## International Data Encryption Algorithm (IDEA)

The international Data Encryption Algorithm is a symmetric block cipher developed by Xuejia Lai and James Massey of the Swiss Federal Institute of Technology in 1990. IDEA is one of a number of conventional encryption algorithms that have been proposed in recent years to replace DES.

**Design principles.** IDEA is a block cipher that uses a 128-bit key to encrypt data in blocks of 64- bits. The design goals for IDEA can be grouped into those related to cryptographic strength and those related to easy of implementation. The following characteristics of IDEA relate to its cryptographic strength:

- **Block length:** The block length should be deter statistical analysis. On the other hand, the complexity of implementing an effective encryption function appear to grow exponentially with block size
- **Key strength:** The key length should be long enough to prevent exhaustive key searches. With a length of 128 bits, IDEA seems to be secure in this area far into the future.
- **Confusion:** The ciphertext should depend on the plaintext and key in a complicated and involved way. The objective is to complicate the determination of how the statistics of the ciphertext depend on the statistics of the plaintext. IDEA achieves this goal by using three different operations, as explained later. This is in contrast to DES, which relies principally on the XOR operation and on small nonlinear S-boxes.
- **Diffusion:** Each plaintext bit should influence every ciphertext bit, and each key bit should influence every ciphertext bit. The spreading out of a single plaintext bit over many ciphertext bits hides the statistical structure of the plaintext. IDEA is very effective in this regard.

The operations used in IDEA are

- Bit-by-bit exclusive-OR, denoted as $\vee$.
- Addition of integers modulo $2^{16}$ (modulo 65536), with inputs and outputs treated as unsigned 16-bit integers. This operation is denoted as $\oplus$.
- Multiplication of integers modulo $2^{16}$+1 (modulo 65537), with inputs and outputs treated as unsigned 16-bit integers, except that a block of all zeros is treated as representing $2^{16}$. This operation is denoted as $\otimes$.

Functions used in IDEA for operand length of 2 bits are illustrated below:

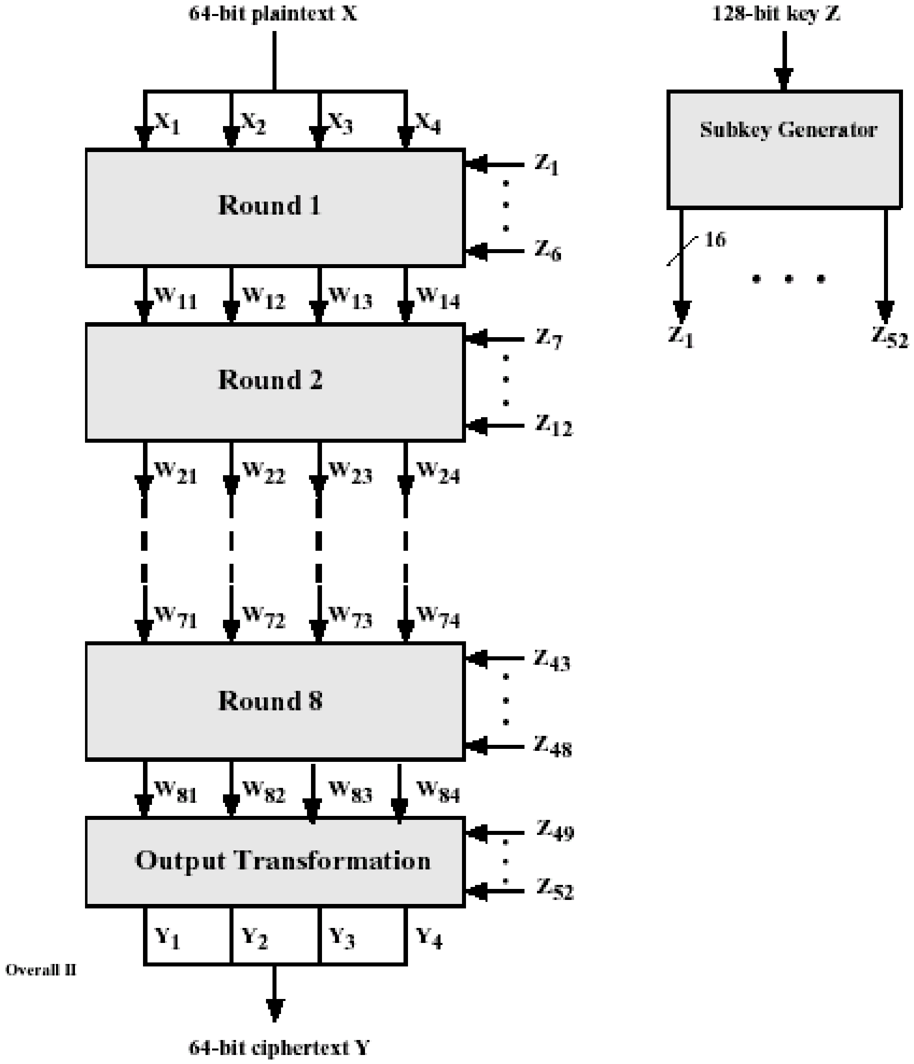
| **X** | | **Y** | | **X$\oplus$Y** | | **X$\otimes$Y** | | **X$\vee$Y** | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 00 | 0 | 00 | 0 | 00 | 1 | 01 | 0 | 00 |
| 0 | 00 | 1 | 01 | 1 | 01 | 0 | 00 | 1 | 01 |
| 0 | 00 | 2 | 10 | 2 | 0 | 3 | 11 | 2 | 10 |
| 0 | 00 | 3 | 11 | 3 | 11 | 2 | 10 | 3 | 11 |
| 1 | 01 | 0 | 00 | 1 | 01 | 0 | 00 | 1 | 01 |
| 1 | 01 | 1 | 01 | 2 | 10 | 1 | 01 | 0 | 00 |
| 1 | 01 | 2 | 10 | 3 | 11 | 2 | 10 | 3 | 11 |
| 1 | 01 | 3 | 11 | 0 | 00 | 3 | 11 | 2 | 10 |
| 2 | 10 | 0 | 00 | 2 | 10 | 3 | 11 | 2 | 10 |
| 2 | 10 | 1 | 01 | 3 | 11 | 2 | 10 | 3 | 11 |
| 2 | 10 | 2 | 10 | 0 | 00 | 0 | 00 | 0 | 00 |
| 2 | 10 | 3 | 11 | 1 | 01 | 1 | 01 | 1 | 01 |
| 3 | 11 | 0 | 00 | 3 | 11 | 2 | 10 | 3 | 11 |
| 3 | 11 | 1 | 01 | 0 | 00 | 3 | 11 | 2 | 10 |
| 3 | 11 | 2 | 10 | 1 | 01 | 1 | 01 | 1 | 01 |
| 3 | 11 | 3 | 11 | 2 | 10 | 0 | 00 | 0 | 00 |

