PENYAMARAN TEKS DENGAN SKEMA *HYBRID* MENGGUNAKAN ALGORITMA ENIGMA DAN ALGORITMA ELGAMAL

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar

Sarjana Matematika

Oleh:

Athala Dwi Cahyani

1800986

PROGRAM STUDI MATEMATIKA
DEPARTEMEN PENDIDIKAN MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2022

LEMBAR HAK CIPTA

PENYAMARAN TEKS DENGAN SKEMA *HYBRID* MENGGUNAKAN ALGORITMA ENIGMA DAN ALGORITMA ELGAMAL

Oleh:

Athala Dwi Cahyani

1800986

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2022

LEMBAR PENGESAHAN

ATHALA DWI CAHYANI

PENYAMARAN TEKS DENGAN SKEMA *HYBRID* MENGGUNAKAN ALGORITMA ENIGMA DAN ALGORITMA ELGAMAL

disetujui dan disahkan oleh pembimbing:

Pembimbing I

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

Pembimbing II

Ririn Sispiyati, S.Si., M.Si.
NIP. 198106282005012001

Mengetahui,

Ketua Departemen Pendidikan Matematika

Dr. H. Dadang Juandi, M. Si.
NIP. 196401171992021001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Penyamaran Teks Dengan Skema *Hybrid* Menggunakan Algoritma Enigma Dan Algoritma Elgamal" 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. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Agustus 2022

Yang Membuat Pernyataan

Athala Dwi Cahyani

NIM. 1800986

KATA PENGANTAR

Assalamu'alaikum wr. wb.

Dengan mengucapkan puji syukur kehadirat Allah swt. serta salawat dan salam kepada Nabi Muhammad saw., penulis dapat menyelesaikan skripsi yang berjudul "Penyamaran Teks Dengan Skema *Hybrid* Menggunakan Algoritma Enigma Dan Algoritma Elgamal".

Skripsi ini diajukan untuk memenuhi sebagian syarat untuk memenuhi gelar Sarjana Matematika di Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia. Penulis mengucapkan terima kasih kepada pihak-pihak yang senantiasa memberi dukungan dan dalam proses penulisan skripsi ini dari awal hingga akhir.

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

Bandung, Agustus 2022

Penulis

UCAPAN TERIMA KASIH

Dengan mengucapkan puji syukur kehadirat Allah swt. serta salawat dan salam kepada Nabi Muhammad saw., penulis dapat menyelesaikan skripsi dengan tepat waktu. 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 Dra. Hj. Rini Marwati, M.S., selaku Dosen Pembimbing I yang telah meluangkan waktu, memberi arahan, masukan, dan motivasi yang banyak membantu dari awal hingga akhir penyusunan skripsi ini;
2. Ibu Ririn Sispiyati, S.Si, M.Si., selaku Dosen Pembimbing II yang telah meluangkan waktu, memberi arahan, masukan, dan motivasi yang banyak membantu dari awal hingga akhir penyusunan skripsi ini;
3. Kedua orang tua tercinta, Ayah dan Mama, yang telah memberikan dukungan moral dan materil, kasih sayang, serta doa yang tak terhingga kepada penulis;
4. Bapak Drs. H. Cece Kustiawan, M.Si., selaku Ketua Program Studi Matematika, Universitas Pendidikan Indonesia;
5. Ibu Dr. Kartika Yulianti, M.Si., selaku Ketua KBK Terapan, Program Studi Matematika, Universitas Pendidikan Indonesia;
6. Seluruh dosen dan civitas akademika di lingkungan Departemen Pendidikan Matematika, Universitas Pendidikan Indonesia;
7. Kakak dan kakak ipar yang telah memberikan dukungan serta bantuan ilmunya dalam proses penulisan skripsi ini;
8. Teman dan sahabat selama kuliah, Wanda, Fadhilah, Caki, Hanna, Andika, Hilmi, dan Rian, yang telah membersamai, menghibur, membantu, memberi dukungan, memotivasi, dan mendengarkan keluh kesah penulis dari awal perkuliahan sampai akhir perkuliahan;
9. Teman dan sahabat, Bunga, Fairuz, teman-teman “SMA”: Alda, Vincent, Caca, Clarissa, Arsyad, Fadil, Rafii, dan Reza yang selalu menemani,

mendengarkan, menghibur, membantu, memberi dukungan, dan memotivasi dalam keadaan suka maupun duka yang dialami penulis;

10. Seluruh rekan-rekan mahasiswa Departemen Pendidikan Matematika 2018 dan Kesospol HIU;
11. Pihak-pihak yang tidak dapat penulis cantumkan namanya, yang telah secara langsung dan/atau tidak langsung memberi saran dan dukungan, memberi rasa senang, sedih, aman, tenang, sakit, serta kecewa selama proses penulisan skripsi ini sehingga memotivasi penulis untuk menyelesaikannya.

Semoga Allah swt. senantiasa memberikan balasan yang berkali-kali lipat atas dukungan-dukungan yang telah diberikan kepada penulis dalam menyelesaikan skripsi ini.

