名词解释标准解答（背诵/考试用）

定义 2.2.2 (扩散 (Diffusion))

解答：
将明文的统计结构扩散、打乱到长串的密文中。使得明文的每一位影响密文的许多位，从而隐藏明文的统计结构。其目的是阻断通过分析密文统计特性来推测明文的攻击途径。

如P盒通过置换(线性变换)实现扩散。

定义 2.2.3 (混乱 (Confusion))

解答：
指使密文的统计特性与密钥取值之间的关系变得尽可能复杂（通常是非线性的），使得攻击者无法从密文和明文的对应关系中推导出密钥。

如S盒通过非线性代换实现混乱。

定义 2.2.4 (完善保密性 / 理想密码系统)

解答：
指在理想密码系统中，密文不提供关于明文的任何信息（如一次一密）。在此系统中，攻击者拥有无限计算资源和时间也无法破解。安全不依赖于任何计算假设。。

定义 2.2.5 (雪崩效应 (Avalanche Effect))

解答：
指密码算法的一种理想特性，即明文或密钥发生微小的改变（例如仅改变 1 比特），都应导致输出的密文发生显著变化（理想情况下，密文有一半的比特位发生翻转）。这体现了算法具有良好的随机性和对输入的敏感性。

计算题：

0. S-DES 算法运算详解

复习重点：注意流程、S盒行列索引规则、以及第二轮加密前 SW (交换) 操作的输入顺序。

步骤0：参数准备

参数项	二进制值	备注
主密钥 K	`1010000010`	10 bits
明文 M	`01110010`	8 bits

步骤1：子密钥生成

流程概述：

- **P10** 置换：`3 5 2 7 4 10 1 9 8 6`
- 移位规则：第1轮 (LS-1)，第2轮 (LS-2)
- **P8** 置换：`6 3 7 4 8 5 10 9`
- 核心：移位 $\rightarrow$ P8 生成子密钥

(1) 初始处理：P10 置换 & 拆分

- 输入：`1010000010`
- **P10** 置换：`1000001100` (重排后)
- 拆分：
  - $L_0 = 10000$

- $R_0 = 01100$

(2) 计算 K_1：LS-1 → P8

对 L_0, R_0 进行 循环左移 **1** 位：

- $L_1 = 00001$
- $R_1 = 11000$
- 合并：`0000111000`

应用 **P8** 置换 (取位：6, 3, 7, 4, 8, 5, 10, 9)：

```
源位置：1  2  3  4  5  | 6  7  8  9  10
源数值：0  0  0  0  1  | 1  1  0  0  0
          ↓
P8取位：6  3  7  4  8  | 5  10 9
结果值：1  0  1  0  0  | 1  0  0
```

$$K_1 = 10100100$$

(3) 计算 K_2：LS-2 → P8

对 L_1, R_1 继续 循环左移 **2** 位：

- $L_2 = 00100$ (从 `00001` 左移 2 位)
- $R_2 = 00011$ (从 `11000` 左移 2 位)
- 合并：`0010000011`

应用 **P8** 置换：

```
源位置：1  2  3  4  5  | 6  7  8  9  10
源数值：0  0  1  0  0  | 0  0  0  1  1
          ↓
P8取位：6  3  7  4  8  | 5  10 9
结果值：0  1  0  0  0  | 0  1  1
```

$$K_2 = 01000011$$

三、 加密流程

S盒查表 ：首尾定位行，中间定位列。

阶段 1: 初始置换 (IP)

- 输入 : `0111 0010`
- **IP(2,6,3,1...)** : `1010 1001`
- 状态拆分 : $L = 1010, R = 1001$

阶段 2: 第一轮 (f_K 使用 K_1)

1. 扩展 **(EP) &** 密钥加 :

```
R (输入)   : 1001
EP扩展(R)  : 1100 0011  (扩展至8位)
异或 K1    : 1010 0100
--------------------
结果       : 0110 0111
```

1. **S**盒代换 :

