密 码 学

密码学复习课

网络空间安全学院
朱 丹
zhudan@nwpu.edu.cn

密码学课程复习

- 信息安全概述
- 密码学基本概念
- 序列密码（线性/非线性反馈移位寄存器）
- 分组密码（AES、DES的算法流程、密钥扩展流程，不同算法之间的比较）
- 公钥密码（RSA、 DH、ElGamal、ECC、SM2 ）
- HASH函数（SHA-1、SM3）
- 数字签名（利用公钥算法的签名及DSA）
- 认证（认证和加密、签名的区别，如何应用密码技术进行认证）
- 密钥管理（密钥管理的层次结构，公钥管理的方式（公钥证书））
- 侧信道攻击（类型，不同算法的攻击方式）
- 同态加密（同态概念、性质）

信息安全概述

- 信息安全的属性
- 网络空间安全的概念和范畴
- 网络空间安全的属性
- 密码都能解决哪些安全需求

网 络 空 间

Cyberspace

信 息 化 特 征

Cyberspace 是信息时代人类般以生存的信息环境，是所有信息系统的集合。它以计算机和网络系统实现的信息化为特征

网 络 互 联 特 征

信息空间突出了信息化的特征和核心内涵是信息，网络空间突出了网络互联的特征

复 杂 系 统 特 征

从信息论角度来看，系统是载体，信息是内涵。网络空间是所有信息系统的集合，是一种复杂巨系统

信 息 安 全 特 征

网络空间安全的核心内涵仍是信息安全。没有信息安全，就没有网络空间安全

http://www.cnitpm.com/pm1/57481.html

网络空间安全

Cybersecurity

01

机　密　性

只有授权用户可以获取信息，即信息不应泄漏给非授权用户

02

完　整　性

信息在存储和传输的过程中，不被非法授权修改和破坏，保证数据的一致性

03

真　实　性

对信息的来源进行判断，能对伪造来源的信息予以鉴别

04

可　用　性

保证合法用户对信息和资源的使用不会被不正当地拒绝

05

不可否认性

信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为

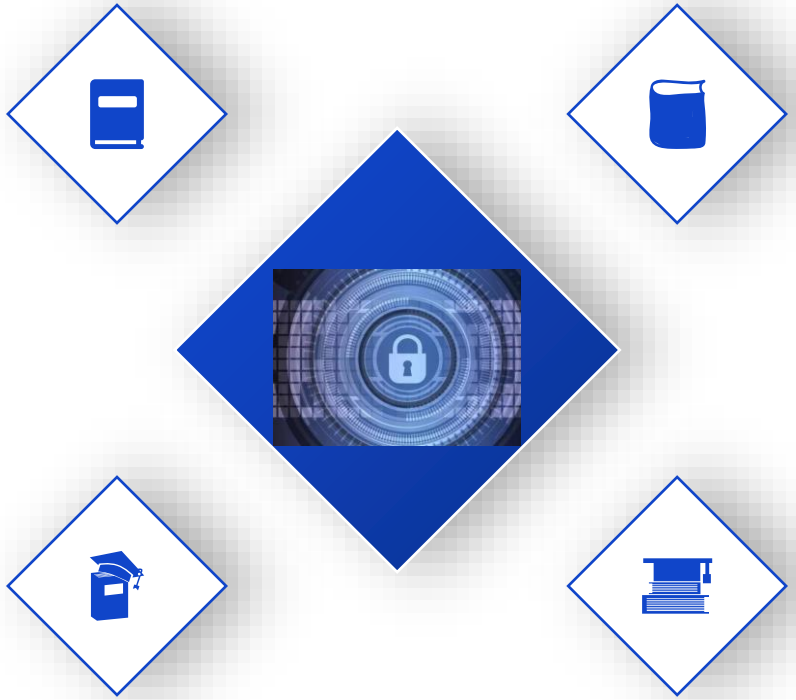
密码学解决的问题

机　密　性

防止敏感信息泄漏

完　整　性

防止关键信息被篡改



真　实　性

防止身份或数据假冒

不 可 否 认 性

防止攻击行为抵赖

凡是有机密性、真实性、完整性、不可否认性安全需求的，都可以用密码技术解决

密码学基本概念

- 密码学的范畴、密码的基本概念
- 密码的发展历程、代表性人物和事件
- 密码体制的分类方法
- 密码体制的安全级别
- 密码分析方法的分类
- 置换、替代密码
- 典型的经典密码算法
- 单表和多表替代密码的破译分析

密码学的发展 – 阶段划分

Developments - Stages

1

古 典 密 码

从古代到19世纪末 - 凯撒密码、维吉尼亚密码

2

近 代 密 码

从20世纪初到1949年 - 恩尼格玛(Enigma)密码机

3

现 代 密 码

从1949年到1976年 – 序列密码、DES

4

公 钥 密 码

从1976年开始 – RSA、ECC

5

下 一 阶 段 ？

后量子密码

密码学的发展 – 第二阶段

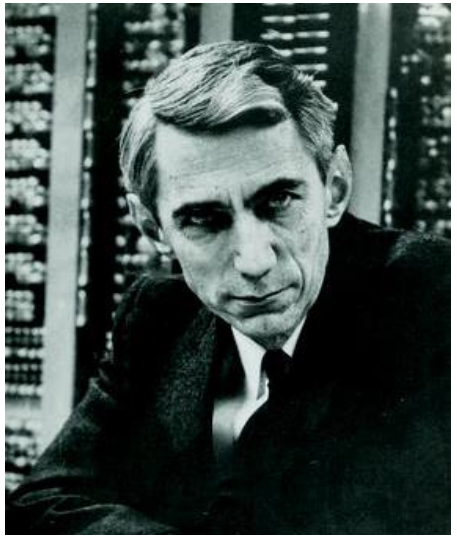
对称密码学早起发展时期（1949– 1975）

1949年，Shannon发表题为《保密系统的通信理论》（Communication Theory of Secrecy Systems）的论文

该文为对称密码系统建立了理论模型

该文创立的信息论为密码学奠定了理论基础

从此，密码学发展成为一门真正的科学



Claude E. Shannon

密码学的发展 – 第三阶段

现代密码学发展时期（1976 – 1996）

1976年，Diffie和Hellman发表题为《密码学的新方向》（New Directions in Cryptography）的论文

该文引入了公钥密码的概念

1977年，美国制定了数据加密标准（Data Encryption Standard，DES）

公钥密码和DES标志着现代密码学的诞生

美国计算机协会（ACM）将2015年的图灵奖授予Sun Microsystems的前首席安全官惠特菲尔德·迪菲（Whitfield Diffie）以及斯坦福大学电气工程系名誉教授马丁·赫尔曼（Martin Hellman），以表彰他们在现代密码学中所起的至关重要的作用。

