计算机和网络安全课程笔记 Week 3

Nite

2025-03-19T12:18:00+11:00

块密码定义与基本属性 (Block Cipher Definition and Properties)

1. 块密码 (Block Cipher) 是一对作用于固定长度块 B 的加密/解密算法 (E, D)。
2. 加密算法 E 和解密算法 D 都使用一个 K 比特的密钥 k。
3. 对于任意的数据块 b，解密应用在加密结果上可以恢复原始块：$D_k(E_k(b)) = b$。
4. 块密码 $E_k : \{0,1\}^n \to \{0,1\}^n$ 必须是**可逆的 (invertible)**。
5. 构造一个**密码学安全的 (cryptographically secure)** 可逆函数是困难的。
6. 构造**伪随机函数 (pseudorandom functions)** (例如散列函数 HASH) 相对容易。

Feistel 网络 (Feistel Network)

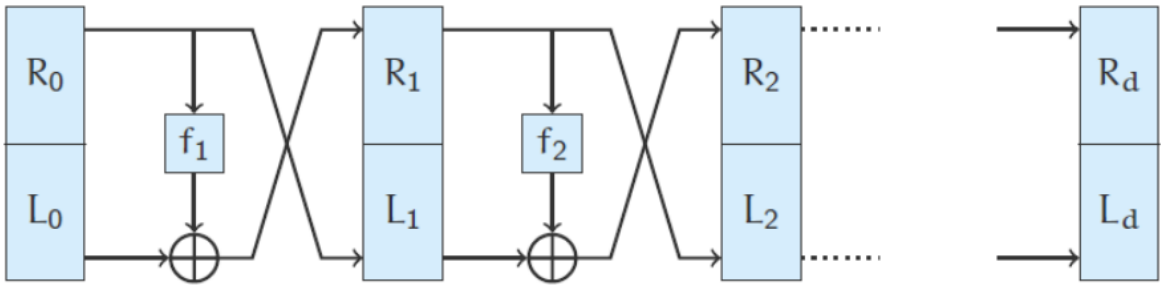


图 1: Feistel 网络结构图示

1. Feistel 网络是一种将 d 个伪随机函数 $f_1, \ldots, f_d$ (每个将 n 位映射到 n 位) 组合成一个**安全的 (secure) 可逆函数 (invertible function)** 的结构。
2. 这个可逆函数将 $2n$ 位映射到 $2n$ 位。
3. 代数上，输入被分成两半 (L_0, R_0)。网络的每一轮迭代如下：

$$L_i = R_{i-1} R_i = f_i(R_{i-1}) \oplus L_{i-1}$$

4. 因为每一步都是可逆的，所以整个网络是可逆的。
5. 其**逆网络 (inverse network)** 是相同的结构，但轮函数的顺序是反转的：$f_d, f_{d-1}, \ldots, f_2, f_1$。
6. 在密码中使用时，$f_1, \ldots, f_d$ 被称为**轮函数 (round functions)**。

数据加密标准 (Data Encryption Standard, DES)

DES 概述

1. DES 是一种块密码，操作块长为 64 位，使用 56 位密钥。
2. DES 接收一个 56 位密钥 k 和一个 64 位块 b 进行加密。

DES 内部结构 (DES Internals)

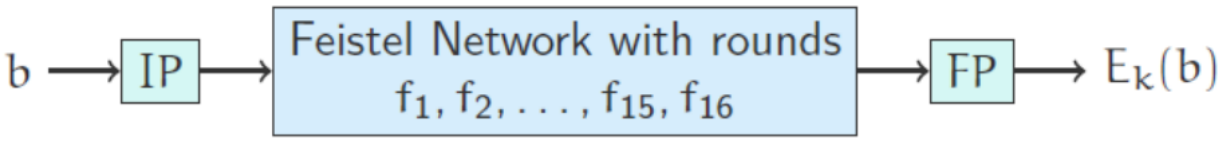


图 2: DES 内部结构图示，包含 IP, Feistel 网络, FP

1. 对输入块应用一个**初始置换 (Initial Permutation, IP)**。
2. 置换后的块被送入一个 16 轮的 Feistel 网络。
3. 轮函数 $f_i(x)$ 的定义是 $F(x, k_i)$。
4. k_i 是从主密钥 k 通过**密钥编排 (key schedule)** 导出的第 i 轮的轮密钥。
5. 每个轮密钥 k_i 是 48 位。
6. Feistel 网络输出后，应用一个**最终置换 (Final Permutation, FP)**。

