Symmetric-Key Encryption

Data Encryption Standard (DES)

Theorem

Let $DES_{K_1 K_2 \cdots K_{16}}$ denote the DES encryption function, where $K_1, K_2, \ldots, K_{16}$ be the 16 round keys of a given 56-bit input key K. Then, for all plaintext messages $x \in \{0, 1\}^{64}$, $DES_{K_{16} K_{15} \cdots K_1}(DES_{K_1 K_2 \cdots K_{16}}(x)) = x$, that is, $DES_{K_{16} K_{15} \cdots K_1}$ becomes the DES decryption function.

Symmetric-Key Encryption

Data Encryption Standard (DES)

Theorem

Let DES : $\{0,1\}^{64} \times \{0,1\}^{56} \rightarrow \{0,1\}^{64}$ *be the DES function. Assume that* $\bar{x}$ *represents the bitwise complement of a bit string* x*. Then,* $DES(\bar{k}, \bar{x}) = \overline{DES(k, x)}$*, for every plaintext* $x \in \{0,1\}^{64}$ *and key* $k \in \{0,1\}^{56}$*.*

Theorem

Using this complementing property of DES, the brute-force attack to break the DES algorithm reduces the complexity from 2^{56} *to* 2^{55}*.*

Diffusion and Confusion Properties of DES

- In a binary block cipher, such as the DES, **diffusion** is accomplished by using permutations on data, and then applying a function to the permutation to produce ciphertext.
- In DES, **confusion** is accomplished by making the use of substitution operations (S-Boxes).

Avalanche Effect on DES

- A small change in the plaintext (or key) should create a significant change in the ciphertext.
- DES has been proved to be strong with regard to this property.
- **An Example:**
  - Set 1: **key: 2333 4519 ABCD 9513** (64-bits after 8-bit parity padding, 16 digits in hexadecimal)
    plaintext: 0000 0000 0000 0000
    ciphertext: C871 779E 2860 D09E
  - Set 2: **same key: 2333 4519 ABCD 9513**
    plaintext: 0000 0000 0000 0001 (single bit change)
    ciphertext: 10F6 2D55 327E 840A

Limitations of DES

Weak Keys

- In DES encryption/decryption, the initial key is of 56 bits. So, the total number of keys in the key space is 2^{56}.
- Four out of these 2^{56} possible keys (0000000 0000000; 0000000 FFFFFFF; FFFFFFF 0000000; FFFFFFF FFFFFFF) are called weak keys.
- A **weak key** is that one, after parity drop operation, consists of either of all 0s, all 1s, or half 0s and half 1s.
- In addition, there are 12 semi-weak keys and 48 possible weak keys, a total of such keys is (4 + 12 + 48) = 64.
- Probability of randomly selecting a weak, a semi-weak, or a possible weak key turns out to be $\frac{64}{2^{56}} = \frac{2^6}{2^{56}} = 2^{-50} \approx 8.8 \times 10^{-16}$, almost impossible.

Symmetric-Key Encryption

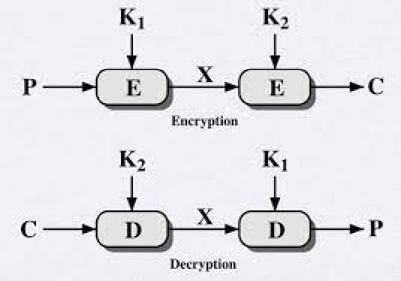
Data Encryption Standard (DES)

- DES finally and definitely proved insecure in July 1998, when the Electronics Frontier Foundation (EFF) announced that it had broken a DES encryption using a special-purpose “DES cracker” machine that was built for less than 250,000 USD.
- The attack took less than three days.

Various modes of operation

Double DES (2DES)

- It uses two 56-bit keys K_1 and K_2, and 64-bit plaintext block.
- It produces 64-bit ciphertext block.
- Known-plaintext attack (meet-in-the-middle attack) is possible against 2DES to derive two keys K_1 and K_2, which has a key size of 112 bits and with an effort on the order of 2^{56}.



Meet-in-the-middle attack in 2DES

- It is based on the observation that, if we have $C = E_{K_2}[E_{K_1}(P)]$, then $X = E_{K_1}(P) = D_{K_2}(C)$.
- Given a known pair, (P, C), the attack proceeds as follows.
  - First, encrypt P for all 2^{56} possible values of K_1 (in offline mode).
  - Store these results in a table and then sort the table by the values of X (in offline mode).
  - Next, decrypt C using all 2^{56} possible values of K_2 (in online mode).
  - As each decryption is produced, check the result against the table for a match.
  - If a match occurs, then test the two resulting keys against a new known plaintextciphertext pair.
  - If the two keys produce the correct ciphertext, accept them as the correct keys.

