Unit II Symmetric Ciphers

International Data Encryption Algorithm (IDEA)

Er. Kobid Karkee
Himalaya College of Engineering

IDEA: Overview

- DES algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications.
- However, its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours
- IDEA is a block cipher designed by Xuejia Lai and James L. Massey in 1991
- It is a minor revision of PES (Proposed Encryption Standard)
- IDEA was originally called IPES (Improved PES) and was developed to replace DES
- It entirely avoids the use of any lookup tables or S-boxes
- IDEA was used as the symmetric cipher in early versions of the Pretty Good Privacy cryptosystem

IDEA: Concept

- IDEA operates on 64-bit blocks using a 128- bit key.
- Completely avoid substitution boxes and table lookups used in the block ciphers
- The algorithm structure has been chosen such that when different key sub-blocks are used, the encryption process is identical to the decryption process
- It consists of a series of eight identical transformations (a round) and an output transformation (the half-round).
- IDEA derives much of its security by interleaving operations from different groups — modular addition and multiplication, and bitwise eXclusive OR (XOR) — which are algebraically "incompatible" in some sense.

IDEA: Concept

- In more detail, these operators, which all deal with 16-bit quantities, are:
  - Bitwise eXclusive OR ($\oplus$).
  - Addition modulo 2^{16} ($\boxplus$)
  - Multiplication modulo $2^{16}+1$ ($\odot$),

  where the all-zero word (0x0000) in inputs is interpreted as 2^{16} and 2^{16} in output is interpreted as the all zero word (0x0000)
- After the eight rounds comes a final —"half round", for the output.

Structure

- XOR is used for both subtraction and add in round function.
- To work with 16 bit words (meaning four inputs instead of two for the 64 bit block size), IDEA uses the Lai-Massey scheme twice in parallel, with the two parallel round functions being interwoven with each other.
- To ensure sufficient diffusion, two of the sub-blocks are swapped after each round.

