Symmetric Cryptography II

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

Overview

IDEA

1. IDEA

1.1. Background

Seems to be the best and most secure block cipher today - Questionable

Designed by X. Lai and J. Massey in 1991

Patented, but freely available for non-commercial use

Used in PGP v2.0

1. IDEA

1.2. Overview

64-bit block cipher

128-bit key

Same algorithm used for encryption and decryption

Uses three basic algebraic operations:

- XOR
- Addition modulo 2^{16}
- Multiplication modulo $2^{16} + 1$

Operations carried out on 16-bit sub-blocks

8 Rounds, 6 subkeys per round, 4 in the last round.

1.3. Design Principles

Two key principles:

1. Cryptographic Strength
   - Block Length → long enough to deter statistical analysis
   - Key length → long enough to prevent exhaustive key searches.
   - Confusion → Complicated relationship between ciphertext, plaintext and key.
   - Diffusion → Each plaintext bit and each key bit should influence every ciphertext bit. Diffusion obtained through the Multiplication Addition structure (MA).

1. IDEA

1.3. Design Principles

2. Implementation Considerations

For Software:

- Operate on sub-blocks (8,16 or 32 bit) natural to software. IDEA → 16-bit sub-blocks.
- Must be easily programmed using addition, shifting and so on

For hardware:

- Similarity of encryption and decryption, should only differ in the key (DES)
- Regular structure, to facilitate implementation.

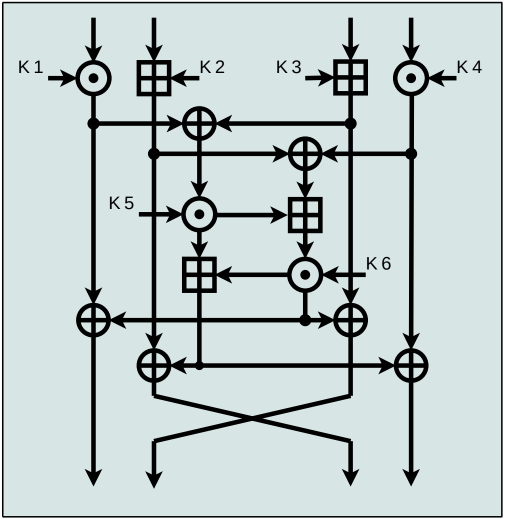
1.4 Operation

All operations work on 16-bit blocks.

Input data is first broken up into 4 × 16-bit blocks: X1, X2, X3, X4.

Sub-blocks enter the first of the 8 rounds

1. IDEA



1.4 Operation

The output of the round is four sub-blocks.

The inner results are swapped with the outer blocks remaining unswapped

Swapping done after every round except the last one.

1. IDEA

1.4 Operation

In the Last Round, the final transformation is:

- Multiply X1 with the 1st subkey to get Y1
- Add X2 to the second subkey to get Y2
- Add X3 to the third subkey to get Y3
- Multiply X4 with the fourth subkey to key Y4

Y1, Y2, Y3, Y4 are the ciphertext outputs.

1. IDEA

1.4 Key Schedule

Total of $8 \times 6 + 4 = 52$ subkeys.

Subkeys generated from 128-bit key

Generation scheme is as follows:

- Subkeys $Z_1^{(1)}$, $Z_2^{(1)}$, $\ldots$, $Z_6^{(1)}$, $Z_1^{(2)}$, $Z_2^{(2)}$ are 16-bit blocks from key.
- Key is circularly left-shifted by 25 bits, divided into next 8 subkeys
- Seventh round produces the four subkeys for the final transformation rest are discarded.

