Asymmetric Ciphers

Cryptographic systems rely on keys for encryption and decryption. Traditionally, a single key is required to encrypt an[4]d to decrypt. In order for the recipient of the ecrypted message to be decrypted by the recipient, the key must also be transmitted. However, sending the key over the channel where the actual message will be sent is insecure. The key must be transmitted on a different and secure channel[4]. This secure channel where the key should be transmitted cannot be used for normal transmission because it is costly and sometimes difficult for users to access and use[4]. This begs the question whether it is possible to send encrypted messages in such a way that the key can also be transmitted over the normal data and insecure channel. In this section, we focus on solving this problem by describing the relevant and important work on asymmetric ciphers.

Secure communication as described by Merkle allows two parties to communicate in a private manner even though a third party tries its best to learn what is being communicated[4].

Diffie-Helman[1]

Rivest-Shamir-Adleman[5]

Elgamal[2]

Elliptic Curve Cryptosystems[3]

References

[1] Whitfield Diffie and Martin Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.

[2] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Information Theory, IEEE Transactions on*, 31(4):469–472, July 1985.

[3] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[4] Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, 1978.

[5] Ronald L. Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.