PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI *LIGHTWEIGHT PRESENT CIPHER* PADA *CIPHER BLOCK CHAINING*

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika

Reksa Alamsyah
NIM 2008475

PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2024

PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI
LIGHTWEIGHT PRESENT CIPHER* PADA *CIPHER BLOCK CHAINING

Oleh
Reksa Alamsyah

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

Universitas Pendidikan Indonesia
Agustus 2024

LEMBAR PENGESAHAN

REKSA ALAMSYAH

PENGAMANAN PESAN TEKS DENGAN KRIPTOGRAFI *LIGHTWEIGHT PRESENT CIPHER* PADA *CIPHER BLOCK CHAINING*

disetujui dan disahkan oleh pembimbing:

Pembimbing I

Prof. Siti Fatimah, S.Pd., M.Si., Ph.D.
NIP. 196808231994032002

Pembimbing II

Dra. Hj. Rini Marwati, M. S.
NIP. 196606251990012001

Mengetahui,
Ketua Program Studi Matematika,

Dr. Kartika Yulianti, S.Pd., M.Si.
NIP. 198207282005012001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Pengamanan Pesan Teks dengan Kriptografi *Lightweight Present Cipher* pada *Cipher Block Chaining*" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Apabila dikemudian hari ditemukan adanya pelanggaran, saya bersedia menanggung resiko atau sanksi yang dijatuhkan kepada saya.

Bandung, Juli 2024

Yang membuat pernyataan

Reksa Alamsyah

NIM. 2008475

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul "Pengamanan Pesan Teks dengan Kriptografi *Lightweight Present Cipher* pada *Cipher Block Chaining*". Tujuan penulisan skripsi ini adalah untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika di Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia.

Penulis menyadari keterbatasan pengetahuan dan kemampuan yang penulis miliki sehingga penulis terbuka terhadap kritik dan saran untuk kesempurnaan skripsi ini. Penulis berharap skripsi ini dapat bermanfaat bagi pembaca.

Bandung, Juli 2024

Penulis

UCAPAN TERIMA KASIH

Penulisan skripsi ini tidak terlepas dari dukungan, bantuan, dan doa dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Ibu Prof. Siti Fatimah, S.Pd., M.Si., Ph.D. selaku Dosen Pembimbing Akademik dan Dosen Pembimbing I yang telah meluangkan waktu, memberi arahan, masukan, dan motivasi yang banyak membantu dari awal hingga akhir penyusunan skripsi ini;
2. Ibu Dra. Rini Marwati, M.S., selaku Dosen Pembimbing II yang telah meluangkan waktu, memberi arahan, masukan, dan motivasi yang banyak membantu dari awal hingga akhir penyusunan skripsi ini;
3. Ibu Dr. Kartika Yulianti, S.Pd., M.Si. selaku Ketua Program Studi Matematika, Universitas Pendidikan Indonesia;
4. Ibu Ririn Sispiyati, S.Si., M.Si., selaku Ketua KBK Terapan, Program Studi Matematika, Universitas Pendidikan Indonesia;
5. Seluruh dosen dan civitas akademika di lingkungan Departemen Pendidikan Matematika, Universitas Pendidikan Indonesia;
6. Kedua orang tua dan kakak yang telah memberikan dukungan moral dan materil, kasih sayang, serta doa yang tak terhingga kepada penulis;
7. Teman dan sahabat Matematika C tahun 2020 selama kuliah khususnya tongkrongan "*The Boys*" Fachri Hidayah Maliki Saddam, Miftah Fadillah Sopian, Muhammad Aqil Nizamuddin, dan Muhamad Teguh Galih Pamenang yang telah membersamai, menghibur, membantu, memberi dukungan, memotivasi, penulis dari awal sampai akhir perkuliahan;
8. Devita Pratiwi yang telah memotivasi dan menyemangati penulis dalam menyelesaikan penulisan skripsi;
9. Pihak-pihak yang tidak dapat penulis cantumkan namanya satu persatu, yang telah secara langsung dan/atau tidak langsung memberi saran dan dukungan selama proses penulisan skripsi ini sehingga memotivasi penulis untuk menyelesaikannya.

