Kriptografi kunci publik berdasarkan kurva eliptis = Public key cryptography based on elliptic curve

Dwi Agy Jatmiko, author

Abstrak

Kriptografi kunci publik merupakan salah satu teknik kriptografi untuk mengamankan transmisi informasi. Pertukaran kunci Diffie-Hellman dan sistem kriptografi ElGamal merupakan dua teknik kriptografi kunci publik yang didasarkan pada Discrete Logarithm Problem (DLP). Pesatnya perkembangan komputer belakangan ini menuntut penggunaan keysize yang relatif besar untuk menjaga tingkat keamanan transmisi informasi melalui pertukaran kunci Diffie-Hellman dan sistem kriptografi ElGamal. Di dalam tugas akhir ini, akan dijelaskan mengenai penerapan kurva eliptis pada pertukaran kunci Diffie-Hellman dan sistem kriptografi ElGamal. Diharapkan penerapan kurva eliptis dapat memberikan tingkat keamanan transmisi informasi yang tinggi namun dengan penggunaan keysize yang relatif lebih kecil.
.....Public key cryptography is one of cryptographic techniques for securing information transmission. Diffie-Hellman key exchange dan ElGamal Cryptosystem are public key cryptography techniques that based on Discrete Logarithm Problem (DLP). Recent rapid-growing of computer made information transmission using Diffie-Hellman key exchange dan ElGamal cryptosystem have to use a relative large keysize to keep its security level. This skripsi will explain about elliptic curve implementation in Diffie-Hellman key exchange dan ElGamal Cryptosystem. Elliptic curve implementation expected to give higher security level in information transmission althought using relative small keysize.