

Aplikasi Pengiriman Email Menggunakan Enkripsi
Elliptic Curve Diffie Hellman

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh
gelar Sarjana Matematika



oleh:

Michael Alberto Ferdinan

1701973

Program Studi Matematika
Departemen Pendidikan Matematika
Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam
Universitas Pendidikan Indonesia
2021

APLIKASI PENGIRIMAN EMAIL MENGGUNAKAN ENKRIPSI
ELLIPTIC CURVE DIFFIE HELLMAN

Oleh
Michael Alberto Ferdinan

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

© Michael Alberto Ferdinan 2021
Universitas Pendidikan Indonesia
Agustus 2021

Hak Cipta dilindungi undang-undang.
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

LEMBAR PENGESAHAN

MICHAEL ALBERTO FERDINAN

Aplikasi Pengiriman Email Menggunakan Enkripsi
Elliptic Curve Diffie Hellman

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

ABSTRAK

Keamanan pesan email merupakan aspek yang sangat esensial. Jika ada pihak yang tidak diharapkan dapat melihat isi pesan email kita maka kita akan dirugikan. Kita ambil contoh misalkan ketika membuat akun untuk *market place*, pengguna diminta untuk mengaitkan akun tersebut dengan akun email yang dia miliki dan wajib menyetujui syarat-syarat yang biasanya langsung mencentangnya atau menyetujuinya tanpa harus membaca apa isi syarat-syarat tersebut. Ternyata di dalam syarat-syarat tersebut salah satunya berisi terkait pihak ketiga atau pemilik perusahaan *market place* dapat melihat isi pesan email kita. Ini mengindikasikan bahwa isi pesan email dapat lihat oleh orang lain dan tidak aman. Oleh karena itu, diperlukan langkah antisipasi berupa peningkatan keamanan pesan email. Salah satunya dengan menerapkan kriptografi. Salah satu contoh algoritma kriptografi yang sering digunakan adalah *Elliptic Curve Cryptography* (ECC). Pada penelitian digunakan perluasan ECC yaitu *Elliptic Curve Diffie Hellman* (ECDH). Hasilnya diperoleh skema pengiriman email menggunakan enkripsi ECDH mulai dari pembangkitan kunci, enkripsi email, pengiriman email, dan dekripsi email. Program aplikasi dikonstruksi dengan menggunakan bahasa pemrograman Python untuk mempermudah penggunaan algoritma yang dikembangkan ini.

Kata Kunci : email, kriptografi, ECC, ECDH

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN.....	iii
KATA PENGANTAR.....	4
ABSTRAK.....	5
DAFTAR ISI.....	6
DAFTAR TABEL.....	9
DAFTAR GAMBAR.....	10
BAB I PENDAHULUAN.....	11
1.1 Latar Belakang.....	11
1.2 Rumusan Masalah.....	13
1.3 Batasan Masalah.....	13
1.4 Tujuan Penelitian.....	13
1.5 Manfaat.....	13
1.6 Sistematika Penulisan.....	14
BAB II LANDASAN TEORI.....	15
2.1 Kekongruenan.....	15
2.1.1 Definisi kekongruenan (Rosen, 1986).....	15
2.1.2 Teorema Balik modulo (Rosen, 1986).....	15
2.1.3 Definisi Faktor Persekutuan Terbesar (Burton, 2011).....	15
2.1.4 Definisi Relatif Prima (Rosen, 1986).....	15
2.2 Grup.....	16
2.2.1 Definisi Grup (Gallian, 2012).....	16
2.2.2 Definisi Grup Berhingga (Gallian, 2012).....	16
2.2.3 Definisi Grup Siklik (Gallian, 2012).....	16
2.2.4 Teorema Grup Siklik (Gallian, 2012).....	16
2.2.5 Teorema Generator (Gallian, 2012).....	16
2.2.6 Definisi Sub Grup (Gallian, 2012).....	16
2.3 Kriptografi (Stinson, 2003).....	17
2.4 Caesar Cipher (Munir, 2019).....	17

2.5 Masalah Logaritma Diskrit	18
2.6 Algoritma Pertukaran Kunci Diffie Hellman	18
2.7 Kurva Eliptik.....	20
2.7.1 Kurva Eliptik pada Lapangan p (Silverman, 2006).....	20
2.7.2 Elliptic Curve Cryptography (ECC)	22
2.7.3 <i>Elliptic Curve Discrete Logarithm Problem</i> (ECDLP).....	26
2.8 Email	26
2.9 ASCII	26
2.10 Bahasa Pemrograman Python.....	27
BAB III METODE PENELITIAN	29
3.1 Model Dasar.....	29
3.2 Pengembangan Model.....	31
3.3 Perancangan Program Komputer	32
3.3.1 Input Output	32
3.3.2 Rancangan Tampilan.....	32
3.4 Algoritma	34
3.4.1 Pembangkitan Kunci:.....	34
3.4.2 Enkripsi:.....	34
3.4.3 Pengiriman email	35
3.4.4 Dekripsi.....	35
3.5 Validasi	36
BAB IV HASIL DAN PEMBAHASAN	37
4.1 Skema Pengiriman Email Menggunakan Enkripsi	37
4.2 Program Aplikasi Pengiriman Email Menggunakan Enkripsi ECDH	38
4.2.1 Tampilan Program Aplikasi Pembangkitan Kunci.....	38
4.2.2 Enkripsi dan Dekripsi.....	41
4.2.3 Pengiriman Email.....	42
4.3 Validasi Program dengan Contoh	43
BAB V SIMPULAN DAN SARAN.....	46
5.1 Kesimpulan	46
5.2 Saran	46
DAFTAR PUSTAKA.....	47
LAMPIRAN.....	49

