PERANCANGAN ALGORITMA KRIPTOGRAFI BLOCK CIPHER BERBASIS PERMAINAN POLA CATUR SEBAGAI KUNCI DINAMIS

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh
gelar Sarjana Teknik pada Program Studi Teknik Komputer

oleh
Muhammad Rizki Wahyudin
NIM 2005752

PROGRAM STUDI S1 TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA

2024

HALAMAN HAK CIPTA

PERANCANGAN ALGORITMA KRIPTOGRAFI *BLOCK CIPHER* BERBASIS PERMAINAN POLA CATUR SEBAGAI KUNCI DINAMIS

oleh
Muhammad Rizki Wahyudin
NIM 2005752

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer

HALAMAN PENGESAHAN SKRIPSI

MUHAMMAD RIZKI WAHYUDIN

PERANCANGAN ALGORITMA KRIPTOGRAFI *BLOCK CIPHER* BERBASIS PERMAINAN POLA CATUR SEBAGAI KUNCI DINAMIS

disetujui dan disahkan oleh pembimbing:

Pembimbing I

Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

Pembimbing II

Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

Mengetahui,

Ketua Program Studi Teknik Komputer

Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

HALAMAN PERNYATAAN
KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini menyatakan bahwa skripsi yang berjudul "Perancangan Algoritma Kriptografi *Block Cipher* Berbasis Permainan Pola Catur Sebagai Kunci Dinamis" beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan. Atas pernyataan ini, saya bersedia menerima sanksi akademik sesuai dengan peraturan yang berlaku apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Juli 2024
Yang membuat pernyataan,

Muhammad Rizki Wahyudin
NIM. 2005752

HALAMAN UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Perancangan Algoritma Kriptografi *Block Cipher* Berbasis Permainan Pola Catur Sebagai Kunci Dinamis" sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer. Dalam penyusunan skripsi ini, penulis mengalami banyak hambatan. Namun, penulisan skripsi ini akhirnya dapat terselesaikan tidak terlepas atas bantuan dan dukungan dari berbagai pihak. Pada kesempatan ini, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Deden Pradeka, S.T., M.Kom., selaku Ketua Program Studi Teknik Komputer Universitas Pendidikan Indonesia di Cibiru sekaligus Dosen Pembimbing 1 yang telah menuntun dan memberikan arahan mengenai ide skripsi ini sejak sidang seminar proposal serta mengawasi dan memberikan *insight* baru mengenai kriptografi.
2. Bapak Dr. Eng. Munawir, S.Kom., M.T., selaku Dosen Pembimbing 2 yang telah membantu dan tiada hentinya memberikan masukan yang bermanfaat dalam penulisan serta dukungan moral dalam perjalanan mengerjakan skripsi ini.
3. Ibu Ana Rahma Yuniarti, S.T., M.Eng., selaku Dosen Pembimbing Akademik yang telah menyemangati sejak pemilihan judul dan selalu memberikan dukungan moral yang baik agar tidak mengulang semester.
4. Bapak/Ibu Dosen, dan Staf Program Studi Teknik Komputer, yang telah memberikan ilmu dan bantuan selama penulis menempuh pendidikan.
5. Kedua orang tua dan adik tercinta, yang selalu memberikan dukungan moral dan material serta doa yang tiada henti.
6. Teman-teman dan rekan-rekan mahasiswa Teknik Komputer, yang selalu memberikan semangat dan etos pantang menyerah selama penulisan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna. Oleh karena itu, segala bentuk kritik, saran, dan masukan akan dengan senang hati

diterima dan diharapkan dapat membantu perbaikan di masa yang akan datang. Akhir kata, semoga skripsi ini dapat berguna sebagaimana mestinya dan bermanfaat bagi pembaca serta masyarakat umum.

