Abstract

The Cipher Block Chaining (CBC) and the Merkle-Hellman algorithm are two different cryptosystems for encrypting messages. But using these cryptosystems separately has many drawbacks. However there are several ways of getting rid of these drawbacks. This paper demonstrates how to use the combination of both the cryptographic algorithms along with randomized vectors, keys and super-increasing sequence to encrypt messages. The encrypted message is stored in secret buffers and these positions are encrypted by use of discrete logarithmics and sent. This not only strengthens the encrypted message but also makes the transmission more secure, so that only the intended recipient of the message is able to decipher the message. This paper focuses on enhancing the confidentiality of the message transfer.

References

- B. Padhmavathi, Arghya Ray, Alisha Anjum, Santhoshi Bhat, "Improvement of CBC Encryption Technique by using the Merkle - Hellman Knapsack Cryptosystem"; IEEE
Madras sponsored ISCO 2013
   - http://www.mast.queensu.ca/~math418/m418oh/m418oh04.pdf

Index Terms

Computer Science
Security

Keywords

Security  cryptography  cryptosystem  blocks cipher  cipher block chaining  discrete logarithms
knapsack problem
randomizers
superincreasing vector