密码算法的要求

不可破译性：理论和实际上都是不可破译的

算法覆盖性：覆盖整个密钥空间

一切秘密寓于密钥之中（Kerckhoffs原则）

实现性能：便于实现，性能好

奥古斯特·柯克霍夫在19世纪提出：密码系统应该就算被所有人知道系统的运作步骤，仍然是安全的。

克劳德·艾尔伍德·香农有句近似的话「敌人知道系统」，称为香农公理。

Kerckhoffs

密码算法分类

Classification

密码体制安全性

计　　算　　安　　全

当前计算条件（时间和存储器资源）无法满足密码破译的需求

1

可　　证　　明　　安　　全

把密码体制的安全性归约为某个经过深入研究的数学难题

2

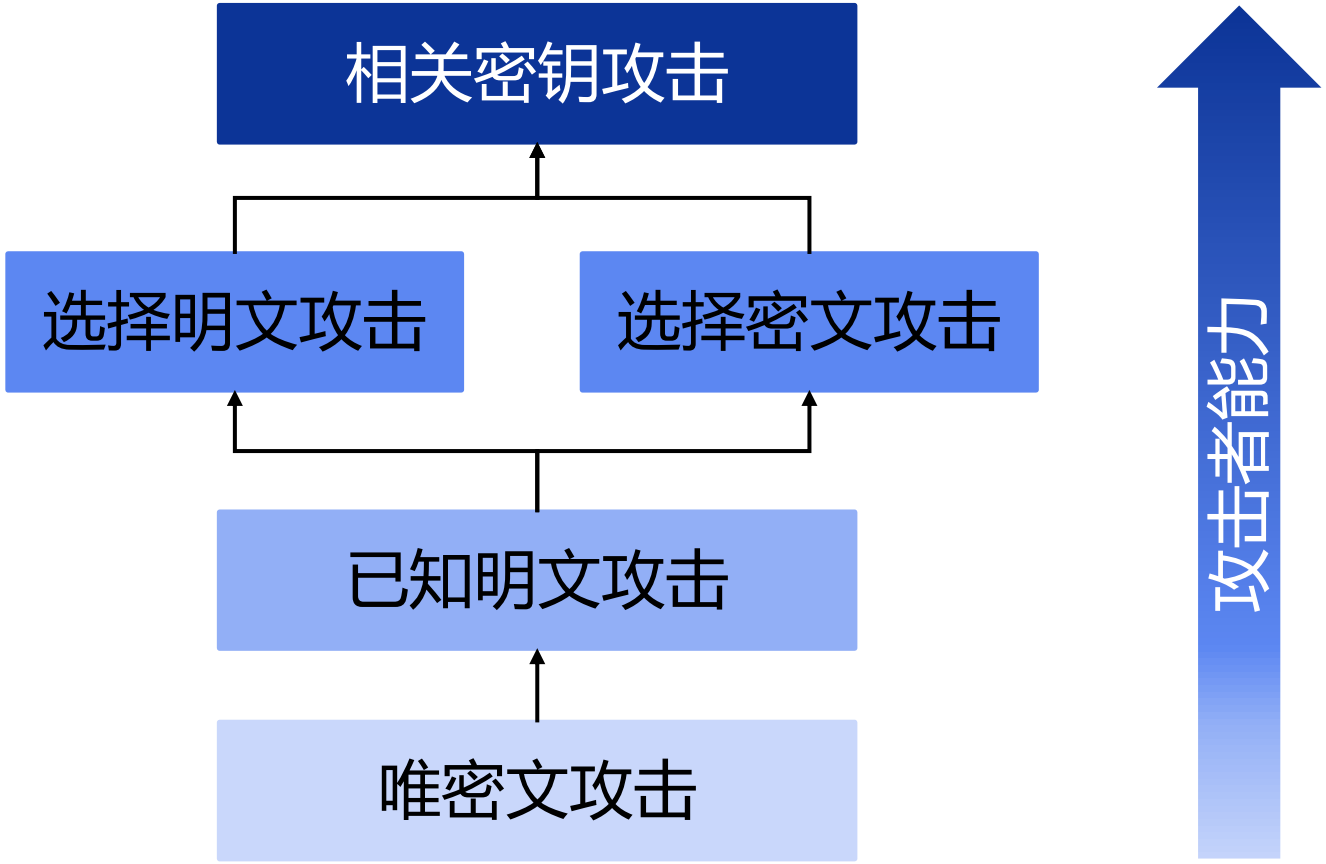
无　　条　　件　　安　　全

密码分析者具有无限的计算能力，密码体制也不能破译

3

主要任务：破译密码或伪造消息

按照攻击者掌握的信息类别（攻击者能力）分为：



密 码 分 析 学

Cryptanalysis

穷 举 攻 击

暴力攻击

统 计 攻 击

利用明文、密文之间的内在统计规律来破译

解 析 攻 击

数学分析攻击，破译密码算法所依赖的数学问题

代 数 攻 击

将密码破译问题归结为有限域上的低次多元方程组来求解

置 换 与 替 代

Permutation and Substitution

01 置 换 密 码

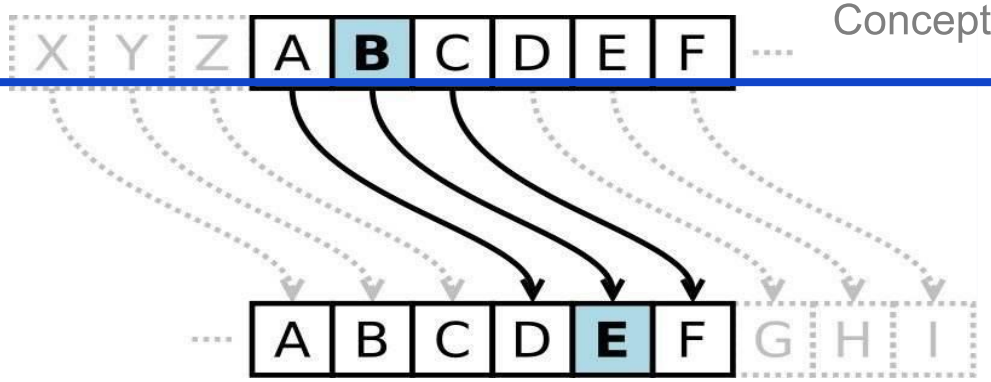
置换密码算法的原理是不改变明文字符，只将字符在明文中的排列顺序改变，从而实现明文信息的加密。置换密码有时又称为换位密码