DES 轮函数 (DES Round Function) $F(x, k_i)$

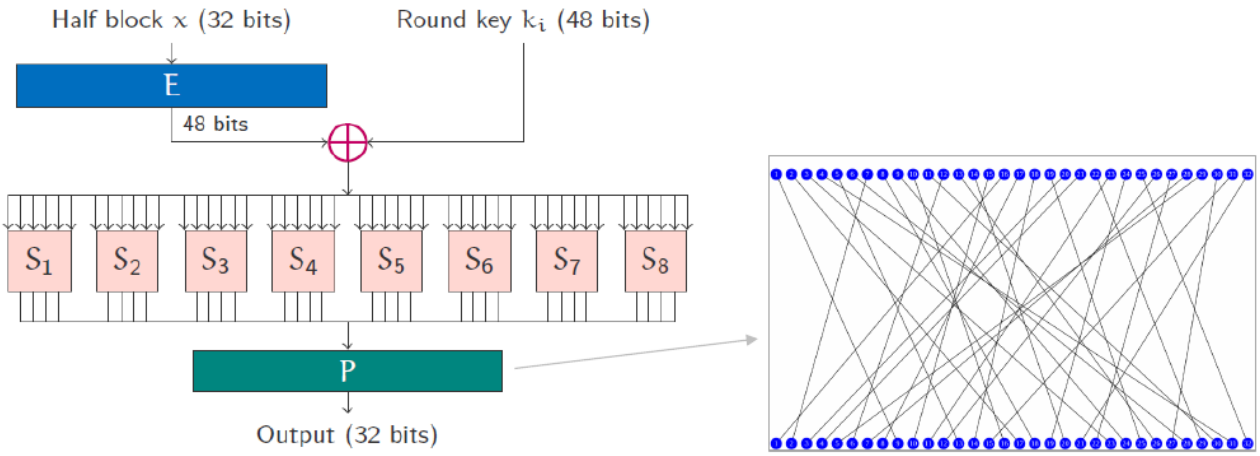


图 3: DES 轮函数内部结构图示，包含 E, S-boxes, P-box

1. 轮函数 $f_i(x) = F(x, k_i)$ 由以下部分组成：
    1. **扩展置换 (Expansion Permutation)** E: 将 x (32 位) 扩展到 48 位。
    2. **替换盒 (Substitution Boxes, S-boxes)** S_j: 将 6 位输入塌缩为 4 位输出。
    3. **固定置换 (Fixed Permutation, P-box)** P: 一个固定的置换操作。

密码设计原则：扩散与混淆 (Diffusion and Confusion)

重要性

1. **扩散 (Diffusion)** 和**混淆 (Confusion)** 是块密码期望拥有的特性，用于阻止**基于统计的密码分析 (statistic-based cryptanalysis)**。

扩散 (Diffusion)

1. **扩散**是明文**统计信息消散 (dissipation of statistical information)** 的过程。
2. 翻转明文中的一位应该导致密文约一半的比特发生改变。
3. 翻转密文中的一位应该导致明文约一半的比特发生改变。
4. 扩散与**置换密码 (permutation ciphers)** 相关。

混淆 (Confusion)

1. **混淆**是使密钥与密文之间的关系尽可能复杂的过程。
2. 密文的每一个比特都应该依赖于密钥的多个比特。
3. 即使攻击者收集到许多使用相同密钥加密的 (明文, 密文) 对，他们也应该无法推导出密钥。
4. 混淆与**替换密码 (substitution ciphers)** 相关。

如何实现扩散与混淆

1. 当**高度非线性 (highly nonlinear)** 的 S-boxes 与**好的** P-boxes 结合使用时，就会同时产生混淆和扩散的特性。
2. 使用线性 S-boxes 会使整个 DES 成为一个线性函数，容易被分析。
3. 如果 P-boxes 不能充分地散播比特，DES 可以被分解成更小的独立子问题。
4. 定性地说，“好的”S-boxes 和 P-boxes 是协同工作的。
    1. S-boxes 是高度非线性的，翻转一个输入比特应该导致其输出比特约一半翻转。
    2. 其后的 P-box 应该将这些翻转的比特均匀地分布到下一轮的 S-boxes 中。

块密码的使用：填充与工作模式

块密码填充 (Block Cipher Padding)

1. 当明文长度不能正好适配块长时，需要对明文进行**填充 (pad)**。
2. 填充是通过在最终块后附加预定义的比特序列来“填满”该块。
3. 选择用于填充的比特非常重要，因为它具有**密码学含义 (cryptographic implications)**。
4. 一些可接受的填充函数包括：ANSI X9.23、PKCS#5 和 PKCS#7。

块密码工作模式 (Block Cipher Modes of Operation)

1. 选定并加载密钥 k 后，块密码 E_k 只能操作**单个数据块 (single blocks of data)**。
2. 块大小通常较小 (例如 AES 使用 16 字节块)，而要发送的消息通常较大。
3. 需要一种方法来使用相同的密钥重复应用于大型消息的加密。
4. **工作模式 (Mode of Operation)** 描述了块密码如何重复应用于加密消息。每种工作模式都有其优缺点。

5. 通过使用不同的工作模式，任意长度的消息可以被分割成块并使用块密码进行加密。

评估块密码与工作模式 (Evaluating Block Ciphers & Modes)

1. 评估一个密码和一个工作模式时，需要检查以下方面：
    1. **密钥大小 (Key Size)**: 安全性的上限，但密钥越长成本越高 (生成、存储等)。
    2. **块大小 (Block Size)**: 越大越好以减少开销，但成本也越高。
    3. **估计安全级别 (Estimated Security Level)**: 分析越多，信心越高；某些模式有已知失败案例。
    4. **吞吐量 (Throughput)**: 加密/解密的速度如何？是否可以**预先计算 (pre-computed)**？是否可以**并行化 (parallelised)**?
    5. **错误传播 (Error Propagation)**: 位错误或位丢失会导致什么后果?
2. 密钥大小和块大小只与**密码本身 (cipher)** 相关。
3. 估计安全级别、吞吐量和错误传播与**密码和工作模式 (cipher and mode of operation)** 都相关。

