Data Encryption Standard (DES)

History, method, application and strength

Data Encryption Standard (DES)

- Published 1977 NBS
- Original IBM design
- 64 bit input → 64 bit encrypted output
- 56 bit key with odd parity (total 64 bits)
- Suitable for hardware not software
- 56 bits no longer secure

KEY TRANSFORMS IN BLOCK CIPHERS

For a k-bit block cipher
- Substitution
  For every k-bit i/p specify a k-bit o/p
  This requires $k \cdot 2^k$ bits
- Permutation
  For every bit specify new position in block
  This requires $k \cdot \log_2 k$ bits

Round Structure for Block Encryption

- Take 64-bit i/p
- Break into 8x8-bit blocks
- Perform substitution and reassemble into 64 bits
- Perform permutation and repeat
- After several rounds single i/p bit affects every o/p bit
- Optimum number of rounds
- Can be run in reverse for decryption
DES Overview (Encryption)

- 64 bit input
- Initial permutation
- Round 1: 48 bit key $k_1$
- Round 2: 48 bit key $k_2$
- Round 16: 48 bit key $k_{16}$
- Left/right reversal
- Final permutation (inverse of initial)

DES Overview (Decryption)

- 64 bit input
- Initial permutation
- Round 1: 48 bit key $k_{16}$
- Round 2: 48 bit key $k_{15}$
- Round 16: 48 bit key $k_1$
- Left/right reversal
- Final permutation (inverse of initial)

DES Overview (Decryption)

Encryption run in reverse

i.e. Initial permutation
- Round 1 with $k_{16}$
- Round 2 with $k_{15}$
- Round 16 with $k_1$

Left/right reversal

Final permutation

NB Initial and final permutations are inverses of each other and have no security value

The 16 Per Round Keys

- Same keys as for Encryption but in Reverse order
- Rotate left
- Final permutation (inverse of initial)

NB Initial permutation to produce $c_0$ and $d_0$ is not random and has no security value
A DES Round (encryption)

A DES Round (decryption)

Encrypt/Decrypt in a DES Round

From encryption \( L_{n+1} = R_n \) and

\[
R_{n+1} = L_n \oplus M_{k_n}(R_n)
\]

Therefore

\[
R_{n+1} \oplus M_{k_n}(R_n) = L_n
\]

and hence decryption

NB Mangler function does not require an inverse

Mangler Overview

\( R = 32 \text{ bits} = 8 \times 4 \text{ bits} \rightarrow 8 \times 6 \text{ bits} \) by copying last 2 bits in every 4

Take 48 bit key \( k \) and add mod 2 to expanded 48 bit \( R \)

Result is 48 bits = 8 x 6 bits

Compress each 6 bits to 4 bits through S box giving 32 bits

Permute 32 bit result

NB Importance of permutation to influence next round
International Data Encryption Algorithm (IDEA)

- Established 1991
- 64-bit plaintext → 64-bit ciphertext
- 128-bit key
- Round structure and Mangler similar to DES

IDEA Primitive Operations

- Two 16-bit numbers → one 16 bit number
- Bitwise exclusive or (+)
- Addition + modulo 2
- Multiplication × modulo 2
- All operations are “reversible”

IDEA Overview
IDEA Odd Round

IDEA Even Round

IDEA Decryption

- All processes the same
- Even round is its own inverse (use same keys)
- Odd rounds use inverse keys

Advanced Encryption Standard
Advanced Encryption Standard

- Uses Rijndael system
- In a pure Rijndael system block and key sizes may be chosen independently (128, 160, 192, 224 and 256 bits) but AES specifies 128-bit block size
- Number of rounds = 6 + max (block, key size expressed in 32-bit words)