

IDEA

The International Data Encryption Algorithm was developed in 1990 by Xuejia Lai and James Massey of the Swiss Federal Institute of Technology.

It is a block cipher which uses a 128-bit key to encrypt a 64-bit block. Its design goals are public and include the following considerations:

Block length: Long enough to deter statistical analysis. 64 bits is long enough.

Key length: Long enough to prevent exhaustive key search. 128 bits should be secure far into the future.

Confusion: Three different operations make the ciphertext depend on the plaintext in a complicated and involved way. (DES uses only two operations: XOR and S-boxes.)

Diffusion: Every plaintext bit and every key bit should affect every ciphertext bit.

Ease of software implementation: 16-bit sub-blocks, simple operations (add, shift, XOR).

Ease of hardware implementation: Regular structure to facilitate VLSI implementation. Encryption and decryption are similar operations.

Operations of IDEA

Bit-by-bit XOR

Addition of integers modulo $2^{16} = 65536$.

Multiplication of integers modulo $2^{16} + 1 = 65537$, with input and output treated as unsigned 16-bit integers, except that a block of all 0's is treated as representing 2^{16} , that is, as -1 .

Note that no two of these three operations satisfies a distributive law.

Note that no two of these three operations satisfies an associative law.

IDEA uses the same four modes of operation as DES: ECB, CBC, CFB and OFB.