常见块密码工作模式

我们将考虑五种不同的工作模式：

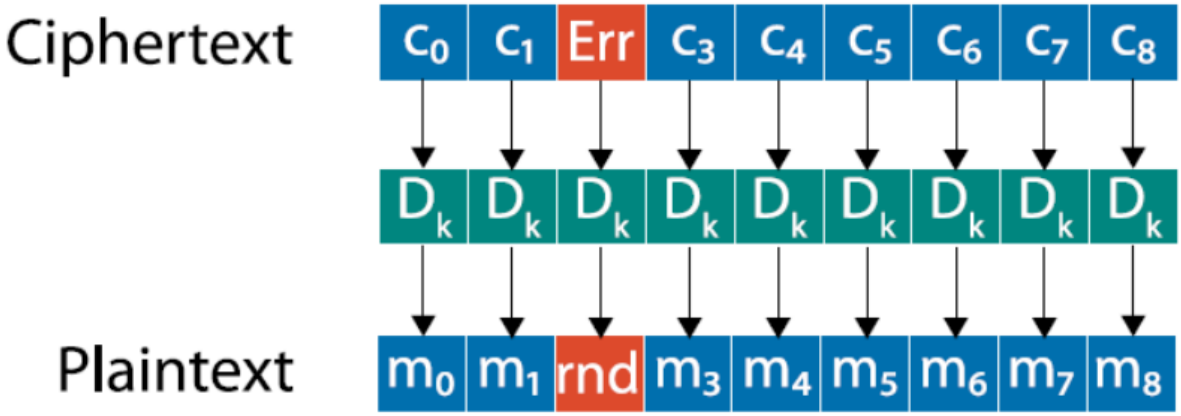
- 电子密码本模式 (Electronic Code Book, ECB)
- 密码块链模式 (Cipher Block Chaining, CBC)
- 输出反馈模式 (Output Feedback, OFB)
- 计数器模式 (Counter Mode, CTR)
- 伽罗瓦/计数器模式 (Galois/Counter Mode, GCM)

电子密码本模式 (Electronic Code Book, ECB)

1. ECB 模式**独立地 (separately)** 加密每个块。
2. 实现简单，但容易受到字典攻击和频率攻击。
3. ECB 的问题在于它本质上是**一个替换密码 (a substitution cipher)**，只是操作单位是块而不是字母。

ECB 属性 (ECB Properties)

1. **相同的明文块产生相同的密文块 (Identical plaintext blocks result in identical ciphertext blocks)**。
2. 由于块是独立加密的，密文块的重排会导致明文块的重排。
3. 因此，ECB **不推荐用于 (not recommended)** 长度超过 1 个块的消息。
4. **本地错误传播 (Local error propagation)**: 比特错误只影响被损坏块的解密 (该块解密后将是乱码)。



密码块链模式 (Cipher Block Chaining, CBC)

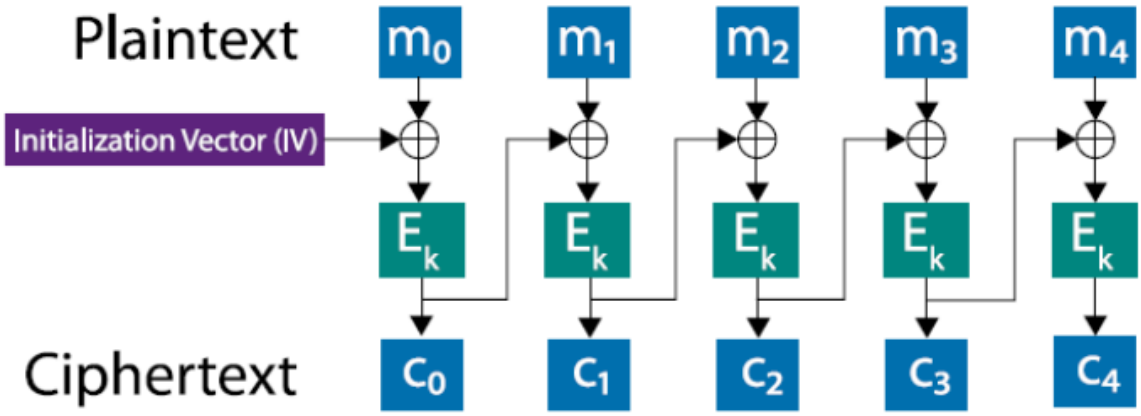


图 4: CBC 模式加密图示

1. CBC 模式使用 XOR 操作将块**链式连接 (chained together)** 起来。
2. **初始化向量 (Initialisation Vector, IV)** 是一个随机值，用于确保相同的明文和密钥不会产生相同的密文；IV **不需要 (does not need)** 保密。

CBC 解密 (CBC Decryption)

