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

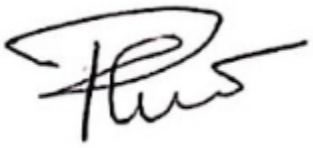
LEMBAR PENGESAHAN

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 perusahan *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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

Agustina, E. R. & Kurniati, A. (2009). *Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Indormasi Pada E-Voting di Indonesia*. Seminar Nasioal 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 Cryotography*. 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 Crytography 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)*.