In IDEA diffusion is provided by the basic building block of the algorithm, known as the multiplication/addition (MA) structure. This structure takes as inputs two 16-bit values derived from the plaintext and two 16-bit subkeys derived from the key and produces two 16-bit outputs. This particular structure is repeated eight times in the algorithm providing very effective diffusion.

### IDEA encryption

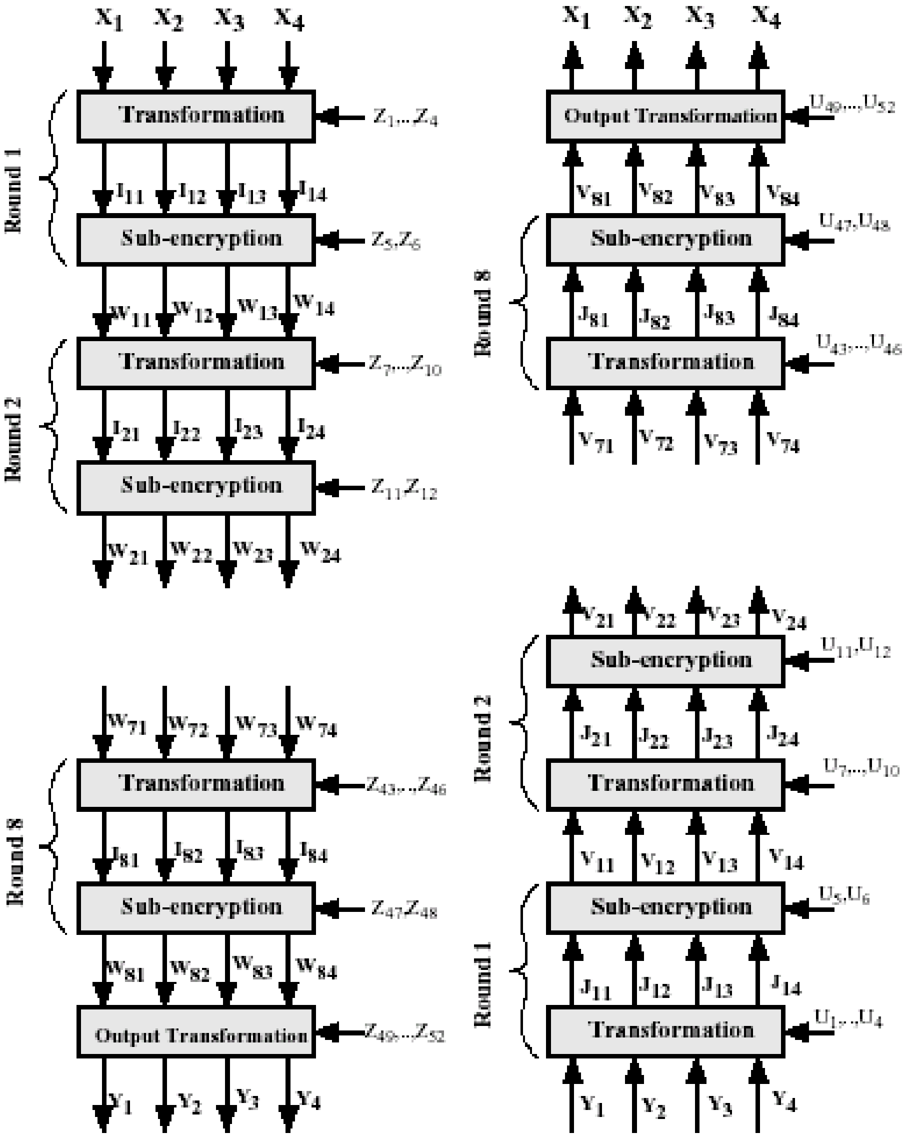
There are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext is 64 bits in length, and the key is 128 bits in length.