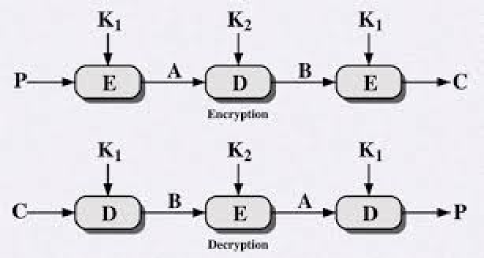
Meet-in-the-middle attack in 2DES

- For any given plaintext P , there are 2^{64} possible ciphertext values that could be produced by double DES.
- Double DES uses, in effect, a 112-bit key, so that there are 2^{112} possible keys. Therefore, on average, for a given plaintext P, the number of different 112-bit keys that will produce a given ciphertext C is $\frac{2^{112}}{2^{64}} = 2^{48}$.
- Thus, the foregoing procedure will produce about 2^{48} false alarms on the first (P, C) pair.
- A similar argument indicates that with an additional 64 bits of known plaintext and ciphertext, the false alarm rate is reduced to $\frac{2^{48}}{2^{64}} = 2^{-16}$.
- If the meet-in-the-middle attack is performed on two blocks of known plaintextciphertext, the probability that the correct keys are determined is $1 - 2^{-16}$.
- The result is that a known plaintext attack will succeed against double DES, which has a key size of 112 bits, with an effort on the order of 2^{56}, which is not much more than the 2^{55} required for single DES.

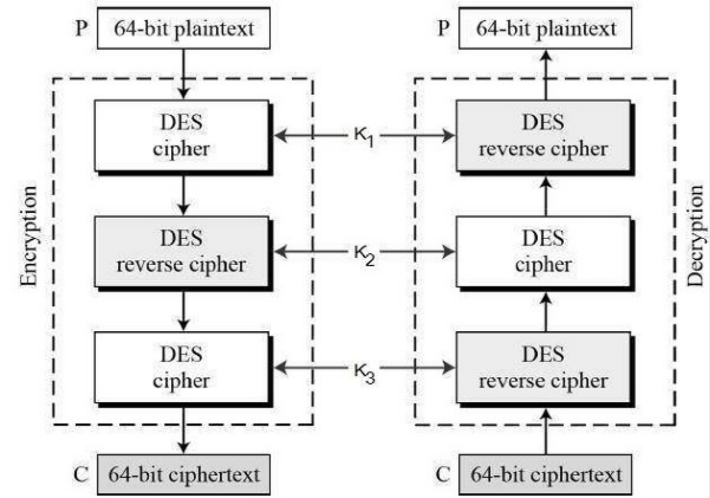
Symmetric-Key Encryption

Triple DES with Two Keys (3DES with Two Keys)

- It uses two 56-bit keys K_1 and K_2, and 64-bit plaintext block.
- It produces 64-bit ciphertext block.
- It is also vulnerable to known-plaintext attack (meet-in-the-middle attack) to derive two keys K_1 and K_2.
- The expected running time of this attack is on the order of $2^{120-\log_2 n}$, where n is the number of plaintext-ciphertext pairs.



Triple DES with Three Keys (3DES with Three Keys)



Symmetric-Key Encryption

Alternatives to Data Encryption Standard (DES)

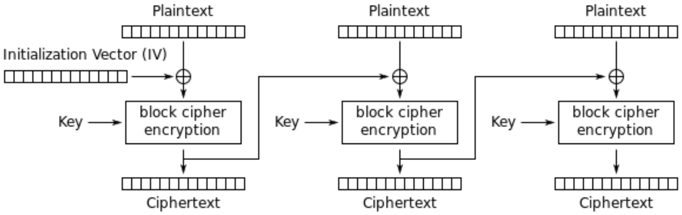
- **Triple DES with Three Keys (3DES with Three Keys)**
  - It uses three 56-bit keys K_1, K_2 and K_3, and 64-bit plaintext block.
  - It produces 64-bit ciphertext block.
  - No practical attack is found on this cipher so far. It is secure.
  - Application: It is used in all Internet-based applications such as PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Main Extension) protocols.
- **AES (Advanced Encryption Standard)**
  - AES takes 128-bit key and 128-bit plaintext blacks as input.
  - AES produces 128-bit cipertext blocks.
  - AES is very efficient.
  - AES is secure against all possible attacks.

Symmetric-Key Encryption

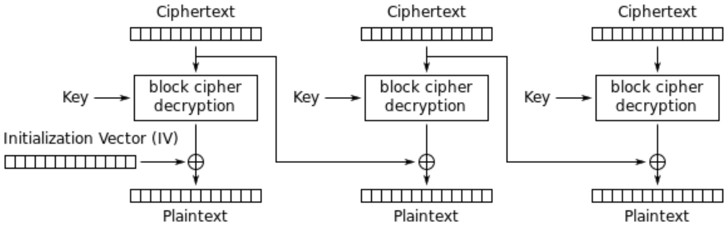
Various modes of operation of Data Encryption Standard (DES)

- Electronic Codebook Mode (ECB)
- Cipher Block Chaining Mode (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)

Various modes of operation



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Thank you