ABSTRAK

Algoritma kriptografi *lightweight* dirancang sedemikian sehingga dapat diterapkan pada suatu perangkat IoT yang terbatas. Salah satu *cipher* yang termasuk ke dalam kriptografi *lightweight* adalah *Present Cipher*. Menurut beberapa artikel, *Present Cipher* sangat efisien dari segi *hardware* maupun *software* sehingga *Present Cipher* menjadi contoh terbaik dari algoritma kriptografi *lightweight*. Terlebih lagi *Present Cipher* telah distandarisasi oleh ISO/IEC. *Present Cipher* merupakan Blok *Cipher* dengan skema SPN sehingga dibutuhkan suatu mode operasi. Oleh karena itu, dipilih *Cipher Block Chaining* sebagai mode operasi pada penelitian ini. Penelitian ini bertujuan untuk memperoleh pengamanan pesan teks dengan kriptografi *lightweight Present Cipher* pada *Cipher Block Chaining* dan mengimplementasikannya dalam sebuah aplikasi menggunakan bahasa pemrograman Python. Berikutnya aplikasi tersebut divalidasi dengan bantuan Excel. Hasil dari penelitian ini berupa aplikasi yang dapat digunakan pengguna untuk mengamankan pesan teks dengan kriptografi *lightweight Present Cipher* pada *Cipher Block Chaining*.

Kata Kunci: Kriptografi *Lightweight*, Blok Cipher, *Present Cipher*, *Cipher Block Chaining*.

ABSTRACT

The Lightweight Cryptography algorithm is design in such a way that it can be implemented on a constrained IoT device. One of the ciphers falling under lightweight cryptography is the Present Cipher. According to several articles, the Present Cipher is highly efficient in terms of both hardware and software, making it an excellent example of lightweight cryptography algorithms. Moreover, Present Cipher has been standardized by ISO/IEC. Present Cipher is a Block Cipher with an SPN scheme, requiring a mode of operation. Therefore, Cipher Block Chaining was chosen as the mode of operation in this study. The objective of this research is to achieve secure plaintext communication using lightweight cryptography Present Cipher in Cipher Block Chaining mode and to implement it in an application using the Python programming language. Furthermore, this application is validated with the assistance of Excel. The outcome of this research is an application that allows users to secure plaintext messages using lightweight cryptography Present Cipher in Cipher Block Chaining mode.

***Key Words**: Lightweight Cryptography, Block Cipher, Present Cipher, Cipher Block Chaining.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Bhardwaj, I., Kumar, A., & Bansal, M. (2017, September). A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 504-509). IEEE.

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*, *9*, 28177-28193.

Çamur, Z. (2020). *A study of lightweight cryptography* (Master's thesis, Middle East Technical University).

Katagi, M., & Moriai, S. (2008). Lightweight Cryptography for the Internet of Things. *Sony Corporation*, *2008*, 7-10.

Sallam, S., & Beheshti, B. D. (2018, October). A Survey on Lightweight Cryptographic Algorithms. In *TENCON 2018-2018 IEEE Region 10 Conference* (pp. 1784-1789). IEEE.

Munir, R. (2019). *Kriptografi*. Edisi ke-2, Bandung: Informatika Bandung.

Putri, W. E., Dewanta, F., & Afianti, F. (2022). Analisis Perbandingan Block Cipher Simon-Speck, Simeck, Skinny pada Komunikasi Berbasis LoRa. *MULTINETICS*, *8*(2), 97-104.

Biryukov, A., & Perrin, L. (2017). State of the Art in Lightweight Symmetric Cryptography. *Cryptology ePrint Archive*.

Bartle, R. G., & Sherbert, D. R., (2011). *Introduction to Real Analysis.* Edisi ke-4, Urbana: John Wiley & Sons, Inc.

Burton, D. M., (2010). *Elementary Number Theory.* Edisi ke-7, New York: The McGraw Hill Companies

Stinson, D. R. (2019). *Cryptography Theory and Practice*. Edisi ke-4. Boca Raton: CRC Press.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007). *PRESENT*: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th*

International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9 (pp. 450-466). Springer Berlin Heidelberg.

Brookshear, J. G., & Brylow, D. (2015). *Computer Science: An Overview (12th Edition)*. Pearson

Diehl, W., Farahmand, F., Yalla, P., Kaps, J. P., & Gaj, K. (2017, September). Comparison of hardware and software implementations of selected lightweight block ciphers. In *2017 27th International Conference on Field Programmable Logic and Applications (FPL)* (pp. 1-4). IEEE.

Bellizia, D., Scotti, G., & Trifiletti, A. (2016, June). Implementation of the *PRESENT*-80 block cipher and analysis of its vulnerability to Side Channel Attacks Exploiting Static Power. In *2016 MIXDES-23rd International Conference Mixed Design of Integrated Circuits and Systems* (pp. 211-216). IEEE.

Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2017). Lightweight hardware architectures for the *Present Cipher* in FPGA. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *64*(9), 2544-2555.

Bujari, D., & Aribas, E. (2017). Comparative Analysis of Block Cipher Modes of Operation