AUST 现代密码学复习

——期末真传

anyunyeyi

2026 年 2 月 16 日

前言

2025 – 2026(1) 秋季课程, 老师李邵莹.

anyunyeyi

2026 年 2 月 16 日

目录

第一章　章节复习

1.1　第 1 章 密码学概论

1. 信息安全五大目标 (CIAAN)

   - 机密性 (C): 防泄露. 手段: 加密.
   - 完整性 (I): 防篡改. 手段: 哈希函数.
   - 认证性 (A): 辨真伪. 分实体认证和消息认证.
   - 可用性 (A): 保服务. 抵御 DoS 攻击.
   - 不可否认性 (N): 防抵赖. 手段: 数字签名.

2. 安全威胁与攻击分类

   - 被动攻击: 威胁机密性. 如截取 (窃听)、通信量分析.
   - 主动攻击: 威胁其他四性. 主要形式: 中断 (DoS)、篡改、伪造、重放.

3. 密码学发展史

   - 传统密码学 (1949 年前): 技巧为主, 如凯撒密码、栅栏密码、Enigma 机.
   - 现代密码学开端:1949 年香农发表《保密系统的通信理论》, 引入信息论.

- 两大里程碑:
  - 1977 年 DES(对称密码代表).
  - 1976 年 Diffie & Hellman 发表《密码学的新方向》, 提出公钥密码思想.
  - 1978 年 RSA 算法诞生.

1.2　第 2 章 密码学基础

1. 密码学两大学科
   - 密码编码学 (Cryptography): 如何设计安全系统 (“造锁”).
   - 密码分析学 (Cryptanalysis): 如何分析/破解系统 (“开锁”).
2. 核心原则: 科克霍夫原则
   - 核心: 系统的安全性应完全依赖于密钥的保密, 而算法本身可以公开.
3. 保密系统模型
   - 五元组: 明文、密文、密钥、加密算法、解密算法.
   - 三个空间: 明文空间、密文空间、密钥空间.
4. 密码系统安全性评价
   - 无条件安全: 无限资源也无法破解. 仅 “一次一密” 达到此标准.
   - 计算安全 (实际安全): 破解所需计算量在实际中不可行. 当今所有实用密码均属此类 (如 RSA 基于大整数分解难题).
5. 攻击类型 (按攻击者所知信息, 强度递增)

- 唯密文攻击: 只有密文. 最难, 是最基本要求.
- 已知明文攻击: 拥有一些明文-密文对.
- 选择明文攻击: 可任意选明文获对应密文 (如控制加密机).
- 选择密文攻击: 可任意选密文获对应明文 (如控制解密机).
- 选择文本攻击: 同时具备 3 和 4 的能力.
- 结论: 能抵御强攻击, 则必能抵御弱攻击.

1.3　第 3 章 古典密码体制

1. 两大基本思想
   - 代换密码: 将明文字母替换为其他字符.
   - 置换密码: 保持字母不变, 只打乱顺序.
2. 核心密码体制与公式
   - 仿射密码
     - 加密:$C = (a \cdot P + b) \mod 26$
     - 解密:$P = a^{-1} \cdot (C - b) \mod 26$
     - 关键:$\gcd(a, 26) = 1$ 才能求逆元 a^{-1}.
   - 维吉尼亚密码 (多表代换代表)
     - 加密:$C_i = (P_i + K_i) \mod 26$ (密钥循环使用)
     - 解密:$P_i = (C_i - K_i) \mod 26$
   - 希尔密码
     - 加密:$C = P \cdot K(\mod 26)$ (矩阵乘法)
     - 解密:$P = C \cdot K^{-1}(\mod 26)$

  - 关键: 密钥矩阵 K 必须可逆 (行列式值与 26 互素).

3. 古典密码的唯密文攻击方法

- 单表代换 (含移位、仿射): 直接使用频率分析.
  - 重合指数 (IC):$IC = \sum (\text{字母频率})^2$.
    - 英文文本 ~ 0.065
    - 随机文本 ~ 0.038
    - 若密文 IC 接近 0.065, 则为单表代换.
- 维吉尼亚密码 (多表代换): 分两步:
  - 确定密钥长度 m:
    - 卡西斯基测试: 找重复密文片段, 计算间距的最大公约数.
    - 重合指数法: 尝试不同的 m, 对密文分组, 计算每组 IC 的平均值, 最接近 0.065 的 m 即为正确长度.
  - 确定密钥具体值:
    - 将密文按长度 m 分组, 得到 m 个移位密码子串.
    - 对每个子串使用拟重合指数法, 与标准英文分布计算相关系数, 找出最佳位移量.

4. 重要区分与概念

- Playfair 密码: 基于 5×5 矩阵的成对代换密码.
- 一次一密: 明文与等长的真随机密钥逐位异或. 是唯一无条件安全的密码, 但不实用.
- 转轮密码机: 机械实现的、周期极长的多表代换 (如 Enigma).

1.4　第 4 章 分组密码

1.5　第 5 章 序列密码

1.6　第 6 章 Hash 函数和消息认证

1.7　第 7 章 公钥密码体制

1.8　第 8 章 数字签名技术

1.9　第 10 章 密钥管理

第二章　学习通作业

2.1　第 1 章

2.1.1　填空题

题目 1. 信息安全的五大目标 CIAAN.

解答.

1. 机密性 (Confidentiality)
2. 完整性 (Integrity)
3. 可用性 (Availability)
4. 认证性 (Authentication)
5. 不 (抗) 可否认性 (Non-repudiation)

题目 2. 根据对信息流造成的影响, 可以把攻击分为五类.

解答.

1. 中断 (Interruption)
2. 截取 (Interception)
3. 篡改 (Modification)

4. 伪造 (Fabrication)

5. 重放 (Replay)

题目 3. 密码学的发展大致经历了两个阶段.

解答.

1. 传统密码学 (或古典密码学)

2. 现代密码学

题目 4. 1949 年, 信息论鼻祖 Shannon 发表在《贝尔实验室技术杂志》第 28 卷第 4 期 (第 656~715 页) 上的经典论文 ( ), 他将 Information Theory 引入到密码学中, 为密码学的发展奠定了坚实的理论基础. 此为现代密码学开始的标志.

解答. Communication Theory of Secrecy Systems(《保密系统的通信理论》).

题目 5. 传统密码学的第二阶段是以机械为工具的近代密码, 近代密码的主要形式.

解答.

1. 单表代换 (如仿射密码)

2. 多表代换 (如 Vigenere 密码)

3. 转轮密码机 (如 Enigma, TYPEX 等)

4. Vernam 密码.(答出其中三种即可)

题目 6. 1976 年以前的所有的密码系统属于对称密码学 (symmetric cryptosystem) 的范畴, 其中包括 1977 年 NBS 确定的 ( ) 算法, 2000 年选定的 ( ) 算法.1976 年 Diffie & Hellman 在 IEEE Transactions on Information Theory 期刊上发表了一篇著名论文 ( ), 其中提出了 ( ) 思想.

解答.

1. DES(数据加密标准)
2. AES(高级加密标准)
3. "New Directions in Cryptography"(《密码学的新方向》)
4. 公钥密码 (或非对称密码) 思想

题目 7. 公钥密码思想提出后的 1978 年, MIT 的 ( )、( )、( ) 提出了实现公钥密码思想的 ( ) 算法. 后来广泛使用公钥密码算法还有 ( )、( ). 近年来, 随着计算技术及其他相关技术的发展, 还出现了前沿的新的密码技术, 如 ( )、( )、( ).

解答.

1. Rivest
2. Shamir
3. Adleman
4. RSA
5. ElGamal
6. ECC(椭圆曲线密码)
7. DNA 密码
8. 混沌密码
9. 量子密码.(前沿密码技术答案不唯一, 也可填格密码、同态加密等)

题目 8. 传统密码学发展的第一阶段是以手工为主的古代密码术, 典型的代表.

解答.

1. 古希腊棋盘密码

2. 古罗马凯撒密码

3. 美国南北战争栅栏密码.(或斯巴达密码棒、隐写术等)

2.1.2　论述题

题目 9.　谈谈你对安全 (security) 的认识? 它与我们平常所说的安全 (safety) 有何区别?

解答.　计算机或网络空间中讲到的 security 一般是指实现信息的机密性、完整性、可用性、抗否认性、认证性的目标所涉及到的理论、方法、技术. 而我们平常所说的安全 (safety) 一般是指人身或财产的安全.

题目 10.　现代密码学中讲到的“密码”与我们日常生活中说到的”密码“有何不同?

解答.　现代密码学中讲到的“密码”是指密码学 (cryptography), 可实现信息的机密性、完整性、抗否认性. 我们日常生活中说到的”密码”是指 password 即口令字, 是实现身份认证的一种方式.

2.1.3　计算题

题目 11.　在字长为 32 位的计算机中, -125.5 在内存中的存储形式是什么? 试编程以二进制或十六进制形式输出.

解答.

```
import struct
def float_to_hex(f):
    # 使用struct.pack将浮点数转换为32位二进制数据
    packed = struct.pack('!f', f)
    # 使用struct.unpack将二进制数据转换为十六进制表示
```

```
    hex_representation = struct.unpack('!I', packed)[0]
    return hex_representation
# 测试 -125.5
float_value = -125.5
hex_representation = float_to_hex(float_value)
print(f"The hexadecimal representation of -125.5
is: 0x{hex_representation:08X}")
The hexadecimal representation of -125.5 is: 0xC2A04000
```

题目 12. 请对.. -. ..-. --- .-. -- .- - .. --- -. ... . -.-. ..- .-. .. - -.--进行解码, 给出解码后的结果.

解答. information security

题目 13. 请对 YmxvY2tjaGFpbg== 进行解码, 给出解码后的结果.

解答. blockchain

题目 14. 查找资料, 了解类 UNIX 操作系统 (如 CentOS) 下, 与操作系统账户信息相关的两个文件/etc/shadow, /etc/passwd 的格式.

解答.

1. shadow 文件格式:

   用户名: 加密后的口令: 最后一次修改时间: 最小时间间隔: 最大时间间隔: 警告时间: 账号限制时间: 失效时间: 标志.

2. passwd 文件格式:

   用户名: 口令: 用户标识号: 组标识号: 注释性描述: 主目录: 登录 Shell

   Liuxiangtao: x:1000: 1000: this is Liuxiangtao: /home/liuxiangtao: /bin/bash

2.2　第 2 章

2.2.1　填空题

题目 15.　密码学是研究信息及信息系统安全的科学, 密码学又分为 ( ) 学和 ( ) 学.

解答.

1. 密码编码学 (cryptography)
2. 密码分析学 (cryptoanalysis)

题目 15 的注记.　密码学 (Cryptology) 分为两个主要分支: 密码编码学 (Cryptography) 研究如何设计安全的密码系统; 密码分析学 (Cryptanalysis) 研究如何破解密码系统.

题目 16.　一个密码系统一般是 ( )、( )、( )、( )、( ) 五部分组成.

解答.

1. 明文
2. 密文
3. 密钥
4. 加密算法
5. 解密算法

题目 17.　密码体制 (cryptosystem) 是指实现加密和解密功能的密码方案, 从使用密钥策略上, 可分为 ( ) 和 ( ) .

解答.

1. 对称密码体制
2. 非对称密码体制 (公钥密码体制)

题目 18. 密码学 (Cryptology) 是一门交叉学科, 涉及到 ( )、( )、( )、( )、( )、( )、( )、( ) 等多学科或专业知识.