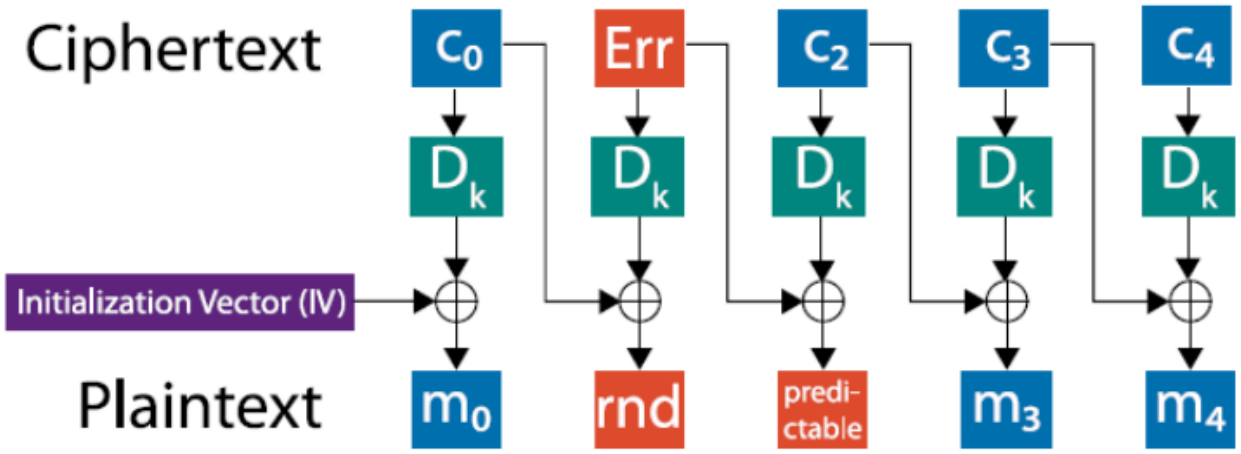


图 5: CBC 模式解密图示

1. 密文错误只影响两个明文块，其中一个是以**可预测的方式 (in a predictable way)** 受影响。
2. 加密必须**顺序 (sequentially)** 进行。
3. 解密可以**随机访问 (random-access)** 且**完全可并行化 (fully parallelisable)**。

CBC 属性 (CBC Properties)

1. 当使用相同的密钥和 IV 加密相同的明文时，产生**相同的密文 (identical ciphertexts)**。
2. 改变密钥 k、IV 或消息的第一个块 m_0 中的至少一个可以解决上述问题。
3. 密文块的重排会影响解密，因为密文部分 c_j 依赖于所有先前的明文块 $[m_0, m_1, \dots, m_j]$。
4. **错误传播 (Error propagation)**:
   - 密文 c_j 中的比特错误会影响当前块 c_j 和下一个块 c_{j+1} 的解密。恢复的块 m'_j 通常会是随机比特。
   - 在恢复的块 m'_{j+1} 中的比特错误精确地发生在 c_j 中出错的位置。
   - 攻击者可以通过修改 c_j 导致 m_{j+1} 中**可预测的比特改变 (predictable bit changes)**。
5. **错误恢复 (Bit recovery)**: CBC 是**自同步的 (self-synchronising)**。如果在 c_j 中发生比特错误但 c_{j+1} 中没有，那么 c_{j+2} 将正确地解密为 m_{j+2}。只有两个块受到错误影响。

输出反馈模式 (Output Feedback, OFB)

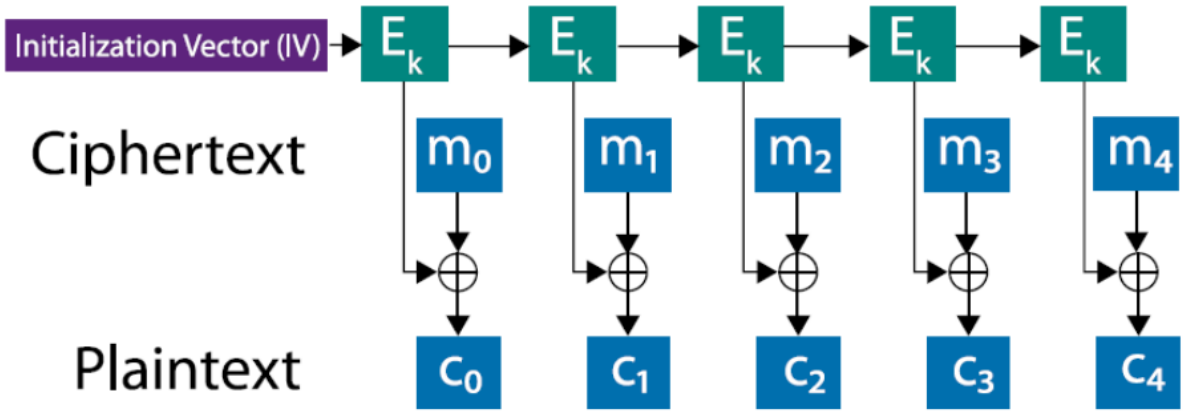


图 6: OFB 模式图示

1. OFB 模式将块密码转变为**同步流密码 (synchronous stream cipher)**。
2. 使用**初始化向量 (IV)** 和**密钥 (key)** 生成一个**密钥流 (keystream)**。加密/解密是明文/密文与密钥流的 XOR (图示隐含)。

OFB 属性 (OFB Properties)

