ABSTRACT

Cryptosystem elliptic curve (elliptic curve cryptosystem) is one of Asymmetric cryptography which is using the discrete logarithm (discrete logarithm problem). The structure of elliptic curve is used as a mathematical operation group to establish a review process of encryption and decryption. Diffie-Hellman method is the first method to create a shared secret between two parties through unguided communication. This algorithm can be used to distribute public keys that is well known with key exchange protocol.

In this final task is designed the basic fundamental techniques Elliptic Curves Cryptosystem (ECC) which implemented the Protocol in exchange Diffie-Hellman public key. The key generation key is shown the exchange key public between two users and then it will be calculated at each user to generate the same shared secret key. The key is used to encrypt the AES symmetric key after the symmetric-key is used in encryption of speech processing. The key encryption is done in numerous testing and then it is tested in the transmitted and received process.

*The results from testing conducted in this final project, the ECC algorithms can be combined with Diffie-Hellman for key exchange process and for symmetric AES encryption key. The combination of parameter ecdh is obtained the best performance based on correlation coefficient and total computational time is a combination of low value. That is point curve: (4,29), privatekey1: 10, privatekey2: 7. Based on processing time include encryption and decryption process (84.669ms), result of coefficient correlation (0.1621), and avalanche effect value (*48.2357*%), Elliptic Curve Diffie-Hellman performance is good. Based on difficulty to break key, ECDH more difficult than DH. The key that has encrypted can be decrypted and used to decrypt sound for AES algorithm and generates sound decryption similar with the sent one. It can be seen from shape spectrum of sound, graphics power spectral density as well as SNR values between signal sound sent and the sound signal decryption.*

Keywords : Cryptography, Elliptic Curve, key exchange, Diffie-Hellman, symmetric algorithm.