解答.

1. 数论
2. 近世代数
3. 概率论
4. 组合逻辑
5. 复杂度理论
6. 操作系统
7. 算法与数据结构
8. 计算机网络

2.2.2 简答题

题目 19. 攻击密码体制的常用方法有哪些?

解答.

1. 穷举攻击
2. 统计分析攻击
3. 数学分析攻击

题目 20. 根据密码分析者获得的信息量把密码体制的攻击分为哪五种类型?

解答.

1. 唯密文攻击 (Ciphertext-only Attack)
2. 已知明文攻击 (Known-plaintext Attack)
3. 选择明文攻击 (Chosen-plaintext Attack)
4. 选择密文攻击 (Chosen-ciphertext Attack)
5. 选择文本攻击 (Chosen-text Attack)

2.2.3　名词解释题

题目 21.　密码编码学.

解答.　密码编码学 (Cryptography) 是研究如何对信息编码以实现信息和通信安全的科学.

题目 22.　密码分析学.

解答.　密码分析学 (Cryptanalysis) 是研究如何破解或攻击受保护的信息的科学.

2.2.4　计算题

题目 23.　现代密码学研究的体系结构分为三个层次, 最底层是数学基础, 中间层是密码技术, 最上层是应用. 试画出现代密码学研究的体系结构图.

解答.

题目 24.　画出保密通信系统的模型.

解答.

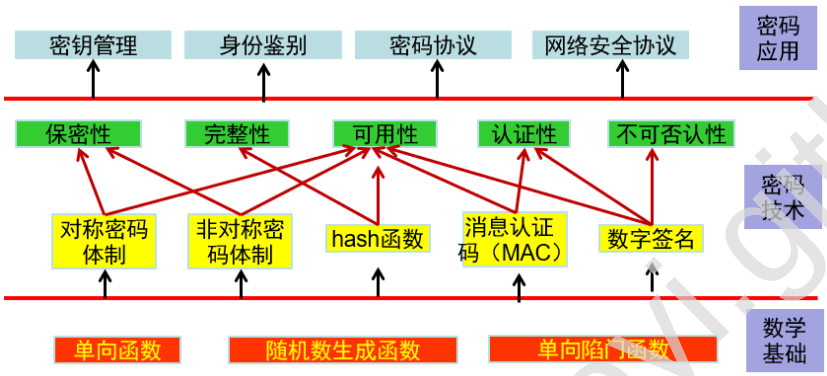

图 2.1: 题目 23 图

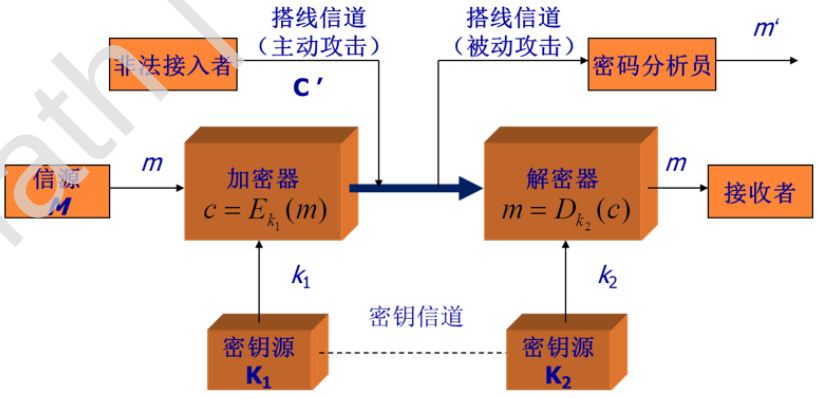

图 2.2: 题目 24 图

2.2.5　论述题

题目 25.　计算上的安全性是指若破解一个密码系统是可行的, 但使用已知的算法和现有的计算机不可能完成攻击所需要的计算量, 则称该密码体制是计算上安全的. 当前的密码体制都属于计算上的安全性 (多数是基于数学难题求解), 试举一个例子加以说明.

解答.　著名的公钥密码体制算法 RSA, 其计算上的安全性就是依赖于大整数的素因子分析的数学难题. 若 RSA 的公钥为 (n, e), n 是大整数 (通常大于 1024bits), e 是与 $\phi(n)$ 互素的整数, 若能将 n 分解成 2 个素因子 p, q 的乘积, 则容易求 $\phi(n) = (p-1)\cdot(q-1)$, 那么根据扩展的 Euclid 算法可求出解密密钥 $d, e \cdot d \equiv 1 \mod \phi(n)$.

题目 26.　阐述什么是无条件安全性? 有条件安全性? 什么是计算上的安全性?

解答.

1. 无条件安全性:

   对一种密码体制, 无论破解者知道多少密文、采用何种方法都得不到明文或密钥的信息, 即具有无限计算资源 (时间、空间、设备、资金) 的情况下, 破解者也无法破解该密码系统.

2. 有条件安全性:

   是根据破解密码系统所需的计算量 (时间、空间) 来评价其安全性, 又称为计算安全性或实际安全性.

3. 计算上的安全性:

   若破解一个密码系统是可行的, 但使用已知的算法和现有的计算机不可能完成攻击所需要的计算量, 则称该密码体制是计算上安全的. 当前的密码体制都属于计算上的安全性 (多数是基于数学难题求解)!

2.3　第 3 章

2.3.1　填空题

题目 27.　两种主要的古典密码体制为 ( )、( ).

解答.

1. 代换密码 (substitution)
2. 置换密码 (permutation)

2.3.2　计算题

题目 28.　用维吉尼亚密码加密明文“please keep this message in secret”，使用的密钥为“computer”，试求其密文.

解答.　rzqpm xovgd fwclq vugmv yrjgq dtn

题目 29.　已知以下密文是由仿射密码得到的，试求其明文. “FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH”

解答.　ALGORITHMS ARE QUITE GENERALIZED DEFINITIONS OF ARITHMETIC PROCESSES

题目 30.　DES 算法中的初始置换为:

$$IP = \begin{Bmatrix} 58,50,42,34,26,18,10,2 \\ 60,52,44,36,28,20,12,4 \\ 62,54,46,38,30,22,14,6 \\ 64,56,48,40,32,24,16,8 \\ 57,49,41,33,25,17,9,1 \\ 59,51,43,35,27,19,11,3 \\ 61,53,45,37,29,21,13,5 \\ 63,55,47,39,31,23,15,7 \end{Bmatrix}$$

求该置换 IP 的逆置换.

解答.

$$IP^{-1} = \begin{Bmatrix} 40, 8, 48, 16, 56, 24, 64, 32 \\ 39, 7, 47, 15, 55, 23, 63, 31 \\ 38, 6, 46, 14, 54, 22, 62, 30 \\ 37, 5, 45, 13, 53, 21, 61, 29 \\ 36, 4, 44, 12, 52, 20, 60, 28 \\ 35, 3, 43, 11, 51, 19, 59, 27 \\ 34, 2, 42, 10, 50, 18, 58, 26 \\ 33, 1, 41, 9, 49, 17, 57, 25 \end{Bmatrix}$$

题目 31. 现有一个置换 $\sigma = (1423)$, 计算利用 σ 对 “security” 进行周期置换加密的结果.

解答. cuestyir

题目 32. 仿射加密 $c = k_1 \cdot m + k_2 \mod 26$ 中的明文 m、密文 c、密钥 (k_1, k_2) 皆定义在如下的字符集及编码上:

charset	a	b	c	d	e	f	g	h	i	j	k	l	m
encoding	0	1	2	3	4	5	6	7	8	9	10	11	12

charset	n	o	p	q	r	s	t	u	v	w	x	y	z
encoding	13	14	15	16	17	18	19	20	21	22	23	24	25

表 2.1: 字符集与编码对照表

现取密钥 $(k_1, k_2) = (3, 4)$, 要求计算明文 “aust” 经过该仿射加密后的密文.

解答. emgi

题目 33. 用于密钥生成的语句为 “cryptography” , 求 Playfair 密码的 key matrix.

解答.

$$\begin{pmatrix} c,r,y,p,t \\ o,g,a,h,b \\ d,e,f,i/j,k \\ l,m,n,q,s \\ u,v,w,x,z \end{pmatrix}$$

题目 34. 维吉尼亚加密的的明文、密文、密钥都定义在以下的字符集与编码上:

charset	a	b	c	d	e	f	g	h	i	j	k	l	m
encoding	0	1	2	3	4	5	6	7	8	9	10	11	12

charset	n	o	p	q	r	s	t	u	v	w	x	y	z
encoding	13	14	15	16	17	18	19	20	21	22	23	24	25

表 2.2: 字符集与编码对照表

现要求利用密钥 key = "info" 对明文 "computer "进行加密之后的密文.

解答. kbrd cgjf

2.4 第 4 章

2.4.1 填空题

题目 35. 轮函数是分组密码结构的核心, 评价轮函数设计质量的三个主要指标是 ( )、( )、( ).

解答.

1. 扩散
2. 混乱

3. 乘积密码

题目 36. DES 的轮函数 F 是由四个部分组成 ( )、( )、( )、( ).

解答.

1. 扩展置换
2. 密钥加 (XOR, 异或)
3. S 盒
4. P 盒

题目 37. 关于 DES 算法, 密钥的长度 (即有效位数) 是 ( ) 位, 又其 ( ) 性使 DES 在选择明文攻击下所需的工作量减半, 时间复杂度为 ( ).

解答.

1. 56
2. 互补性
3. $O(2^{55})$

题目 38. 分组密码的加解密算法中最关键部分是非线性运算部分, 那么, DES 加密算法的非线性运算部分是指 ( ),AES 加密算法的非线性运算部分是指 ( ).

解答.

1. S-BOX
2. 字节代换

题目 39. DES 的算法属性为, Blocksize=( ), keysize=( ), rounds=( ), 运算对象为 ( ).

解答.

1. 64bits
2. 56bits
3. 16
4. bit

题目 40. AES-128 的算法属性为, Blocksize=( ), keysize=( ), rounds=( ), 运算对象为 ( ).

解答.

1. 128bits
2. 128bits
3. 10
4. byte

题目 41. AES 加密算法的结构中的四个不同的模块是 ( )、( )、( )、( ).

解答.

1. 字节代换
2. 行移位
3. 列混淆
4. 轮密钥加

2.4.2 论述题

题目 42. 证明 DES 的互补性会使 DES 在选择明文攻击下所需的工作量减半.

解答. 在选择明文攻击下, 可得:

$$c_1 = E_k(m) \quad (1)$$

$$c_2 = E_k(\overline{m}) \quad (2)$$

根据互补性由 (2) 得:

$$\overline{c_2} = E_k(m) \quad (3)$$

根据 (1) 式穷举搜索密钥 k 时, 若输出密文是 c_1, 则加密密钥就是所应用的密钥; 若输出密文是 $\overline{c_2}$, 根据 (3) 可知加密密钥是所应用的密钥的补; 这样, 利用一个密钥的加密尝试, 能够检测两个密钥是否为真正的加密密钥. 因此, DES 的互补性会使 DES 在选择明文攻击下所需的工作量减半.

题目 43. 为什么二重 DES 并不像人们想象的那样可提高密钥长度到 112 比特而相当 57 比特.