1. 当使用相同的密钥和 IV 加密相同的明文时，产生相同的密文。
2. **链式依赖 (Chaining Dependencies)**: (与流密码相同) **密钥流独立于明文 (The key stream is plaintext independent)**。
3. **错误传播 (Error propagation)**: (与流密码相同) 密文块中的比特错误会导致明文相应位置发生错误。
4. **错误恢复 (Error recovery)**: (与流密码相同) 可以从比特错误中恢复，但**不能从比特丢失 (bit loss)** 中恢复 (会导致密钥流错位)。
5. **吞吐量 (Throughput)**: 密钥流可以独立计算，例如**预先计算 (pre-computed)**，之后加密/解密可以并行化。

6. IV **必须改变 (must change)**。否则，它会变成一个“两时间垫板”(two time pad)，这是不安全的。

计数器模式 (Counter Mode, CTR)

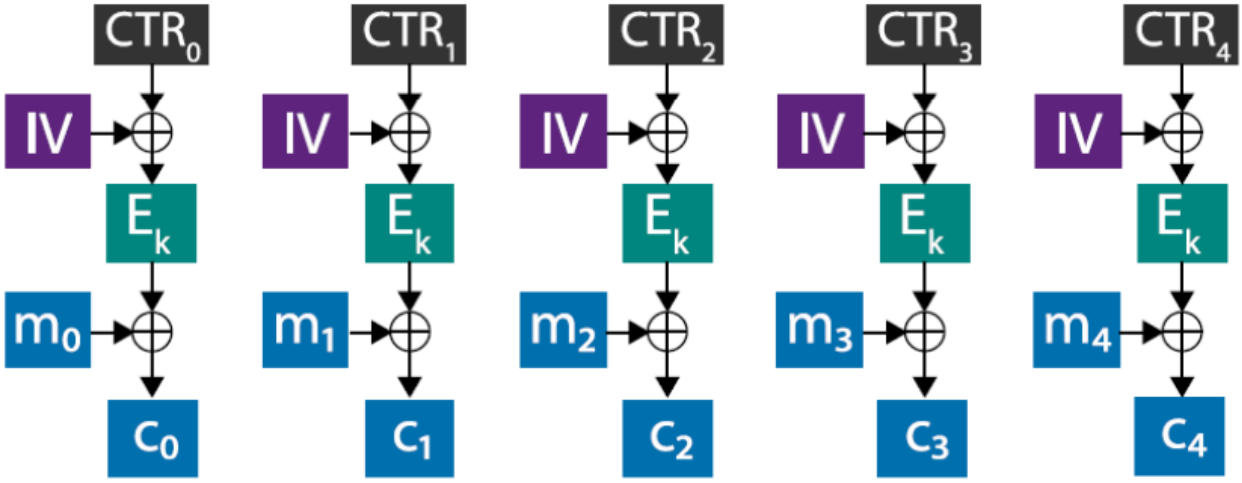


图 7: CTR 模式图示

1. CTR 模式使用一个**可预测的计数器函数 (predictable counter function)** 为每个块修改 IV，将块密码转变为**流密码 (stream cipher)**。
2. 计数器可以是任何函数 (例如伪随机数生成器 PRNG)，但通常只是一个递增整数。加密/解密是明文/密文与通过计数器和密钥生成的密钥流的 XOR (图示隐含)。

CTR 属性 (CTR Properties)

1. 当使用相同的密钥和 IV 加密相同的明文时，产生相同的密文。
2. **链式依赖 (Chaining Dependencies)**: (与流密码相同) **密钥流独立于明文 (The key stream is plaintext independent)**。
3. **错误传播 (Error propagation)**: (与流密码相同) 密文块中的比特错误会导致明文相应位置发生错误。
4. **错误恢复 (Error recovery)**: (与流密码相同) 可以从比特错误中恢复，但**不能从比特丢失 (bit loss)** 中恢复 (会导致密钥流错位)。
5. **吞吐量 (Throughput)**: 加密和解密都可以**随机访问 (randomly accessed)** 和/或**并行化 (parallelised)**。这是我们能期望的最好情况。
6. IV **必须改变 (must change)**。否则，它会变成一个“两时间垫板”。
7. OFB 和 CTR 共享相似的属性，因为它们都使块密码表现得像流密码。

伽罗瓦/计数器模式 (Galois/Counter Mode, GCM)

1. GCM 模式**不严格地 (not strictly)** 算作一种块密码工作模式。
2. 因为它还提供了一种**机制来验证数据的完整性 (mechanism to verify the integrity of data)**：确保密文没有被篡改。
3. 它是 CTR 模式的**扩展 (extension)**。
4. 在加密进行的同时，密文块被组合成某种类似于**消息认证码 (MAC)** 的东西。
5. 与 HMAC 不同，GCM 的 MAC 部分可以**并行化 (parallelisable)**。
6. 常用于**低延迟 (low-latency)**、**高吞吐量 (high-throughput)** 的专用硬件应用 (例如网络数据包)。

DES 密码分析 (DES Cryptanalysis)

密钥唯一性 (DES Keys)

1. 给定一对 (明文, 密文) 对 (m, c)，只有一个密钥满足 $c = DES(m, k)$ 的**概率很高 (high probability)**。
2. 将 DES 视为排列的集合。对于所有 (m, k)，存在不同密钥 $k_1 \neq k$ 使得 $DES(m, k_1) = DES(m, k)$ 的概率极低，约为 2^{-56}。
3. 因此，给定一对 (m, c) 对，密钥几乎肯定是唯一确定的。问题在于**如何找到 k (to find k)**。

