

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE DIFFIE HELLMAN*
PADA *TWO WAY CHALLENGE-RESPONSE PROTOCOL*
SEBAGAI PROTOKOL AUTENTIKASI *USER***

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika



Oleh

Hilda Kurnia Fitri 1801288

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

2022

LEMBAR HAK CIPTA

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE DIFFIE HELLMAN*
PADA *TWO WAY CHALLENGE-RESPONSE PROTOCOL*
SEBAGAI PROTOKOL AUTENTIKASI *USER***

Oleh

Hilda Kurnia Fitri

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

©Hilda Kurnia Fitri

Universitas Pendidikan Indonesia

2022

Hak cipta dilindungi undang-undang

Skripsi ini tidak boleh diperbayak seluruhnya atau sebagian,
dengan dicetak ulang, difotokopi, atau lainnya tanpa izin dari penulis

LEMBAR PENGESAHAN

HILDA KURNIA FITRI

IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE DIFFIE HELLMAN* PADA
TWO WAY CHALLENGE-RESPONSE PROTOCOL SEBAGAI PROTOKOL
AUTENTIKASI *USER*

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 informasi menjadi hal penting yang harus diperhatikan pada era perkembangan teknologi informasi seperti saat ini. Salah satu upaya pengamanan informasi adalah dengan mengotentikasi pihak yang akan mengaksesnya sesuai dengan protokol tertentu. Protokol autentikasi yang telah diterapkan secara umum yaitu dengan penggunaan *username* dan *password* saat ingin mengakses suatu akun. Namun penggunaan *password* menjadi tidak aman jika *password* sampai diketahui oleh pihak asing. Pihak asing ini dapat berpura-pura menjadi pemilik akun asli dan mengakses informasi dalam akun untuk kepentingannya. Dengan demikian, maka diperlukan suatu protokol autentikasi lainnya yang tetap menjamin keamanan akun meskipun informasi tentang autentikasi yang dilakukan saat ini sampai bocor pada orang asing. Pada penelitian ini, dirancang sebuah protokol autentikasi dengan *Two Way Challenge-Response Protocol* yang mana pemberian *challenge* dan *response* dilakukan dengan menggunakan Algoritma *Elliptic Curve Diffie-Hellman* (ECDH). Aspek yang dimanfaatkan dari Algoritma ECDH adalah kegunaannya untuk pertukaran kunci simetri. Dengan menggunakan Algoritma ECDH, maka *challenge* akan berubah tiap kali melakukan *log in* pada akun. Hal ini membuat *response* yang diberikan juga akan berbeda, sehingga meskipun *response* saat ini diketahui pihak asing, pihak asing tidak dapat menggunakan *response* yang sama untuk mengakses akun kita di lain waktu. Algoritma ECDH memiliki komputasi yang lebih sederhana dan efisien, namun dengan keamanan tetap tinggi karena didasarkan pada sulitnya memecahkan masalah logaritma diskrit. Hasil akhir yang diperoleh dari penelitian ini adalah sebuah program menggunakan bahasa pemrograman Python yang dapat digunakan untuk mengotentikasi pihak yang akan mengakses akun.

Kata Kunci : Protokol Autentikasi, Algoritma Elliptic Curve Diffie-Hellman, Two Way Challenge-Response Protocol

ABSTRACT

Security of information has become an important issue which must be considered in this era of information technology development. One of the efforts to secure the information is by authenticating the party accessing it according to certain protocol. The protocol of authentication that has been applied in general is to use username and password when accessing an account. However, the use of a password becomes insecure if the password is known by a foreign party. This foreigner can pretend to be the real account owner and access the information in the account for the foreigner's own sake. Thus, we need another authentication protocol which still guarantees account security even though information about the current authentication is leaked to foreign parties. In this research, was designed an authentication protocol with Two Way Challenge-Response Protocol in which the process of giving challenges and responses uses Elliptic Curve Diffie-Hellman (ECDH) Algorithm. The aspect that is utilized by the algorithm is its usefulness for symmetric key exchange. By using ECDH, the challenge will change every time you log in to the account. This means the response given will also be different, so that the foreign parties can not use the same response to access our account at a later time. ECDH has simpler and more efficient computations but with high security because it is based on the difficulty of solving discrete logarithm problem. The final result of this research is a Python-based program which can be used to authenticate the party who accesses an account.