解答. 二重 DES 指的是取独立的两个密钥 k_1 和 k_2

加密:$C = DES_{k_2}(DES_{k_1}(m))$

解密:$m = DES_{k_1}^{-1}(DES_{k_2}^{-1}(C))$

则 $DES_{k_1}(m) = DES_{k_2}^{-1}(C)$

可对 m 采取一切可能的 k_1 加密并存储, 再对 C 取一切可能的 k_2 解密, 并与存储的 $DES_{k_1}(m)$ 比较, 若有相等的, 则 k_1 和 k_2 便可获得.

二重 DES 并不像人们相像那样可提高密钥长度到 112 比特, 而相当 57 比特.(中途相遇攻击)

题目 44. 指出 RC6 加密算法中的非线性部分, 并证明这部分是双射函数.

解答. RC6 是一种对称密钥块密码算法, 其设计包含了非线性的部分.RC6 的非线性部分是通过运用两个不同的操作来实现的: 模加 (MOD addition) 和模乘 (MOD multiplication). 具体来说, RC6 的非线性部分涉及到两个变换: 模加和模乘, 它们被称为 + 和 ×. 这两个运算定义如下:

1. 模加 $+_m$: 对两个输入 a 和 b 执行模 2^{32} 相加, 得到 $a +_m b$. 这个操

作在 RC6 中用于混淆和扩散.

$$a +_m b = (a + b) \mod 2^{32}$$

2. 模乘 $\times_m$: 对两个输入 a 和 b 执行模 2^{32} 相乘, 得到 $a \times_m b$. 这个操作在 RC6 中用于引入非线性性.

$$a \times_m b = (a \times b) \mod 2^{32}$$

可对 m 采取一切可能的 k_1 加密并存储, 在对 C 取一切可能的 k_2 解密, 并与存储的 $DES_{k_1}(m)$ 比较, 若有相等的, 则 k_1 和 k_2 便可获得. 二重 DES 并不像人们相像那样可提高密钥长度到 112 比特, 而相当 57 比特.

(中途相遇攻击)

RC6 的非线性部分使用了这两个运算来增加算法的复杂性和安全性. 现在, 我们来证明这个非线性部分是一个双射函数.

证明非线性部分是双射函数:

首先, 我们需要证明 $+$ 和 $\times$ 这两个运算是封闭的, 即对于 $a, b \in \mathbb{Z}_{2^{32}}$, 有 $a +_m b \in \mathbb{Z}_{2^{32}}$ 和 $a \times_m b \in \mathbb{Z}_{2^{32}}$.

对于 $+$ 操作, 显然 $a +_m b$ 是模 2^{32} 加法的结果, 因此 $a +_m b \in \mathbb{Z}_{2^{32}}$.

对于 $\times$ 操作, 同样 $a \times_m b$ 是模 2^{32} 乘法的结果, 因此 $a \times_m b \in \mathbb{Z}_{2^{32}}$.

接下来, 我们需要证明 $+$ 和 $\times$ 是一一映射 (单射和满射).

1. 单射性: 如果 $a_1 \neq a_2$ 或 $b_1 \neq b_2$, 则 $a_1 +_m b_1 \neq a_2 +_m b_2$ 和 $a_1 \times_m b_1 \neq a_2 \times_m b_2$. 这是因为模 2^{32} 加法和乘法都是单射的.

2. 满射性: 对于任意 $c \in \mathbb{Z}_{2^{32}}$, 可以找到 a, b 使得 $a +_m b = c$ 和 $a \times_m b = c$. 这是因为模 2^{32} 加法和乘法都是满射的.

因此, 我们证明了 $+$ 和 $\times$ 都是封闭的且是一一映射, 这意味着非线性部分是一个双射函数. 在密码学中, 双射函数对于保证密钥空间和算法的安全性至关重要.

题目 45. 分析 RC6 加密算法的扩散性.

解答. RC6 是一种对称密钥块密码算法, 其设计中包含了扩散性, 即对明文和密钥的小变化会引起密文的广泛变化.RC6 的扩散性主要通过以下几个方面来实现:

1. 轮函数设计:RC6 的加密算法采用了多轮迭代的结构. 每轮中都有多个步骤, 包括混合 (Mixing) 和扩展 (Expansion) 等. 多轮结构确保了算法具有较强的扩散性, 因为每一轮都引入了新的变换, 使得输出对输入的任何微小变化都会有显著的影响.

2. 非线性运算:RC6 中的运算主要涉及到模加 (MOD addition) 和模乘 (MOD multiplication) 这两个非线性运算. 这些运算增加了算法的复杂性, 同时引入了非线性性质, 从而提高了扩散性.

3. 密钥扩展:RC6 通过对密钥进行扩展来生成轮密钥. 这样可以确保每一轮中使用的密钥都是不同的, 从而提高了密钥变化对输出的扩散性.

4. 分组大小:RC6 的分组大小为字长的整数倍, 这有助于确保算法在进行运算时能够更好地利用整个分组的信息, 提高了扩散性.

5. 轮常数:RC6 中使用了轮常数, 这些常数在每一轮中都与轮密钥进行混合. 这种引入的常数确保了每一轮都有独特的运算, 从而提高了扩散性.

总体而言, RC6 通过上述设计特点, 尤其是多轮结构、非线性运算和密钥扩展, 来确保算法在面对输入的微小变化时产生广泛的输出变化, 从而具有良好的扩散性. 这种性质对于密码算法的安全性至关重要, 因为它使得攻击者难以通过分析输出来推断出关于密钥或明文的信息.

题目 46. 评价 RC6 密钥扩展方案

解答. RC6 的密钥扩展方案是其设计中关键的组成部分之一, 它负责生成轮密钥, 确保密钥的有效性和安全性. 以下是对 RC6 密钥扩展方案的一些评价:

1. 灵活性:RC6 的密钥扩展方案相对灵活, 可以适应不同密钥长度. 算法允许使用不同的轮数和密钥长度, 从而可以在不同的安全性需求下调整. 这种灵活性是在实际应用中非常有用的.

2. 安全性: 密钥扩展方案的安全性对整个密码算法的安全性至关重要.RC6 的密钥扩展方案使用了密钥混合、轮常数和非线性运算, 这些元素有助于提高密钥的随机性, 增加了算法的安全性.

3. 复杂性:RC6 的密钥扩展方案相对复杂, 需要进行多轮运算和复杂的数学运算. 这提高了算法的复杂性, 但也增加了理解和实现的难度. 在一些特定的嵌入式系统或资源受限的环境中, 可能会对性能产生一定影响.

4. 密钥变化的影响: 密钥扩展方案应该能够有效地处理密钥的微小变化, 以确保算法在面对密钥变化时能够产生广泛的输出变化.RC6 的密钥扩展方案通过轮常数和非线性运算的引入, 以及密钥的合理变化, 能够提供良好的密钥变化影响.

5. 抗差分攻击:RC6 密钥扩展方案的设计考虑了抗差分攻击的需求, 这是一种常见的密码分析方法. 这有助于提高算法对某些攻击的抵抗能力.

总体而言, RC6 的密钥扩展方案在其设计目标中取得了平衡, 提供了灵活性和安全性, 但也带来了一定的复杂性. 在实际应用中, 密钥扩展方案的性能和安全性需根据具体需求进行权衡.

2.4.3 计算题

题目 47. 设计利用 DES-CBC 模式生成消息 M 的消息认证码 (MAC) 的形式化描述, 假如消息 M 分成了 N 个分组 D_1, D_2, ..., D_N.

解答.

$$
\begin{aligned}
O_1 &= E(K, D_1) \\
O_2 &= E(K, [D_2 \oplus O_1]) \\
O_3 &= E(K, [D_3 \oplus O_2]) \\
&\vdots \\
O_N &= E(K, [D_N \oplus O_{N-1}])
\end{aligned}
$$

则最后的 O_N 即是消息 M 的 MAC

题目 48. 画出分组密码 CBC 模式图.

解答.

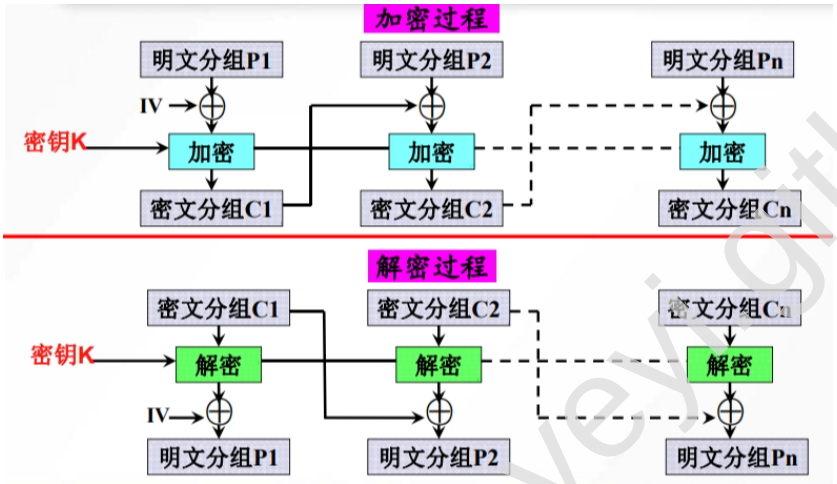

图 2.3: 题目 48 图

2.5 第 5 章

2.5.1 计算题

题目 49. 一个 3 级的 LFSR 的初始状态为 100, 其反馈函数为 $f(\quad) = b_2 \oplus b_3$, 求其 LFSR 的输出序列, 并判断其输出序列的周期.

解答. 其输出序列为 0 011 011 011...

其输出序列的周期为 3, 不是 m 序列.

题目 50. 次数 $n = 6$ 的多项式中, 有多少个本原多项式存在?

解答. 6 个.

假设基域为二元域 $\mathbb{F}_2$. 一个次数为 n 的多项式称为本原多项式, 如果它在 $\mathbb{F}_2[x]$ 中不可约, 并且其根是乘法群 $\mathbb{F}_{2^n}^{\times}$ 的本原元. 由于 $\mathbb{F}_{2^n}^{\times}$ 是循环群, 其阶为 $2^n - 1$, 故本原元的个数为欧拉函数 $\varphi(2^n - 1)$. 每个次数为 n 的本

原多项式恰有 n 个不同的本原根 (即其所有根), 因此本原多项式的个数为 $\dfrac{\varphi(2^n-1)}{n}$.

当 $n=6$ 时, $2^6-1=63$. 计算 $\varphi(63)$: 因 $63=3^2\times 7$, 故

$$\varphi(63)=63\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)=63\times\frac{2}{3}\times\frac{6}{7}=63\times\frac{4}{7}=36.$$

因此, 次数为 6 的本原多项式的个数为 $\dfrac{36}{6}=6$.

题目 51. 一个 4 级的 LFSR 是以生成多项式 $G(x)=x^4+x+1$ 来构造反馈函数. 请判断 $G(x)$ 是否是本原多项式, 以 $G(x)$ 构造的 LFSR 的反馈函数是什么? 若该 4 级的 LFSR 的初始状态为 1001, 求其输出序列, 并指出其输出的密钥流是不是 m 序列.

解答. 由于:

(1) $G(x)$ 都不能被 $x, x+1, x^2+x+1$ 整除, 所以 $G(x)$ 是不可约多项式.

(2) $G(x)|(x^k-1)$, 其中 $k=2^4-1=15$, 且不存在一个整数 $m<15$, $G(x)|(x^m-1)$ 因此 $G(x)$ 是本原多项式.

