信息安全技术 Project:DES 算法实现

21307174 刘俊杰

May 2024

1 算法介绍

1.1 算法简介

DES (Data Encryption Standard) 是一种对称密钥加密算法，由 IBM 于上世纪 70 年代初开发，并在 1977 年被美国国家标准局 (NIST) 确定为联邦信息处理标准 (FIPS) 中的一部分。DES 是历史上最常用的加密算法之一，尽管因为使用的 56 位密钥过短导致它在现代计算机环境下已被认为是不安全的，但它的设计原理对于理解其他现代加密算法仍然具有重要意义。

1.2 算法特点

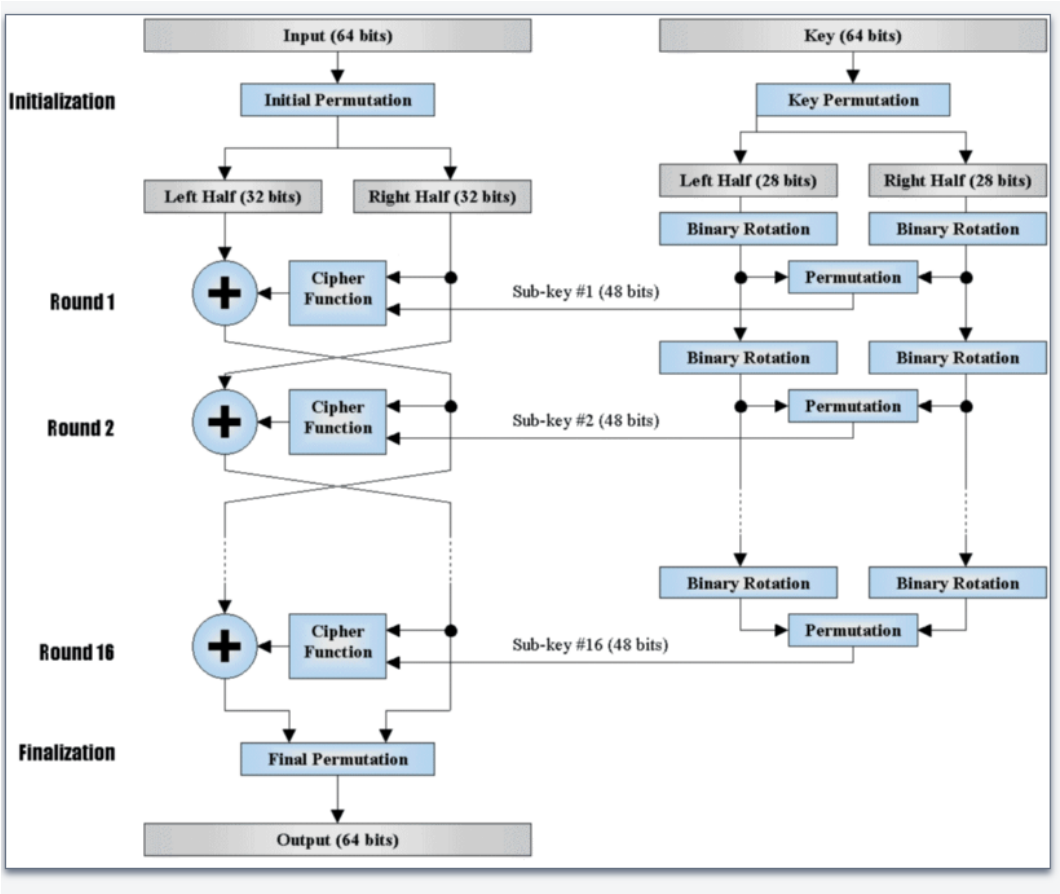
DES 算法具有以下特点:

1. 对称加密算法: DES 是一种对称密钥加密算法，这意味着加密和解密使用相同的密钥。这种算法的优点是速度快，但需要解决密钥分发的问题。
2. 分组密码: DES 是一种分组密码，它将明文分成固定大小 (64 位) 的块，并对每个块进行加密。由于 DES 是分组密码，因此它需要填充 (padding) 来处理不完整的块。
3. 密钥长度: DES 的密钥长度为 64 位，这意味着 DES 使用 65 位密钥对 64 位的明文进行加密。然而，由于每个字节的奇偶校验位，实际上只有 56 位用于加密。这在现代计算机环境下已被认为是不够安全的。
4. 轮函数: DES 使用一系列的轮函数 (round function) 来对明文进行加密。每一轮中，明文块被分成左右两部分，经过一系列的置换和替换操作，然后与上一轮的结果进行混合。

