KRIPTOGRAFI *HYBRID ATBASH, AUTOKEY CIPHER,* DAN ALGORITMA EL GAMAL DALAM PENGAMANAN PESAN DAN PENGUJIAN *AVALANCHE EFFECT*

SKRIPSI

Diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:
Khairita Wardini
NIM. 2000336

PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA

2024

LEMBAR HAK CIPTA

KRIPTOGRAFI *HYBRID ATBASH, AUTOKEY CIPHER,* DAN ALGORITMA EL GAMAL DALAM PENGAMANAN PESAN DAN PENGUJIAN *AVALANCHE EFFECT*

Oleh
Khairita Wardini
2000336

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar Sarjana Matematika pada Program Studi Matematika Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia

© Khairita Wardini, 2024
Universitas Pendidikan Indonesia
Juli 2024

Hak cipta dilindungi Undang-Undang.
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian.
Dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa izin dari penulis.

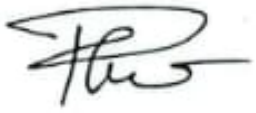
LEMBAR PENGESAHAN

KHAIRITA WARDINI

KRIPTOGRAFI *HYBRID ATBASH, AUTOKEY CIPHER,* DAN ALGORITMA EL GAMAL DALAM PENGAMANAN PESAN DAN PENGUJIAN *AVALANCHE EFFECT*

disetujui dan disahkan oleh pembimbing:

Pembimbing I



Dra. H. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II

Hj. Dewi Rachmatin, M.Si.

NIP. 196909291994122001

Mengetahui,

Ketua Program Studi Matematika

Dr. Kartika Yulianti, S.Pd.,M.Si.

NIP. 198207282005012001

ABSTRAK

"Kriptografi *Hybrid Atbash-Autokey Cipher,* dan Algoritma El Gamal dalam Pengamanan Pesan dan Pengujian *Avalanche Effect*"

Di era digital isu keamanan data menjadi salah satu isu pokok. Adapun informasi yang bersifat rahasia tentu harus terjaga keamanannya. Kriptografi adalah salah satu ilmu yang berbasis pada keamanan data. *Atbash Cipher* dan *Autokey Cipher* adalah contoh kriptografi simetri. Karena kunci kriptografi simetri rentan diretas, maka diperlukan peningkatan keamanan pesan dengan memanfaatkan kriptografi *hybrid*. Kriptografi *hybrid* merupakan teknik gabungan dari kriptografi simetri dan kriptografi asimetri. Menggabungkan *atbash-autokey cipher* dan algoritma El Gamal merupakan contoh kriptografi *hybrid* yang memanfaatkan algoritma El Gamal sebagai salah satu kriptografi asimetri. Algoritma El Gamal dipilih karena sukarnya pemecahan masalah logaritma diskrit. Untuk mengetahui kinerja dari algoritma *hybrid*, perlu dilakukan pengujian keamanan. Pengujian tingkat keamanan dapat dilakukan dengan pengujian *Avalanche Effect* (AE). Pengujian *Avalanche Effect* (AE) sebagai salah satu alat ukur keamanan kriptografi di mana pengujian *Avalanche Effect* (AE) memanfaatkan perubahan bit yang terjadi dalam cipherteks. Berdasarkan hasil uji, diperoleh pernyataan bahwa kriptografi hybrid yang diusulkan mampu meningkatkan keamanan pesan walau tidak signifikan. Program aplikasi kriptografi *hybrid* a*tbash-autokey cipher,* dan algoritma El Gamal serta Pengujian *Avalanche Effect* (AE) dibuat dengan bahasa pemrograman Python yang memanfaatkan *Graphical User Interface* (GUI).

Kata Kunci: Algoritma El Gamal, *Atbash Cipher*, *Autokey Cipher*, *Avalanche Effect*, Kriptografi *Hybrid*.

ABSTRACT

"Hybrid Cryptography Atbash-Autokey Cipher, and El Gamal Algorithm in Message Security and Avalanche Effect Testing"

In the digital era, the issue of data security is one of the main issues. Cryptography is a science that focuses on protecting sensitive information. Atbash Cipher and Autokey Cipher are examples of symmetry cryptography. Symmetry cryptography is susceptible to hacking due to the vulnerability of symmetric keys. To enhance message security, hybrid cryptography combines symmetric and asymmetric cryptography techniques. Combining the atbash-autokey cipher and the El Gamal algorithm is an example of hybrid cryptography that utilizes the El Gamal algorithm as one of the asymmetric cryptosystems. The El Gamal algorithm was chosen due to the difficulty of solving the discrete logarithm problem. To evaluate the performance of this hybrid algorithm, security testing is necessary. Avalanche Effect (AE) testing is a cryptographic security measurement tool that measures the bit changes in ciphertext. However, based on the test results, it is concluded that the proposed hybrid cryptography does improve massage security but not significantly. The hybrid cryptography application program, utilizing the atbash-autokey cipher, El Gamal algorithm, and Avalanche Effect (AE) Testing, is developed using the Python programming language with a Graphical User Interface (GUI).