依据 $G(x)$ 构造的反馈函数 $f(a_4,a_3,a_2,a_1)=a_4\oplus a_1$

该 LFSR 输出的序列为:

$$1001\ 0001\ 1110\ 101\ 1001\ 0001\ 1110\ 101\ldots$$

其周期为 $15=2^4-1$, 因此以此生成的密钥序列为 m 序列.

题目 52. 画出序列密码用于加密通信的模型图.

解答.

2.5.2 论述题

题目 53. 在 GF(2) 上的一个多项式 $G(x)$ 是本原多项式要满足的条件有哪些?

$$G(x)=\sum_{i=0}^{n}a_ix^i$$

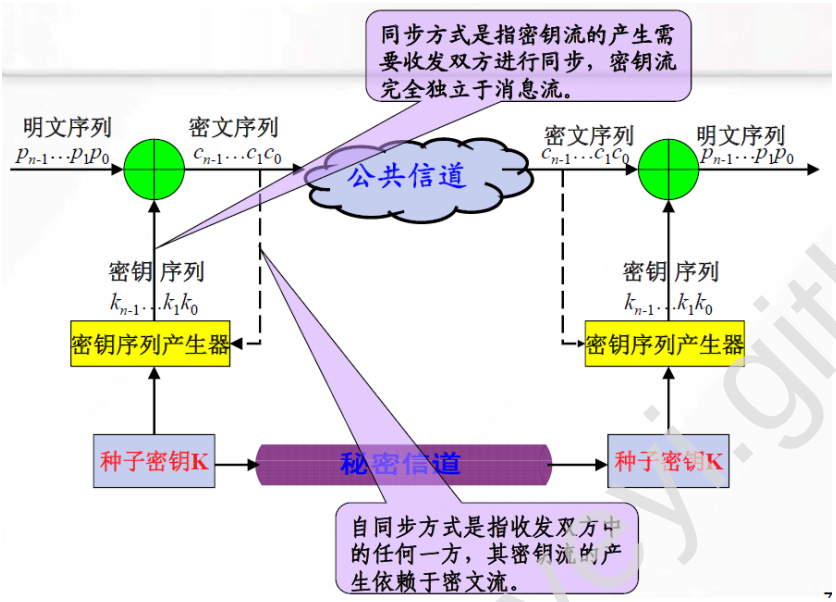

图 2.4: 题目 52 图

解答.

(1) $G(x)$ 是不可约的, 即不能再分解因式;

(2) $G(x)|(x^m+1)$, 其中 $m=2^n-1$;

2.5.3 简答题

题目 54. 字节级别的 RC4 算法中, 生成密钥序列的周期是多少?

解答. 10 的 100 次方.

题目 55. 评价 RC4 算法的密钥序列产生器的混乱性与扩散性.

解答. RC4 算法的密钥序列产生器在其设计初期被认为是相当强大的, 因为它具有较好的混乱性和扩散性.

混乱性 (Confusion):

混乱性指的是算法的输出对密钥的小变化应该具有很大的影响, 使得统计学攻击难以成功.RC4 在这方面具有以下特点:

1. 初始置换阶段: 初始时, RC4 对 S 盒进行了一次初始置换, 其中通过多轮的交换操作, 导致 S 盒中的元素与密钥的相关性较强.

2. 伪随机数生成: 在生成密钥流的阶段, RC4 通过多次迭代的交换操作, 进一步混淆了 S 盒中的元素, 产生了伪随机的密钥流.

然而, 一些统计学攻击和偏差分析方法已经证明了 RC4 在混乱性方面的弱点, 特别是在大量密文被生成的情况下.

扩散性 (Diffusion):

扩散性指的是对输入的微小变化应该导致输出的大变化, 使得密文的统计特性难以被破解. 在 RC4 中:

1. 密钥变化影响:RC4 对密钥的每一位变化都会影响 S 盒的状态, 因此它在扩散方面表现较好.

2. 密文的影响: 密钥流作为伪随机序列与明文进行异或操作, 因此密钥的微小变化会导致密文的大变化.

尽管 RC4 在扩散性方面有优点, 但一些攻击模型表明在某些情况下, 密钥流的可预测性和偏差可能会被利用, 从而降低了其安全性.

尽管 RC4 在设计初期被广泛使用并被认为是相对强大的加密算法, 但由于安全性问题, 现今不再被推荐使用. 更为安全的加密算法, 如 AES, 已经取代了 RC4 在许多实际应用中的位置.

2.6　第 6 章

2.6.1　简答题

题目 56. 什么是 Hash 函数的弱碰撞攻击? 什么是强碰撞攻击?

解答. 对任何给定的消息 x, 找到满足 $y \neq x$ 且 $H(x) = H(y)$ 的消息 y, 称为 weak collision attack.

找到任何满足 $H(x) = H(y)$ 的偶对 (x, y), 称为 strong collision attack.

2.6.2　论述题

题目 57.　MD5 算法包括 4 轮, 每轮 16 次迭代, 在每轮 16 次迭代中, 在每一步中, 四个寄存器 A,B,C,D 之间是如何赋值的?16 次循环四个寄存器 A,B,C,D 之间赋值关系如何?

解答.　每一步赋值:

$$A = D$$
$$B = B + ((A + g(B, C, D) + X[k] + T[i]) \lll s)$$
$$C = B$$
$$D = C$$

16 次循环步骤中, 四个寄存器之间的赋值关系如下:

1. ABCD
2. DABC
3. CDAB
4. BCDA
5. ABCD
6. DABC
7. CDAB
8. BCDA
9. ABCD
10. DABC
11. CDAB

12. BCDA

13. ABCD

14. DABC

15. CDAB

16. BCDA

题目 58. 论述国密算法中的对称加密算法、非对称加密算法、Hash 函数.

解答.

1. SM1, 对称加密算法中的分组加密算法, 其分组长度、密钥长度都是 128bit, 算法安全保密强度跟 AES 相当, 但是算法不公开.

2. SM4, SM4 算法与 AES 算法具有相同的密钥长度、分组长度, 都是 128bit.

3. SM7, 该算法没有公开.SM7 适用于非接 IC 卡应用包括身份识别类应用 (门禁卡、工作证、参赛证), 票务类应用 (大型赛事门票、展会门票), 支付与通卡类应用 (积分消费卡、校园一卡通、企业一卡通、公交一卡通).

4. ZUC(祖冲之算法), 它是中国自主研究的流密码算法, 该机密性算法可适用于 3GPP LTE 通信中的加密和解密, 该算法包括祖冲之算法 (ZUC)、加密算法 (128-EEA3) 和完整性算法 (128-EIA3) 三个部分. 目前已有对 ZUC 算法的优化实现, 有专门针对 128-EEA3 和 128-EIA3 的硬件实现与优化, 由国家密码管理局于 2012 年 3 月 21 日发布.

5. SM2, 它是基于椭圆曲线密码的公钥密码算法标准, 其密钥长度 256bit, 包含数字签名、密钥交换和公钥加密, 用于替换 RSA/DH/ECDSA/ECDH 等国际算法.

6. SM9, 主要用于用户的身份认证, SM9 的加密强度等同于 3072 位密钥的 RSA 加密算法, 于 2016 年 3 月 28 日发布.

7. SM3, 它是在 SHA-256 基础上改进实现的一种算法, 采用 Merkle-Damgard 结构, 消息分组长度为 512bit, 输出的摘要值长度为 256bit.

2.6.3 填空题

题目 59. 给出下列 Hash 算法的算法属性:

1. MD5

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

2. SHA1

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

3. SHA256

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

4. SHA512

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

5. RIPEMD-160

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

解答.

- MD5: 512bits, 4, 16, 128bits
- SHA1: 512bits, 4, 20, 160bits
- SHA256: 512bits, 4, 16, 256bits

- SHA512: 1024bits, 4, 20, 512bits
- RIPEMD: 512bits, 5, 16, 160bits

题目 60. 国密算法中非对称加密 (公钥密码) 算法有 ( )、( ), Hash 函数有 ( ).

解答.

(1) SM2, 它是基于椭圆曲线密码的公钥密码算法标准.

(2) SM9, 等同于 3072 位密钥的 RSA 加密算法.

(3) SM3, 等同于 SHA-256.

题目 61. 请给出 SHA1 算法的算法属性:blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( ).

解答.

(1) 512bits

(2) 4

(3) 20

(4) 160bits

题目 62. 设 Hash 函数的输出长度为 nbits, 则安全的 Hash 函数寻找碰撞的复杂度为 ( ).

解答. $O(2^{\frac{n}{2}})$.

2.6.4 计算题

题目 63. 画出利用对称密码体制实现消息认证的模型 (不提供机密性).

解答.

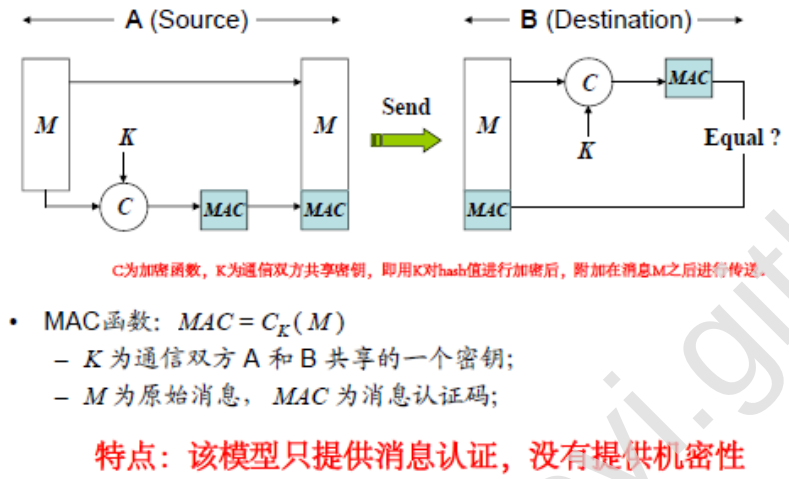

图 2.5: 题目 63 图

题目 64. 画出即实现对消息 m 进行认证 (消息认证与明文有关), 又对消息 m 实现机密性的模型.

解答.

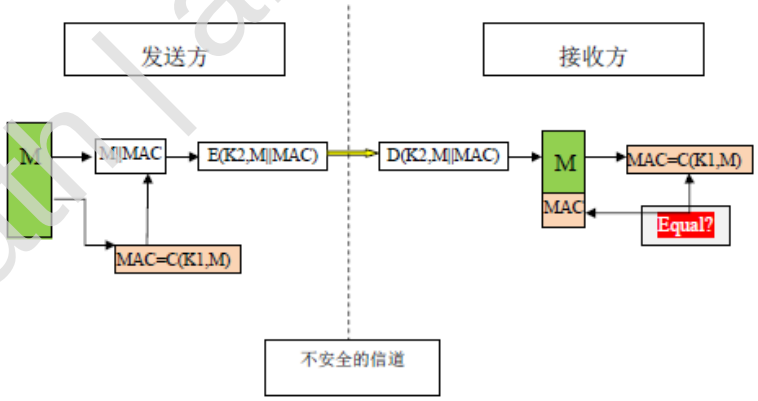

图 2.6: 题目 64 图

题目 65. 若有消息 m=”Computer Science”, 若求其 Hash 值需要对其进行预处理填充. 请计算对 m 进行填充后形成的一个 512bits 的分组是什么?