- 左半 `0110` **(S0)** :
  - 行 `00` (0), 列 `11` (3) → $S0[0][3] = 2 \rightarrow$ `10`
- 右半 `0111` **(S1)** :
  - 行 `01` (1), 列 `11` (3) → $S1[1][3] = 3 \rightarrow$ `11`

- **S**盒输出：`1011`

1. **P4**置换 **&** 更新 **R**：

- $P4$(‘1011‘) $\rightarrow$ ‘0111‘
- 新_$R = L \oplus P4$_输出 = ‘1010‘ $\oplus$ ‘0111‘ = ‘1101‘

第一轮结束 **(SW**交换 前**):**

- $L_{end1} = 1001$ (原 R)
- $R_{end1} = 1101$ (新计算值)

阶段 3: 第二轮 (f_K **使用** K_2**)**

> **注意** ： 进入第二轮前，通常将左右部分 **交换 (Switch)** 。
> **输入** ： $L = 1101, R = 1001$

1. 扩展 **(EP) &** 密钥加：

```
R (输入)   : 1001
EP扩展(R)  : 1100 0011
异或 K2    : 0100 0011  <-- 使用修正后的 K2
--------------------
结果       : 1000 0000
```

1. **S**盒代换：

- 左半 `1000` **(S0)**：
  - 行 `10` (2), 列 `00` (0) $\rightarrow S0[2][0] = 0 \rightarrow$ `00`
- 右半 `0000` **(S1)**：
  - 行 `00` (0), 列 `00` (0) $\rightarrow S1[0][0] = 0 \rightarrow$ `00`
- **S**盒输出：`0000`

1. **P4**置换 **&** 更新 **R**：

- $P4$(‘0000‘) $\rightarrow$ ‘0000‘
- 新_$R = L \oplus P4$_输出 = ‘1101‘ $\oplus$ ‘0000‘ = ‘1101‘

第二轮结束**:**

- 输出序列：新_R + 原_R (注意：标准 S-DES 最后一步不交换，直接合并)
- 逆置换前输入：`1101 1001`

阶段 4: 逆初始置换 (IP^{-1}**)**

- 输入：`1101 1001`
- 映射 (4, 1, 3, 5, 7, 2, 8, 6)😀 输出位	来源位 (输入位置)	来源值
Bit 1	4	**1**
Bit 2	1	**1**
Bit 3	3	**0**
Bit 4	5	**1**
Bit 5	7	**0**
Bit 6	2	**1**
Bit 7	8	**1**
Bit 8	6	**0**
- 最终密文：`1101 0110`

1.RSA 算法手算练习

(1)计算私钥 d

(2)加密明文 $m=5$

1. 第一题解答：

步骤0：参数准备

- $p = 7$
- $q = 17$
- $n = p \times q = 7 \times 17 = 119$
- $\phi(n) = (p-1)(q-1) = 6 \times 16 = 96$
- $e = 11$

我们需要求解 d，满足 $11d \equiv 1 \pmod{96}$。

步骤1：辗转相除法 (Euclidean Algorithm)

计算 $\gcd(96, 11)$：

1. $96 = 8 \times 11 + 8$
2. $11 = 1 \times 8 + 3$
3. $8 = 2 \times 3 + 2$
4. $3 = 1 \times 2 + 1$ <-- 得到余数 1，停止

步骤2：逆向回代 (Extended Euclidean)

我们将余数 1 表示为 11 和 96 的线性组合：

1. 从第4式移项：

$$1 = 3 - 1 \times 2$$

2. 代入第3式 ($2 = 8 - 2 \times 3$)：

$$1 = 3 - 1 \times (8 - 2 \times 3) = 3 - 8 + 2 \times 3 = 3 \times 3 - 8$$

3. 代入第2式 ($3 = 11 - 1 \times 8$)：

$$1 = 3 \times (11 - 8) - 8 = 3 \times 11 - 3 \times 8 - 8 = 3 \times 11 - 4 \times 8$$

