilai umpan dijadikan dibelakang X_0 yaitu 0,6341
   3. Menentukan nilai r dengan memilih nilai antara 1 sampai 4.Yang saya gunakan yaitu 3.
   4. Dapatkan bilangan real ke-1 dengan rumus $X_1 = rX_0\ (1\text{-}X_0)$. Didapat bahwa r = 3, x_0 = 0,6341
   5. Maka hitung x_i :
      $X_i = r\ x_o\ (1\text{-}X_0)$
      $X_1 = rX_0\ (1\text{-}X_0)$
      $X_1 = 3 * 0{,}6341\ (\ 1\text{-}\ 0{,}6341) = 0{,}69605157 = 69$
      $X_2 = 3 * 0{,}69605157\ (\ 1\text{-}\ 0{,}69605157\ ) = 0{,}6346913457 = 63$
      $X_3 = 3 * 0{,}6346913457\ (\ 1\text{-}\ 0{,}6346913457\ ) = 0{,}69557472418 = 69$
      Lakukanlah proses di atas sebanyak jumlah karakter pada *plaintext*. Adapun tabel kunci dari hasil perhitungan di atas, yaitu :

Tabel 2. Kunci

Kunci	Hasil	Desimal	Karakter
X1	0,69605157	69	E
X2	0,6346913457	63	?
X3	0,69557472418	69	E
X4	0,63525158179	63	?
X5	0,69512102887	69	E
X6	0,63578335228	63	?
X7	0,69468864373	69	E
X8	0,63628899601	63	?
X9	0,6942759287	69	E
X10	0,6942759287	69	E
X11	0,69388141666	69	E
X12	0,63722998882	63	?

6. Proses enkripsi
   Proses enkripsi yang dilakukan berdasarkan modifikasi *one time pad* yang menggunakan pembangkit kunci *chaostic function* diselesaikan dalam bentuk perhitungan ASCII, yang dimana enkripsi dapat dinyatakan sebagai penjumlahan modulo 256 dari satu karakter *plaintext* dengan satu karakter kunci hasil pembangkitan BBS. Kemudian dari hasil dari perhitungan tersebut akan diperoleh nilai desimal. Berikut adalah proses enkripsi yang menggunakan persamaan 2 yang ada pada bab sebelumnya $C_1 = (H + K_1) \bmod 256 = (72 + 69) \bmod 256 = 141 \bmod 256 = 141 =$ Ì
   $C_2 = (i + K_2) \bmod 256 = (105 + 63) \bmod 256 = 168 \bmod 256 = 168 =$ ¿
   $C_3 = (d + K_3) \bmod 256 = (100 + 69) \bmod 256 = 169 \bmod 256 = 169 =$ ®
   $C_4 = (u + K_4) \bmod 256 = (117 + 63) \bmod 256 = 180 \bmod 256 = 180 =$ -|
   $C_5 = (p + K_5) \bmod 256 = (112 + 69) \bmod 256 = 181 \bmod 256 = 181 =$ À
   $C_6 = (\text{spasi} + K_6) \bmod 256 = (32 + 63) \bmod 256 = 95 \bmod 256 = 95 =$ - $C_7 = (s + K_7) \bmod 256 = (115 + 69) \bmod 256 = 184 \bmod 256 = 184 =$ ©
   $C_8 = (e + K_8) \bmod 256 = (101 + 63) \bmod 256 = 164 \bmod 256 = 164 =$ Ñ
   C9= (n + K9) mod 256 = (110 + 69) mod 256 = 179 mod 256 = 179 = |
   $C_{10} = (a + K_{10}) \bmod 256 = (97 + 69) \bmod 256 = 166 \bmod 256 = 166 =$ ³

TIN: Terapan Informatika Nusantara
Vol 3, No 1, June 2022, page 1-4
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v3i1.1699

C_{11} = (n + K_{11}) mod 256 = (110 + 69) mod 256 = 179 mod 256 = 179 = |
C_{12} = (g + K_{12}) mod 256 = (67 + 63) mod 256 = 130 mod 256 = 130 = é Hasil enkripsi di atas akan menjadi *ciphertext*. *Ciphertext* yang didapat dari hasil perhitungan di atas adalah Ì¿ ®|-| À-© Ñ|³| é