5. **密钥调度：在 DES 加密过程中，密钥需要经过一系列的置换和轮密钥生成算法来生成子密钥。这些子密钥用于每一轮的加密操作。**
6. Feistel **结构：DES 采用了 Feistel 结构，这意味着加密和解密过程是相同的，只是在轮密钥的应用顺序上有所不同。**

1.3 算法过程

DES 算法的整体框架：



上述框架左侧是 DES 加解密的基本流程，右侧是密钥调度流程

1.3.1 初始置换 (Initial Permutation)

将明文按规定的置换表做一次置换
(IP 和 FP 都是简单置换，对于密码安全没有任何意义)

1.3.2 round 轮转

$$L' = R$$
$$R' = L \oplus F(R, subkey)$$

1.3.3 Feistel 函数

1.3.4 密钥调度

1.3.5 最终置换 (Final Permutation)

将最终的 R 和 L 拼接，做最后一次置换
(IP 和 FP 都是简单置换，对于密码安全没有任何意义)

2 算法实现

3 实验结果

4 总结与感悟

4.1 DES 算法的优缺点

4.1.1 DES 算法的优点:

1. 速度较快：DES 是一种相对较快的加密算法，这使得它在许多应用中都有着良好的性能表现。
2. 结构简单：DES 的算法结构相对简单，易于理解和实现。
3. 对普通攻击有一定抵抗力：DES 能够抵抗一些基本的攻击，如差分攻击、线性攻击等，这使得它在某些情况下仍然可以被使用。

4.1.2 DES 算法的缺点：

1．密钥长度短：DES 的密钥长度只有 56 位，这在当前的计算能力下已经不够安全。使用较短的密钥长度容易受到穷举搜索等暴力攻击的威胁。
2．已被破解：由于 DES 的密钥长度较短，使得它易受到巨大计算能力的现代计算机和专用硬件的攻击。DES 已经被证明是不安全的，并且可以在相对较短的时间内被破解。
3．未来不可持续：随着计算能力的不断增强和密码分析技术的不断发展，DES 已经不再具有足够的安全性,因此不适合用于保护敏感数据或长期使用。

4.1.3 DES 算法的替代方案

安全性方面的考虑使得研究者在 1980 年代晚期和 1990 年代早期提出了一系列替代的块密码设计，包括 RC5，Blowfish，IDEA，NewDES，SAFER，CAST5 和 FEAL。这些设计的大多数保持了 DES 的 64 位的块大小，可以作为 DES 的直接替代方案，虽然这些方案通常使用 64 位或 128 位的密钥。苏联导入了 GOST 28147-89 算法，该算法的块大小为 64 位，而密钥长度为 256 位，并在晚些时候的俄罗斯得到了应用。

2000 年代，DES 逐渐被 3DES 替代。3DES 相当于用两个（2TDES）或三个（3TDES）不同的密钥对数据进行三次 DES 加密。2010 年代，3DES 逐渐被更安全的高级加密标准（AES）替代。

2000 年 10 月，在历时接近 5 年的征集和选拔之后，NIST 选择了高级加密标准（AES）替代 DES 和 3DES。2001 年 2 月 28 日，联邦公报发表了 AES 标准，以此开始了其标准化进程，并于 2001 年 11 月 26 日成为 FIPS PUB 197 标准。AES 算法在提交的时候称为 Rijndael。选拔中其它进入决赛的算法包括 RC6，Serpent，MARS 和 Twofish。

4.2 实验感悟

通过本次课程项目，我学习了 DES 对称加密算法，了解了 DES 算法加解密的框架和过程，并用代码来实现 DES 算法。这不仅让我对该算法的对称密码体系结构:Feistel 网络结构以及密钥调度等基本概念和原理更加熟悉，而且了解到了 DES 的安全性逐渐受到挑战。这提醒我们在设计和选择加密算法时，需要考虑到未来的发展和计算环境，以确保数据的安全性和机密性。

因此，DES 算法不仅在于它的历史地位和影响，更在于它对密码学发展的启示和警示，为我们理解和应用密码学提供了宝贵的经验和教训。