1. IDEA

1.4 Key Schedule

Decryption:
Same algorithm is used

Decryption keys are reversed and slightly altered

Subkeys can be unaltered, multiplicative inverse or additive inverse

1. IDEA

1.4 Key Schedule - Decryption

Round	Subkeys					
1st	$Z_1^{(9)-1}$	$-Z_2^{(9)}$	$-Z_3^{(9)}$	$Z_4^{(9)-1}$	$Z_5^{(8)}$	$Z_6^{(8)}$
2nd	$Z_1^{(8)-1}$	$-Z_3^{(8)}$	$-Z_2^{(8)}$	$Z_4^{(8)-1}$	$Z_5^{(7)}$	$Z_6^{(7)}$
3th	$Z_1^{(7)-1}$	$-Z_3^{(7)}$	$-Z_2^{(7)}$	$Z_4^{(7)-1}$	$Z_5^{(6)}$	$Z_6^{(6)}$
4th	$Z_1^{(6)-1}$	$-Z_3^{(6)}$	$-Z_2^{(6)}$	$Z_4^{(6)-1}$	$Z_5^{(5)}$	$Z_6^{(5)}$
5th	$Z_1^{(5)-1}$	$-Z_3^{(5)}$	$-Z_2^{(5)}$	$Z_4^{(5)-1}$	$Z_5^{(4)}$	$Z_6^{(4)}$
6th	$Z_1^{(4)-1}$	$-Z_3^{(4)}$	$-Z_2^{(4)}$	$Z_4^{(4)-1}$	$Z_5^{(3)}$	$Z_6^{(3)}$
7th	$Z_1^{(3)-1}$	$-Z_3^{(3)}$	$-Z_2^{(3)}$	$Z_4^{(3)-1}$	$Z_5^{(2)}$	$Z_6^{(2)}$
8th	$Z_1^{(2)-1}$	$-Z_3^{(2)}$	$-Z_2^{(2)}$	$Z_4^{(2)-1}$	$Z_5^{(1)}$	$Z_6^{(1)}$
Last	$Z_1^{(1)-1}$	$-Z_2^{(1)}$	$-Z_3^{(1)}$	$Z_4^{(1)-1}$		

1. IDEA

1.4 Key Schedule

Multiplicative inverses modulo $(2^{16}+1) \rightarrow Z^{-1}$.

Additive inverses modulo $(2^{16}) \rightarrow$ -Z

Note that $2^{16}+1$ is a prime

Thus, $x \mod (2^{16}+1)$ forms a finite group

Define 0x0000 as -1, thus inverse is -1 (0x0000)

1. IDEA

1.5 Cryptanalysis

Long key makes brute force attack infeasible.

Cryptanalysis of IDEA has shown that is resistant to differential and linear cryptanalysis.

Has a small number of weak keys (not weak as in the DES sense)

- If these keys are used, they can be identified using a chosen plaintext attack.
- The keys are: 0000 0000 0x00 0000 0000 000x xxxx x000
- X is any hex-digit. Chance of choosing one of these keys is so small as to be negligible.

1. IDEA

1.5 Cryptanalysis

IDEA is still relatively new, so many properties such as closed properties, and whether or not the use of independent subkeys is useful has not been proven.

Any double-IDEA would be susceptible to the meet-in-the-middle attack (as DES), but since the key length is so long this attack is impractical.

Characteristics of Advanced Symmetric Block Ciphers

All modern symmetric ciphers are similar to DES and the Feistel block cipher structure.

Advances in cryptanalysis have made some advances in cipher technology. Some features (not in DES):

- Variable key length → Strength in key gives strength to cipher under cryptanalysis. Blowfish, RC5, CAST-128 and RC2
- Mixed Operations → Use of more than one arithmetic and/or Boolean operation complicates cryptanalysis.
- Data dependant rotation → With enough rounds this can give excellent diffusion and confusion. RC5
- Key-dependant rotation → rotation depends on key not on the data
- Key-dependant S-boxes → Instead of fixed S-boxes, have content of the boxes dependant on the key. Blowfish

Characteristics of Advanced Symmetric Block Ciphers

- Lengthy key schedule → Key generation is longer than the encryption/decryption process itself and makes a brute force attack more difficult. Blowfish
- Variable number of rounds → Increase in rounds, increase in strength, but longer time. RC5
- Operation on both halves each round → In classical Feistel structure, only one half of the data is altered in each round. Operating on both halves increases strength without much increase in time. IDEA, Blowfish, RC5.

Summary

DES:

- Secure, 64-bit cipher, 64-bit key, 16 rounds.
- Meet-in-the-middle attack for double encryption.
- Secure in tripleDES, with three keys in EDE mode

IDEA:

- Secure, 64-bit, 128-bit key, 8 rounds + Output transformation.
- Patented, but used in PGP.

Blowfish:
Not for Examination