Lampiran 1 : ECMath.py	49
Lampiran 2 : EllipticCurve.py	54
Lampiran 3 : Point.py	59
Lampiran 4 : Skripsi App.py.....	64

DAFTAR TABEL

Tabel 1. Substitusi	18
Tabel 2. Substitusi x ke $x^3 + x + 1$	20
Tabel 3. Substitusi y ke y^2	20

DAFTAR GAMBAR

Gambar 2. 1 Skema Algoritma Pertukaran Kunci Diffie-Hellman.....	19
Gambar 2. 2 Kurva E	23
Gambar 2. 3 Kurva E dengan titik P dan Q	23
Gambar 2. 4 Kurva E dengan garis L.....	23
Gambar 2. 5 Kurva E dengan titik R.....	23
Gambar 2. 6 Kurva E dengan garis vertikal yang melalui titik R dengan titik P+Q.....	24
Gambar 2. 7 Kurva E dengan titik P	24
Gambar 2. 8 Kurva E dengan garis L yang melalui P.....	24
Gambar 2. 9 Kurva E dengan garis vertikal R	25
Gambar 2. 10 Kurva E dengan titik P dan Q	25
Gambar 2. 11 Kurva E dengan garis yang melalui titik P dan Q	25
Gambar 2. 12 Kurva E dengan titik tambahan ∞	26
Gambar 2. 13 Tabel ASCII	27
Gambar 3. 1 Algoritma ECC.....	30
Gambar 3. 2 Algoritma ECDH	31
Gambar 3. 3 Skema pengembangan ECDH untuk enkripsi email	32
Gambar 3. 4 Tampilan Utama.....	33
Gambar 3. 5 Pembangkitan Kunci	34
Gambar 3. 6 Enkripsi dan Dekripsi.....	34
Gambar 3. 7 Pengiriman Email.....	35
Gambar 4. 1 Skema Pengiriman Email menggunakan Enkripsi ECDH	38
Gambar 4. 2 Tampilan Tab Pembangkitan Kunci Oleh Alice	40
Gambar 4. 3 Tampilan Tab Pembangkitan Kunci Oleh Bob	41
Gambar 4. 4 Tampilan Tab Enkripsi Oleh Alice	42
Gambar 4. 5 Tampilan Tab Dekripsi Oleh Bob	43
Gambar 4. 6 Tampilan Tab Pengiriman Email	44
Gambar 4. 7 Pada saat Bob mendapatkan pesan email dari Alice	44

DAFTAR PUSTAKA

- Agustina, E. R. & Kurniati, A. (2009). *Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada E-Voting di Indonesia*. Seminar Nasional Informatika.
- Buchanan, W. J. (2020). *Golang ECDH*. Asecuritysite. doi: <https://asecuritysite.com/encryption/goecdh>
- Burton, D. M. (2011). *Elementary Number Theory Seventh Edition*. New York: McGraw-Hill.
- Cameron, P. J. (2003). *Notes on cryptography*. London: Queen Mary, University of London.
- Gallian, J. A. (2012). *Contemporary Abstract Algebra*. University of Minnesota Duluth.
- Lutz, M. (2009). *Learning Python*. United States of America: O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.
- Monica dkk (2020). *Implementation of Elliptic – Curve Cryptography*. International Journal of Electrical Engineering and Technology (IJEET) Volume 11, Issue 2, March-April 2020, pp. 178-189.
- Munir, R. (2012). *Matematika Diskrit*. Bandung: Penerbit Informatika.
- Munir, R. (2013). *Elliptic Curve Cryptography*. Bandung : Informatika Bandung.
- Munir, R. (2019). *Kriptografi Edisi Kedua*. Bandung: Penerbit Informatika.
- Nakov, S. (2018). *Practical Cryptography for developers*.
- Palme, J. (2019). *Electronic Mail*. London : Artech House Boston.
- Rosen, K. H. (1983). *Elementary Number Theory and Its Applications*. London: ADDISON-WESLEY
- Schneier, B. (1996). *Applied Cryptography Second Edition*.
- Sihotang, T. R. (2017). *Kriptosistem Gabungan antara S-ECIES dan RSA*.

- Silverman, J. H (2006, June - July June 19 - July 7,). *An Introduction to the Applications to Cryptography*. Computational Number Theory and, hal. 1-103.
- Sobari, A. I. (2017). *Aplikasi Pengirim Email dengan Penerapan Enkripsi Caesar Cipher yang Telah Ditingkatkan Keamannya Menggunakan Enkripsi Row Transpositon Cipher*.
- Stalling, W., (2011), *Cryptography and network security, principle and practice 2nd edition*, Pearson Education, Inc.
- Stinson, D. R. (2003). *Cryptography Theory and Practice Third Edition*. London: Capman & Hall/CRC.
- Tumbur, S. T. (2014). *Hyper Elliptic Curve Cryptography for e-Commerce Channel*. Institut Teknologi Bandung.
- Zahra, D. A. (2020). *Kriptografi Visual Pada Gambar Berwarna (RGB) Menggunakan Algoritma Elliptic Curve Cryotography*.
- Zulkifar, M. I. dkk (2019). *Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)*.