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

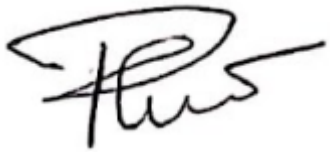
LEMBAR PENGESAHAN

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

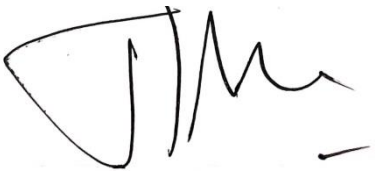


Dra. Hj. Rini Marwati, M.S.
NIP 196606251990012001

Pembimbing II

Ririn Sispiyati, S.S.i., 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 mengautentikasi 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 logaritmaa diskrit. Hasil akhir yang diperoleh dari penelitian ini adalah sebuah program menggunakan bahasa pemrograman Python yang dapat digunakan untuk mengautentikasi 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

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 Crytography Using Pyhton*. 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.

Dwijaksara, M. H. (2008). *Studi dan Implementasi Kriptografi Kunci Publik untuk Otentikasi Perangkat dan Pengguna pada Komunikasi Bloetooth*. (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 Againts Sybil Attack Using Cahllenge 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 Pyhton* (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 Challeng-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 Algortima Elliptic Curve Cryptography. *EurekaMatika, 9(2)* 152-163.