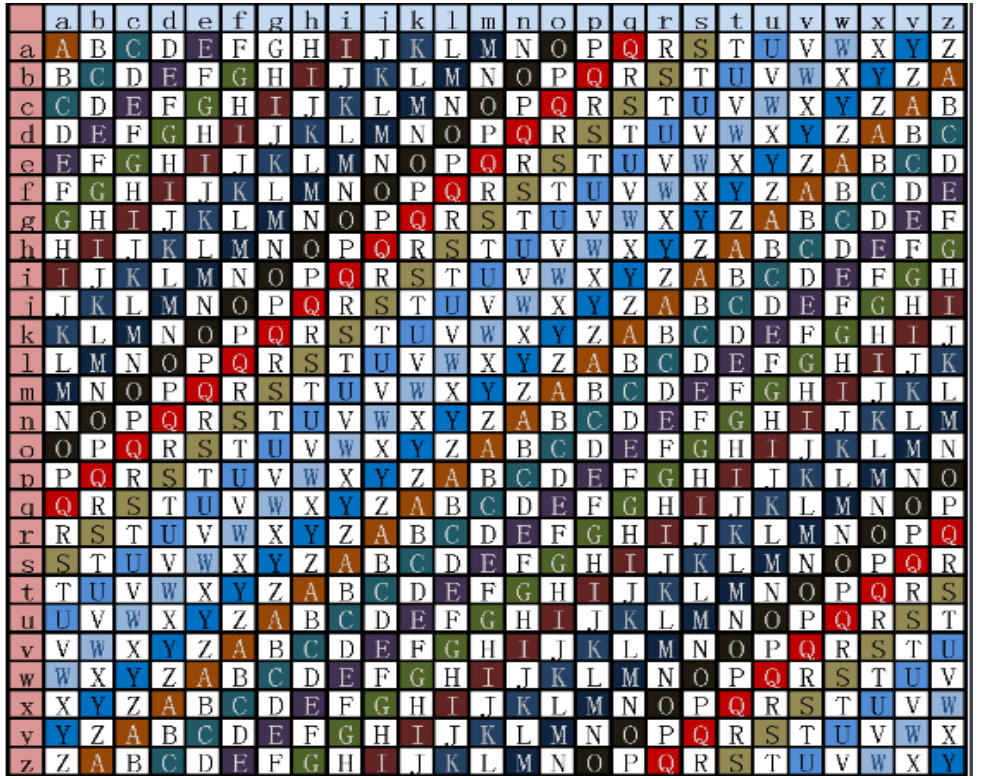
02 替 代 密 码

替代密码替代密码算法的原理是使用替代法进行加密，就是将明文中的字符用其它字符替代后形成密文。加密后明文字符的形态会发生变化

经典密码算法

- 加法密码
- 乘法密码
- 仿射密码
- 凯撒密码
- 维吉利亚密码
- Vernam密码





英文字母频率分布

Statistics of English Characters

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
频率	8.167	1.492	2.782	4.253	12.702	2.228	2.015	6.094	6.966	0.153	0.722	4.025	2.406
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
频率	6.749	7.507	1.929	0.095	5.987	6.327	9.056	2.758	0.978	2.360	0.150	1.974	0.074

Londoners are under starter's orders as the city gets ready for the Olympic Games, which will begin one year today. To mark the start of the 366-day countdown (2012 is a leap year), special events are planned for today. The design of the Olympic medals will be unveiled tonight in a live ceremony from Trafalgar Square. Over at the brand new Aquatics Centre, Britain's star diver Tom Daley is going to perform an official launch dive into the Olympic pool. With this building, the organizers have attempted to give London a landmark to rival Beijing's Water Cube from 2008. It was designed by the prestigious architect Zaha Hadid and has a wave-like roof that is 160 meters long. Today's special events are designed to arouse interest in the Olympics around the world and to encourage British fans too. Many failed to get Olympic tickets in the recent sales process. According to a new survey for the BBC, 53% of Londoners think the process was "not fair". But the same survey found support is growing for London 2012. Of the 1,000 people surveyed, 73% said they backed the Games - up from 69% in 2006. Olympics minister Hugh Robertson said: "We are under budget and ahead of time and as a nation we have a reputation of really getting behind these big events."

粗糙度(Measure of Roughness, M.R)定义为每个密文字母出现的频率与均匀分布时每个字母出现的频率之差的平方和

设各密文字母出现的频率为p_i (i = 0, 1, 2, …, 25)，则有$\sum_{i=0}^{25} p_i = 1$

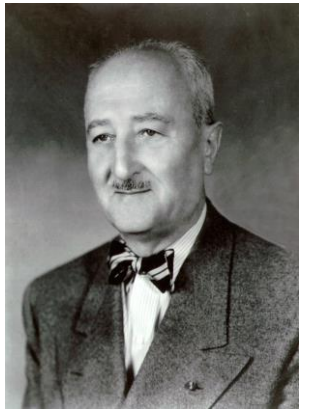
对于英文报文，则n = 26。均匀分布下，每个字母出现的概率为1/26

$$M.R = \sum_{i=0}^{25} (p_i - \frac{1}{26})^2$$

$$= \sum_{i=0}^{25} p_i^2 - \frac{1}{26} = \sum_{i=0}^{25} p_i^2 - 0.0385$$

重 合 指 数

重合指数（Index of Coincidence, IC）的概念由Friedman于1918年提出，其论文《重合指数及其在密码学中的应用》是1949年以前最有影响的密码学文献



William F. Friedman

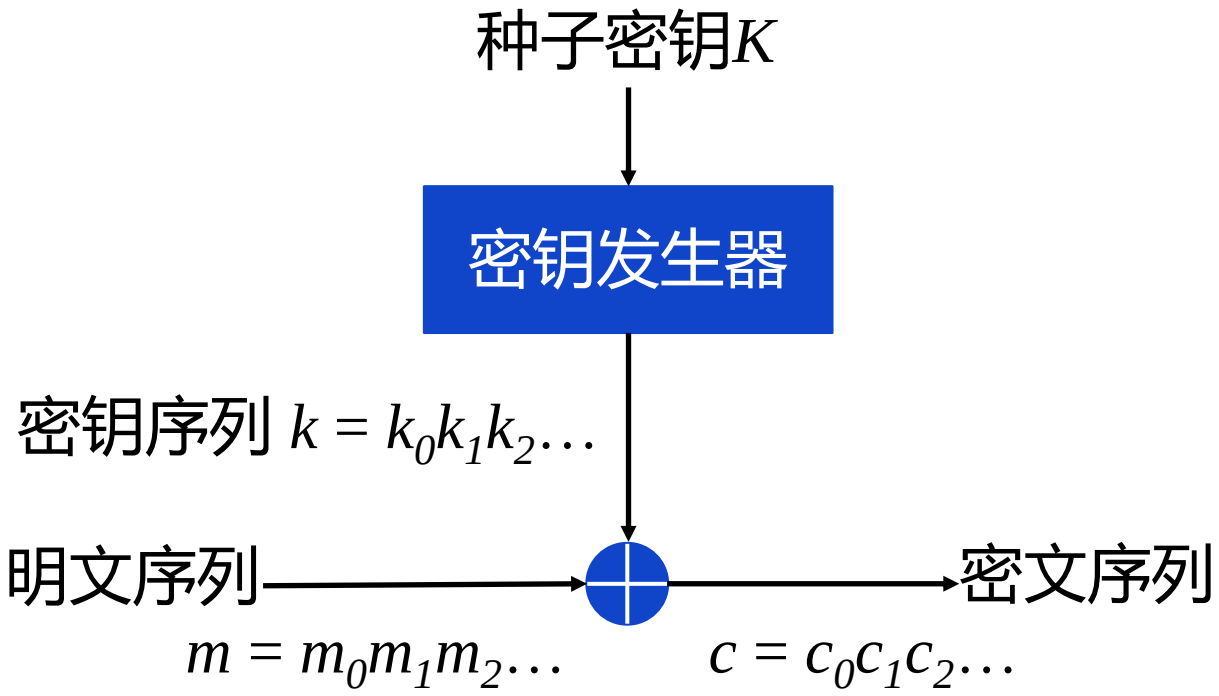
定义：设某种语言由n个字母组成，第i个字母出现的概率为p_i，$0 \leq i < n$，重合指数是指两个随机字母相同的概率：