已知明文穷举密钥搜索 (Known Plaintext Exhaustive Key Search)

1. 对于一个强的 n 比特块密码和 j 比特密钥，给定少量 (< $(j + 4)/n$) 明文/密文对，平均需要 2^{j-1} 次暴力尝试才能恢复密钥。
2. 对于 DES，$j = 56, n = 64$，预期需要 2^{55} 次操作才能找到密钥。

利用补码性质 (Exploiting Complementation Property)

1. 由于 DES 是一个 Feistel 网络，它具有**补码性质 (complementation property)**: $DES(\neg m, \neg k) = \neg DES(m, k)$。($\neg$ 表示按位取反)
2. 可以利用**选择明文攻击 (Chosen Plaintext Attack, CPA)** 来利用这个性质。
3. 如果可以获取消息 m 及其补码 $\neg m$ 的加密结果，暴力尝试可以减少一半。
4. 因此，搜索空间减半。

差分密码分析 (Differential Cryptanalysis)

1. 差分密码分析比**暴力破解 (brute-force)** 攻击 DES 更有效。
2. 它利用**选择明文攻击 (CPA)** 获取 (明文, 密文) 对。
3. 涉及分析两个不同文本的**异或 (XOR)**。
4. 考虑 S-box 函数 $F(x, k_i)$，输入是 6 比特的 b_1, b_2，其异或差分 $\Delta = b_1 \oplus b_2$ 不依赖于密钥 k_i。

   $$\Delta = b_1 \oplus b_2 = (x_1 \oplus k_i) \oplus (x_2 \oplus k_i) = x_1 \oplus x_2$$

   其中 x_1 和 x_2 是经过扩展置换 E 后的对应 48 位输入到 XOR 之前的 32 位部分，再取对应 S-box 输入的 6 位。
5. 然而，对应的**输出异或 (output XOR)** $(e_1 \oplus e_2)$ 仍然取决于密钥 (此处原文似乎有误，应为 $b_1 \oplus b_2$ 不依赖于密钥，而输出 $e_1 \oplus e_2$ 也不直接依赖密钥，依赖于输入差分和 S-box 特性)。正确的理解是，对于特定的输入差分 $\Delta_{in} = b_1 \oplus b_2$，S-box 输出的差分 $\Delta_{out} = e_1 \oplus e_2$ 具有非均匀的分布，即某些输出差分出现的概率高于其他差分。
6. 通过分析大量具有相同输入差分的明文对及其对应的密文对的 S-box 输出差分，可以利用这种概率不均匀性来推断密钥比特。
7. 例如，如果输入差分 $(b_1 \oplus b_2) = 110100$，而输出差分 $(e_1 \oplus e_2) = 0001$，根据 S-box 的差分分布表，知道 (b_1, b_2) 对可能只有 8 种。
8. 因为 $b_1 = x_1 \oplus k_i$，且 x_1 是由已知明文派生出的，所以 k_i 中对应于这 6 比特的部分只有 16 种可能值 (由于 b_1 和 b_2 可互换)。
9. 通过对不同的输入差分重复此过程，可以对密钥进行推断。

线性密码分析 (Linear Cryptanalysis)

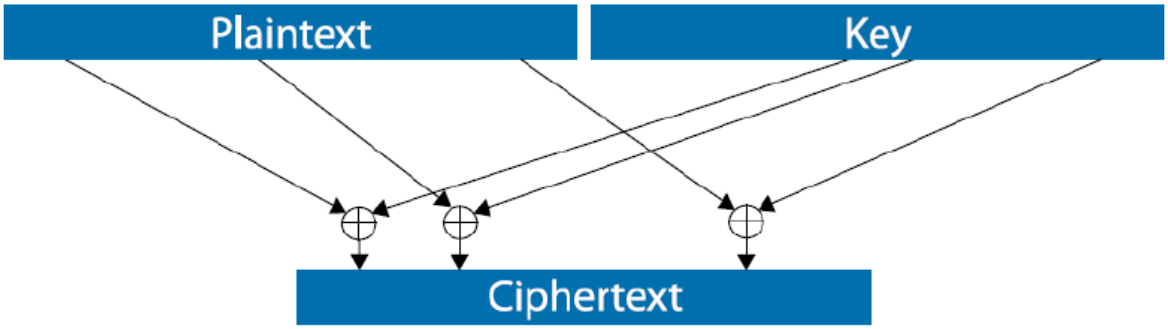


图 8: 线性密码分析示例表达式

1. 线性密码分析的目标是找到一个适用于给定密码算法的 **“有效”线性表达式 (“effective” linear expression)**。
2. 表达式形式为：$p[i_1, \dots, i_u] \oplus c[j_1, \dots, j_v] = k[s_1, \dots, s_w]$

$$p[i_1, \dots, i_u] \oplus c[j_1, \dots, j_v] = k[s_1, \dots, s_w]$$

   其中 $i_1, \dots, i_u, j_1, \dots, j_v$ 和 $s_1, \dots, s_w$ 是固定的比特位置。
3. 攻击者希望上述表达式对于随机给定的明文 P 和对应的密文 C 成立的**概率 ρ 不等于 0.5 (probability, $\rho \neq 0.5$)**。
4. 如果 $|\rho - 0.5|$ 的值很大，攻击者就可以**准确地猜测 (accurately guess)** 密钥比特组合 $k[s_1, \dots, s_w]$。
5. 最优情况下，为了攻破密码，$|\rho - 0.5| = 0.5$ (即 $\rho = 0$ 或 1)，而一个完美的密码应该有 $\rho = 0.5$。