4. 代入第1式 ($8 = 96 - 8 \times 11$)：

$$1 = 3 \times 11 - 4 \times (96 - 8 \times 11) = 35 \times 11 - 4 \times 96$$

结论

$$35 \times 11 \equiv 1 \pmod{96}$$

私钥 $d = 35$。

2. 第二题解答：

我们需要计算 $c \equiv 5^{11} \pmod{119}$。

步骤1：指数二进制化

$e = 11$，其二进制为 **1011** $(8 + 2 + 1)$。
这意味着 $c \equiv 5^8 \times 5^2 \times 5^1 \pmod{119}$。

步骤2：模重复平方法 (Square and Mod)

我们需要依次计算 $m^1, m^2, m^4, m^8 \pmod{119}$。

指数幂次	计算过程 (上一步结果的平方)	取模结果 (mod 119)	备注
5^1	-	**5**	(需要)
5^2	25	**25**	(需要)
5^4	$25^2 = 625$	$625 = 5 \times 119 + 30 \Rightarrow \mathbf{30}$	
5^8	$30^2 = 900$	$900 = 7 \times 119 + 67 \Rightarrow \mathbf{67}$	(需要)

步骤三：组合相乘

根据二进制 1011，选取 $5^8, 5^2, 5^1$：

$$c \equiv 67 \times 25 \times 5 \pmod{119}$$

1. 先算 $25 \times 5 = 125$

$$125 \pmod{119} = 6$$

1. 再算 67×6:

$$67 \times 6 = 402$$

2. 最后取模：

$$402 \div 119 = 3 \ldots 45$$

(验证：$3 \times 119 = 357$, $402 - 357 = 45$)

结论

加密后的密文 $c = 45$。

重要辨析：

计算机网络 5 层体系的加密方式总结

总体说明

- 端到端加密：数据在源端系统加密，目的端系统解密，中间节点仅转发密文，无法获知载荷内容。工作在传输层及以上，以及网络层的传输模式。
- 链路加密：数据在每一跳链路上独立加密/解密，中间节点必须解密以读取路由信息，然后重新加密转发。工作在数据链路层及以下，以及网络层的隧道模式（段到段加密）。

加密方式分类表

层次	典型协议	加密策略	对上层数据的处理	本层添加的头部	封装后的数据包逻辑结构
应用层	PGP, S/MIME	端到端	加密消息体 + 数字签名	应用协议头 (可选加密)	`[应用头(可选)][{消息体}]`
传输层	TLS/SSL, SSH, DTLS	端到端	加密应用层完整报文	传输层头部明文	`[TCP头][{应用层报文}]`
网络层	**IPSec-AH** 传输模式	端到端	认证传输层报文 (不加密)	原 **IP** 头明文 + AH头	`[原IP头][AH头][<传输层头+数据>]`
网络层	**IPSec-ESP** 传输模式	端到端	加密 + 认证传输层报文	原 **IP** 头明文 + ESP头/尾	`[原IP头][ESP头][{传输层头+数据}][`
网络层	**IPSec-AH** 隧道模式	链路 **(段到段)**	认证整个原IP包 (不加密)	新 **IP** 头明文 + AH头	`[新IP头][AH头][<原IP包>]`
网络层	**IPSec-ESP** 隧道模式	链路 **(段到段)**	加密 + 认证整个原IP包	新 **IP** 头明文 + ESP头/尾	`[新IP头][ESP头][{原IP包}][ESP尾]`
链路层	WPA2/WPA3, MACSec(802.1AE)	链路 **(逐跳)**	加密网络层分组	**MAC** 帧头明文 + FCS	`[MAC头][{网络层数据包}][FCS]`
物理层	专线加密机, SONET加密	链路 **(逐跳)**	加密链路层帧 (比特流)	物理层编码/调制	`[{编码后的密文比特流}]`

符号说明：

- `{ }`：加密内容（提供机密性，Confidentiality）
- `< >`：认证内容（提供完整性，Integrity，但内容可见）
- `[ ]`：协议数据单元边界