解答. 1. 原始消息转换: 将字符串转换为 ASCII 码 (每个字符 8 位), 得到

16 字节 (128 位) 的序列:

43 6F 6D 70 75 74 65 72 20 53 63 69 65 6E 63 65

2. 填充步骤:

- 在消息后添加一个 1 比特, 随后添加足够的 0 比特, 使得总长度 (不含长度附加) 达到 448 位 (56 字节).
- 原始消息 16 字节, 需填充 40 字节. 第一个填充字节为 `0x80`(二进制 `10000000`, 即 1 比特后跟 7 个 0), 其余 39 字节为 `0x00`.
- 最后附加 64 位的原始消息长度 (大端序表示). 长度 128 位对应的十六进制为 `0x00000000000000%80`, 即最后 8 字节为 `00 00 00 00 00 00 00 80`.

3. 填充后的 512 位分组 (共 64 字节) 的十六进制表示为:

436F6D70757465722053636965E63658

其余填充 0

该分组满足哈希函数预处理要求, 可直接用于后续哈希计算.

题目 66. 设 A: 签名方, B: 验证方, 签名的消息为 m.A 的 key paire=(Pka, Ska), Hash 函数为 H( ), 签名值为 s, 加密算法为 E, 解密算法为 D. 请给出数字签名原理的形式化描述.

解答.

- step1, A: $h = H(m)$, $s = D(Ska, h)$, $m \parallel s \longrightarrow B$
- step2, B: $h = H(m)$, $h' = E(Pka, s)$, if $(h == h')$ then 验证签名成功 else 验证签名不成功.

题目 67. Hash 函数有着广泛的重要用途, 其中之一就是用于消息在传输之后的完整性验证. 假设 A 发送消息 m 给接收方 B, 并且 A、B 都拥有 AES 加密的会话密钥 key. 现要求设计 A 发送消息 m 给 B 并能实现 m 的完整性验证的模型, 以形式化表达或图的形式给出模型.

解答. 模型的形式化表达:

1. A: $h = \text{hash}(m)$, $h' = \text{encryption-AES}(h, \text{key})$, $m \parallel h' \longrightarrow B$
2. B: $hb = \text{hash}(m)$, $hb' = \text{decryption-AES}(h', \text{key})$, if $(hb = hb')$ then 消息在传输过程中没有被篡改 else 消息 m 在传输过程中被篡改.

题目 68. 在一个广域网的环境中, 用户使用用户名和口令的方式的登录远程服务器, 服务器的管理员给每个用户设置一个初始口令, 请利用 Hash 函数的技术实现以下安全需求:

(1) 用户口令在广域网上安全传输, 也就是说即使攻击者窃取用户网上传输的信息, 也分析不出口令;

(2) 管理员也不知道用户的口令. 设计一个方案满足上述安全需求并分析其安全性.

解答. 安全性分析:

口令和哈希值均不在网络中传输, 防止窃听. 随机挑战防止重放攻击. 服务器只存储哈希值, 管理员无法获知口令.

建议加盐存储以防御彩虹表攻击 (存储 salt, H(口令, salt); salt, H(口令, salt), 响应计算为 H(H(口令, salt), R)H(H(口令, salt), R)).

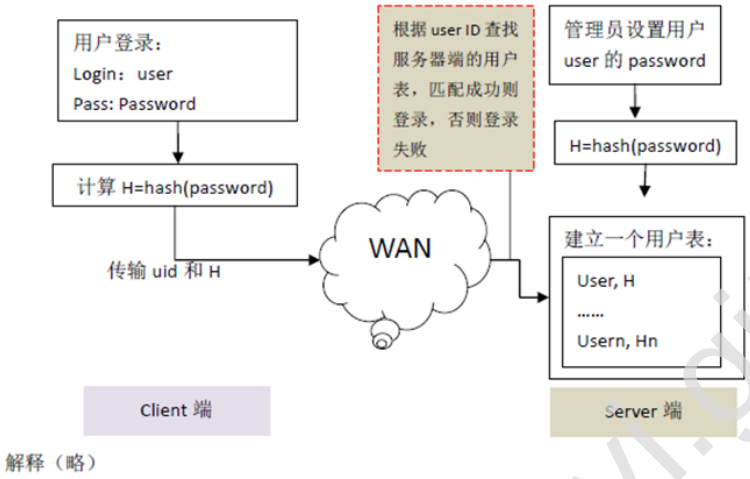

图 2.7: 题目 68 图

2.7　第 7 章

2.7.1　论述题

题目 69.　public key cryptosystem(公钥密码体系, 或非对称密码体系) 的思想主要包括哪些方面?

解答.

1. 通信双方各有一对密钥 (Pk, Sk), Pk 是加密密钥, Sk 是解密密钥, 加密 key 不等于解密 key;
2. 加密 key 是 public, 解密 key 是 secure(private);
3. 由 public key 推导出 secure key, 在计算上不可行;
4. 既可以实现机密性, 也可以实现抗否认性
5. 加密、解密次序可交换, 即 $D(Sk, E(Pk, m)) = E(Pk, D(Sk, m))$

题目 70.　阐述 ECC 中针对用户 A 的密钥生成算法.

解答.

- step1: 选择一个椭圆曲线 $E: y^2 \equiv x^3 + ax + b \pmod{p}$, 构造一个椭圆群 $E_p(a, b)$.(2 分)
- step2: 在 $E_p(a, b)$ 中挑选生成元点 $G = (x_0, y_0)$, G 应使得满足 $nG = O$ 的最小的 n 是一个非常大的素数.(2 分)
- step3: 选择一个小于 n 的整数 nA 作为其私钥, 然后计算 $Pubkey = nA * G$, 则 (2 分)
  - A 的公钥为 $Pk = (p, a, b, n, G, Pubkey)$
  - A 的私钥为 $Sk = nA$

题目 71. 论述 ECC 数字签名方案.

解答.

1. 选择一个椭圆曲线 $E_p(a, b): y^2 = x^3 + ax + b \mod p$
2. 选择一个生成元 G, 其阶 n 是一个大素数
3. 选择一个小于 n 的整数 nA 作为签名方 A 的私钥
4. 计算 $Pka = nA * G$ 作为 A 的公钥
5. 签名:A 随机选择一个整数 k $(1 \leq k \leq n-1)$, 对消息 m 进行如下计算得到签名值 (r, s)
   - 计算点 $kG = (x, y)$
   - 计算 $r = x \mod n$, 若 $r = 0$ 则重新选择 k
   - 计算消息的哈希值 $e = H(m)$ (转换为整数)
   - 计算 $s = k^{-1}(e + nA \cdot r) \mod n$, 若 $s = 0$ 则重新选择 k
6. 验证签名: 验证方收到消息 m 和签名 (r, s) 后, 执行以下步骤

- 验证 r, s 是否满足 $1 \leq r \leq n-1, 1 \leq s \leq n-1$
- 计算 $e = H(m)$
- 计算 $w = s^{-1} \mod n$
- 计算 $u_1 = e \cdot w \mod n$, $u_2 = r \cdot w \mod n$
- 计算点 $X = u_1 \cdot G + u_2 \cdot Pka = (x_1, y_1)$
- 若 X 为无穷远点, 则验证失败; 否则计算 $v = x_1 \mod n$
- 当且仅当 $v = r$ 时, 验证签名成功; 否则失败.

2.7.2 计算题

题目 72. 假如通信的双方为 A, B, A 为 sender, B 为 receiver, A 发送给 B 的消息为 m, A 的公钥私钥对为 (PKa, SKa), B 的公钥私钥对为 (PKb, SKb), 现要求用公钥密码体系实现 A 发送消息 m 给 B 的机密性. 用形式化的语言描述实现的步骤.

解答.

- step1: A: $c = E(m, PKb) \longrightarrow B : c$
- step2: B: $m = D(c, SKb)$

题目 73. 假如通信的双方为 A, B, A 为 sender, B 为 receiver, A 发送给 B 的消息为 m, A 的公钥私钥对为 (PKa, SKa), B 的公钥私钥对为 (PKb, SKb), 现要求用公钥密码体系实现 A 发送消息 m 给 B 的抗否认性. 用形式化的语言描述实现的步骤.

解答.

- step1, A: $s = D(m, SKa)$, $m \parallel s \longrightarrow B : m \parallel s$
- step2, B: $m' = E(s, PKa)$, if $(m == m')$ verifying sign is successful else failure.

题目 74. 写出 RSA 算法的共模攻击算法.

解答. user1 的公钥为 (e_1, n), user2 的公钥为 (e_2, n).$\gcd(e_1, e_2) = 1$, 设对明文消息为 m 进行加密的结果为:

$$c_1 = m^{e_1} \mod n, \quad c_2 = m^{e_2} \mod n,$$

假如敌手截获了 c_1, c_2, 则可通过以下算法破解出明文 m:

step1: 根据扩展的 Euclidean 算法求出满足条件 $re_1 + se_2 \equiv 1 \mod n$ 的 r, s;

step2: 计算 $c_1^r * c_2^s \mod n = m^{re_1} * m^{se_2} \mod n = m^{(re_1+se_2)} \mod n = m$, 即获得明文 m.

题目 75. ECC 的一个椭圆曲线 $E_{23}(-4, 1) : y^2 = x^3 - 4x + 1 \mod 23$, $P(4, 7)$、$Q(2, 1)$ 是椭圆曲线上的两个点, 求

(1) $R = (x_3, y_3) = P + Q$

(2) $2P$

解答.

(1) 计算 $P + Q$

$\lambda = 3, \quad (1\ 分)$

$x_3 = 3^2 - 4 - 2 = 3 \quad (1\ 分)$

$y_3 = 3 \cdot (4 - 3) - 7 = -4 = 19 \quad (1\ 分)$

因此, $R = P + Q = (x_3, y_3) = (3, 19)$

(2) 计算 $2P$

$\lambda = (3^4 \cdot 4^2 - 4)/(2 \cdot 7) \mod 23 = 44/14 \mod 23 = 22/7 \mod 23 = 22 \cdot 1/7 \mod 23 = 22 \cdot 10 \mod 23 = 13 \quad (3\ 分)$

$x_3 = 13^2 - 4 - 4 = 161 \mod 23 = 0 \quad (1\ 分)$

$y_3 = 2 \cdot (4 - 0) - 7 = 45 \mod 23 = 22 \quad (1\ 分)$

$2P = (0, 22)$

题目 76. ECC 上的椭圆 $E_{11}(1,6): y^2 = x^3+x+6 \mod 11$, 假设 $G=(2,7)$ 为生成元.

(1) 利用 G 生成椭圆曲线上的所有点的集合.

(2) 求 G 的阶.

解答.

$$G=(2,7),\quad 2G=(5,2),\quad 3G=(8,3),\quad 4G=(10,2),\quad 5G=(3,6),$$
$$6G=(7,9), 7G=(7,2),\quad 8G=(3,5),\quad 9G=(10,9),\quad 10G=(8,8),$$
$$11G=(5,9),\quad 12G=(2,4),\quad 13G=(\inf,\inf)=O$$

G 为生成元, 其阶为 13.

题目 77. 椭圆曲线加密 (ECC) 中的椭圆曲线一般是指一种简单的维尔斯特拉斯方程, 并且其定义域是在有限域上 GF(p) 上. 请写出用于 ECC 中的椭圆曲线方程.

解答. $E_p(a,b): y^2 = x^3 + ax + b \mod p$, 其中 p 是一个大素数, 且根的判别式 $4a^3 + 27b^2 \mod p \neq 0$

题目 78. 阐述 ELGamal 公钥密码的密钥生成算法、加密、解密算法.

解答. key_generator:

(1) 选择一个大素数 p, 并计算有限域 Z_p 的一个生成元 $g \in Z_p^*$

(2) 选择一个随机数 $x, (1<x<p-1)$, 计算 $y = g^x \pmod p$, 则: public key $= (y,g,p)$, secure key $= x$

encryption: 假如明文分组编码为长度小于 $\log_2 p$ bits 的整数 m

随机选择一个整数 $r(1<r<p-1)$, 计算 $c = g^r \pmod p$, $c' = m \cdot y^r \pmod p$

则密文 $= (c, c')$

decryption: 明文 $= \dfrac{c'}{c^x}$

证明其正确性

$$\frac{c'}{c^x} = \frac{m \cdot y^r}{g^{rx}} = \frac{m \cdot g^{rx}}{g^{rx}} = m \mod p$$

2.8 第 8 章

2.8.1 论述题

题目 79. 论述数字签名的过程.

解答.

1. 系统初始化过程

   生成数字签名方案用到的所有参数.

2. 签名生成过程

   用户利用给定的算法对消息产生签名 $s = \mathrm{Sign}(m)$.

3. 签名验证过程

   验证者利用公开的验证方法对给定消息的签名进行验证, 得出签名的有效性.$\mathrm{Ver}(s, m) = 0$ 或 1.

题目 80. 论述 ECC 数字签名方案.

解答.

1. 选择一个椭圆曲线 $E_p(a, b) : y^2 = x^3 + ax + b \mod p$

2. 选择一个生成元 G, 其阶 n 是一个大素数

3. 选择一个小于 n 的整数 nA 作为签名方 A 的私钥

4. 计算 $Pka = nA * G$ 作为 A 的公钥

5. 签名:A 随机选择一个整数 k $(1 \leq k \leq n-1)$, 对消息 m 进行如下计算得到签名值 (r, s)

   - 计算点 $kG = (x, y)$
   - 计算 $r = x \mod n$, 若 $r = 0$ 则重新选择 k
   - 计算消息的哈希值 $e = H(m)$ (转换为整数)
   - 计算 $s = k^{-1}(e + nA \cdot r) \mod n$, 若 $s = 0$ 则重新选择 k

6. 验证签名: 验证方收到消息 m 和签名 (r, s) 后, 执行以下步骤

   - 验证 r, s 是否满足 $1 \leq r \leq n-1$, $1 \leq s \leq n-1$
   - 计算 $e = H(m)$
   - 计算 $w = s^{-1} \mod n$
   - 计算 $u_1 = e \cdot w \mod n$, $u_2 = r \cdot w \mod n$
   - 计算点 $X = u_1 \cdot G + u_2 \cdot Pka = (x_1, y_1)$
   - 若 X 为无穷远点, 则验证失败; 否则计算 $v = x_1 \mod n$
   - 当且仅当 $v = r$ 时, 验证签名成功; 否则失败.

题目 81. 论述国密算法中的对称加密算法、非对称加密算法、Hash 函数.

解答.

1. SM1, 对称加密算法中的分组加密算法, 其分组长度、密钥长度都是 128bit, 算法安全保密强度跟 AES 相当, 但是算法不公开.

2. SM4, SM4 算法与 AES 算法具有相同的密钥长度、分组长度, 都是 128bit.

3. SM7, 该算法没有公开.SM7 适用于非接 IC 卡应用包括身份识别类应用 (门禁卡、工作证、参赛证), 票务类应用 (大型赛事门票、展会门

票), 支付与通卡类应用 (积分消费卡、校园一卡通、企业一卡通、公交一卡通).

4. ZUC(祖冲之算法), 它是中国自主研究的流密码算法, 该机密性算法可适用于 3GPP LTE 通信中的加密和解密, 该算法包括祖冲之算法 (ZUC)、加密算法 (128-EEA3) 和完整性算法 (128-EIA3) 三个部分. 目前已有对 ZUC 算法的优化实现, 有专门针对 128-EEA3 和 128-EIA3 的硬件实现与优化, 由国家密码管理局于 2012 年 3 月 21 日发布.

5. SM2, 它是基于椭圆曲线密码的公钥密码算法标准, 其密钥长度 256bit, 包含数字签名、密钥交换和公钥加密, 用于替换 RSA/DH/ECDSA/ECDH 等国际算法.

6. SM9, 主要用于用户的身份认证, SM9 的加密强度等同于 3072 位密钥的 RSA 加密算法, 于 2016 年 3 月 28 日发布.

7. SM3, 它是在 SHA-256 基础上改进实现的一种算法, 采用 Merkle-Damgard 结构, 消息分组长度为 512bit, 输出的摘要值长度为 256bit.

题目 82. 论述 DSA 数字签名算法, 包括密钥生成算法、签名算法、验证算法.

解答. (1) 密钥生成算法:

选取一个 160 比特的素数 q, 接着选取一个长度在 512-1024bits 的素数 p, 使得 $p-1$ 能被 q 整除, 最后选择

$$g \equiv h^{(p-1)/q} \mod p$$

其中 h 是整数, 满足 $1 < h < p-1$, 且 $g > 1$. 用户 A 选择 1 到 q 之间的随机数 x 作为其私钥, 计算

$$y \equiv g^x \mod p$$

用户的公钥为 (p, g, g, y).

(2) 签名算法:

签名者选择随机数 k, 对消息 m 计算签名值 (r, s)

$$r = (g^x \mod p) \mod q, \quad s = [h(m) + xr]k^{-1} \mod q$$

其中 h 为 Hash 函数 SHA1 算法.

(3) 签名验证算法:

接收者得到 m 和签名值 (r, s), 进行以下运算:

$$w \equiv s^{-1} \mod q, \quad u_1 \equiv h(m)w \mod q$$

$$u_2 \equiv rw \mod q, \quad v \equiv (g^{u_1}y^{u_2} \mod p) \mod q$$

如果 $r = v$, 则签名有效, 否则无效.

2.8.2　计算题

题目 83.　画出数字签名的原理图.A: 签名方, B: 验证方, 签名的消息为 m.

解答.

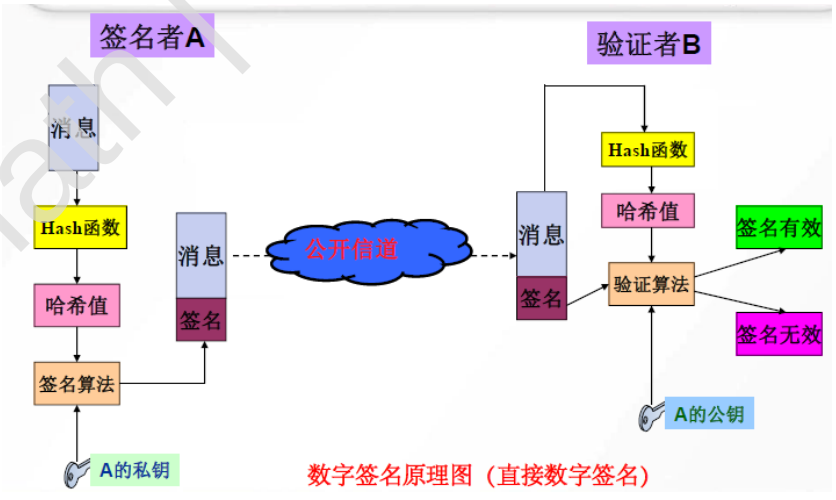

图 2.8: 题目 83 图

题目 84.　设 A: 签名方, B: 验证方, 签名的消息为 m.A 的 key paire = (Pka, Ska), Hash 函数为 H( ), 签名值为 s, 加密算法为 E, 解密算法为 D. 请给出数字签名原理的形式化描述.

解答.　step1, A:$h = H(m)$, $s = D(Ska, h)$, $m||s \to B$

step2, B:$h = H(m)$, $h' = E(Pka, s)$, if $(h == h')$ then 验证签名成功 else 验证签名不成功.

题目 85.　计算 RSA 数字签名值、验证签名. 设 RSA 算法中的 public key = $(143, 13)$, secure $key = 37$. 假设消息 m 的 Hash 值 = 16, 试计算 m 的签名值 s.

解答.　签名值:$s = h(m)^d \mod n = 16^{37} \mod 143 = 3$

因为 $143 = 11 \times 13$, 分别计算模 11 和模 13 的结果.

1. 模 11:

$$16 \equiv 5 \pmod{11}, \text{需计算} 5^{37} \mod 11.$$

由费马小定理, $5^{10} \equiv 1 \pmod{11}$, 所以 $5^{37} = 5^{10\times 3+7} \equiv 5^7 \pmod{11}$.

计算 5^7:

$$\begin{aligned}
5^2 &= 25 \equiv 3 \pmod{11},\\
5^4 &\equiv 3^2 = 9 \pmod{11},\\
5^7 &= 5^4 \times 5^2 \times 5\\
&\equiv 9 \times 3 \times 5\\
&= 135 \equiv 135 - 12 \times 11\\
&= 135 - 132\\
&= 3 \pmod{11}.
\end{aligned}$$

所以 $16^{37} \equiv 3 \pmod{11}$.

2. 模 13:

$$16 \equiv 3 \pmod{13}, \text{需计算} 3^{37} \mod 13.$$

由费马小定理, $3^{12} \equiv 1 \pmod{13}$, 所以 $3^{37} = 3^{12\times 3+1} \equiv 3^1 \equiv 3 \pmod{13}$.

所以 $16^{37} \equiv 3 \pmod{13}$.

3. 解同余方程组:

$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 3 \pmod{13} \end{cases}$$

显然 $x \equiv 3 \pmod{143}$, 因此 $s = 3$.

验证签名: 收到签名值 s 之后, 计算

$$s^e \mod n = 3^{13} \mod 143 = 16,$$

1. 模 11:

$3^{13} \mod 11$.

由费马小定理, $3^{10} \equiv 1 \pmod{11}$,

所以$3^{13} = 3^{10} \times 3^3 \equiv 1 \times 3^3 = 27 \equiv 5 \pmod{11}$.

2. 模 13:

$3^{13} \mod 13$.

由费马小定理, $3^{12} \equiv 1 \pmod{13}$,

所以$3^{13} = 3^{12} \times 3 \equiv 1 \times 3 = 3 \pmod{13}$.

3. 解同余方程组:

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{13} \end{cases}$$

设 $x = 13a + 3$, 代入第一个同余式:

$$13a + 3 \equiv 5 \pmod{11} \Rightarrow 2a \equiv 2 \pmod{11} \Rightarrow a \equiv 1 \pmod{11}.$$

取 $a = 1$, 则 $x = 13 \times 1 + 3 = 16$, 满足 $x < 143$.

所以 $3^{13} \mod 143 = 16$.

$$h(m) = 16 \equiv s^e = 16 \mod 143$$

验证签名有效.

题目 86. ElGamal 签名方案的签名值计算、验证签名计算. 设 A 选取素数 $p = 19$, Zp^* 的生产元 $g = 2$, 选取 secure key $x = 15$, 计算 $y = g^x \mod p = 2^{15} \mod 19 \equiv 12$, 则 A 的公钥 $= (p = 19, g = 2, y = 12)$.A 要签名的消息 m 的 Hash 值 $h(m) = 16$, A 选取的秘密数 $k = 11$, 试计算 A 的签名值、验证签名的过程.

解答.

$$r = g^k \mod p = 2^{11} \mod 19 = 15,$$

$$k^{-1} \mod (p-1) = 5$$

$$s = (h(m) - xr)k^{-1} \mod (p-1) = (16 - 15 \times 15) \times 5 \mod 18 = 17$$

则 A 对 m 的签名值 $(r, s) = (15, 17)$

验证签名:

$$y^r r^s \mod p = 12^{15}15^{17} \mod 19 = 5$$

$$g^{h(m)} \mod p = 2^{16} \mod 19 = 5$$

$$y^r r^s \equiv g^{h(m)} \mod p$$

成立, B 接收签名

2.8.3 填空题

题目 87. 基于离散对数问题的签名方案包括 ( )、( )、( ).

解答.

1. ElGamal 签名方案

2. DSA 签名方案

3. Schnorr 签名方案

2.9　第 10 章

2.9.1　计算题

题目 88. Needham-Schroeder 的密钥分配协议.

解答. Needham-Schroeder 密钥分配协议是一个由中心生成密钥的密分配协议, 即 Needham-Schroeder 密钥分配协议, 它是由格. 尼德哈姆和麦克. 绍罗耶德 (Roger needham,Mike Schroeder) 于 1978 年提出来的, 该议是密钥分配技术的里程碑, 之后许多协议都是由此继承而来.

(a) A-C: IDA, IDB, NA

(b) C-A: EKac (IDB, NA, Ks, Ekbc (IDA, Ks))

(c) A-B: Ekbc(IDA, Ks)

(d) B-A: EKs(NB)

(e) A-B: EKs(NB-1)

上面中 C 代表密钥分发中心, A 和 B 为通信双方, 以下解释上述五步的实现过程:

1. A 向密钥分发中心发送明文消息 IDA, IDB, NA, 意思是 “我是 A, 我想同 B 进行保密通信, 我的随机数是 NA.

2. 密钥分发中心收到了 A 的请求后为 A 生成一个会话密钥 Ks, 并给 A 一个证书 Ekbc(IDA, Ks), 并经由 A 把此证书转交 B. 由于只有 A 拥

有他同密钥分发中心之间的密钥 Kac, 因而, 只有 A 能够解密这条消息. 从而防止了有人冒充 A 向密钥分发中心提交请求所造成的风险.

3. A 向 B 转交证书 Ekbc(IDA, Ks), 由于只有 B 拥有 Kbc, 因而, 只有 B 能够解读这个证书以取得会话密钥 Ks. 这样, 攻击者即使截取证书, 也无法解读.

4. B 同 A 进行一次质询响应.

5. 响应 B 的请求, 并将随机数 NB-1, 表明 A 在线并且是可以通信的.

但这个协议也存在漏洞: 譬如 B 无法判断他从密钥分发中心经由 A 收到的 Ks 是否是新的. 因而, 一旦 Ks 泄露, 任何人都可以通过重发协议第 3 步来冒充 A. 虽然存在这个漏洞, 但其设计思想影响深远, 其中最著名的派生协议是 Kerberos 密分发协议.

题目 89. 请给出 X.509 数字证书的内容及含义.

解答.

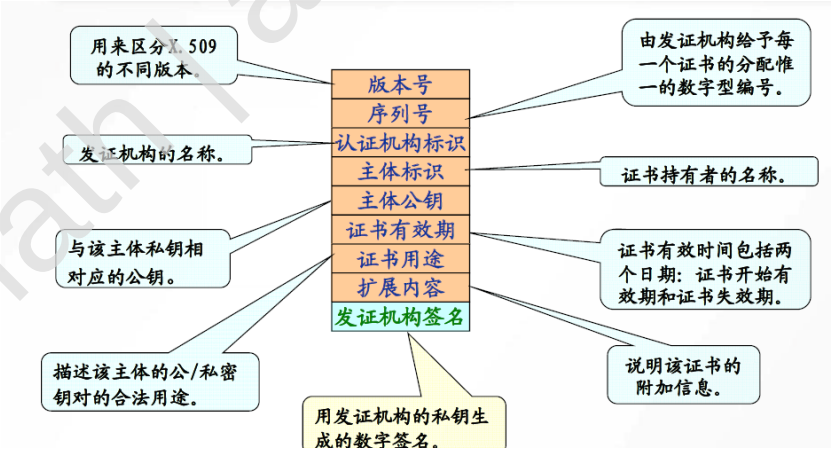

图 2.9: 题目 89 图

题目 90. 以下是用户 Tom 的数字证书, 其安全机制是保障用户 Tom 的身份和其公钥不能被分割替换. 简述其原理及用途.

版本:v3

序列号:00dea4d5fa33cf9e9e

签名算法:sha256RSA

证书颁发机构:Sangfor Technologies Inc.

主体标识:Tom

主体公钥RSA 2048:00 e8 48 96 2d fe f8 1a ec d6……

有效期:2117年4月3日 23:27:19

……

证书颁发机构签名:a9062c5c1721ff87ebcbd89df03719755560e7a0

解答.

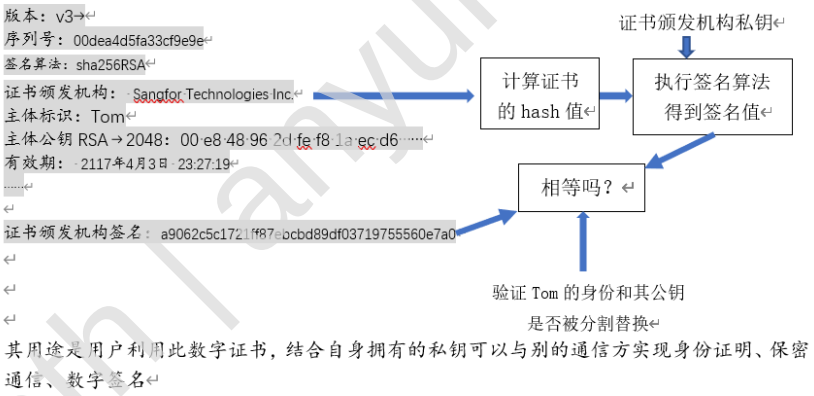

图 2.10: 题目 90 图

题目 91. 写出基于对称密码体制的由第三方参与的会话密钥分配协议:

(1) session key 由通信方发起方生成

(2) session key 由 KDC 生成

画出以上两种密钥分配方案.

解答.

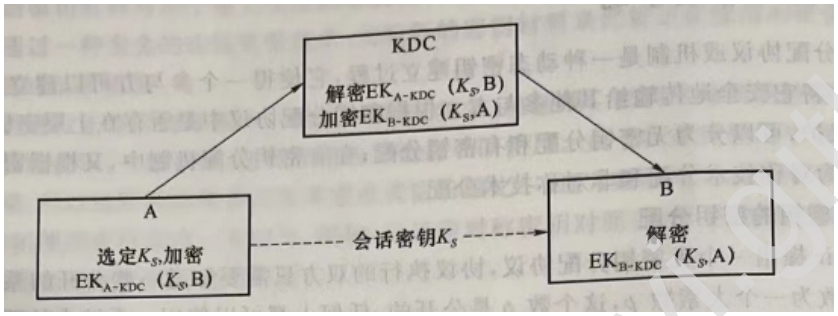

图 2.11: 题目 91 图 (1)

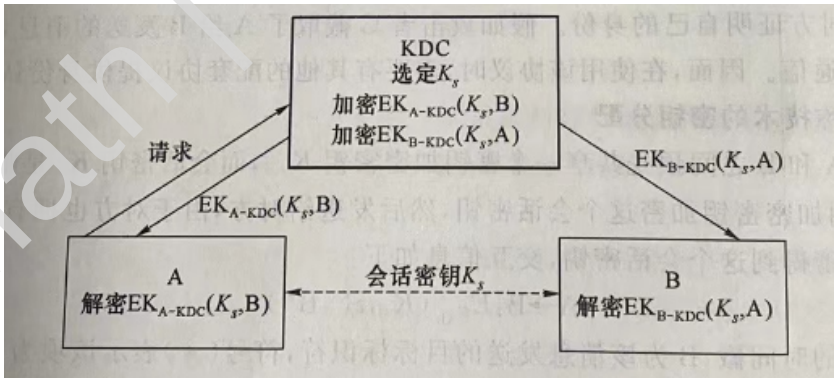

图 2.12: 题目 91 图 (2)

2.9.2　简答题

题目 92.　密钥管理的层次结构是什么?

解答.

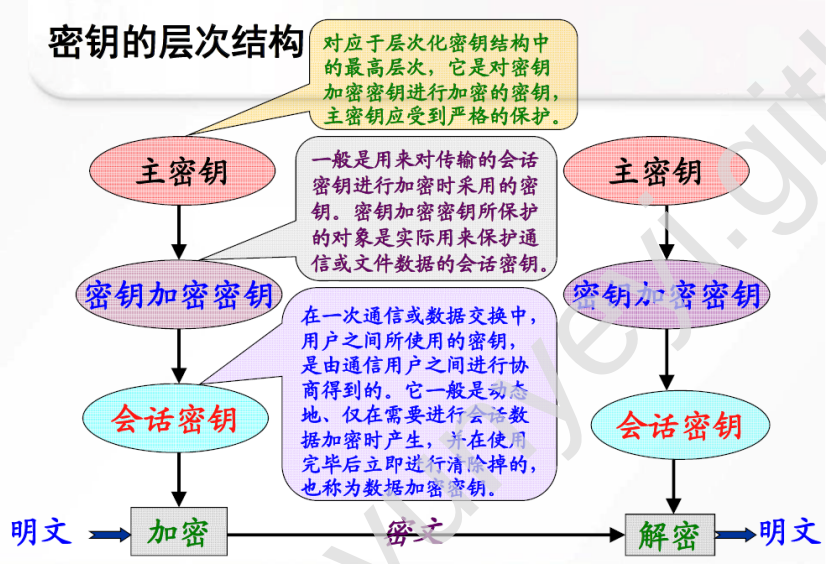

图 2.13: 题目 92 图

第三章　往年复习参考

3.1　2021 级试卷 A

题目 93. 用于密钥生成的语句为 “cryptography”, 求 Playfair 密码的 key matrix.

题目 94. 论述 RSA 密钥生成算法.

解答.

1. 选两个安全的大素数 p 和 q.
2. 计算 $n = p \times q$, $\varphi(n) = (p-1)(q-1)$, 其中 $\varphi(n)$ 是 n 的欧拉函数值.
3. 选一整数 e, 满足 $1 < e < \varphi(n)$, 且 $\gcd(\varphi(n), e) = 1$.
4. 计算 d, 满足 $d \cdot e \equiv 1 \mod \varphi(n)$, 即 d 是 e 在模 $\varphi(n)$ 下的乘法逆元, 因 e 与 $\varphi(n)$ 互素, 由模运算可知, 它的乘法逆元一定存在.
5. 以 $\{e, n\}$ 为公开钥, $\{d, n\}$ 为秘密钥.

题目 95. 论述 RSA 的加密解密算法

解答. 加密算法:$c = E(m) \equiv m^e \pmod{n}$

解密算法:$m = D(c) \equiv c^d \pmod{n}$

题目 96. 阐述 ECC 中针对用户 A 的密钥生成算法.

题目 97. 由于对称加密解密具有速度快的优点, 因此实现机密性通常使用对称密码体制, 但对称密码体制在实现时需要通信双方 A、B 共享 session

key. 如何安全地传送对称密码体制中的 key 就成为一个非常重要的问题. 现假设通信双方 A、B 都拥有自己的公钥私钥对:A(P_{ka}, S_{ka}), B(P_{kb}, S_{kb}). 如的一方 A 已拥有 session key K, 现要求不借助于第三方, 设计一个将 session key K 安全地传送给 B 的协议.

