Meningkatkan Keamanan Data Dalam Berbagi *File* Menggunakan Kriptografi Asimetris *Elliptic Curve Cryptography* P-521

Ashry Ramadhan[1)], Noveri Lysbetti Marpaung[2)]
[1)]Mahasiswa Program Studi Teknik Informatika, [2)]Dosen Teknik Informatika
Program Studi Teknik Informatika S1, Fakultas Teknik Universitas Riau
Kampus Bina Widya Jl. HR. Soebrantas Km. 12,5 Simpang Baru, Panam, Pekanbaru 28293
Email: ashry.ramadhan @student.unri.ac.id

ABSTRACT

Cryptography has been aplicated into securing information. Cryptography divided into two types, Symmetric and Asymmetric Cryptography. Symmetric Cryptography commonly used for encrypt a file, while Asymmetric Cryptography used for create public key and private key for key exchange.. Elliptic Curve Cryptography (ECC) is the one of asymmetric cryptography that is commonly used for create a secure public and private key depending on the bit length of ECC, in this research use 521-bit length. Advanced Encryption Standard (AES) is the one of symmetric cryptography has been used as a standard for securing private data, in this research use 256-bit length. AES and ECC are provided by National Security of Standards and Technology (NIST) as a standard for national security applications. The system in this research created into Web Application base using HTML5, CSS3, and JavaScript. The results obtained from this research is the system can encrypt and decrypt any type of file like systems, videos, documents, images and audios file and has avalanche effect property.

Keywords: *Securing Information, Cryptography, ECC P-521, AES-256, Web Application*

1. PENDAHULUAN

Kriptografi merupakan sebuah metode untuk mengamankan informasi ataupun data. Kriptografi terdiri dari dua tipe, yaitu kriptografi asimetris dan kriptografi simetris. Kriptografi asimetris pada umumnya digunakan untuk pertukaran kunci (*key exchange*) dan pembuatan tanda tangan digital (*digital signature*), sedangkan kriptografi simetris digunakan untuk proses enkripsi dan dekripsi data. *The Commercial National Security Algorithm* (CNSA) *Suite* merupakan kumpulan algoritma asimetris dan simetris yang dikeluarkan oleh *National Institute of Standards and Technology* (NIST) sebagai standar algoritma kriptografi yang digunakan untuk keperluan keamanan, salah satunya adalah *Elliptic Curve Cryptographyi* (ECC) P-384. Pada penilitian ini dilakukan peningkatan panjang bit pada ECC P-384 menjadi P-521 dengan spesifikasi yang berbeda, bertujuan untuk peningkatan keamanan karena pada masa sekarang ini merupakan masa transisi dari algoritma yang ada pada CNSA menjadi Algoritma yang tahan terhadap komputer kuantum yang masih dilakukan standarisasi oleh NIST, maka dibutuhkan peningkatan pada standar yang diberikan. ECC P-521 diimplementasikan kedalam bentuk sistem dengan nama *Data Secrecy System* sebagai alat untuk melakukan proses enkripsi dan dekripsi menggunakan gabungan algoritma ECC-P521 dan AES-256. AES-256 merupakan salah satu algoritma yang terdapat dalam CNSA *Suite*. Oleh karena

itu dibutuhkan sistem yang memiliki kedua algoritma yaitu ECC P-521 dan AES-256 tersebut, maka dibuat skripsi ini dengan judul ***"Meningkatkan Keamanan Data Dalam Berbagi File Mengguanakan Kriptografi Asimetris Elliptic Curve Cryptography P-521"***

2. TINJAUAN PUSTAKA

Elliptic Curve Cryptography (ECC) merupakan Algoritma Kriptografi yang menggunakan persamaan Kurva Eliptik, persamaan yang digunakan adalah.

$$y^2 = x^3 + ax + b$$

Dua operasi utama dalam ECC adalah *point addition* dan *point doubling*. Kedua operasi ini digunakan untuk proses pembuatan *private Key* dan *public Key* (Hoffstein dkk, 2010).

Advanced Ecnryption Standard (AES) merupakan Algoritma Kriptografi Simetris yang dikeluarkan oleh NIST pada FIPS 197. Nama sebenarnya dari AES adalah *Rijndael* yang merupakan sebuah Algoritma Kriptografi *block cipher*, artinya algoritma ini menggunakan blok-blok dalam melakukan proses enkripsi dan dekripsi. AES menerima masukan 128-bit dengan keluaran 128-bit juga dan memiliki panjang kunci rahasia antra lain, 128-bit, 192-bit dan 256-bit (FIPS 197, 2001).

