Computer-Generated Elastic Block Ciphers for Encryption and Decryption

Technology #m04-016

“Name of the inventor: Angelos D. Keromytis

Computer generation produces flexible block cipher Methods and systems for converting an elastic block cipher from an original block cipher using a round function are described.

The method and system for converting an elastic block cipher comprises of receiving a data string. The original block cipher is expanded based on the block size. The bits of the data string are divided into subsets and the block length of the subset is equivalent to the block size. The subsets are input into the round function. The round function comprises of performing the round function of the original block cipher on the subset. An exclusive OR operation is performed between the subsets.

The computer-implemented methods and systems provide a flexible and improved block cipher. ”

Inventors

Angelos D. Keromytis