Keyword : *Authentication Protocol, Elliptic Curve Diffie-Hellman Algorithm, Two Way Challenge-Response Protocol*

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN.....	iii
KATA PENGANTAR	iv
UCAPAN TERIMA KASIH	v
ABSTRAK.....	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan	4
1.4 Manfaat	4
BAB II LANDASAN TEORI.....	5
2.1 Teori Bilangan.....	5
2.1.1 Faktor Persekutuan Terbesar (Burton, 2011).....	5
2.1.2 Relatif Prima (Burton, 2011)	5
2.1.3 Fungsi Phi Euler (Burton, 2011).....	5
2.1.4 Pangkat dari Suatu Modulo n (Rosen, 2011)	6
2.1.5 Akar primitif (Rosen, 2011).....	6
2.1.6 Logaritma Diskrit (Rosen, 2011).....	6
2.1.7 Masalah Logaritma Diskrit	7
2.2 Kriptografi	7
2.2.1 Kriptografi Kunci Publik (Munir, 2019).....	7
2.2.2 Algoritma Pertukaran Kunci Diffie Hellman (Munir, 2019).....	8
2.3 Kriptografi Kurva Eliptik	9
2.3.1 Kurva Eliptik (Munir, 2019).....	9

2.3.2	Kurva Eliptik pada Galois Field (Munir, 2019)	10
2.3.3	Algoritma Kurva Eliptik (Stein, 2008).....	15
2.3.4	Elliptic Curve Diffie Hellman	15
2.4	Protokol Kriptografi (Munir, 2019)	16
2.4.1	Autentikasi	16
2.5	<i>Two Way Challenge-Response Protocol</i>	17
2.6	Bahasa Pemrograman Python.....	17
BAB III METODE PENELITIAN.....		19
3.1	Identifikasi Masalah.....	19
3.2	Model Dasar	19
3.2.1	<i>Two Way Challenge-Response Protocol</i>	19
3.2.2	Algoritma Elliptic Curve Diffie Hellman	20
3.3	Pengembangan Model.....	21
3.4	Konstruksi Program	22
3.4.1	<i>Input Output</i>	22
3.4.2	Rancangan Tampilan.....	22
3.4.3	Algoritma	24
3.5	Validasi	25
3.6	Kesimpulan.....	25
BAB IV HASIL DAN PEMBAHASAN		26
4.1	Protokol Autentikasi	26
4.2	Program Aplikasi	26
4.1.1	Tampilan Utama	27
4.1.2	Sign In	27
4.1.3	Log In	30
4.1.4	Kalkulator User.....	32
4.3	Validasi Program.....	35
BAB V SIMPULAN DAN SARAN		42
5.1	Simpulan	42
5.2	Saran	42
DAFTAR PUSTAKA		44
LAMPIRAN		46

Lampiran 1: MenuUtama.py	46
Lampiran 2: Points.py	49
Lampiran 3: Calc.py	51
Lampiran4: Helper.py	53

DAFTAR TABEL

Tabel 4. 1 Penentuan Titik dalam Kurva $y^2 \equiv x^3 + 44x + 56 \pmod{29}$ 36

DAFTAR GAMBAR

Gambar 3. 1 Skema <i>Two Way Challenge-Response Protocol</i>	20
Gambar 3. 2 Skema <i>Elliptic Curve Diffie Hellman</i>	20
Gambar 3. 3 Skema Protokol Autentikasi dengan <i>Elliptic Curve Diffie Hellman</i>	21
Gambar 3. 4 Tampilan Utama	22
Gambar 3. 5 Tampilan Menu <i>Sign-In</i>	23
Gambar 3. 6 Input <i>Username</i> dan PA	23
Gambar 3. 7 Input K	24
Gambar 3. 8 Kalkulator <i>user</i>	24
Gambar 4. 1 Tampilan Menu Utama.....	27
Gambar 4. 2 Menu <i>Sign In</i>	28
Gambar 4. 3 Penentuan <i>Username</i> dan Kurva Eliptik	29
Gambar 4. 4 Pembuatan Akun Berhasil.....	29
Gambar 4. 5 Menu <i>Log In</i>	30
Gambar 4. 6 <i>Log in</i> Awal.....	30
Gambar 4. 7 Pemberian <i>Challenge</i>	31
Gambar 4. 8 Input <i>Response</i>	31
Gambar 4. 9 <i>Log In</i> Berhasil.....	32
Gambar 4. 10 Menu Inisiasi.....	32
Gambar 4. 11 Inisiasi Kurva Eliptik	33
Gambar 4. 12 Menu Hitung	34
Gambar 4. 13 Titik Hasil PA	34
Gambar 4. 14 Titik Hasil <i>Response</i>	35
Gambar 4. 15 Titik Pada Kurva.....	37
Gambar 4. 16 Titik Pada Kurva.....	37