7. Proses Dekripsi
Adapun proses dekripsi modifikasi *one time pad* dengan pembangkit kunci *chaostic function* yang menggunakan persamaan 4 yang telah dibahas pada bab sebelumnya, yaitu :
P_1 = (Ì – K_1) mod 256 = (141 - 69) mod 256 = 72 mod 256 = 72 = H
P_2 = (¿ – K_2) mod 256 = (168 - 63) mod 256 = 105 mod 256 = 105 = i
P_3 = (® - K_1) mod 256 = (169 - 69) mod 256 = 100 mod 256 = 100 = d
P_4 = (-| - K_1) mod 256 = (180 - 63) mod 256 = 117 mod 256 = 117 = u
P_5 = (À - K_1) mod 256 = (181 - 69) mod 256 = 112 mod 256 = 112 = p
P_6 = (- - K_1) mod 256 = (95 - 63) mod 256 = 32 mod 256 = 32 = spasi
P_7 = (© - K_1) mod 256 = (184 - 69) mod 256 = 115 mod 256 = 115 = s
P_8 = (Ñ - K_1) mod 256 = (164 - 63) mod 256 = 101 mod 256 = 101 = e
P_9 = (| - K_1) mod 256 = (179 - 69) mod 256 = 110 mod 256 = 110 = n
P_{10} = (³ - K_1) mod 256 = (166 - 69) mod 256 = 97 mod 256 = 97 = a
P_{11} = (| - K_1) mod 256 = (179 - 69) mod 256 = 110 mod 256 = 110 = n
P_{12} = (é - K_1) mod 256 = (130 - 63) mod 256 = 67 mod 256 = 67 = g
Maka *plaintext* dari proses dekripsi di atas adalah **Hidup senang**.

4. KESIMPULAN

Hasil dari modifikasi *one time pad* dengan pembangkit kunci *chaostic function* menghasilkan kunci yang lebih optimal dibandingkan dengan kunci pada *one time pad* yang belum dimodifikasi. Hal ini dibuktikan dari setiap pengujian yang dilakukan menghasilkan kunci yang lebih kuat dan optimal sehingga *plaintext* dan kuncinya sulit untuk ditebak.

REFERENCES

Aminudin, A., & Hariyady, H. (2021). Analisa Kombinasi Algoritma AES Dengan Blum-Blum Shub Dan Chaotic Function. *Prosiding SENTRA (Seminar Teknologi Dan Rekayasa)*, *6*, 365–373.

Dakhi, O., Masril, M., Novalinda, R., Jufrinaldi, J., & Ambiyar, A. (2020). Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Chiper. *Jurnal Inovasi Vokasional Dan Teknologi*, *20*(1), 27–36.

Dharmaadi, I. P. A., Barmawi, A. M., S, G. B., Informatika, F., & Telkom, I. T. (n.d.). *Enkripsi Gambar Parsial dengan Kombinasi Metode Stream Cipher RC4 dan Chaotic Function*. 1–8.

Fadillah, R., Idris, A. S., lumban Gaol, D. M., Lubis, G., Meisisri, R., & Syahrizal, M. (2022). Implementasi Algoritma Fast Encryption Algorithm (FEAL) Dan Algoritma Fibonacci Mengamankan File Teks. *Prosiding Seminar Nasional Sosial, Humaniora, Dan Teknologi*, 295–300.

Fitriyansyah, A. Y., & Hazri, M. (2020). Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password. *Sainstech: Jurnal Penelitian Dan Pengkajian Sains Dan Teknologi*, *30*(1).

Harahap, M. K., & Khairina, N. (2017). Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks. *Jurnal & Penelitian Teknik Informatika*, *1*(2), 58–62.

Ii, B. A. B. (2010). *Bab ii landasan teori 2.1. M*.

Maghfiroh, J. (2022). *Pengamanan pesan menggunakan algoritma One Time Pad (OTP) dengan Linear Congruential Generator (LCG) sebagai pembangkit kunci*. Universitas Islam Negeri Maulana Malik Ibrahim.

Ramadhani, F., Ramadhani, U., & Basit, L. (2020). Combination of hybrid cryptography in one time pad (otp) algorithm and keyed-hash message authentication code (hmac) in securing the whatsapp communication application. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, *1*(1), 31–36.

Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi, S. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *6*(1), 1–10. https://doi.org/10.33330/jurteksi.v6i1.395

Sulaiman, O. K., Nasution, K., & Prayogi, S. Y. (2020). Base64 Sebagai Kunci Keamanan pada One Time Pad (OTP). *CESS (Journal of Computer Engineering, System and Science)*, *5*(2), 241–244.

Utomo, P., & Zarlis, M. (2017). *Algoritma Split-Merge One Time Pad Dalam Peningkatan Enkripsi Data*. 0–4.

Wijaya, R. (2022). Enkripsi Nilai Piksel Pada Citra Digital Dengan Algoritma Piecewise Linear Chaotic Map. *Bulletin of Computer Science Research*, *3*(1), 161–169.

Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 29–37.

Zakti, I. W., Fauzi, A., & Sihombing, A. (2022). Pengacakan Citra Digital Dengan Metode Vertical Bit Rotation (VBR) Memanfaatkan Algoritma One Time Pad (OTP) Sebagai Keamanan Biner. *JTIK (Jurnal Teknik Informatika Kaputama)*, *6*(1), 182–190.