核心规律与深度解析

1. 端到端加密（End-to-End, E2E）

主要集中在 传输层 与 应用层，以及网络层的 **IPSec** 传输模式。

- 封装逻辑：

$$extHeader_{IP} \,||\, \text{Header}_{TCP} \,||\, \mathbf{Encrypted}(\mathbf{Data})$$

(注：TLS 加密范围包含部分应用层握手信息，IPSec 传输模式加密 TCP 头+Data)

- 关键特征：
  - 通信实体：进程 (Port) 或 用户 (User)。
  - 中间节点行为：路由器只读取明文的 IP 头部进行转发，对负载内容“视而不见”。
  - 缺陷：无法抵抗流量分析 **(Traffic Analysis)**。攻击者虽然解不开内容，但可以通过明文的 IP 和 Port 知道“谁在和谁通信”、“业务类型是什么”（如 443 端口通常是 Web，22 是 SSH）。

2. 链路加密（Hop-by-Hop / Link Encryption）

主要集中在 数据链路层 和 物理层。

- 封装逻辑：

$$extHeader_{MAC} \,||\, \mathbf{Encrypted}(\text{Header}_{\mathbf{IP}} \,||\, \text{Data})$$

- 关键特征：
  - 通信实体：网卡 (NIC) 到 网卡，或 基站 到 手机。
  - 中间节点行为：必须解密。路由器 R1 收到帧后，解密取出 IP 包，查看 IP 头选路，然后用下一跳的密钥再次加密封装发给 R2。
  - 优势：流量机密性极高。在链路上截获数据的人，连源 IP 和目的 IP 都看不到（被加密在帧载荷里了）。
  - 缺陷：

a. 信任链脆弱：路径上所有路由器必须是“好人”，任何一个路由器被攻破，全链路明文裸奔。

b. 延迟高：每一跳都要进行 `Decrypt -> Route -> Encrypt` 操作。

3. 特殊情况：网络层的“双面性” (IPSec)

网络层处于承上启下的位置，IPSec 的两种模式完美诠释了加密范围的权衡：

- 传输模式 **(Transport Mode)**：
  - 场景：两台主机直接通信（如服务器 A 到数据库 B）。
  - 行为：只加密 Payload (TCP/UDP)，保留原 IP 头。
  - 性质：端到端。路由器看原 IP 头转发。
- 隧道模式 **(Tunnel Mode)**：
  - 场景：VPN 网关之间（如 公司北京分部 ↔ Internet ↔ 公司上海分部）。
  - 行为：将整个原 **IP** 包（含原 IP 头）加密，变成一段密文，然后外面再套一个新的 IP 头（源=北京网关，目=上海网关）。
  - 性质：虚拟的逐跳（更准确说是“逻辑链路”）。对于公网路由器来说，它只看到两个网关在通信，看不到内部其实是员工 A 发给内网服务器 B 的包。

实际部署中的组合策略

现代网络通常分层组合多种加密策略：

场景示例：员工通过VPN访问公司内网HTTPS服务

```
用户主机 ↔ WiFi ↔ ISP路由器 ↔ 互联网 ↔ 公司VPN网关 ↔ 内网Web服务器

加密层次：
1. 链路层：WPA2加密（用户↔WiFi AP）
2. 网络层：IPSec隧道（用户↔VPN网关）
3. 传输层：TLS加密（用户浏览器↔Web服务器）
```

防护效果：

- WPA2：防止WiFi环境的本地窃听
- IPSec隧道：在公网上隐藏真实通信端点和流量特征
- TLS：提供应用层的端到端机密性，即使VPN网关也无法解密HTTP内容

快速记忆概念

1.Blowfish vs RC5 比较表

维度	**Blowfish (**河豚**)**	**RC5 (**变形金刚**)**
设计者	**B**ruce Schneier	**R**on Rivest
杀手锏	极致的速度+ 小内存	高度灵活性(参数化)
核心操作	S-Box 查表 + 异或	数据相关的循环移位
可变性	仅密钥长度可变	字长、轮数、密钥全由你定
应用场景	密码存储 (bcrypt)、嵌入式	学术研究、特定硬件架构适配