DES 增强 (DES Enhancements)

双重 DES (2DES)

1. 使用两个密钥 k_1, k_2 进行双重加密：$2DES_{k_1,k_2}(m) = E_{k_1}(E_{k_2}(m))$。
2. 容易受到**已知明文中间相遇攻击 (known plaintext meet-in-the-middle attack)**。
3. **中间相遇攻击 (Meet-in-the-Middle Attack)** 原理：
   1. 对于一个固定消息 m，使用所有可能的 56 位密钥 k 计算 $E_k(m)$ 并存储在表中。
   2. 对于密文 $c = E_{k_1}(E_{k_2}(m))$，尝试使用所有可能的 56 位密钥 k 计算 $D_k(c)$。
   3. 直到 $D_k(c)$ 出现在步骤 1 的表中。
   4. 如果找到匹配项 $D_{k_1'}(c) = E_{k_2'}(m)$，则有很高概率找到正确的密钥对 (k_1', k_2')，因为 $D_{k_1}(c) = E_{k_2}(m)$。
4. 这意味着 2DES (密钥长度 $56 + 56 = 112$ 位) 平均可以在 2^{56} 次操作和 2^{56} 内存槽的情况下被攻破。这不足以抵抗 112 位密钥的攻击。

三重 DES (3DES)

1. 使用两个密钥 k_1, k_2 进行三次 DES 操作 (112 位有效密钥长度)：$3DES_{k_1,k_2}(m) = E_{k_1}(D_{k_2}(E_{k_1}(m)))$。
2. 在 2016 年发现了一个名为 CVE 的主要安全漏洞。
3. NIST 在 2017 年弃用 (deprecated) DES/3DES 用于新应用，并在 2023 年底弃用于所有应用。

DESX

1. DESX 是 DES 的一种修改，旨在避免穷举密钥搜索。
2. 它使用一个 56 位 DES 密钥 k_1 和两个 64 位**增白密钥 (Whitening Key)** k_2, k_3。
3. 加密定义为：$DESX_{k_1,k_2,k_3}(m) = k_3 \oplus E_{k_1}(m \oplus k_2)$。

$$DESX * k_1, k_2, k_3(m) = k_3 \oplus E * k_1(m \oplus k_2)$$

4. 增白密钥 k_2, k_3 提供了更好的抗暴力破解能力。

高级加密标准 (Advanced Encryption Standard, AES)

1. 1997 年，NIST 宣布了一项竞赛，选择一个新的密码来取代过时的 DES。新密码被命名为**高级加密标准 (Advanced Encryption Standard, AES)**。
2. 在 15 个国际竞争者中，选择了 **Rijndael** 作为 AES。
3. AES 是一种**块密码 (Block cipher)**。
4. 操作**块长为 128 位 (128-bit blocks)**。
5. **密钥长度是可变的 (Key length is variable)**：128/192/256 位密钥。
6. 它是一种 **SP 网络 (substitution-permutation network)**。
7. 使用**单个非线性 S-box (single non-linear S‐box)**，作用于一个字节输入产生一个字节输出 (一个 256 字节的查找表)。
8. 其结构设计提供了**紧密的差分和线性界限 (tight differential and linear bounds)**，提高了抗差分密码分析和线性密码分析的能力。
9. 轮数是可变的：
   - 10 轮用于 128 位密钥。
   - 12 轮用于 192 位密钥。
   - 14 轮用于 256 位密钥。
10. 基于当前已知攻击，设计的轮数有 50% 的**安全裕度 (margin of safety)**。

可能的考点与例题 (Potential Exam Points and Sample Questions)

重要考点总结:

- **块密码**和**流密码**的定义及区别。
- **Feistel 网络**的结构、工作原理以及**可逆性**如何实现。
- **扩散 (Diffusion)** 和**混淆 (Confusion)** 的**概念、目的**以及它们在密码设计中的**重要性**。
- DES 中 **S-boxes** 和 **P-boxes** 如何协同实现**扩散**和**混淆**。
- 块密码**填充 (Padding)** 的**必要性**。
- **工作模式 (Modes of Operation)** 的**目的**和**必要性**，如何处理任意长度消息。
- 评估块密码和工作模式的**标准** (密钥大小、块大小、安全性、吞吐量、错误传播)，以及这些标准分别**与密码本身还是工作模式相关**。
- **ECB、CBC、OFB、CTR** 等主要工作模式的**基本原理**。
- **初始化向量 (IV)** 在 CBC、OFB、CTR 中的**作用**和**要求** (是否需要保密，是否需要改变)。
- 不同工作模式在**错误传播 (Error Propagation)** 和**并行化 (Parallelisation)** 方面的**差异**及其**原因**。
  - ECB：本地错误传播，加密/解密可并行。
  - CBC：密文错误影响两块（当前和下一块），加密顺序，解密并行。