PERANCANGAN ALGORITMA KRIPTOGRAFI BLOCK CIPHER BERBASIS PERMAINAN POLA CATUR SEBAGAI KUNCI DINAMIS

Muhammad Rizki Wahyudin

2005752

ABSTRAK

Keamanan data merupakan aspek krusial dalam era digital saat ini, dengan kriptografi sebagai salah satu metode pengamanannya. Penelitian ini mengembangkan algoritma kriptografi simetris *block cipher* 64-bit berbasis pola permainan catur sebagai kunci dinamis. Algoritma ini menggunakan dua kunci yaitu, kunci 1 berupa 8 karakter ASCII dan kunci 2 berdasarkan langkah-langkah bidak catur. Tujuan penelitian ini adalah menciptakan algoritma kriptografi dengan pola kunci dinamis, berbeda dari pola statis yang umum digunakan. Dalam perancangan algoritma, diterapkan metode enkripsi seperti Transposisi Bit dengan matriks 8x8, Substitusi Bit menggunakan S-box, Operasi Logika XOR, dan Transposisi Bit sederhana yaitu dengan menggeser bit ke arah kiri atau kanan. Pengujian algoritma menggunakan uji korelasi Pearson untuk mengukur hubungan antara plainteks dan cipherteks, serta uji *Avalanche Effect* (AE) untuk mengukur tingkat keacakan enkripsi saat terjadi perubahan minimal 1 bit pada *input* plainteks atau kunci. Pengujian dilakukan sebanyak 32 kali, terdiri dari 16 uji korelasi dan 16 uji AE. Hasil uji menunjukkan nilai korelasi terbaik sebesar 0,00852 (korelasi sangat lemah) dan terburuk sebesar 0,25638 (korelasi lemah), serta nilai rata-rata AE sebesar 49,17% dengan perubahan 1 karakter plainteks (8 bit). Dari hasil pengujian tersebut dapat disimpulkan bahwa algoritma kriptografi *block cipher* berbasis pola permainan catur sebagai kunci dinamis memiliki kualitas yang baik dan layak diimplementasikan dalam berbagai kebutuhan di dunia nyata.

Kata Kunci: Kriptografi, Kriptografi Simetris, *Block Cipher*, Korelasi Pearson, *Avalanche Effect*, Kriptografi menggunakan Catur

DESIGN OF A BLOCK CIPHER CRYPTOGRAPHY ALGORITHM BASED ON CHESS PATTERN GAME AS A DYNAMIC KEY

Muhammad Rizki Wahyudin

2005752

ABSTRACT

Data security is a crucial aspect in today's digital era, with cryptography being one of its methods of protection. This research develops a 64-bit symmetric block cipher cryptographic algorithm based on chess game patterns as dynamic keys. The algorithm uses two keys: Key 1, consisting of 8 ASCII characters, and Key 2, based on the movements of chess pieces. The goal of this research is to create a cryptographic algorithm with dynamic key patterns, differing from the commonly used static patterns. In the algorithm design, encryption methods such as Bit Transposition with an 8x8 matrix, Bit Substitution using S-box, XOR Logical Operations, and simple Bit Transposition by shifting bits to the left or right are applied. The algorithm is tested using the Pearson correlation test to measure the relationship between plaintext and ciphertext, and the Avalanche Effect (AE) test to measure the randomness of encryption when there is a minimal 1-bit change in the plaintext input or key. Testing was conducted 32 times, consisting of 16 correlation tests and 16 AE tests. The test results showed the best correlation value of 0.00852 (very weak correlation) and the worst of 0.25638 (weak correlation), with an average AE value of 49.17% with a 1-character change in plaintext (8 bits). From these test results, it can be concluded that the block cipher cryptographic algorithm based on chess game patterns as dynamic keys has good quality and is suitable for implementation in various real-world needs.

Keywords: *Cryptography, Symmetric Cryptography, Block Cipher, Pearson Correlation, Avalanche Effect, Chess-based Cryptography*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PERSAMAAN

DAFTAR PUSTAKA

Aemy, N., & Al-Husaini, M. (2023). CHESTEGA: Steganografi menggunakan standar PGN dalam permainan catur berbasis web. *Jurnal Sistem dan Teknologi Informasi, 11*(3), 515-523. doi: https://dx.doi.org/10.26418/justin.v11i3.66716

Apdilah, D. (2017). Analisa suku kata yang sama menggunakan metode brute force. In *Semantika (Seminar Nasional Teknik Informatika), 1*(1), 204-209.

