

**PENGAMANAN DATA TEKS MENGGUNAKAN ALGORITMA
KRIPTOGRAFI ELGAMAL DAN XOR DARI SERANGAN HACKER**

SKRIPSI

Oleh

**KHAIRANI
71180915008**



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM SUMATRA UTARA
MEDAN
2023**

KATA PENGANTAR

Assalamu alaikum warrahmatullahi wabbarakaatuh

Alhamdulillahirobbil'alamin, puji syukur kehadirat Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul : **PENGAMANAN DATA TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI ELGAMAL DAN XOR DARI SERANGAN HACKER**

Shalawat serta salam senantiasa penulis sanjungkan kepada baginda Rasulullah SAW beserta keluarga, sahabat-sahabat dan para pengikutnya yang telah membawa cahaya Islam dan masih berkembang hingga saat ini.

Penulis menyadari bahwa terselesaikannya skripsi ini bukanlah hasil jerih payah penulis sendiri. Melainkan terdapat usaha dan bantuan baik berupa moral maupun spiritual dari berbagai pihak kepada penulis. Oleh karena itu, penulis hendak sampaikan terimakasih kepada :

1. Bapak Dr. H. Yanhar Jamluddin, MAP, selaku Rektor Universitas Islam Sumatera Utara
2. Bapak Ir. Abdul Haris Nasution, MT, selaku Dekan Fakultas Teknik Universitas Islam Sumatera Utara.
3. Bapak Mhd. Zulfansyuri Siambaton, ST, M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Islam Sumatera Utara.
4. Bapak Oris Krianto Sulaiman, ST, M.Kom selaku Pembimbing I, yang telah memberikan arahan dan bimbingan dalam menyelesaikan skripsi ini.
5. Bapak Mhd. Zulfansyuri Siambaton, ST, M.Kom. selaku Pembimbing II, yang telah memberikan arahan dan bimbingan dalam menyelesaikan skripsi ini.
6. Seluruh Dosen dan Staff Program Studi Teknik Informatika yang telah membantu dan menjadi tempat bertanya jika saya mengalami kesulitan dalam penulisan skripsi ini.
7. Kedua orang tua dan keluarga dirumah yang memberikan Rahmat dan

Hidayah sehingga dapat menyelesaikan skripsi ini.

8. Teman-teman kuliah khususnya Program Studi Teknik Infomatika Univesitas Islam Sumatera Utara yang telah memberikan motivasi, kritik dan saran.

Penulis menyadari adanya kekurangan dan ketidaksempurnaan dalam penulisan skripsi ini, karena itu penulis menerima kritik, saran dan masukan dari pembaca sehingga penulis dapat lebih baik dimasa yang akan datang. Akhirnya penulis berharap semoga laporan skripsi ini bias bermanfaat khususnya bagi penulis dan umumnya bagi para pembaca.

Medan, 2023

Penulis

Khairani

DAFTAR ISI

	Halaman
KATA PENGANTAR.....	i
ABSTRAK	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR.....	vi
DAFTAR TABEL	vii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	4
1.6. Sistematika Penulisan.....	4
BAB II LANDASAN TEORI	5
2.1. Kriptografi	5
2.1.1. Tujuan Kriptografi.....	6
2.2. Elgamal	7
2.2.1. Proses Pembentukan Kunci Elgamal.....	7
2.2.2. Contoh Perhitungan ElGamal.....	8
2.3. Xor	12
2.3.1. Proses Enkripsi Xor.....	12
2.3.2 Contoh Perhitungan Enkripsi XOR.....	13
2.3.3 Contoh Perhitungan Proses Dekripsi XOR	14

BAB III METODE PENELITIAN	16
3.1. Pengertian Perancangan.....	16
3.2. Alat dan Bahan	16
3.3. Rancangan Penelitian.....	17
3.4. Algoritma Elgamal.....	21
3.5. XOR (<i>eXclusive OR</i>)	25
3.6 Perancangan Antarmuka.....	27
3.6.1 Perancangan Antarmuka Pembangkit Kunci.....	27
3.6.2 Perancangan Antarmuka Enkripsi	28
3.6.3 Perancangan Antarmuka Dekripsi.....	30
BAB IV IMPLEMENTASI DAN HASIL	31
4.1. Implementasi Sistem.....	31
4.1.1. Pembangkitan Kunci Enhanced ElGamal Dan XOR.....	31
4.1.2. Proses Enkripsi.....	33
4.1.3. Proses Dekripsi.....	37
4.2. Hasil.....	41
BAB V KESIMPULAN DAN SARAN	42
5.1. Kesimpulan	42
5.2. Saran	42
DAFTAR PUSTAKA	43
LAMPIRAN.....	45