$$IC = \sum_{i=0}^{n-1} p_i^2$$

序 列 密 码

- 序列密密码的基本概念
- 序列密码的分类及各自特点
- 线性反馈移位寄存器
- 线性反馈移位寄存器的分析破译原理
- 非线性反馈移位寄存器

- 将一串较短的种子密钥K通过密钥流发生器扩展成足够长的伪随机密钥流$k = k_0k_1k_2\ldots$
- 加密变换：$c_i = m_i \oplus k_i$
- 解密变换：$m_i = c_i \oplus k_i$



同步序列密码（Synchronous Stream Cipher）

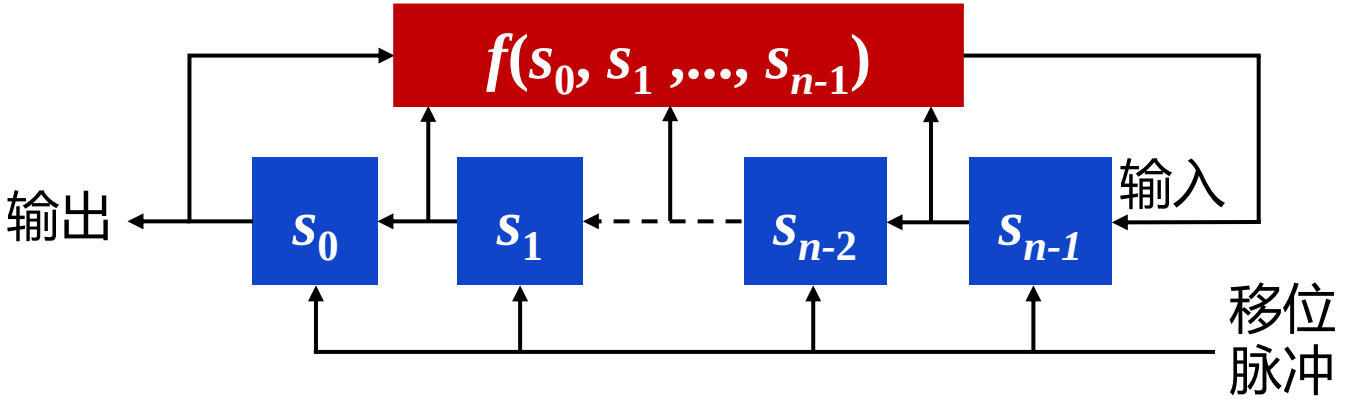
密钥序列产生算法与明文（密文）无关，通信双方必须保持精确的同步，失步将导致无法解密

自同步序列密码（Self- Synchronous Stream Cipher）

密钥序列产生算法与明文（密文）相关，加解密出错会造成错误的有界传播

线性反馈移位寄存器

- 称每一时刻移位寄存器的取值$S = (s_0, s_1, \ldots, s_{n-1})$为一个状态
- 移位寄存器在输出同时将新值要送入s_{n-1}，其值要通过函数$f(s_0, s_1, \ldots, s_{n-1})$计算产生，该函数为反馈函数
- 若反馈函数是 $s_0, s_1, \ldots, s_{n-1}$的线性函数，则称为线性反馈移位寄存器，否则称为非线性反馈移位寄存器