Astuti, N., Arfiani, I., & Aribowo, E. (2019). Analysis of the security level of modified CBC algorithm cryptography using avalanche effect. In *IOP Conference Series: Materials Science and Engineering*, *674*(1). doi: 10.1088/1757-899X/674/1/012056

Aziiz, A., & Pakereng, M. (2019). Perancangan teknik kriptografi block cipher berbasis pola batik ceplok Yogyakarta. *Jurnal Sistem dan Teknologi Informasi*, *8*(1), 68-77. doi: https://dx.doi.org/10.26418/justin.v8i1.37135

Blessing, L., & Chakrabarti, A. (2009). *DRM, a design research methodology*. Springer.

Bulamey, T., & Hendry. (2021). Perancangan kriptografi block cipher menggunakan pola logo media sosial. *Jurnal Sistem Komputer dan Informatika (JSON), 2*(2), 115-122. doi: http://dx.doi.org/10.30865/json.v2i2.2535

Dianta, I. (2021). *Logika dan algoritma untuk merancang aplikasi komputer*. Semarang: Yayasan Prima Agus Teknik.

Echeverri, C. (2017). *Visualization of the avalanche effect in CT2*. (Skripsi). Fakultas Matematika Bisnis, University of Mannheim, Mannheim.

Fachrurozi, M. F. (2006). *Enkripsi pesan rahasia menggunakan algoritma (Advanced Encryption Standard) AES: RIJNDAEL*. (Skripsi). Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah, Jakarta.

Fauzi, R., & Wellem, T. (2021). Perancangan kriptografi block cipher berbasis pola dribbling practice. *AITI: Jurnal Teknologi Informasi, 18*(1), 158-172. doi: https://doi.org/10.24246/aiti.v18i2.158-172

FIDE. (2009). *The laws of chess*. Diakses dari

https://www.fide.com/FIDE/handbook/LawsOfChess.pdf

Firdaus, I. L., Marwati, R., & Sispiyati, R. (2017). Aplikasi kriptografi komposisi one time pad cipher dan affine cipher. *Jurnal EurekaMatika*, *5*(2), 42-51.

Huda, M. (2023). *Implementasi model pemelajaran mesin dengan metode ensambel dan teknik seleksi fitur pada prediksi tingkat kemampuan pemeliharaan perangkat lunak.* (Skripsi). Fakultas Kampus UPI di Cibiru, Universitas Pendidikan Indonesia, Bandung.

Khairina, N., & Harahap, M. (2019). Modifikasi Myszkowski transposition cipher dengan chess board pattern. *Seminar Nasional Teknologi Informatika (SEMANTIKA)*, *2*(1), 28-34.

Kumbara, P., & Pakereng, M. (2019). Perancangan teknik kriptografi block cipher berbasis pola permainan tradisional rangku alu. *Jurnal Teknik Informatika dan Sistem Informasi, 5*(2), 189-200. doi: https://doi.org/10.28932/jutisi.v5i2.1714

Kurnia, A. (2014). *Keamanan web foto galery dengan menggunakan algoritma 3DES (Triple DES encryption standard)*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Kusumawardhani, D. (2017). *Implementasi algoritma BC3 dan RSA dalam sistem keamanan pesan electronic mail (email).* (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Leordian, A., & Pakereng, M. (2016). *Pengaruh perubahan ciphertext terhadap perancangan kriptografi block cipher 64 bit berbasis pola ikatan jimbe dengan menggunakan kombinasi S-box.* (Skripsi). Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

Louhenapessy, N., & Pakereng, M. (2016). *Perancangan kriptografi block cipher berbasis pola formasi futsal 1-2-1.* (Skripsi). Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

Mardiah. (2022). *Implementasi algoritma cipher block chaining dan transposisi grup simetri S4 pada pengamanan pesan teks.* (Skripsi). Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim, Malang.

Mawardina, M. (2016). *Aplikasi kriptografi dengan metode Vigenere cipher berbasis web*. (Skripsi). Fakultas Sains dan Teknologi, UIN Sunan Gunung Djati, Bandung.

