Message based random variable length key encryption algorithm.

ABSTRACT

Problem statement: A block ciphers provides confidentiality in cryptography but cryptanalysis of the classical block ciphers demonstrated some old weaknesses grabbing a partial key in any stage of encryption procedure leads to reconstructing the whole key. Exhaustive key search shows that key generation should be indeterminist and random for each round. Matching cipher-text attack shows that larger size of block is more secure. In order to overcome analysis mentioned above a new algorithm is designed that is based on random numbers and also can defeat time and memory constraints. Approach: Dynamic and message dependent key generator was created by producing a random number and it was selected as the size of first chunk. Residual value of second chunk divided by first chunk concatenating with first chunk forms the first cipher as an input for SP-boxes. These processes repeated until whole mesaage get involved into the last cipher. Encrypted messages are not equal under different run. Value of random number should be greater than 35 bits and plaintext must be at least 7 bits. A padding algorithm was used for small size messages or big random numbers. Results: Attack on the key generation process was prevented because of random key generation and its dependency to input message. Encryption and decryption times measured between 5 and 27 m sec in 2 GHz Pentium and java platform so time variant and fast enough key generation had been kept collision and timing attacks away due to small seized storage. Long and variable key length made key exhaustive search and differential attack impossible. None fixed size key caused avoidance of replaying and other attacks that can happen on fixed sized key algorithms. Conclusion: Random process employed in this block cipher increased confidentiality of the message and dynamic length substitution in proposed algorithm may lead to maximum cryptographic confusion and consequently makes it difficult for cryptanalysis.

Keyword: Security; Encryption; Block cipher; Variable key length.