ABSTRAK

"Penyamaran Teks Dengan Skema *Hybrid* Menggunakan Algoritma Enigma Dan Algoritma ElGamal"

Pada perkembangan digital dalam pertukaran informasi, kriptografi masih mejadi metode yang digunakan untuk merahasiakan suatu informasi (pesan). Algoritma Enigma adalah salah satu kriptografi simetris. Karena kunci Enigma rentan diretas, perlu adanya peningkatan kerahasiaan pesan memanfaatkan metode kriptografi *hybrid*. Kriptografi *hybrid* adalah gabungan antara kriptografi simetris dan kriptografi asimetris. Salah satu contoh kriptografi asimetris adalah algoritma ElGamal. Pada penelitian ini dikonstruksi sebuah program untuk menyamarkan pesan memanfaatkan kriptografi *hybrid* antara algoritma Enigma dan algoritma ElGamal, di mana kunci Enigma akan dienkripsi kembali menggunakan algoritma ElGamal untuk menghindari pesan diretas oleh pihak lain. Algoritma ElGamal dipilih karena sulitnya menyelesaikan masalah logaritma diskrit akibat bilangan acak k yang dipilih saat proses enkripsi dirahasiakan. Hasil dari penelitian ini adalah terbentuknya suatu skema *hybrid* yang memanfaatkan alogritma Enigma dan algoritma ElGamal serta sebuah program aplikasi yang dibuat dengan bahasa pemrograman Python dengan memanfaatkan *Graphical User Interface* (GUI) sehingga memudahkan pengguna (*user-friendly*).

Kata Kunci: Kriptografi, kriptografi simetris, kriptografi asimetris, algoritma Enigma, algoritma ElGamal.

ABSTRACT

"Encoding Text with Hybrid Scheme Using the Enigma Algorithm and the ElGamal Algorithm"

In digital developments in the exchange of information, cryptography is still the method used to keep information (message) secret. The Enigma algorithm is one of symmetric cryptography. Since Enigma keys are susceptible to be hacked, it is necessary to increase message's secrecy using hybrid cryptography methods. Hybrid cryptography is a combination of symmetric cryptography and asymmetric cryptography. One example of asymmetric cryptography is the ElGamal algorithm. In this research, a program is constructed to encode messages using hybrid cryptography between the Enigma algorithm and the ElGamal algorithm, which the Enigma key will be re-encrypted using the ElGamal algorithm to avoid messages being hacked by other parties. The ElGamal algorithm was chosen because of the difficulty of solving the discrete logarithm problem due the random number k chosen during the encryption process to be kept secret. The results of this research are the formation of hybrid scheme using the Enigma algorithm and the ElGamal algorithm as well as a application program made in the Python programming language by utilizing the Graphical User Interface (GUI) to make it easier for user (user-friendly).

Key Words: Cryptography, symmetric cryptography, asymmetric cryptography, the Enigma algorithm, the ElGamal algorithm

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi.* Yogyakarta: CV ANDI OFFSET

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

Christensen, C. (2007). Polish Mathematicians Finding Patterns in Enigma Messages. *Mathematics Magazine*, *80*(4). 247-273.

Dent, A. W. (2005). *Hybrid Cryptography*. Egham Hill: Royal Holloway, University of London.

Dummit, E. (2016). *Discrete Logarithms in Cryptography*. Rochester: University of Rochester.

Firdaus, J., Marwati, R., & Gozali, S. (2018). Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang Ditingkatkan dengan Algoritma Elgamal. *EurekaMatika, 6*(1). 23-32.

Hikmah, A. N. (2020). *Penyandian Pesan Dengan Menggunakan Kriptografi Hybrid Autokey Vigènere Cipher Dan Algoritma Elgamal*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Lingga, M. (2019). *Implementasi Algoritma Enigma Cipher dan Caesar Cipher Pada Pengamanan Data Teks Dalam Pembangkitan QR Code*. (Skripsi). Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Medan.

Nugroho, E. F. (2006). *Studi Enkripsi dan Kriptanalisis terhadap Enigma.* Bandung: Institut Teknologi Bandung.

Nursalim, R. (2019*). Struktur Aljabar: Teorema Grup.* [*Online*]. Diakses dari https://www.rahmateduc.com/2019/02/struktur-aljabar-grup-modulo.html

Prasetio, Y., Triandi, B., & Hardianto. (2018). Perancangan Aplikasi Pengamanan File Teks dengan Skema *Hybrid* Menggunakan Algoritma Enigma dan Algortitma RSA. *IT Journal, 6*(1) 46-55.

Raharjo, B. (2015). *Mudah Belajar Python untuk Aplikasi Desktop dan Web.* Bandung: Penerbit INFORMATIKA.

Smart, N. P. (2016). *Cryptography Made Simple.* Bristol: Springer International Publishing Switzerland.

Stinson, D., & Paterson, M. (2019). *Cryptography Theory and Practice Fourth Edition.* Boca Raton: Taylor & Francis Group.

Welchman, G. (1997). *The Hut Six Story: Breaking the Enigma Codes.* Worcestershire: Classic Crypto Books.