Strict Avalanche Criterion (SAC) merupakan sebuah pengujian untuk mendapatkan nilai tingkat korelasi antara *input* dengan *output* yang dihasilkan dari sebuah *block cipher*. Rumus yang digunakan adalah.

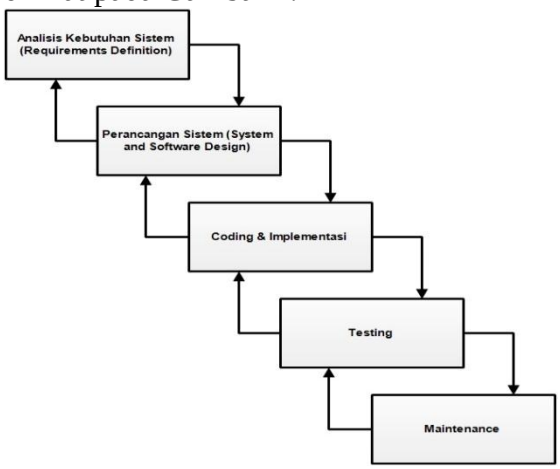
$$SAC = \frac{Hamming\ Distance}{Block\ Size} \times 100\ \%$$

SAC merupakan properti yang sangat penting dalam sebuah algoritma kriptografi, karena menentukan keamanan sebuah algoritma kriptografi jenis *block cipher*, properti atau karakteristik tersebut ditentukan dengan mengubah 1 bit pada *plaintext* dapat mengubah bit sebanyak 50% dari *ciphertext* awal sebelum *plaintext* diubah (Al-Mamun dkk, 2017).

3. METODOLOGI PENELITIAN

3.1. Metode Pengembangan Sistem

Penelitian ini dilakukan dengan menggunakan metode pengembangan sistem *waterfall*. Metode ini melakukan pendekatan secara sistematis dan urut, mulai dari level indentifikasi kebutuhan sistem hingga tahap analisis dan pengujian sistem. Tahap metode *waterfall* dapat dilihat pada Gambar 1.



Gambar 1. Metode *Waterfall*

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Sistem

Berikut adalah tampilan dari sistem *Data Secrecy System* (DSS).

Gambar 2. Tampilan Utama Sistem.

4.2. Pengujian SAC

Pengujian SAC menggunakan *plaintext* "KRIPTOGRAFI1" dan *key* "143b737a8b36fc4c9c32d7e6e28869676a c53e8b485a84a485f8e8539f704a1b".
Hasil pengujian SAC pada AES-256 dapat dilihat yang digunakan oleh sistem pada Tabel 1.

Tabel 1. Pengujian SAC Pada AES-256

Plaintext	*Bit Variance*	*Avalanche Effect* (%)
KRIPTOGRAFI1	63	49,21
KRIPTOGRAFI2		
KRIPTOGRAFI3	59	46,09
KRIPTOGRAFI4		
KRIPTOGRAFI5	59	46,09
KRIPTOGRAFI6		
KRIPTOGRAFI7	58	53,12
KRIPTOGRAFI8		
KRIPTOGRAFI9	64	50
KRIPTOGRAFI0		
Rata-rata a*valanche effect* (%)		48,90

5. KESIMPULAN

Kesimpulan yang didapatkan berdasarkan pengujian SAC, didapatkan nilai rata-rata *avalanche effect* 48,90% mendekati nilai 50%, sehingga dapat dikatakan sistem yang dibuat memiliki properti *avalanche effect* tersebut, sehingga DSS dapat digunakan untuk mengamankan data sensitif.

Daftar Pustaka

Al-Mamun, Abdullah., Shawon S. M. Rahman, Tanvir Ahmed Shaon, Md Alam Hossain, 2017, *Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte*, International Jurnal of Computer Networks & Communications (IJCNC), No.2, Vol.9, pp.69-88.

FIPS 197, 2001, *Advanced Encryption Standard (AES), National Institute of Standards and Technology* (NIST), pp.13-23

FIPS PUB 186-4, 2013, *Digital Signature Standard* (DSS), *National Institute of Standards and Technology* (NIST), pp.15-19, pp.26-40, pp.104

Hoffstein, Jeffery., Jill Pipher, Joseph H Silverman, 2010, *An Introduction to Mathematical Cryptography*, Springer, New York, pp.279 – pp.283