INTISARI

PLAYFAIR CIPHER BLOCK CHAINING DAN ELLIPTIC CURVE UNTUK PENGAMANAN PERTUKARAN DATA REPRESENTATIONAL STATE TRANSFER

USMAN ZAMARI
15/388507/PPA/04946

Aplikasi perangkat lunak didunia ini ada potensi untuk saling berkomunikasi. Komunikasi tersebut tidak dibatasi oleh lokasi, *platform*, sistem operasi, bahasa dan *protocol*. Kemudahan pertukaran komunikasi tersebut jika tidak dilakukan pengamanan bisa mengakibatkan informasi terbaca oleh pihak yang tidak berwenang. *REpresentational State Transfer* (REST) dapat diimplementasikan untuk pertukaran data atau komunikasi yang aman dengan menerapkan Algoritme kriptografi.

Memodifikasi Algoritme kriptografi dalam bentuk lain dari metode dasar, akan mendapatkan berbagai variasi metode tersebut. Algoritme *Playfair Cipher Block Chaining* (*Playfair* CBC) digunakan untuk mengamankan data *request* dengan menerapkan *digraph* terenkripsi untuk membangun kunci kembali. Kelemahan algoritme ini terletak pada pengamanan kuncinya sehingga diperlukan algoritme lain untuk melakukannya. Algoritme *Elliptic Curve* digunakan untuk menyelesaikan masalah pada pengamanan kunci tersebut.

Pengujian dilakukan dengan menggunakan 10 data yang bervariasi. Pengujian menunjukkan bahwa kunci dapat digunakan untuk melakukan enkripsi dan dekripsi, serta hasil perhitungan antara manual dan sitem mendapatkan hasil yang sama. *Brute force attack* dari kecepatan komputer 93 $petaflop$ terhadap kunci algoritme *Playfair* CBC akan lebih lama jika menggunakan karakter kunci yang diganti lebih dari 40 dan untuk *Elliptic Curve* akan lebih lama jika menggunakan order *group* lebih dari 186 *bits*.

Kata kunci : REST, Kriptografi, *Playfair* CBC, *Elliptic Curve*

ABSTRACT

PLAYFAIR CIPHER BLOCK CHAINING AND ELLIPTIC CURVE FOR REPRESENTATIONAL STATE TRANSFER DATA EXCHANGE SECURITY

USMAN ZAMARI
15/388507/PPA/04946

Software application in this world have the potential to communicate with each other. Communication is not limited by location, platform, operating system, language and protocol. The ease of communication exchange if no safeguard can effect information readed by unauthorized persons. REpresentational State Transfer (REST) can be implemented for secure data exchange or communication by implementing cryptographic algorithm.

Modifying the cryptography algorithm in another from the basic method, will get a variety of it method. Playfair Cipher Block Chaining (Playfair CBC) algorithm is used to secure request data by applying encrypted digraph to build lock again. The weakness of this algorithm lies in securing the key so that another algorithm is needed to do so. The Elliptic Curve algorithm is used to solve the security lock problem.

Testing had done by using 10 different data. Testing indicates that the key can be used to perform encryption and decryption and the results of calculations between the manual and the system same get results. Brute force attack from computer speed 93 petaflop to Playfair CBC algorithm key will be longer if using key characters replaced more than 40 and for Elliptic Curve will be longer if using order group more than 186 bits.

Keywords : REST, Cryptography, Playfair CBC, Elliptic Curve