  - OFB/CTR：密文错误影响相同位置，对比特丢失敏感，密钥流生成/加密/解密可并行 (取决于模式)。
- GCM 模式的**特点** (基于 CTR、提供**数据完整性**、MAC、并行性)。
- 对 DES 的**密码分析方法**：
  - **穷举密钥搜索**的复杂度。
  - 利用**补码性质**的**选择明文攻击**如何将搜索空间减半。
  - **差分密码分析 (Differential Cryptanalysis)** 的**基本思想** (利用输入/输出差分、S-box 特性、CPA) 和**攻击方式**。
  - **线性密码分析 (Linear Cryptanalysis)** 的**基本思想** (寻找线性关系、概率偏差) 和**攻击方式**。
- DES 的增强方案：**2DES** 和 **3DES** 的结构、**2DES** 存在的**中间相遇攻击 (Meet-in-the-Middle Attack)** 漏洞及其复杂度。
- **AES** 取代 DES 的**原因**，AES 的**关键特性** (SP 网络、块/密钥大小、轮数、S-box)。

示例考题:

1. 简要说明块密码（Block Cipher）与流密码（Stream Cipher）的主要区别。
2. 解释 Feistel 网络（Feistel Network）如何通过简单的轮函数构建可逆的块密码。画出基本的 Feistel 轮结构图，并说明其逆过程。
3. 定义并区分密码学中的**扩散（Diffusion）**和**混淆（Confusion）**。在 DES 中，**S-boxes** 和 **P-boxes** 分别主要贡献于哪种特性，以及它们如何协同工作?
4. 为什么在块密码工作模式中需要引入**初始化向量（IV）**？以 CBC 模式为例，说明 IV 的作用。IV 需要保密吗？为什么?
5. 比较 ECB、CBC 和 CTR 三种工作模式在**错误传播（Error Propagation）**特性上的主要差异。假设密文中有一个比特错误，在不同模式下解密时，明文受影响的情况如何?
6. 解释为什么 ECB 模式不推荐用于加密长度超过一个块的消息。请从其工作原理和安全性角度进行说明。
7. 什么是**中间相遇攻击（Meet-in-the-Middle Attack）**？简述这种攻击如何成功应用于 2DES，并说明为什么 2DES 的安全性并没有达到其密钥长度看似应有的水平（例如，两个 56 位密钥的 2DES 安全性低于 112 位密钥的块密码）。
8. 简述**差分密码分析（Differential Cryptanalysis）**和**线性密码分析（Linear Cryptanalysis）**这两种攻击 DES 的密码分析方法的基本思想。它们各自侧重于利用密码算法的什么特性?

参考答案要点:

1. 块密码处理固定大小的数据块，流密码处理连续的数据流（通常是比特或字节）。块密码通常是逐块加密，流密码生成一个密钥流与明文异或。
2. Feistel 网络将输入分左右两半，右半进入轮函数后与左半异或成为新的右半，原右半成为新的左半。结构 $L_i = R_{i-1}, R_i = f_i(R_{i-1}) \oplus L_{i-1}$。逆过程是将 (L_i, R_i) 还原到 (L_{i-1}, R_{i-1})，利用 XOR 的性质和轮函数的逆序应用。
3. **扩散**：消散明文统计信息，使明文一位变化影响密文多位；与置换相关。**混淆**：使密钥与密文关系复杂，使密文一位依赖密钥多位；与替换相关。在 DES 中，S-boxes 是非线性替换，主要提供**混淆**；P-box 和 E 扩展置换负责扩散，将 S-box 的输出散播开。它们协同工作，通过多轮迭代实现强扩散和混淆。
4. IV 的作用是**增加随机性 (add randomness)**，使得即使使用相同的密钥加密相同的明文，也能产生不同的密文，避免攻击者识别重复的明文块。在 CBC 中，IV 与第一个明文块 XOR 后加密，影响后续所有块。IV **不需要保密**，但通常需要**不可预测且每次使用不同**。
5. ECB：本地错误，一个密文块错误只影响解密后的对应明文块。CBC：错误传播，一个密文块错误影

响解密后的当前块（通常随机化）和下一块（可预测的比特错误）。OFB/CTR：流密码性质，密文错误导致明文对应位置错误。

6. 因为 ECB 对相同的明文块使用相同的密钥加密会产生相同的密文块。这暴露了明文中的模式和频率信息，使得攻击者可以通过观察密文块的重复性来推断明文内容，特别是在明文具有结构性或重复模式时。
7. 中间相遇攻击利用了双重加密可以分解为两个独立的单重加密/解密步骤。攻击者对所有可能的第一个密钥计算 $E_{k_1}(m)$ 存储，对所有可能的第二个密钥计算 $D_{k_2}(c)$ 存储。当找到 $E_{k_1}(m) = D_{k_2}(c)$ 的匹配时，就找到了可能的密钥对 (k_1, k_2)。虽然密钥总长 112 位，但攻击复杂度约为 2^{56}，远低于 2^{112}，因此安全性不足。
8. **差分密码分析**：利用明文对输入特定差分时，密文对输出特定差分的概率非均匀性。通过分析大量 (明文, 密文) 对的差分分布来推断密钥。侧重于 S-box 的非线性特性。**线性密码分析**：寻找明文比特子集、密文比特子集和密钥比特子集之间近似线性的关系。通过收集大量 (明文, 密文) 对，利用概率偏差来猜测密钥比特。侧重于算法的线性逼近。