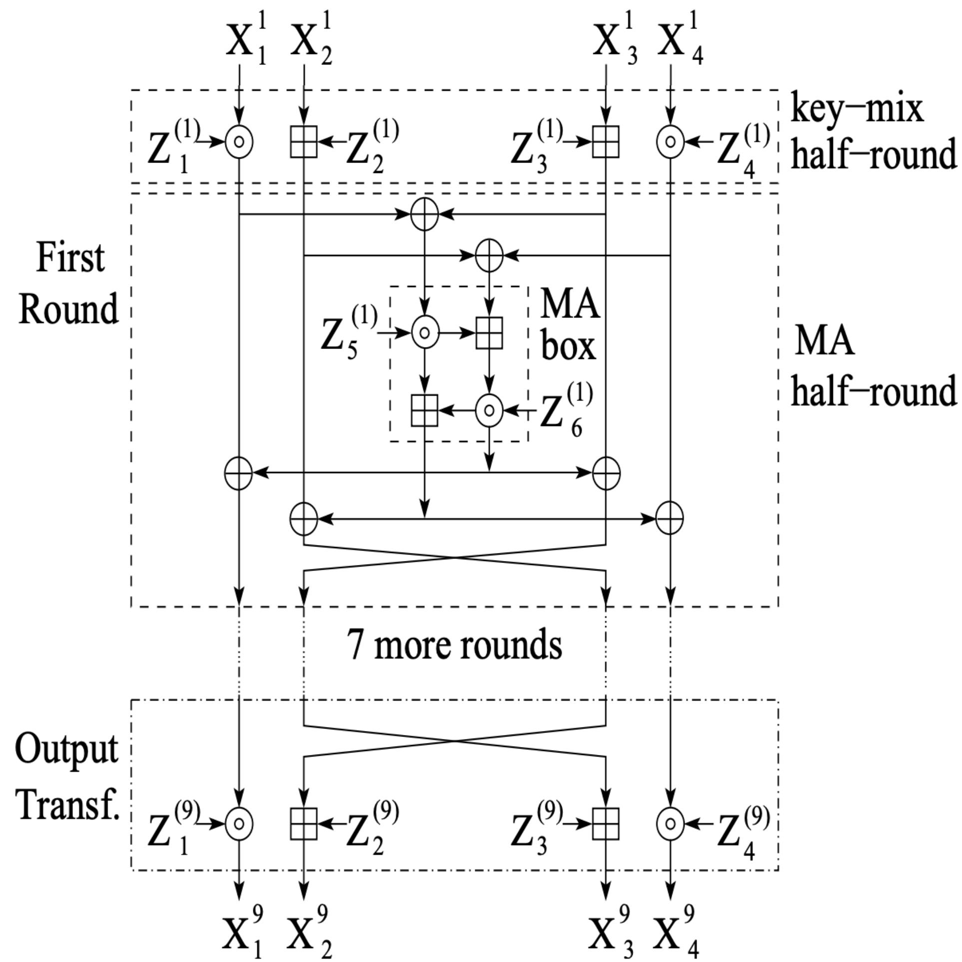

Fig. 1. Encryption scheme of IDEA block cipher.

Key Generation

- The 64-bit plaintext block is partitioned into four 16-bit sub-blocks.

- Six 16-bit key are generated from the 128-bit key for each round.

- Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

Key Generation Process

The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced as follows:

1. First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks
2. The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks
3. The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated

Key Generation Process

Generation of subkey bits from the master key bits of IDEA.

i-th round	$Z_1^{(i)}$	$Z_2^{(i)}$	$Z_3^{(i)}$	$Z_4^{(i)}$	$Z_5^{(i)}$	$Z_6^{(i)}$
1	0–15	16–31	32–47	48–63	64–79	80–95
2	96–111	112–127	25–40	41–56	57–72	73–88
3	89–104	105–120	121–8	9–24	50–65	66–81
4	82–97	98–113	114–1	2–17	18–33	34–49
5	75–90	91–106	107–122	123–10	11–26	27–42
6	43–58	59–74	100–115	116–3	4–19	20–35
7	36–51	52–67	68–83	84–99	125–12	13–28
8	29–44	45–60	61–76	77–92	93–108	109–124
OT	22–37	38–53	54–69	70–85	—	—

IDEA: Encryption

- The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation.
- The structure of IDEA encryption is shown in detail.

Bitwise eXclusive OR ($\oplus$)
Addition modulo 2^{16} ($\boxplus$)
Multiplication modulo 2^{16}+1 ($\odot$)

