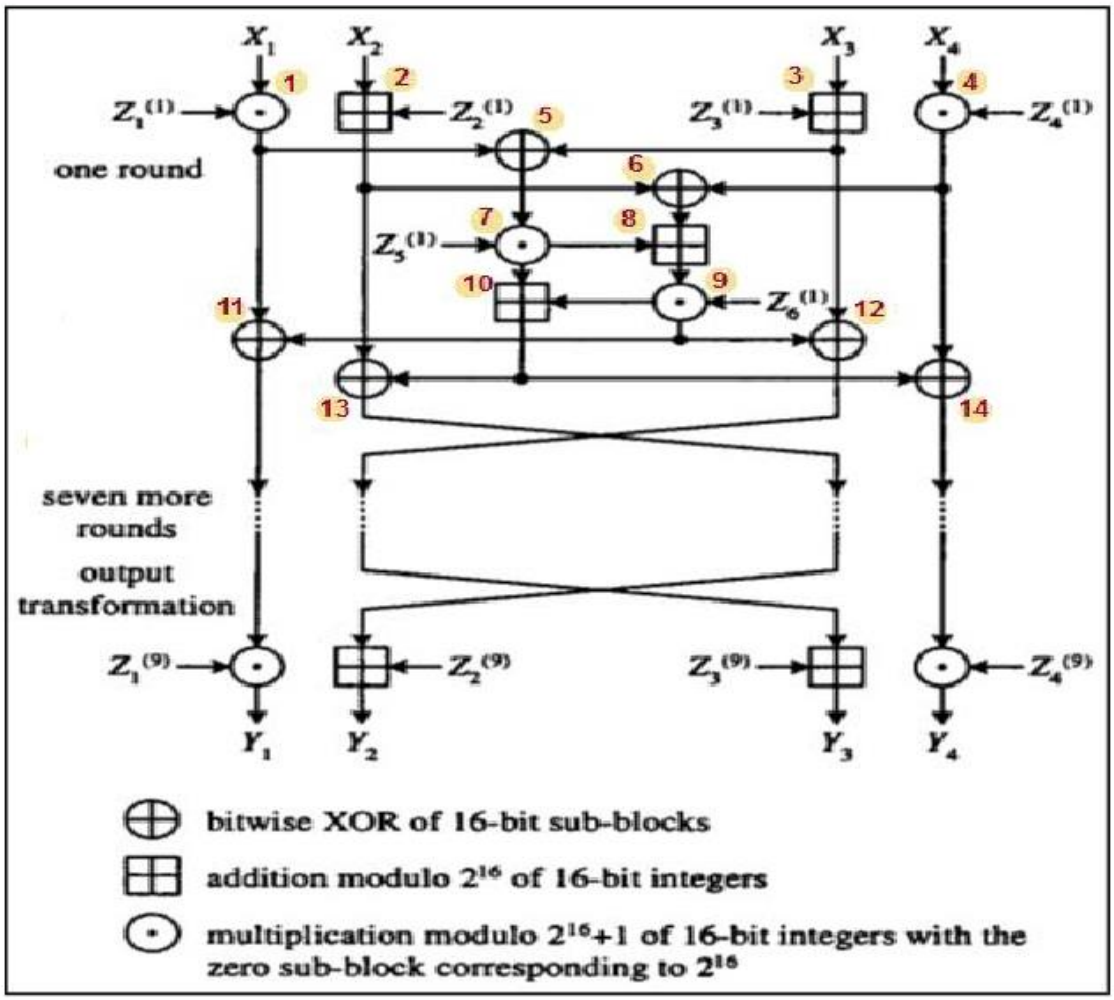
International Data Encryption Algorithm (IDEA)

The Simplified **International Data Encryption Algorithm (IDEA)** is a **symmetric key block** cipher that:

- uses a fixed-length plaintext of **64 bits** and
- encrypts them in **4 chunks of 16 bits** each
- to produce **64 bits ciphertext**.
- The length of the key used is **32 bits**.
- 128 bit key
- Each round six 16-bit key sub blocks required.
- Total of 52(=8X6+4) different 16-bit sub blocks.
- 128 bits to 16-bit eight blocks
- Cyclically left shift by 25 positions …..



This algorithm involves a series of 4 identical complete rounds and 1 half-round. Each complete round involves a series of 14 steps that includes operations like:

- Bitwise XOR
- Addition modulo (2^4)
- Multiplication modulo (2^4)+1

After 4 complete rounds, the final “half-round” consists of only the first 4 out of the 14 steps previously used in the full rounds. To perform these rounds, each binary notation must be converted to its equivalent decimal notation, perform the operation and the result obtained should be converted back to the binary representation for the final result of that particular step.

Key Schedule: 6 subkeys of 4 bits out of the 8 subkeys are used in each complete round, while 4 are used in the half-round. So, 4.5 rounds require 28 subkeys. The given key, ‘K’, directly gives the first 8 subkeys. By rotating the main key left by 6 bits between each group of 8, further groups of 8 subkeys are created, implying less than one rotation per round for the key (3 rotations).

The 16-bit plaintext can be represented as **X1 || X2 || X3 || X4**, each of size 4 bits. The 32-bit key is broken into 8 subkeys denoted as K1 || K2 || K3 || K4 || K5 || K6 || K7 || K8, again of size 4 bits each. Each round of 14 steps uses the three algebraic operation-Addition modulo (2^4), Multiplication modulo (2^4)+1 and Bitwise XOR. The steps involved are as follows:

1. **X1 * K1**
2. **X2 + K2**
3. **X3 + K3**
4. **X4 * K4**
5. **Step 1 ^ Step 3**
6. **Step 2 ^ Step 4**
7. **Step 5 * K5**
8. **Step 6 + Step 7**
9. **Step 8 * K6**
10. **Step 7 + Step 9**
11. **Step 1 ^ Step 9**
12. **Step 3 ^ Step 9**
13. **Step 2 ^ Step 10**
14. **Step 4 ^ Step 10**

The input to the next round is Step 11 || Step 13 || Step 12 || Step 14, which becomes X1 || X2 || X3 || X4. This swap between 12 and 13 takes place after each complete round, except the last complete round (4th round), where the input to the final half round is Step 11 || Step 12 || Step 13 || Step 14

After last complete round, the half-round is as follows:

1. X1 * K1
2. X2 + K2
3. X3 + K3
4. X4 * K4

The final output is obtained by concatenating the blocks.