Subsequent rounds have the same structure but with different subkey and plaintext-derived inputs. The round begins with a transformation that combines the four input subblocks with four subkeys, using the addition and multiplication operations. The MA structure also takes two subkeys as input and combines these inputs to produce two 16-bit outputs.



Overall IDEA Structure

Finally, the four output blocks from the upper transformation are combined with two output blocks of the MA structure using XOR to produce the four output blocks for this round.

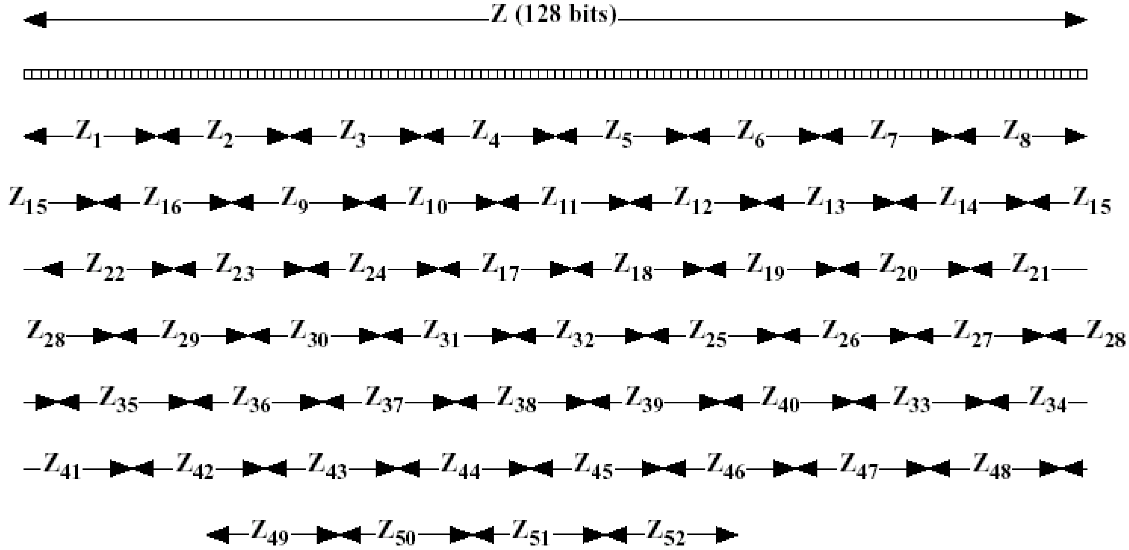


**IDEA Encryption and Decryption**

**Subkey generation**

Altogether 52 16-bit subkeys are generated from 128-bit encryption key. The scheme for generation is as follows. The first eight subkeys, labeled $Z_1$, $Z_2$, $Z_3$, $Z_4$, $Z_5$, $Z_6$, $Z_7$, $Z_8$ are taken directly from the key, with $Z_1$ being equal to the first 16 bits, $Z_2$ corresponding to the next 16 bits, and so on. Then a circular left shift of 25 bit positions is applied to the key, and the next eight subkeys are extracted. This procedure is repeated until all 52 subkeys are generated.