***Keywords**: Atbash Cipher, Autokey Cipher, Avalanche Effect, El Gamal Algorithm, Hybrid Cryptography.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Agrawal, A. dan Patankar, G. (2016). Design of Hybrid Cryptography Algorithm for Secure Communication. *International Research Journal of Engineering and Technology (IRJET)*, 3(1), 1323–1326.

Atika, P. D. (2018). Digital signature dengan algoritma SHA-1 dan RSA sebagai autentikasi. *Jurnal Cendikia*, 16(1), 74-83.

Aufia, Z. (2021). *Enkripsi Dan Dekripsi Pesan Menggunakan Metode Vigenere Cipher Dan Route Cipher*. (Skripsi Sarjana, Universitas Islam Negeri Maulana Malik Ibrahim).

Basri. (2015). Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan). *Jurnal Ilmiah Ilmu Komputer*, *1*(2),31 – 36.

Burton, D. M. (2011). *Elementary Number Theory, Seventh Edition*. New York: McGraw-Hill.

Dewi, N. P., Sembiring, D. J., Ginting, R. B., & Ginting, M. B. (2022). Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma Luc Serta Steganografi Chaotic Lsb. *Jurnal Syntax Admiration*, *3*(2), 341-361.

Echeverri, C. (2017). *Visualization of the Avalanche Effect in CT2*. (Doctoral dissertation, University of Mannheim). doi: https://www.cryptool.org/assets/ctp/documents/BA_Echeverri.pdf

Fadlan, M., Rosmini, R., & Haryansyah, H. (2021). Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data. *Jurnal Media Informatika Budidarma*, 5(3), 806-812.

Fadlan, M., Rosmini, R., & Haryansyah, H. (2021). Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 5(6), 1113 – 1119.*

Fangohr, H. (2004). A comparison of C, MATLAB, and Python as teaching languages in engineering. In *Computational Science-ICCS 2004: 4th International Conference, Kraków, Poland, June 6-9, 2004, Proceedings,*

Part IV 4 (pp. 1210-1217). Springer Berlin Heidelberg.

Feistel, H. (1973). Cryptography and computer privacy. *Scientific american*, *228*(5), 15-23.

Firdaus, J., Marwati, R., & Muhtar, S. (2018). Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang Ditingkatkan dan Algoritma ElGamal. *Jurnal EurekaMatika*, *6*(1), 23-32.

Hikmah, A. N,. (2020). *Penyandian Pesan dengan Menggunakan Kriptografi Hybrid Autokey Vigenere Cipher dan Algoritma Elgamal*. (Skripsi Sarjana, Universitas Pendidikan Indonesia).

Husaini, F., Pardede, A. M., & Gultom, I. (2022). Penerapan Enkripsi Menggunakan Metode Elgamal guna Meningkatkan Keamanan Data. *JUKI: Jurnal Komputer dan Informatika*, *4*(1), 67-73.

Mandangan, A., Hung, C. E., Yin, L. S., & Hussin, C. H. C. (2016). Integration Of Cfea-Compression Technique Into Asymmetric Key Cryptosystems. *Jurnal Teknologi*, *78*(2-2).

Menezes, A., Van Oorschot, P. dan Vanstone, S. (2001). *Handbook of applied cryptography*. CRC Press.

Mohamed, K., Pauzi, M. N. M., Ali, F. H. H. M., Ariffin, S., & Zulkipli, N. H. N. (2014). Study of S-box properties in block cipher. In 2014 International Conference on Computer, Communications, and Control Technology (I4CT) (pp. 362-366). IEEE. doi: https://doi.org/10.1109/I4CT.2014.6914206

Morkel, T., & Eloff, J. H. P. (2004). Encryption techniques: a timeline approach. *Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria*, *2*.

Munir, R. (2006). *Kriptografi*. Bandung: Informatika.

Munir, R. (2019). *Kriptografi*. Bandung: Informatika.

Qozoqova, T. Q. (2023). Teaching Cryptanalysis Of Classic Encryption Methods Using Modern Tools.

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high Avalanche Effect. IJCSNS International Journal of Computer Science and Network Security, 11(1), 106-111. doi:

http://paper.ijcsns.org/07_book/201101/20110116.pdf

Rosen, K. H. (2012). *Discrete mathematics and its applications (7Th Edition)*. New York: McGraw-Hill.

Simbolon, I. A. R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. (2020). Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar. *Journal of Computer System and Informatics (JoSYC)*, *1*(2), 54-60.

Stinson, D.R. (2006). *Cryptography: theory and Practice Third Edition*. Florida: CRC Press.