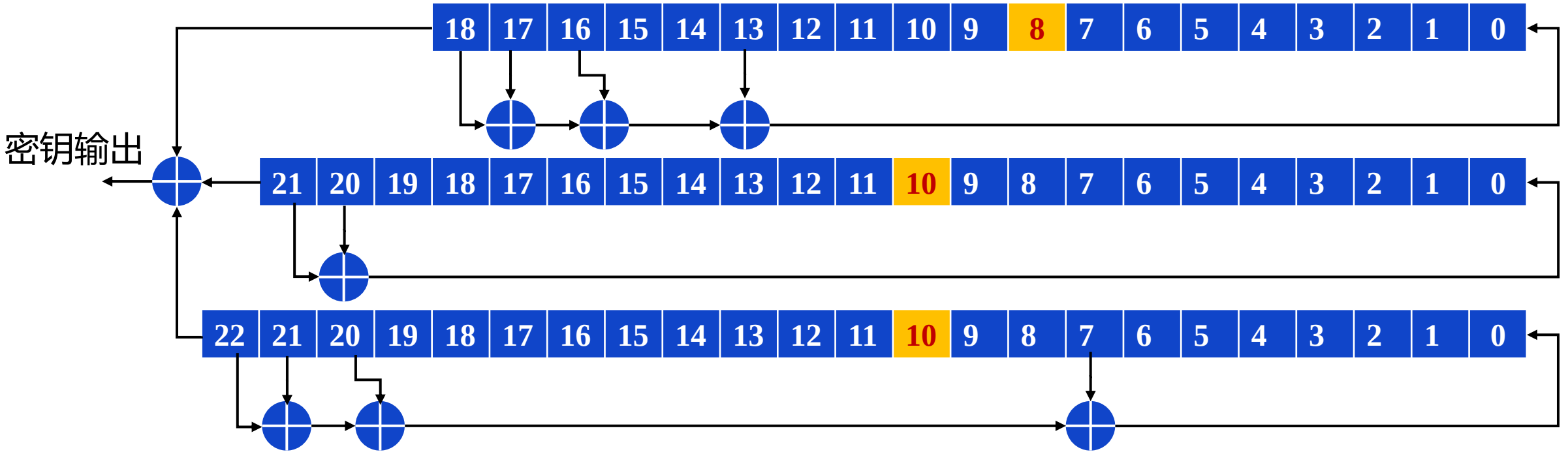


线性反馈移位寄存器

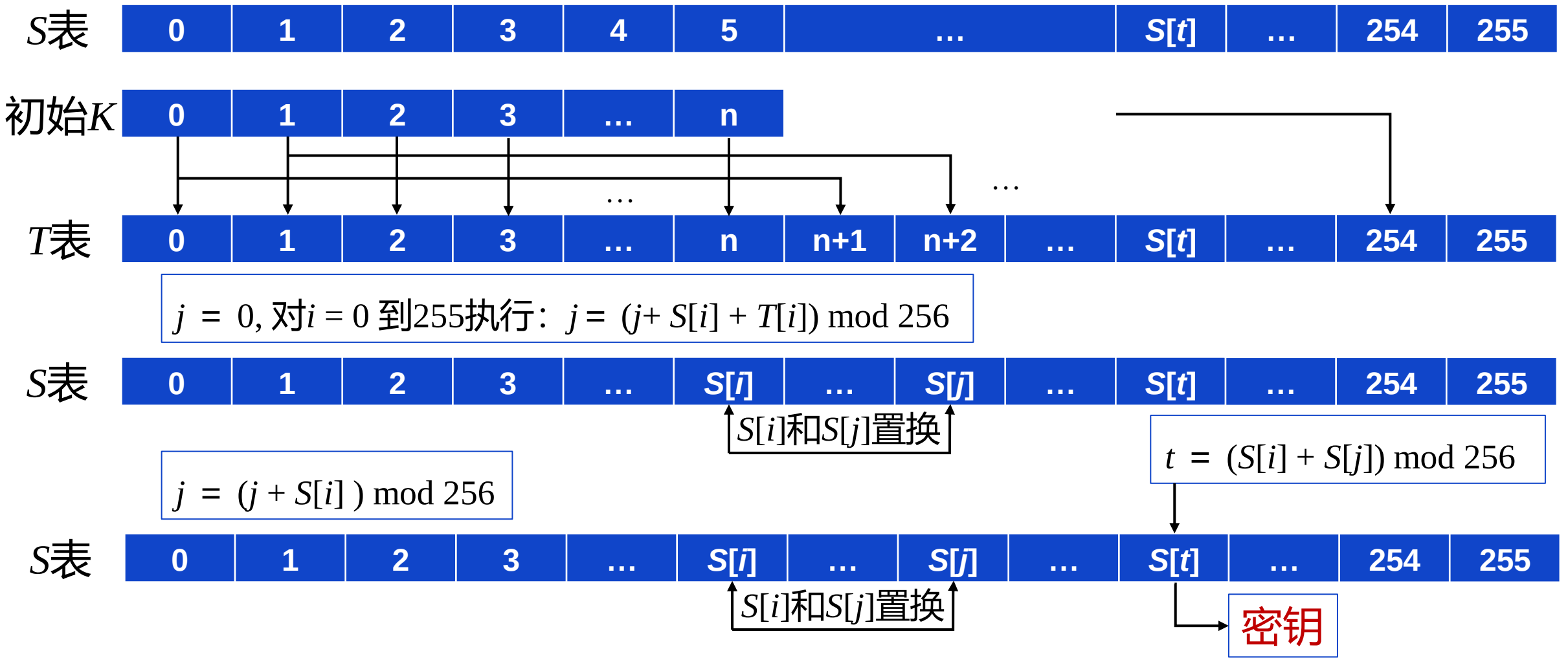
- n级线性移位寄存器最多有2^n个不同的状态
- 若其初始状态为零，则其后续状态恒为零。若其初始状态不为零，则其后续状态也不为零
- 因此，n级线性移位寄存器的状态周期 $\leq 2^n - 1$，其输出序列的周期 $\leq 2^n - 1$
- 选择合适的本原多项式（对应于反馈系数）可使线性移位寄存器的输出序列周期达到最大值$2^n - 1$
- 称此时的输出序列为最大长度线性移位寄存器输出序列，简称为m序列

