Implementasi elliptic curve cryptography untuk enkripsi end-to-end pada aplikasi chat = Implementation of elliptic curve cryptography for end-to-end encryption in chat applications

Aria Lesmana, author

Abstrak

ABSTRAK
Tujuan utama dari keamanan komunikasi adalah mencegah data pesan dari akses pihak ketiga. Solusi dari masalah tersebut adalah menerapkan enkripsi End-to-end. Algoritma enkripsi Elliptic Curve Cryptography (ECC) cocok digunakan sebagai metode enkripsi End-to-end pada sistem komunikasi digital termasuk aplikasi chat. ECC adalah jenis kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis dari kurva eliptik, ECC mempunyai tingkat keamanan yang setara dengan RSA menggunakan kunci berukuran lebih kecil. Penelitian ini membahas perancangan dan implementasi dari algoritma enkripsi dan dekripsi yang menerapkan kriptografi ECC sebagai metode enkripsi End-to-end pada aplikasi chat. Algoritma ini menggunakan operasi matematika dan nilai parameter dari kurva eliptik untuk menghasilkan kunci serta ciphertextnya dan juga melakukan dekripsi. Dari hasil ujicoba dan analisa implementasi enkripsi dan dekripsi menggunakan algoritma ECC, algoritma tersebut cocok digunakan sebagai metode enkripsi End-to-end, karena ukuran kunci yang relatif ringan dan operasi matematika yang menggunakan parameter khusus yang berbeda-beda. Hasil pengujian enkripsi dan dekripsi menggunakan parameter kurva eliptik secp192r1 dan secp192k1 yang mempunyai ukuran kunci sekitar 2¹⁹² bit, menghasilkan kunci dan ciphertext paling ringan dan paling cepat diproses, dengan angka nilai keduanya berukuran sepanjang 58 digit.
<hr>
ABSTRACT
The main purpose of communication security is to prevent message data from third party access. The solution to this problem is to implement End-to-end encryption. Elliptic Curve Cryptography (ECC) encryption algorithm is suitable for use as an End-to-end encryption method on digital communication systems including chat applications. ECC is a type of public key cryptography that bases its security on mathematical problems from elliptic curves, ECC has a level of security equals to RSA while using smaller keys. This study discusses the design and implementation of encryption and decryption algorithms that apply ECC cryptography as an End-to-end encryption method in chat applications. This algorithm uses mathematical operations and parameter values from the elliptic curve to generate keys and their ciphertext and also decrypt them. From the results of testing and analyzing the implementation of encryption and decryption using the ECC algorithm, the algorithm is suitable for use as an End-to-end encryption method, because of the relatively light key size and mathematical operations that use different parameters. The results of encryption and decryption testing using elliptic curve parameters secp192r1 and secp192k1 which have a key size of about 2¹⁹² bits, produce the lightest and fastest to process ciphertext and keys, with the value of both measuring 58 digits.</p>