题目 98. Hash 函数有着广泛的重要用途, 其中之一就是用于消息在传输之后的完整性验证. 假设 A 发送消息 m 给接收方 B, 并且 A、B 都拥有 AES 加密的会话密钥 key. 现要求设计 A 发送消息 m 给 B 并能实现 m 的完整性验证的模型, 以形式化表达或图的形式给出模型.

题目 99. 在一个广域网的环境中, 用户使用用户名和口令的方式的登录远程服务器, 服务器的管理员给每个用户设置一个初始口令, 请利用 Hash 函数的技术实现以下安全需求:

(1) 用户口令在广域网上安全传输, 也就是说即使攻击者窃取用户网上传输的信息, 也分析不出口令;

(2) 管理员也不知道用户的口令. 设计一个方案满足上述安全需求并分析其安全性.

题目 100. 维吉尼亚加密的的明文、密文、密钥都定义在以下的字符集与编码上:

charset	a	b	c	d	e	f	g	h	i	j	k	l	m
encoding	0	1	2	3	4	5	6	7	8	9	10	11	12

charset	n	o	p	q	r	s	t	u	v	w	x	y	z
encoding	13	14	15	16	17	18	19	20	21	22	23	24	25

表 3.1: 字符集与编码对照表

现要求利用密钥 key = ”info” 对明文 “computer “进行加密之后的密文.

题目 101. 一个 3 级的 LFSR 的初始状态为 100, 其反馈函数为 $f(\quad) = b_2 \oplus b_3$, 求其 LFSR 的输出序列, 并判断其输出序列的周期.

题目 102. 次数 $n = 6$ 的多项式中, 有多少个本原多项式存在?

题目 103. 一个 4 级的 LFSR 是以生成多项式 $G(x) = x^4 + x + 1$ 来构造反馈函数. 请判断 $G(x)$ 是否是本原多项式, 以 $G(x)$ 构造的 LFSR 的反馈函数是什么? 若该 4 级的 LFSR 的初始状态为 1001, 求其输出序列, 并指出其输出的密钥流是不是 m 序列.

题目 104. 假如通信的双方为 A, B, A 为 sender, B 为 receiver, A 发送给 B 的消息为 m, A 的公钥私钥对为 (PKa, SKa), B 的公钥私钥对为 (PKb, SKb), 现要求用公钥密码体系实现 A 发送消息 m 给 B 的机密性. 用形式化的语言描述实现的步骤.

题目 105. 假如通信的双方为 A, B, A 为 sender, B 为 receiver, A 发送给 B 的消息为 m, A 的公钥私钥对为 (PKa, SKa), B 的公钥私钥对为 (PKb, SKb), 现要求用公钥密码体系实现 A 发送消息 m 给 B 的抗否认性. 用形式化的语言描述实现的步骤.

题目 106. 写出 RSA 算法的共模攻击算法.

题目 107. 椭圆曲线 $E_{23}(1,1)$, $E : y^2 = x^3 + x + 1 \mod 23$, 设 $P = (3, 10)$, $Q = (9, 7)$. 求

(1) $R = (x_3, y_3) = P + Q$

(2) $2P$

题目 108. ECC 上的椭圆 $E_{11}(1,6) : y^2 = x^3 + x + 6 \mod 11$, 假设 $G = (2, 7)$ 为生成元.

(1) 利用 G 生成椭圆曲线上的所有点的集合.

(2) 求 G 的阶.

题目 109. 设 A: 签名方, B: 验证方, 签名的消息为 m.A 的 key paire = (Pka, Ska), Hash 函数为 H( ), 签名值为 s, 加密算法为 E, 解密算法为 D. 请给出数字签名原理的形式化描述.

题目 110. 请给出 X.509 数字证书的内容及含义.

题目 111. 以下是用户 Tom 的数字证书, 其安全机制是保障用户 Tom 的身份和其公钥不能被分割替换. 简述其原理及用途.

> 版本:v3
> 序列号:00dea4d5fa33cf9e9e
> 签名算法:sha256RSA
> 证书颁发机构:Sangfor Technologies Inc.
> 主体标识:Tom
> 主体公钥RSA 2048:00 e8 48 96 2d fe f8 1a ec d6……
> 有效期:2117年4月3日 23:27:19
> ……
> 证书颁发机构签名:a9062c5c1721ff87ebcbd89df03719755560e7a0

题目 112. 设计利用 DES-CBC 模式生成消息 M 的消息认证码 (MAC) 的形式化描述, 假如消息 M 分成了 N 个分组 D1, D2, ..., DN.

题目 113. 现有一个置换 $\sigma = (1423)$, 计算利用 σ 对 “security” 进行周期置换加密的结果.

题目 114. 仿射加密 $c = k_1 \cdot m + k_2 \mod 26$ 中的明文 m、密文 c、密钥 (k_1, k_2) 皆定义在如下的字符集及编码上:

现取密钥 $(k_1, k_2) = (3, 4)$, 要求计算明文 “aust” 经过该仿射加密后的密文.

题目 115. 椭圆曲线加密 (ECC) 中的椭圆曲线一般是指一种简单的维尔斯特拉斯方程, 并且其定义域是在有限域上 GF(p) 上. 请写出用于 ECC 中的椭圆曲线方程.

charset	a	b	c	d	e	f	g	h	i	j	k	l	m
encoding	0	1	2	3	4	5	6	7	8	9	10	11	12

charset	n	o	p	q	r	s	t	u	v	w	x	y	z
encoding	13	14	15	16	17	18	19	20	21	22	23	24	25

表 3.2: 字符集与编码对照表

题目 116. 证明 DES 的互补性会使 DES 在选择明文攻击下所需的工作量减半.

题目 117. 为什么二重 DES 并不像人们想象的那样可提高密钥长度到 112 比特而相当 57 比特.

题目 118. 在 GF(2) 上的一个多项式 $G(x)$ 是本原多项式要满足的条件有哪些?

$$G(x) = \sum_{i=0}^{n} a_i x^i$$

题目 119. public key cryptosystem(公钥密码体系, 或非对称密码体系) 的思想主要包括哪些方面?

题目 120. 论述数字签名的过程.

题目 121. 论述 ECC 数字签名方案.

题目 122. 论述密码学发展史上两个重要的里程碑事件.

题目 123. 什么是 Hash 函数的弱碰撞攻击? 什么是强碰撞攻击?

3.2　2022 级模拟卷

题目 124. 计算置换 $\delta = (135)(24)$ 的逆置换 $\delta' =$( ), 并利用逆置换 δ' 解密用 δ 作为密钥进行周期置换加密的密文串"evuniytrsi" 所对应的明文为 ( ).

题目 125. 1949 年, 信息论鼻祖 Shannon 发表在《贝尔实验室技术杂志》第 28 卷第 4 期 (第 656~715 页) 上的经典论文 ( ), 他将 Information Theory

引入到密码学中, 为密码学的发展奠定了坚实的理论基础. 此为现代密码学开始的标志.

题目 126. 传统密码学的第二阶段是以机械为工具的近代密码, 近代密码的主要形式有 ( )、( )、( ).

题目 127. 基于离散对数问题的签名方案包括 ( )、( )、( ).

题目 128. 信息安全的五大目标 CIAAN, 分别是指 ( )、( )、可用性 Availability、认证性 Authentication、( ).

题目 129. AES 加密过程主要包括 ( )、( )、( )、( ).

题目 130. 什么是 Hash 函数的弱碰撞攻击? 什么是强碰撞攻击?

题目 131. 椭圆曲线 $E_{23}(1,1)$, $E: y^2 = x^3 + x + 1 \mod 23$, 设 $P = (3, 10)$, $Q = (9, 7)$. 求

(1) $R = (x_3, y_3) = P + Q$

(2) $2P$

题目 132. 计算上的安全性是指若破解一个密码系统是可行的, 但使用已知的算法和现有的计算机不可能完成攻击所需要的计算量, 则称该密码体制是计算上安全的. 当前的密码体制都属于计算上的安全性 (多数是基于数学难题求解), 试举一个例子加以说明.

题目 133. 为什么二重 DES 并不像人们想象的那样可提高密钥长度到 112 比特而相当 57 比特.

题目 134. 论述 RSA 的加密解密算法

题目 135. 计算 RSA 数字签名值、验证签名. 设 RSA 算法中的 public key = (143, 13), secure key = 37. 假设消息 m 的 Hash 值等于 16, 试计算 m 的签名值 s.

题目 136. 现有一个置换 $\delta = (1423)$, 计算利用 δ 对 “security” 进行周期置换加密的结果.

3.3　重难点

题目 137.　为什么二重 DES 并不像人们想象的那样可提高密钥长度到 112 比特, 而相当 57 比特?

题目 138.　一个 3 级的 LFSR 的初始状态为 100, 其反馈函数为 $f(\quad) = b_2 \oplus b_3$, 求其 LFSR 的输出序列, 并判断其输出序列的周期.

题目 139.　论述 ECC 数字签名方案.

题目 140.　ECC 的一个椭圆曲线 $E_{23}(-4,1) : y^2 = x^3 - 4x + 1 \mod 23$, $P(4,7)$、$Q(2,1)$ 是椭圆曲线上的两个点. 求:

(1) $R = (x_3, y_3) = P + Q$

(2) $2P$

题目 141.　论述数字签名的过程.

题目 142.　请给出 X.509 数字证书的内容及含义.

题目 143.　什么是 Hash 函数的弱碰撞攻击? 什么是强碰撞攻击?

题目 144.　设 A: 签名方, B: 验证方, 签名的消息为 m.A 的 key paire = (Pka, Ska), Hash 函数为 H( ), 签名值为 s, 加密算法为 E, 解密算法为 D. 请给出数字签名原理的形式化描述.

题目 145.　假如通信的双方为 A, B, A 为 sender, B 为 receiver, A 发送给 B 的消息为 m, A 的公钥私钥对为 (PKa, SKa), B 的公钥私钥对为 (PKb, SKb), 现要求用公钥密码体系实现 A 发送消息 m 给 B 的抗否认性. 用形式化的语言描述实现的步骤.

题目 146.　假如通信的双方为 A, B, A 为 sender, B 为 receiver, A 发送给 B 的消息为 m, A 的公钥私钥对为 (PKa, SKa), B 的公钥私钥对为 (PKb, SKb), 现要求用公钥密码体系实现 A 发送消息 m 给 B 的机密性. 用形式化的语言描述实现的步骤.

题目 147.　Hash 函数有着广泛的重要用途, 其中之一就是用于消息在传输之后的完整性验证. 假设 A 发送消息 m 给接收方 B, 并且 A、B 都拥有

AES 加密的会话密钥 key. 现要求设计 A 发送消息 m 给 B 并能实现 m 的完整性验证的模型, 以形式化表达或图的形式给出模型.

题目 148. 用维吉尼亚密码加密明文 “please keep this message in secret” , 使用的密钥为 “computer” , 试求其密文.

题目 149. 次数 $n = 6$ 的多项式中, 有多少个本原多项式存在?

题目 150. 给出下列 Hash 算法的算法属性:

1. MD5

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

2. SHA1

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

3. SHA256

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

4. SHA512

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

5. RIPEMD-160

   blocksize=( ), Rounds=( ), iterations/R=( ), hash-value-size=( );

题目 151. 阐述 ECC 中针对用户 A 的密钥生成算法.