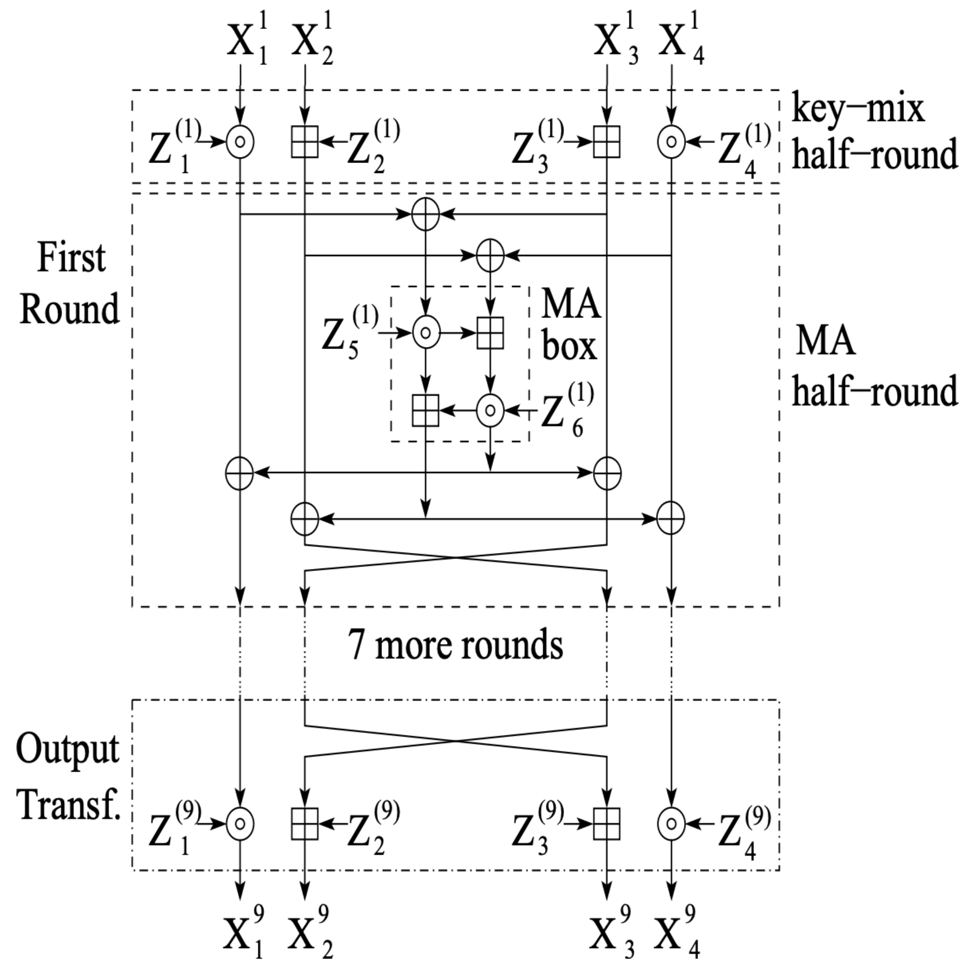

Fig. 1. Encryption scheme of IDEA block cipher.

IDEA: Encryption

- The key sub-blocks used for the encryption and the decryption in the individual rounds are shown as:

Round	Key Schedule
Round 1	$Z_1^{(1)} Z_2^{(1)} Z_3^{(1)} Z_4^{(1)} Z_5^{(1)} Z_6^{(1)}$
Round 2	$Z_1^{(2)} Z_2^{(2)} Z_3^{(2)} Z_4^{(2)} Z_5^{(2)} Z_6^{(2)}$
Round 3	$Z_1^{(3)} Z_2^{(3)} Z_3^{(3)} Z_4^{(3)} Z_5^{(3)} Z_6^{(3)}$
Round 4	$Z_1^{(4)} Z_2^{(4)} Z_3^{(4)} Z_4^{(4)} Z_5^{(4)} Z_6^{(4)}$
Round 5	$Z_1^{(5)} Z_2^{(5)} Z_3^{(5)} Z_4^{(5)} Z_5^{(5)} Z_6^{(5)}$
Round 6	$Z_1^{(6)} Z_2^{(6)} Z_3^{(6)} Z_4^{(6)} Z_5^{(6)} Z_6^{(6)}$
Round 7	$Z_1^{(7)} Z_2^{(7)} Z_3^{(7)} Z_4^{(7)} Z_5^{(7)} Z_6^{(7)}$
Round 8	$Z_1^{(8)} Z_2^{(8)} Z_3^{(8)} Z_4^{(8)} Z_5^{(8)} Z_6^{(8)}$
Output Transform	$Z_1^{(9)} Z_2^{(9)} Z_3^{(9)} Z_4^{(9)}$

IDEA: Encryption

- The first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$
- At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round
- The process is repeated in each of the subsequent 7 encryption rounds
- The four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo $2^{16} + 1$ to form the resulting four 16-bit ciphertext blocks

IDEA: Decryption

- The computational process used for decryption of the ciphertext is essentially the same as that used for encryption
- The only difference is that each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption
- In addition, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process

Applications of IDEA

- Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government
- The IDEA algorithm can easily be embedded in any encryption software. Data encryption can be used to protect data transmission and storage. Typical fields are:
  - Audio and video data for cable TV, pay TV, video conferencing, distance learning
  - Sensitive financial and commercial data
  - Email via public networks
  - Smart cards

Conclusion

- As electronic communications grow in importance, there is also an increasing need for data protection
- When PGP was designed, the developers were looking for maximum security. IDEA was their first choice for data encryption
- The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation