ABSTRACT

METHOD AND APPARATUS FOR ENCRYPTING DATA

In the process of compressing and encrypting data, without increase of a processing time, a cipher capability is secured against the latest cryptanalysis such as differential and linear cryptanalyses. The differential and linear cryptanalyses are executed to collect plural pair of plaintext and cryptosystem for the same key and perform the statistical operation for estimating the key. An I/O process is executed to receive plaintext data and generate a random number. Then, an operation is executed to generate a different key for each data on the random number and set the key to a work key. The encrypted intermediate result or the pre-encrypted result is fed back for frequently changing the work key. These series of operations makes it possible to protect the ciphertext from the differential and the linear cryptanalyses. On the work key, the changing operation is executed to change correspondence between the plaintext data and the compressed data in the compressing process, for providing the compression with the encryption.

(Figure 1)