A5序列密码算法

- A5算法的种子密钥为64位，作为三个线性移位寄存器的初始状态
- 每个时钟周期产生一个比特的密钥，多周期形成密钥流

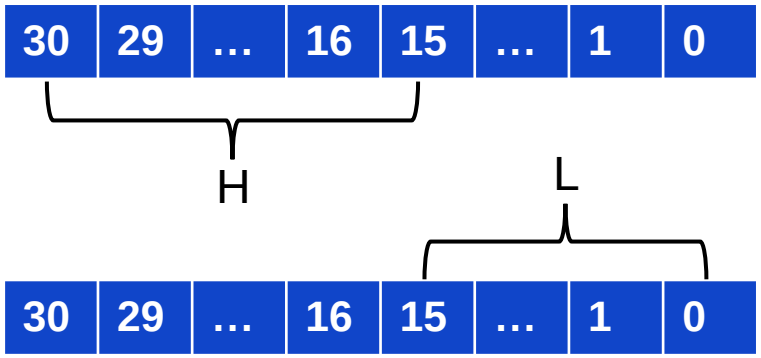


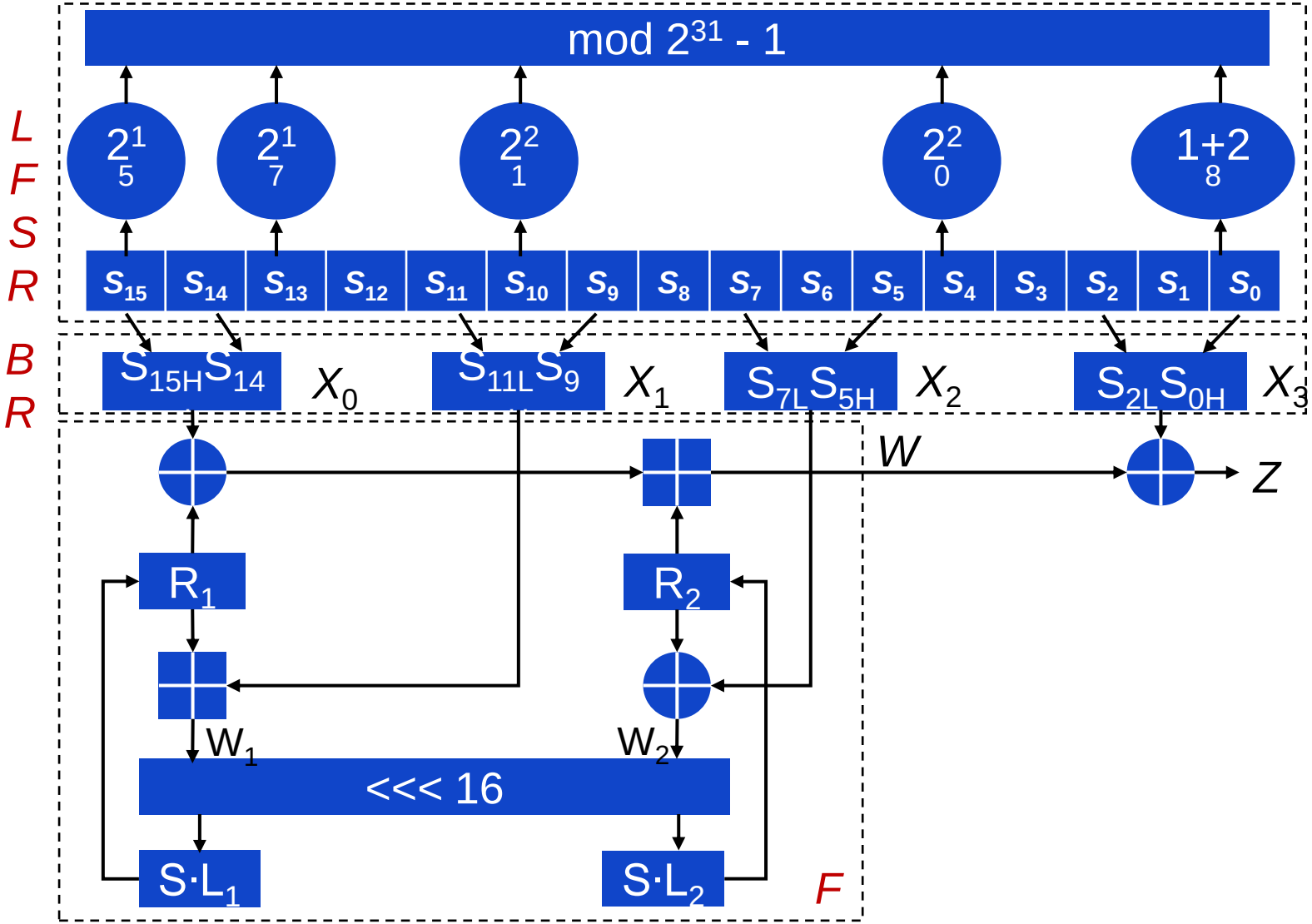
RC4序列密码算法


S表
0 1 2 3 4 5 … S[t] … 254 255
初始K
0 1 2 3 … n
T表
0 1 2 3 … n n+1 n+2 … S[t] … 254 255
j = 0, 对i = 0 到255执行： j = (j+ S[i] + T[i]) mod 256
S表
0 1 2 3 … S[i] … S[j] … S[t] … 254 255
S[i]和S[j]置换
t = (S[i] + S[j]) mod 256
j = (j + S[i]) mod 256
S表
0 1 2 3 … S[i] … S[j] … S[t] … 254 255
S[i]和S[j]置换
密钥

祖冲之序列密码算法

- 三层结构
  - LFSR
  - 比特重组
  - 非线性F函数
  - 两个不同S盒
  - 移位操作





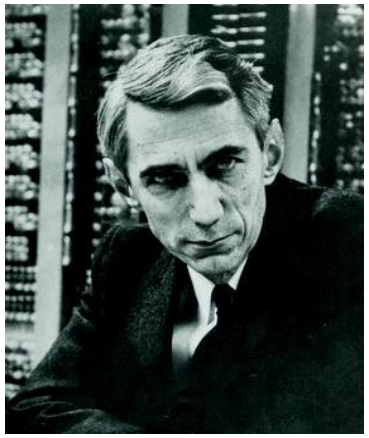
分 组 密 码

- 分组密码的结构和设计思想
- 分组密码的安全性原则
- 分组密码工作模式
- 典型分组密码算法结构和参数
- AES算法数学基础（加、乘）

分组密码设计原则

- 混淆（Confusion）原则：要求所设计的密码应该是密钥和密文之间的依赖关系尽可能复杂，以至于无法被攻击者利用

- 扩散（Diffusion）原则：明文的每个比特位影响密文尽可能多的比特位，输入微小的变化导致输出多位变化



Claude E. Shannon

在密码学当中，**混淆**（confusion）与**扩散**（diffusion）是设计密码学算法的两种主要方法。这样的定义最早出现在克劳德·香农1945年的论文*《密码学的数学理论》*当中。
在克劳德·香农的定义之中，混淆主要是用来使密文和对称式加密方法中密钥的关系变得尽可能的复杂；扩散则主要是用来使用明文和密文关的关系变得尽可能的复杂，明文中任何一点小更动都会使得密文有很大的差异。
混淆用于掩盖密钥与密文之间的关系。这可以挫败通过研究密文以获取冗余度和统计模式的企图。做到这一点最容易的方法是“代替”。
扩散通过将明文冗余度分散到密文中使之分散开来。即将单个明文比特的影响尽可能扩大到更多的密文比特中去。产生扩散最简单的方法是换位（置换）。

S盒

- 密码算法盒中提供混淆用的的非线性部件
- 分组密码的安全强度，特别是抗差分密码分析和线性密码分析的能力，与S盒紧密相关
- 通常，S盒规模越大，密码算法的非线性程度越高，密码算法的混淆性能就越好
- S盒规模越大，密码算法实现的效率就越低

不同密码算法的S盒的规模是什么？

P置换

P substitution

- 代替-置换结构的分组密码算法中，*P*置换一般位于*S*盒之后
- 将*S*盒的混淆效应扩散开来
- 进一步提高算法的混淆程度
- *P*置换一般设计为线性置换