DAFTAR LAMPIRAN

Lampiran 1: MenuUtama.py	46
Lampiran 2: Points.py	49
Lampiran 3: Calc.py	51
Lampiran 4: Helper.py	53

DAFTAR PUSTAKA

- Azizah, H. N., Marwati, R., & Yusnita. I. (2020). Penggabungan Modifikasi *Hill Cipher* dan *Elliptic Curve Cryptography* untuk Meningkatkan Keamanan Pesan. *EurekaMatika*, 8(2) 11-23.
- Barakat, M., Eder, C., & Hanke, T. (2018). *An Introduction To Cryptography*. University of Kaiserslautern.
- Bray, S. W. (2020). *Implementing Cryptography Using Python*. Wiley.
- Burton, D. M. (2011). *Elementary Number Theory* (Edisi Ketujuh). New York: McGraw-Hill.
- Cameron, P. J. (2003). *Notes on Cryptography*. London: University of London.
- Dwijaksana, M. H. (2008). *Studi dan Implementasi Kriptografi Kunci Publik untuk Otentikasi Perangkat dan Pengguna pada Komunikasi Bluetooth*. (Skripsi). Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung.
- Ferdinan, M. A. (2021). *Aplikasi Pengiriman Email Menggunakan Enkripsi Elliptic Curve Diffie Hellman*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia.
- Hoffstein, J., Pipher, J., & Silverman, J. (2014). *An Introduction to Mathematical Cryptography* (Edisi Kedua). New York: Springer.
- Husain, S. N., Sathik, M., & Nisha, S. (2019). Enhanced ID based Data Aggregation and Detection Against Sybil Attack Using Challenge Response Authentication Protocol. *International Research Journal of Engineering and Technology*, 6(3) 481-485.
- Ikhsan, M. (2021). *Ramai Email-Password Bocor di Internet, Cek Data Pribadi [Online]*. Diakses dari https://www.cnnindonesia.com/teknologi/20210208083445-185_603462/ramai-email-password-bocor-di-internet-cek-data-pribadi.

- Lutz, M. (2011). *Programming Python* (Edisi Keempat). Sebastopol: O'Reilly Media.
- Munir, R. (2019). *Kriptografi* (Edisi Kedua). Bandung: Informatika.
- Naufal, A. (2020). *81% Kebocoran Data Disebabkan Password yang Dibobol [Online]*. Diakses dari <http://news.gunadarma.ac.id/2020/09/81-kebocoran-data-disebabkan-password-yang-dibobol/>
- Rambonang, Y. M. (2015). *Klien Autentikasi Menggunakan SHA-1 dengan Protokol Two Way Challenge-Response pada Transaksi Web-Based*. (Skripsi). Fakultas Sains dan Teknologi, Universitas Sanata Dharma, Yogyakarta.
- Rosen, K. H. (2011). *Elementary Number Theory and Its Applications* (Edisi Keenam). Boston: Pearson.
- Rosen, K. H. (2012). *Discrete Mathematics and Its Applications* (Edisi Ketujuh). New York: McGraw-Hill.
- Sitohang, T. R., Marwati, R., & Yusnita, I. (2019). Kriptosistem Gabungan S-ECIES dan RSA. *EurekaMatika*, 7(1) 93-102.
- Stein, W. A. (2008). *Elementary Number Theory: Primes, Congruences, and Secrets A Computational Approach*. New York: Springer.
- Stinson, D. R. (2003). *Cryptography Theory and Practice* (Edisi Ketiga). Boca Raton: Chapman&Hall/CRC.
- Van Der Lubbe, J. C. A. (2005). *Basic Methods of Cryptography*. Delft: VSSD.
- Zahra, D. A., Marwati, R., & Sispiyati, R. (2021). Kriptografi Visual pada Gambar Berwarna (RGB) Menggunakan Algoritma Elliptic Curve Cryptography. *EurekaMatika*, 9(2) 152-163.