Mohamed, K., Mohammed Pauzi, M., Mohd Ali, F., & Ariffin, S. (2022). Analyse on avalanche effect in cryptography algorithm. *European Proceedings of Multidisciplinary Sciences*.

Munir, R. (2019). *Kriptografi* (2nd ed.). Bandung: Informatika.

Nasupun, A., & Sipayung, Y. (2022). *Perancangan sistem penyewaan lapangan futsal pada futsal stadium Babadan Ungaran berbasis web*. (Skripsi). Fakultas Komputer dan Pendidikan, Universitas Ngudi Waluyo, Semarang.

Nasution, H., & Irwansyah, M. (2024). Perancangan teknik kriptografi block cipher berbasis pola peta administrasi Kalimantan Barat menggunakan key-dependent S-box. *Jurnal Informatika Polinema, 10*(3), 323-332. doi: https://doi.org/10.33795/jip.v10i3.5088

Nugroho, S. (2019). Brute force attack pada algoritma SHA-256. In *Talenta Conference Series: Science and Technology (ST) 2*(2). doi: https://doi.org/10.32734/st.v2i2.477

Nurjaman, A. (2016). *Modifikasi algoritma data encryption standard (DES) 64 bit untuk pengamanan pada penyimpanan file*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Pradeka, D. (2019). Implementasi aplikasi kriptografi berbasis Android menggunakan metode substitusi dan permutasi. In *In Search*, 18(1), 161-168). p-ISSN: 2085-7993 e-ISSN: 2580-3239.

Prameshwari, A., & Sastra, N. (2018). Implementasi algoritma Advanced Encryption Standard (AES) 128 untuk enkripsi dan dekripsi file dokumen. *Jurnal Eksplora Informatika, 8*(2), 52-58. doi: http://dx.doi.org/10.30864/eksplora.v8i1.139

Pratama, Z. A., & Sukma, D. (2023). Metodologi Perancangan Layanan Teknologi Informasi Menggunakan Kombinasi *Design Research Methodology* Dan *System Engineering*. *Power Elektronik: Jurnal Orang Elektro*, 12(3), 180-187. doi: https://doi.org/10.30591/polektro.v12i3.6040

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.

Ristiana, M. (2017). *Algoritma hybrid kriptografi RSA dengan kriptografi one time pad.* (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Ritonga, M., Kurniawan, M., & Agustini, S. (2024, *June*). Implementasi Mengamankan Pesan Teks Menggunakan Metode GOST (*Gosundarstevenny Standard*). *In Prosiding Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika (SNESTIK). 1*(1), 514-528. doi: https://doi.org/10.31284/p.snestik.2024.5713

Riyadi, S., & Astutik, I. (2022). Rancang bangun buku tamu berbasis web studi kasus dinas pendidikan Kabupaten Gresik. *JOINCS (Journal of Informatics, Network, and Computer Science, 4*(2), 35-38. doi: https://doi.org/10.21070/joincs.v5i2.1601

Santi, I. (2020). *Analisa perancangan sistem*. Pekalongan: NEM.

Sasongko, J. (2005). Pengamanan data informasi menggunakan kriptografi klasik. *Dinamik, 10*(3), 160-167. doi: https://doi.org/10.35315/dinamik.v10i3.25

Selimis, G., et al. (2007). A low power design for Sbox cryptographic primitive of Advanced Encryption Standard for mobile end-users. *Journal of Low Power Electronics, 3*(3), 1-10. doi: https://doi.org/10.1166/jolpe.2007.139

Sugiyanto, H., & Hapsari, R. (2016). Pengembangan algoritma Advanced Encryption Standard pada sistem keamanan SMS berbasis Android menggunakan algoritma Vigenere. *ULTIMATICS: Jurnal Teknik Informatika, 8*(2), 131-138. doi: https://doi.org/10.31937/ti.v8i2.528

Tuhumury, F. (2016). *Perancangan kriptografi block cipher 256 bit berbasis pada pola tuangan air.* (Skripsi). Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

Verma, R., & Sharma, A. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications, 10*(4), 119-122. doi: http://dx.doi.org/10.29322/IJSRP.10.04.2020.p10013