參 考 文 獻

英文部份

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystem. *Proceedings of Advances in Cryptology-CRYPTO ’90*, Santa Barbara, California, 2-21.

Biham, E., & Knudsen, L. R. (1998). DES, Triple-DES and AES. *CryptoBytes*, *4*(1), 18-23.

Denning, D. (1982). *Cryptography and data security*. New Jersey: Addison-Wesley. 151-158.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6) 644-654.

Kahate, A. (2007). *Cryptography and network security*. India: McGraw-Hill Education, 54-62.

Knudsen, L. R., & Martin, K. (1998). In search of multiple domain key recovery. *Journal of Computer Security*, *6*(4), 219-235.

Lee, H. M. & Lee, T. Y. (2007, September 5-7). *Analysis of Algorithm of cipher text containing data and key in network security*. Paper presented at Second International Conference on Innovative Computing Informatio and Control, Kumamoto, Japan.

Lee, H. M., & Lee, T. Y. (2010, March 24-26), *Verification of stored security data in computer system*. Paper presented at the Second Asian Conference on Intelligent Information and Database Systems, Hue, Vietnam.

Matsui, M. (1994). Linear cryptanalysis method for DES cipher. *Springer-Verlag*, *765*(32), 386-397.

McEliece, R. J. (1978). A public-key system based on algebraic coding theory. *Deep Sace Network Progress Report*, *44*(42), 114-116.

Merkle, R. C. (1990). One way hash function and DES. *Springer-Verlag*, *435*(37), 428-446.

Miyaguchi, S. (1990). The FEAL-8 cryptosystem and call for attack. *Springer Verlag Berlin*, *435*(48), 624-627.

National Institute of Standards and Technology. (1993). *Secure Hash Standard* Virginia：Federal Information Processing Standards Publications.

Pieprzyk, J., Hardjono, T., & Seberry, J. (2003). *Fundamentals of computer security*. Berlin Heidelberg: *Springer-Verlag*., 53-66.

Rivest, R. L., Shamir, A., & Adleman, L. (1978) A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

Shannon, C. E. (1949). Communication theory of security systems. *Bell System Technical Journal*, *28*(47), 657-715.

Stallings, W. (2007). *Cryptography and network security: Principles and practice*(3rd ed.). New Jersey: Prentice-Hall., 41-68.