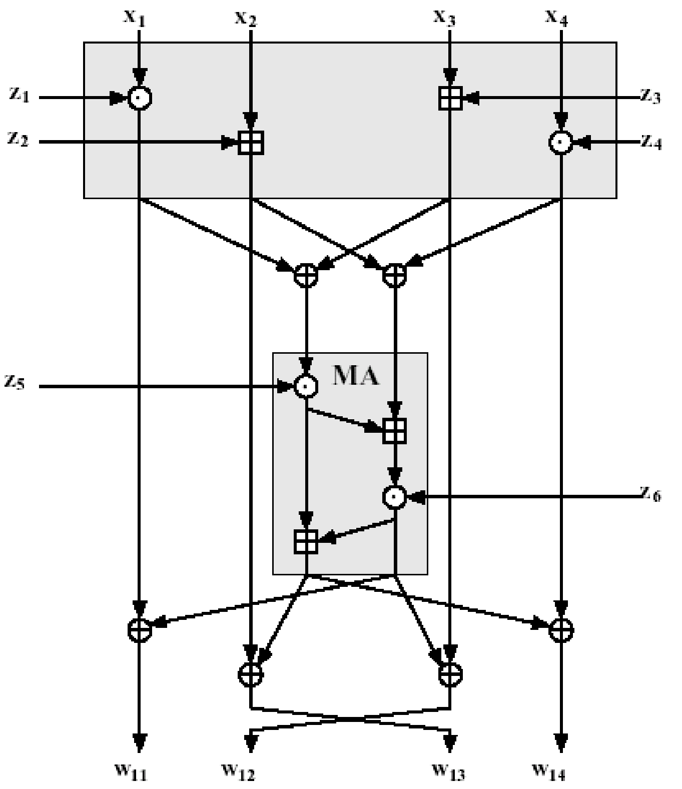
Indication the bit assignments for all subkeys with respect tothe original one is given below


Z (128 bits)
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8
Z15 Z16 Z9 Z10 Z11 Z12 Z13 Z14 Z15
Z22 Z23 Z24 Z17 Z18 Z19 Z20 Z21
Z28 Z29 Z30 Z31 Z32 Z25 Z26 Z27 Z28
Z35 Z36 Z37 Z38 Z39 Z40 Z33 Z34
Z41 Z42 Z43 Z44 Z45 Z46 Z47 Z48
Z49 Z50 Z51 Z52

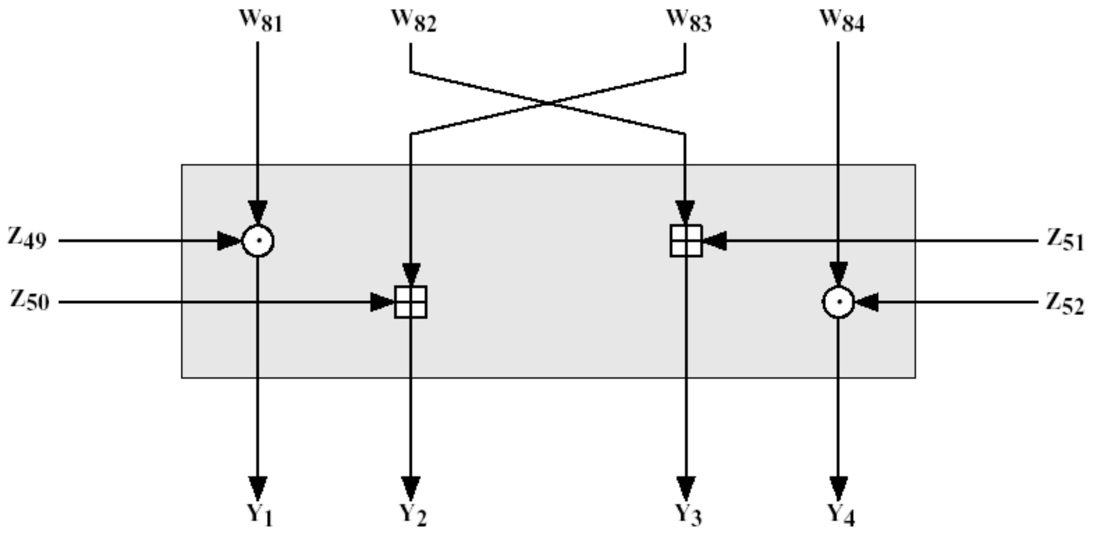
**IDEA Subkeys**

$Z_1$ = $Z$[1 … 16]
$Z_7$ = $Z$[94 … 112]
$Z_{13}$ = $Z$[90 … 105]
$Z_{19}$ = $Z$[83 … 98]

$Z_{25}$ = $Z$[76 … 91]
$Z_{31}$ = $Z$[44 … 59]
$Z_{37}$ = $Z$[34 … 52]
$Z_{43}$ = $Z$[30 … 45]



Single Round of IDEA (first round)



Output Transformation Stage of IDEA