DAFTAR GAMBAR

	Halaman
Gambar 2.1. Skema Ekripsi Dan Dekripsi	6
Gambar 3.1. Skema Umum Pengiriman Pesan Menggunakan Algoritma Kriptografi Elgamal Dan Xor	17
Gambar 3.2. Flowchart Enkripsi Elgamal Dan Xor	18
Gambar 3.3. Flowchart Dekripsi Elgamal Dan Xor	20
Gambar 3.4. Skema Algoritma Elgamal	21
Gambar 3.5. Rancangan Antarmuka Pembangkit Kunci	28
Gambar 3.6. Rancangan Antarmuka Enkripsi	29
Gambar 3.7. Rancangan Antarmuka Dekripsi	30
Gambar 4.1. Antarmuka Pembangkit Kunci Elgamal Xor	31
Gambar 4.2. Hasil Pembangkitan Kunci Elgamal dan Xor	32
Gambar 4.3. Kunci Enkripsi	33
Gambar 4.4. Antarmuka Enkripsi	34
Gambar 4.5. Proses Unggah Kunci Enkripsi	35
Gambar 4.6. Hasil Enkripsi	36
Gambar 4.7. Kunci Dekripsi	37
Gambar 4.8. Antarmuka Dekripsi	38
Gambar 4.9. Proses Unggah Kunci Dekripsi	39
Gambar 4.10. Hasil Dekripsi	40

DAFTAR TABEL

Halaman

Tabel 2.1 Perhitungan $a^2 \bmod p$ dan $a^a \bmod p$	8
Tabel 2.2 Konversi karakter ke kode ASCII	9
Tabel 2.3 Enkripsi <i>Plaintext</i> ke <i>Ciphertext</i>	10
Tabel 2.4 Dekripsi <i>Ciphertext</i> ke <i>Plaintext</i>	11
Tabel 2.5. Tabel Logika Operasi	12

DAFTAR PUSTAKA

- Alfiah, F., Sudarji, R., & Taqiyyuddin Al Fatah, D. (2020). *Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake*. 12260.
- Azis, N., Pribadi, G., & Nurcahaya, M. S. (2020). Analisa dan Perancangan Aplikasi Pembelajaran Bahasa Inggris Dasar Berbasis Android. *Nur Aziz, Gali Pribadi, Manda Savitrie Nurcahya*, 35(5), 1068–1089.
- Iqbal, H., & Krawec, W. O. (2020). Semi-quantum cryptography. In *Quantum Information Processing* (Vol. 19, Issue 3). Springer US. <https://doi.org/10.1007/s11128-020-2595-9>
- Jorgensen, P. (2003). Applied cryptography: Protocols, algorithm, and source code in C. *Government Information Quarterly*, 13(3), 336. [https://doi.org/10.1016/s0740-624x\(96\)90083-0](https://doi.org/10.1016/s0740-624x(96)90083-0)
- Makhomah, R., Santoso, K. A., & Kamsyakawuni, A. (2021). Pengkodean Teks Menggunakan Kombinasi Hill Cipher dan Operasi XOR. *PRISMA, Prosiding Seminar Nasional Matematika*, 4, 548–552.
- Rubinstein_Salzedo, S. (2018). *Cryptography*. Springer Cham. <https://doi.org/10.1007/978-3-319-94818-8>.
- Saputro, Pujo, H. (2023). Implementasi Algoritma Exclusive OR (XOR) Dalam Pengembangan Aplikasi Chat Berbasis Android. *Informatika Fakultas Sains & Teknologi Universitas Labuhan Batu*, 11(1), 71–76.
- Sidik, A. P., Komputer, S., Sains, F., Pembangunan, U., Budi, P., Gatot, J. J., Km, S., Sikambing, S., Medan, K., & Utara, S. (2019). Teknik Xor Pada Mode Operasi Algoritma Cipher Block Chaining (Cbc) Dengan Kunci Acak Blum Blum Shub Dalam Meningkatkan Keamanan Data. *Jurnal Mantik Penusa*, 3(2), 130–135.
- Stinson, D., & Paterson, M. (2019). *Cryptography Theory and Practice*

Fourth Edition (Fourth Edi). Chapman & Hall.
<https://www.ptonline.com/articles/how-to-get-better-mfi-results>

Sulaiman, O. K., Nasution, K., & Siambaton, M. Z. (2020). Three Pass Protocol untuk Keamanan Kunci Berbasis Base64 pada XOR Cipher. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, 4(September), 721–727.

Yousif, S. F., Abboud, A. J., & Radhi, H. Y. (2020). Robust Image Encryption with Scanning Technology, the El-Gamal Algorithm and Chaos Theory. *IEEE Access*, 8, 155184–155209.
<https://doi.org/10.1109/ACCESS.2020.3019216>

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

LAMPIRAN

