1 DES 基本原理

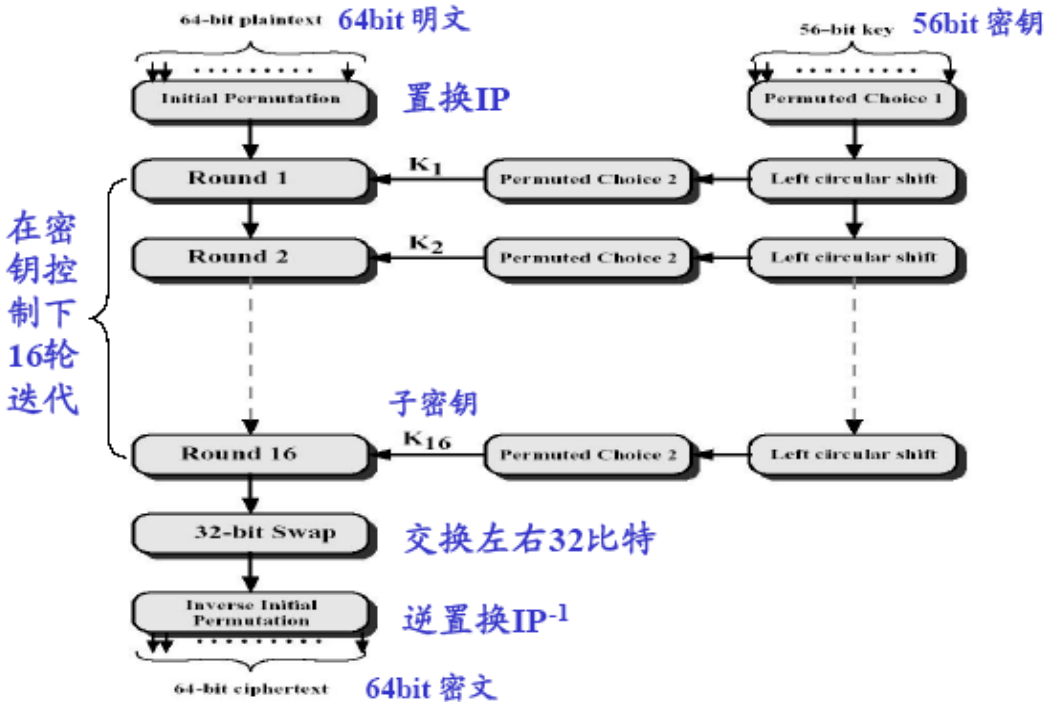
DES 全称为 Data Encryption Standard，即数据加密标准，是一种使用密钥加密的块算法，1977 年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），并授权在非密级政府通信中使用，随后该算法在国际上广泛流传开来。

(1)基本原则：混淆和扩散

DES 设计中使用了分组密码设计的两个原则：混淆（confusion）和扩散(diffusion)，其目的是抗击敌手对密码系统的统计分析。混淆是使密文的统计特性与密钥的取值之间的关系尽可能复杂化，以使密钥和明文以及密文之间的依赖性对密码分析者来说是无法利用的。扩散的作用就是将每一位明文的影响尽可能迅速地作用到较多的输出密文位中，以便在大量的密文中消除明文的统计结构，并且使每一位密钥的影响尽可能迅速地扩展到较多的密文位中，以防对密钥进行逐段破译。

(2)基本流程

用 56 位的密钥对 64 位长的数据块进行 16 轮加密处理由此得到 64 位长的密文。算法包含两部分：迭代加解密和密钥编排。



(3)基本特点

- Feistel 结构（加解密相似）：加密和解密除密钥编排不同外完全相同。
- 密钥长度：56 比特（DES 的密钥空间：2^{56}），每 7 比特后为一个奇偶校验位（第 8 位），共 64 比特。
- 轮函数采用混乱和扩散的组合，共 16 轮。
- DES 的安全性不依赖于算法的保密，安全性仅以加密密钥的保密为基础；密钥可为任意的 56 位数，具有复杂性，使得破译的开销超过可能获得的利益。

- 只使用了标准的算术和逻辑运算，易于实现。

2 DES 加密推导

假设 DES 算法的明文输入 M=FEFEFEFEFEFEFEFE，密钥 K=55555555555555（均为 16 进制表示，密钥没有校验位），推导第一轮的输出。

(1)转化为二进制表示为

$$M = 1111111011111110111111101111111011111110111111101111111011111110$$

$$K = 0101010101010101010101010101010101010101010101010101010101010101$$

(2)初始置换 IP 得

$$M_{IP} = 1111111111111111111111110000000011111111111111111111111111111111$$

$$= FFFFFF00FFFFFFFF$$

(3)轮密钥扩展

(a)经过 PC-1 置换并剔除校验位

$$K_{PC-1} = \text{AA55AA5AA55AA5}$$

$$C_0 = 10101010010101011010100101$$

$$D_0 = 10101010010101011010100101$$

(b)分组，左移位一次

$$1 \ll C_1 = 01010100101010110101001011$$

$$1 \ll D_1 = 01010100101010110101001011$$

(c)经 PC-2 置换得

$$K_1 = 00100001110000010010111110010110000110111110 1001$$

$$= 21C12F961BE9$$

(4)第一轮加密开始

(a)$L_1 = R_0 = FFFFFFFF$

(b) R_0经扩展置换 E 得

$$11111111111111111111111111111111 \rightarrow 11111111111111111111111111111111111111111111$$

$$R_{0E} = FFFFFFFFFFFF$$

(c) R_{0E}与K_1轮密钥加

$$R_{0E} \oplus K_1 = FFFFFFFFFFFF \oplus 21C12F961BE9$$

(d)S 盒替换依次输出为：

$$S_1^1 = 1110 \quad S_2^1 = 1000 \quad S_3^1 = 0101 \quad S_4^1 = 0001$$

$$S_5^1 = 0000 \quad S_6^1 = 1011 \quad S_7^1 = 0011 \quad S_8^1 = 1110$$

$$R_S = 11101000010100010000101100111110$$

(e)对 S 盒输出进行置换 P

$$R_P = 10011110101010111010011000100000$$

(f)轮函数输出与L_0模2加得到R_1

$$R_1 = L_0 \oplus R_P = 01100001010101000101100100100000$$

$$= 61545920$$

(5)第一轮加密结束输出为：$FFFFFFFF61545920$

$$L_1 = FFFFFFFF \quad R_1 = 61545920$$