分组密码结构模型

Structure model

分组密码算法结构模型

S-P网络

非线性代替S层实现分组小块的混淆和扩散，置换P层实现整体扩散

Feistel结构

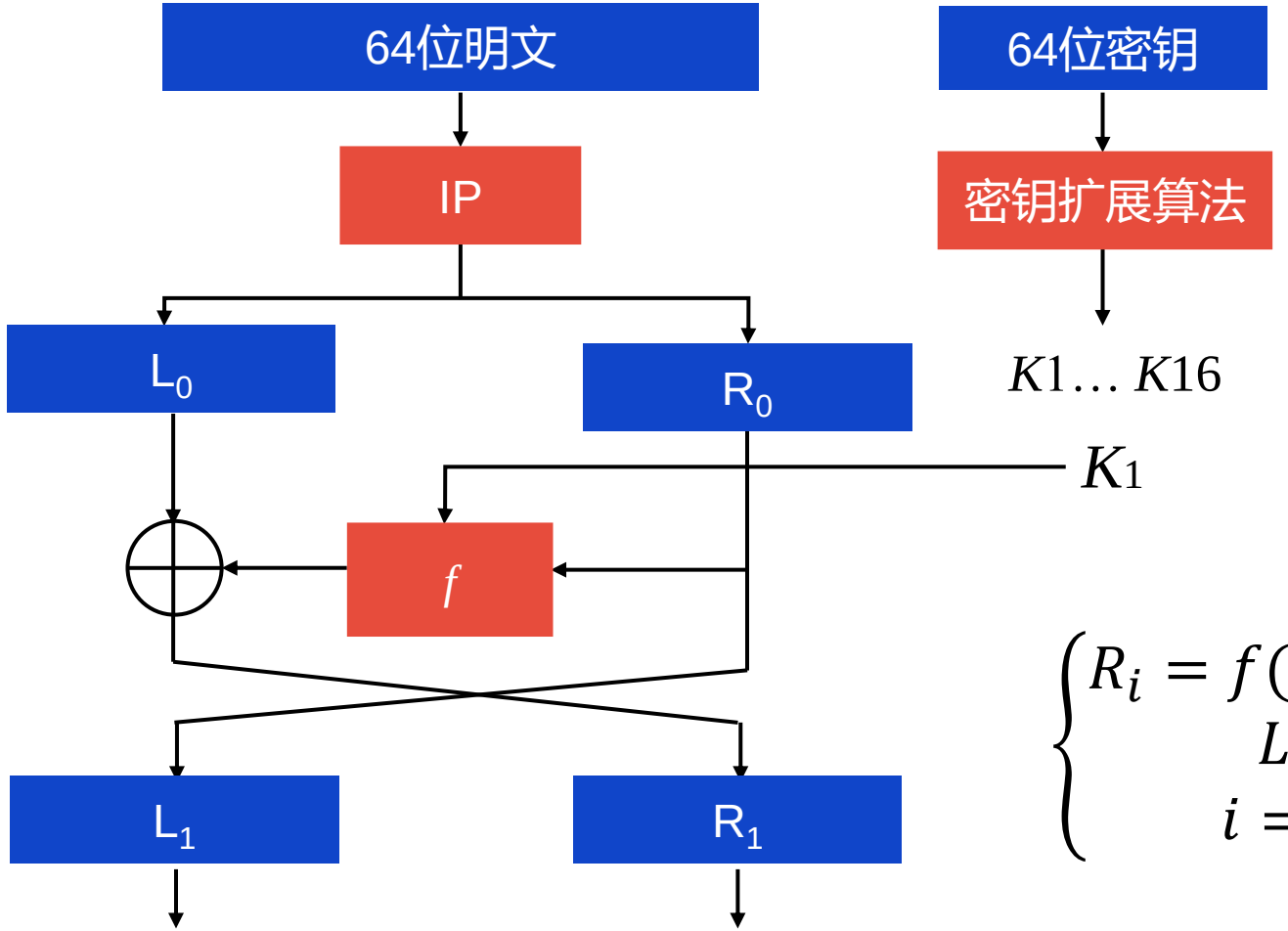
Feistel模型因在DES等分组密码中广泛应用而著名

Lai-Massey结构

Lai-Massey结构是由IDEA算法发展而来的一个分组密码结构

DES算法结构

- Feistel结构

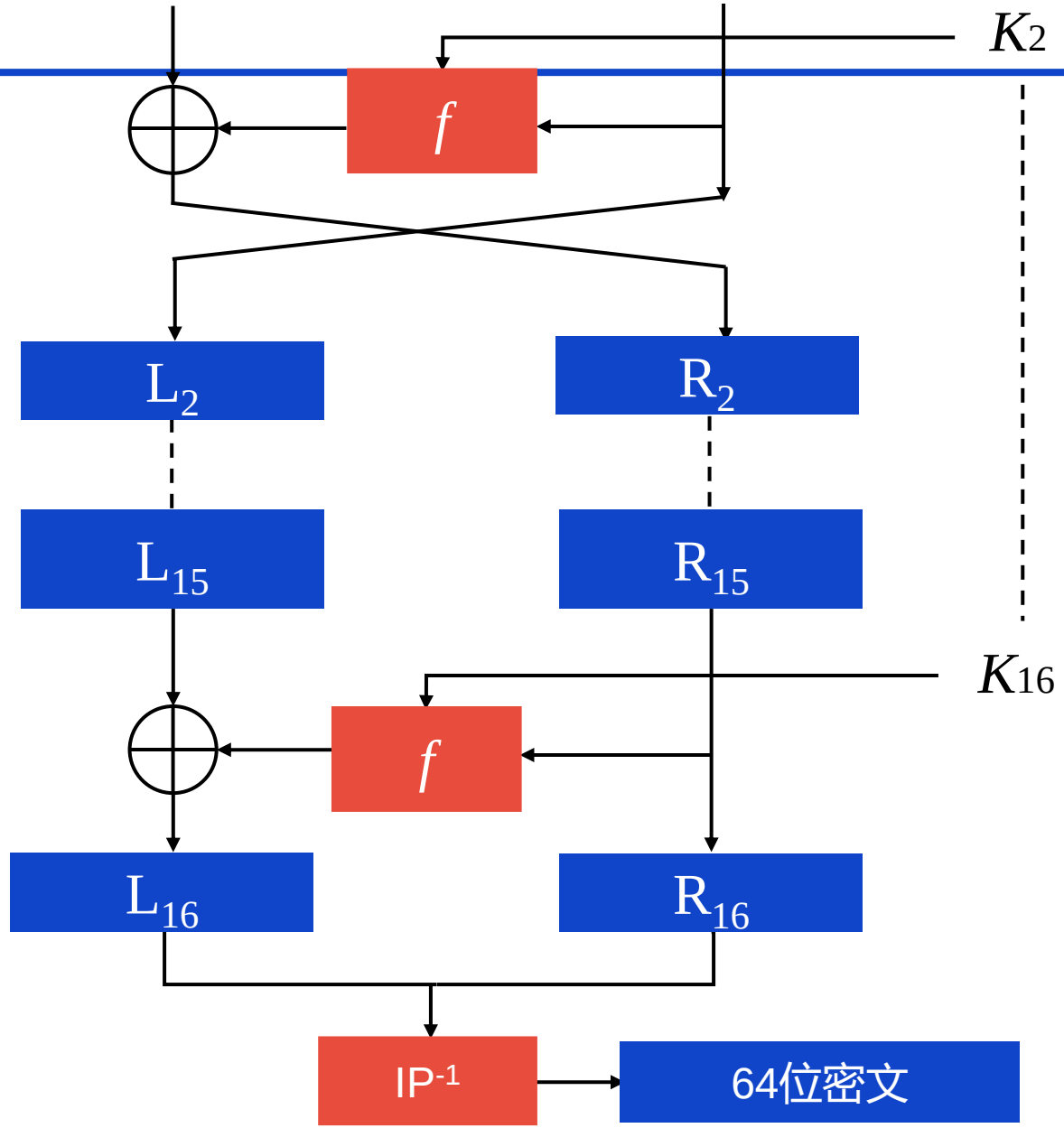


$$\begin{cases} R_i = f(R_{i-1}, k_i) \oplus L_{i-1} \\ L_i = R_{i-1} \\ i = 1,2,\cdots,r \end{cases}$$

