Data Encryption Standard (DES)

Angelo Panariti

February 16, 2024

1 Introduction

A few facts:

- 1974 proposed by the IBM with input from NSA.
- 1977...1998 US Standard.
- Best studied cipher in the world.
- Unsecure today (key too short), but 3DES is very secure (applied three times).

$$x \rightarrow DES(k) \rightarrow y$$

Encrypts blocks of size 64-bit (8 bytes in (x), 8 bytes out(y)).

Uses a key (k) size of 56-bit (7 bytes).

Symmetric cipher as it uses the same key for encryption and decryption.

Uses 16 rounds which all perform the same operation.

Different subkey in each round derived from main key

Question: how do we build a block cipher?

1.1 Claude Shannon

Founder of Information Theory in the 40s. He defined two atomic operations that block cipher should perform

1. **Confusion**: Relationship between plain and cipher text it's obscured.

   Example: substitution table.

2. **Diffusion**: The influence of each plaintext bit is spread over many ciphertext bits.

   Example: permutation.

At the end you combine confusion and diffusion many times to build strong block ciphers.

- Most of today's block ciphers are product ciphers as they consist of rounds which are applied repeatedly to the data.

- Can reach excellent diffusion: changing of one bit of plaintext results on average in the change of half the output bits. (Avalanche effect: you do little changes to the input, and it all spreads out to the output)

2 Feistel Network

Many of today's ciphers are Feistel ciphers.

Algorithm 1 Standard Feistel cipher

```
a message $m$ the ciphertext $c$ let the encrypted word in step $i$ be $m_i := L_i R_i$ with $m_0 := L_0 R_0$ as the unciphered message;
$i \leftarrow 0$ $n$ 1    $L_{i+1} \leftarrow R_i$;
$R_{i+1} \leftarrow L_i \oplus F(L_i, K_i)$;
$m_N := L_{n+1} R_{n+1}$;
$m_N$
```

3 DES Internals

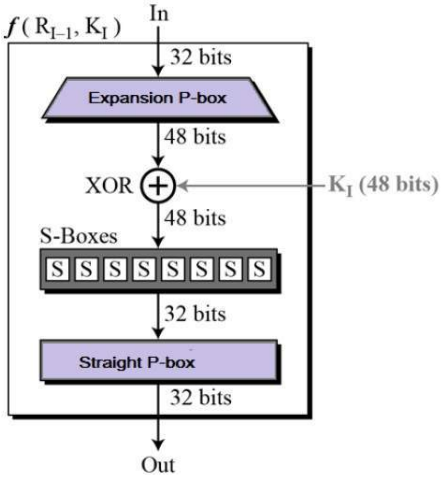
3.1 IP (Initial permutation) and IP^{-1}

Simple bitwise permutation, e.g bit 1 and 58, bit 1 is copied to bit position 40. An initial permutation is required only once at the starting of the encryption process. In DES, after the complete plaintext is divided into blocks of 64 bits each, IP is required on each of them. This initial permutation is a phase in the transposition procedure.

The initial permutation appears only once, and it appears before the first round. It recommend how the transposition in IP should proceed, as display in the table.

We have mentioned that DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

3.2 Details of the f-Function



E-Box provides diffusion

- Main purpose: increases diffusion.

S-Box provides confusion

- The heart of DES
- Eight substitution tables
- 6 bits of input 4 bits of output

Unusual decoding of the S-Box tables.

Input bits 6, 7, 8, 9
Col select 7, 8
Row select 6,9

Ex:

$S_i(37)$

$S_i(100101)$

3.3 IBM, NSA and Differential Cryptanalysis

The discovery of differential cryptanalysis is generally attributed to Eli Biham and Adi Shamir in the late 1980s, who published a number of attacks against various block ciphers and hash functions, including a theoretical weakness in the Data Encryption Standard (DES).

In 1994, a member of the original IBM DES team, Don Coppersmith, published a paper stating that differential cryptanalysis was known to IBM as early as 1974, and that defending against differential cryptanalysis had been a design goal. According to author Steven Levy, IBM had discovered differential cryptanalysis on its own, and the NSA was apparently well aware of the technique.

IBM kept some secrets, as Coppersmith explains: ”After discussions with NSA, it was decided that disclosure of the design considerations would reveal the technique of differential cryptanalysis, a powerful technique that could be used against many ciphers. This in turn would weaken the competitive advantage the United States enjoyed over other countries in the field of cryptography.” Within IBM, differential cryptanalysis was known as the ”T-attack” or ”Tickle attack”.