一 概述

1. 信息安全三要素

2. 古典密码

3. 密码分析

- 分析方法

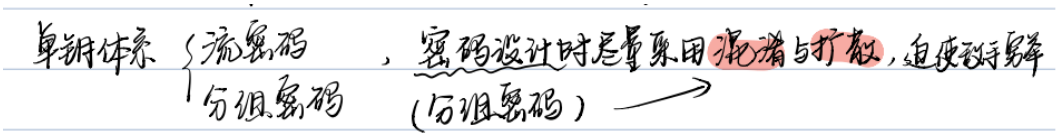
- 密码可能经受的不同水平的攻击

CPA 安全：CPA（Chosen-Plaintext Attack），选择明文攻击

- 密码可能经受的不同水平的攻击

4. 密码体制分类

1） 单钥体制：加密密钥和解密密钥相同主要问题



2）

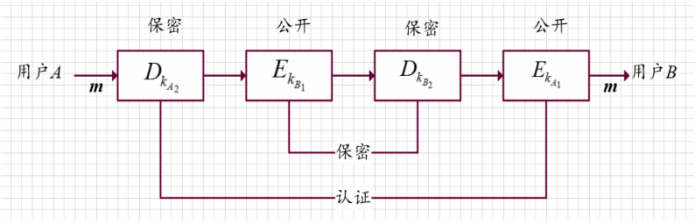
3）双钥体制：加密密钥和解密密钥不同　Diffie 和 Hellman 1976 年首次提出，用户有公钥 k1，私钥 k2，公钥可以公开从而将加密和解密能力分开 安全性：可实现对 A 所发消息的验证

双钥认证体制： 用户A以自己的秘密钥k_{A_2}对消息 m 进行A的专用变换$D_{k_{A_2}}$，A计算密文：$c = D_{k_{A_2}}(m)$送给用户B，B验证 m：

$$m = E_{k_{A_1}}(c) = E_{k_{A_1}}(D_{k_{A_2}}(m)) \qquad (5)$$

双钥保密和认证体制

为了要同时实现保密性和确证性，要采用双重加、解密，如图5 所示：



二 流密码

1. 基本概念、分类

流密码是将

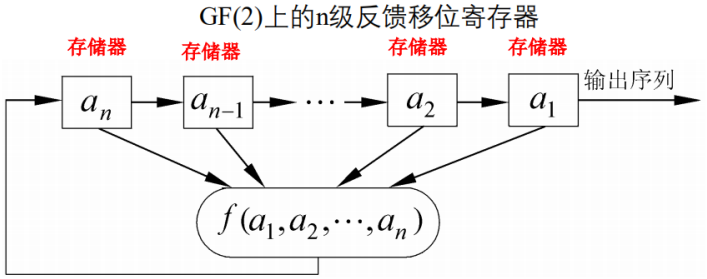
流密码强度完全依赖于

同步流密码：

自同步流密码：

n 级反馈移位寄存器

GF(2)上一个 n 级反馈移位寄存器由 n 个二元存储器与一个反馈函数 $f(a_1,a_2,\ldots,a_n)$组成。



例 图3 是一个3级反馈移位寄存器，其初始状态为$(a_1,a_2,a_3)=(1,0,1)$，输出见右下表。

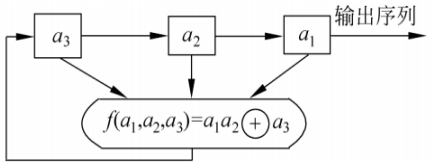


图 一个3级反馈移位寄存器

即输出序列为101110111011...，周期为4。

表 一个3级反馈移位寄存器的状态和输出

状态 (a_3,a_2,a_1)	输出
1 0 1	1
1 1 0	0
1 1 1	1
0 1 1	1
1 0 1	1
1 1 0	0

3. 线性反馈移位寄存器(LFSR)

表达式？：

LFSR 输出序列的性质：完全由其反馈函数决定。

n 级 LFSR 状态数：

n 级 LFSR 的状态周期：

输出序列的周期=状态周期，

m 序列

LFSR 的特征多项式： $p(x)=1+c_1x+\ldots+c_{n-1}x_{n-1}+c_nx_n$

4. m 序列

m 序列的伪随机性性质？：

游程：连续的 0 或者 1 的个数

GF(2)上周期为 T 的序列{ai }的自相关函数

设序列{a_i}满足线性递推关系：$a_{h+n} = c_1 a_{h+n-1} \oplus c_2 a_{h+n-2} \oplus \cdots \oplus c_n a_h$

- **M 序列的破译**

三 分组密码

1. 基本概念

1) **分组密码：**

2) 分组密码优缺点、与流密码对比：

2. 对分组密码的攻击

最主要的威胁就是

如果某一组明文/密文对（*m*，*c*）使得方 程 *m*=*D*(*c*, *z*)特别容易解出 *z*，*m* 就

称为一个弱明文， z 就称为一个弱密钥。加解密算法（E，D）不能存在弱明文和弱密钥

为了抵抗已知明文攻击（甚至选择明文攻击），分组密码应该满足的性质

混淆性：

扩散性：

（1）

（2）

高非线性度：

这里举的两个例子，异或和模 2^n 加

- 分组密码设计

替换/置换网络（SPN）：是啥？有啥用？ 典型代表？

Feistel 网络不能用作分组密码算法。原因？

DES 算法原理：

AES 的明文分组长度是可变的：

AES 的密钥长度：

三重 DES： 先加密后解密在加密

四类工作模式比较和选用

四

公钥体制的基本原理是
陷门单向函数(Trapdoor one-way function)，

单向函数举例：

RSA

- 密钥生成、加密、解密、安全性
    - 基本 RSA 的一个安全性漏洞：

公钥密码 RSA

背包密码（可能出计算）

ElGamal

特点：

五

- 杂凑函数

  生日攻击告诉我们：

- 数字签名应具有的性质：

  - 公钥密码的签名方案（一）

  私钥签名，公钥验证

- 公钥密码的签名方案（二）

- RSA 数字签名

- ElGamal 数字签名

- Schnorr 数字签名（看一看）

六

- Shamir 的秘密共享门限方案

习题 设：p=17；n=5； t=3；
(ID(1)， h(ID(1)))=(1， 8)；
(ID(2)， h(ID(2)))=(2， 7)；
(ID(3)， h(ID(3)))=(3， 10)；
(ID(4)， h(ID(4)))=(4， 0)；
(ID(5)， h(ID(5)))=(5， 11)。
当第1位~第3位参与者同时到场，求共享的秘密

$$h(x) = a_0 + a_1 x + a_2 x^2 \pmod{17}$$

a0=13,a1=-7,a2=2,
如何判断有假的？

- 不经意传输(OT)

- 零知识证明

密钥协商

1. 基于对称密钥技术的密钥协商
分放双方方案

发送一方方案：

存在的安全性问题：

1.一方方案的中间人攻击：

防范策略？并画图

DH 密钥协商

该方法同样也存在中间人攻击：