DES算法结构

Structure model

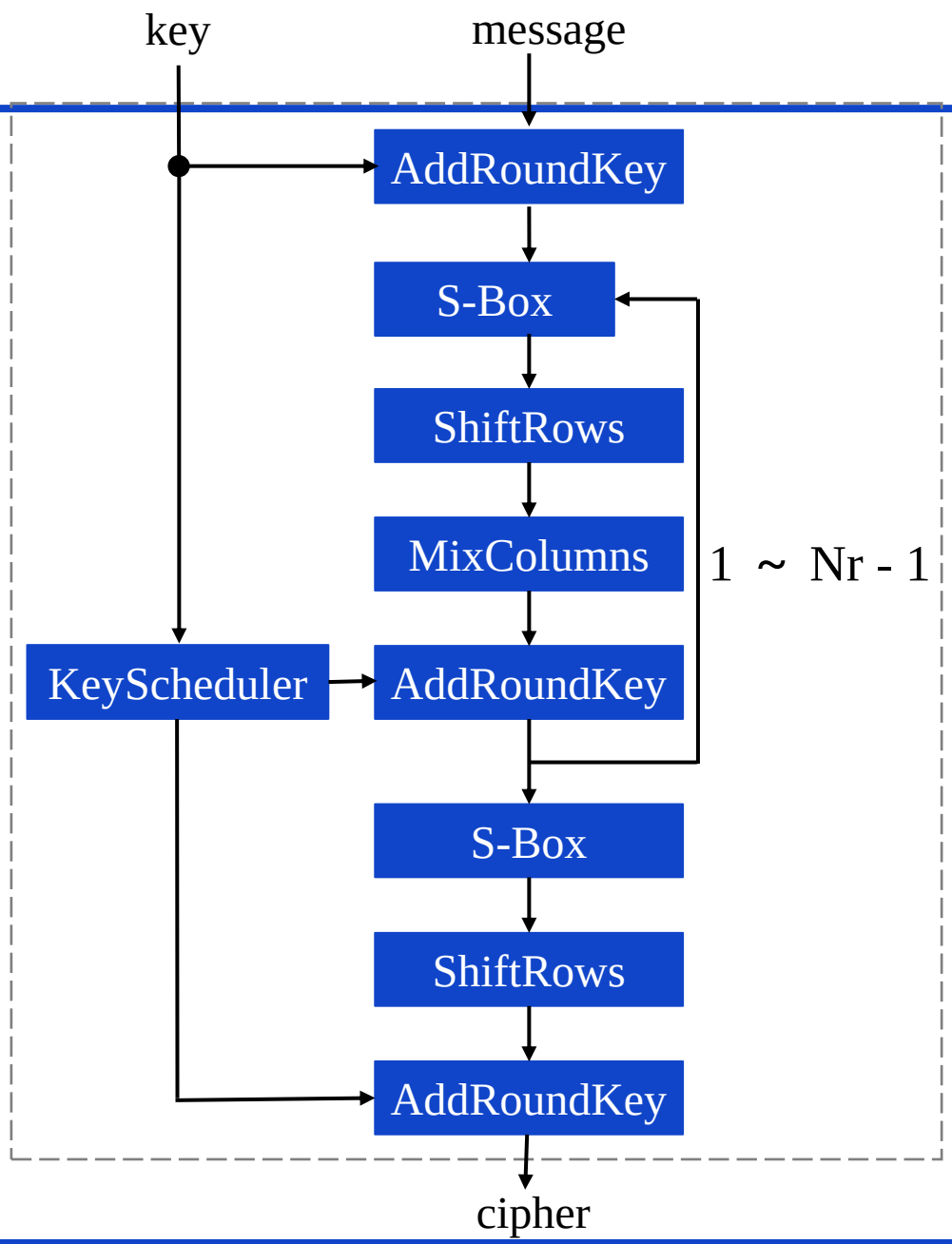
- 迭代密码
- 16轮迭代

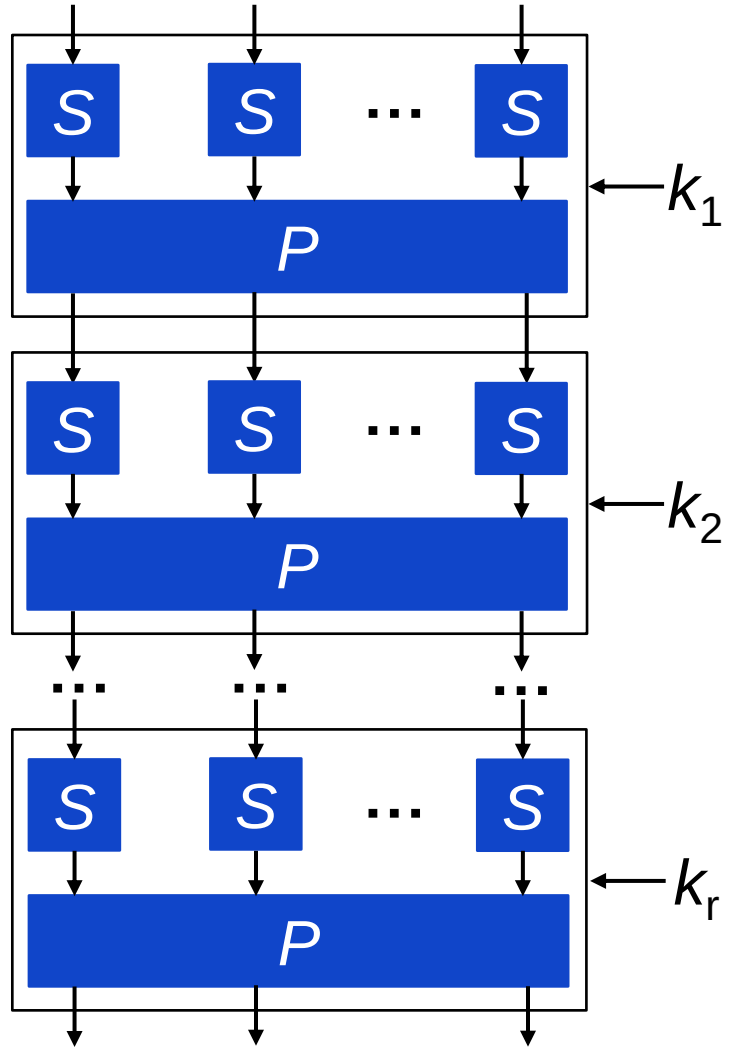


AES算法结构

Structure model

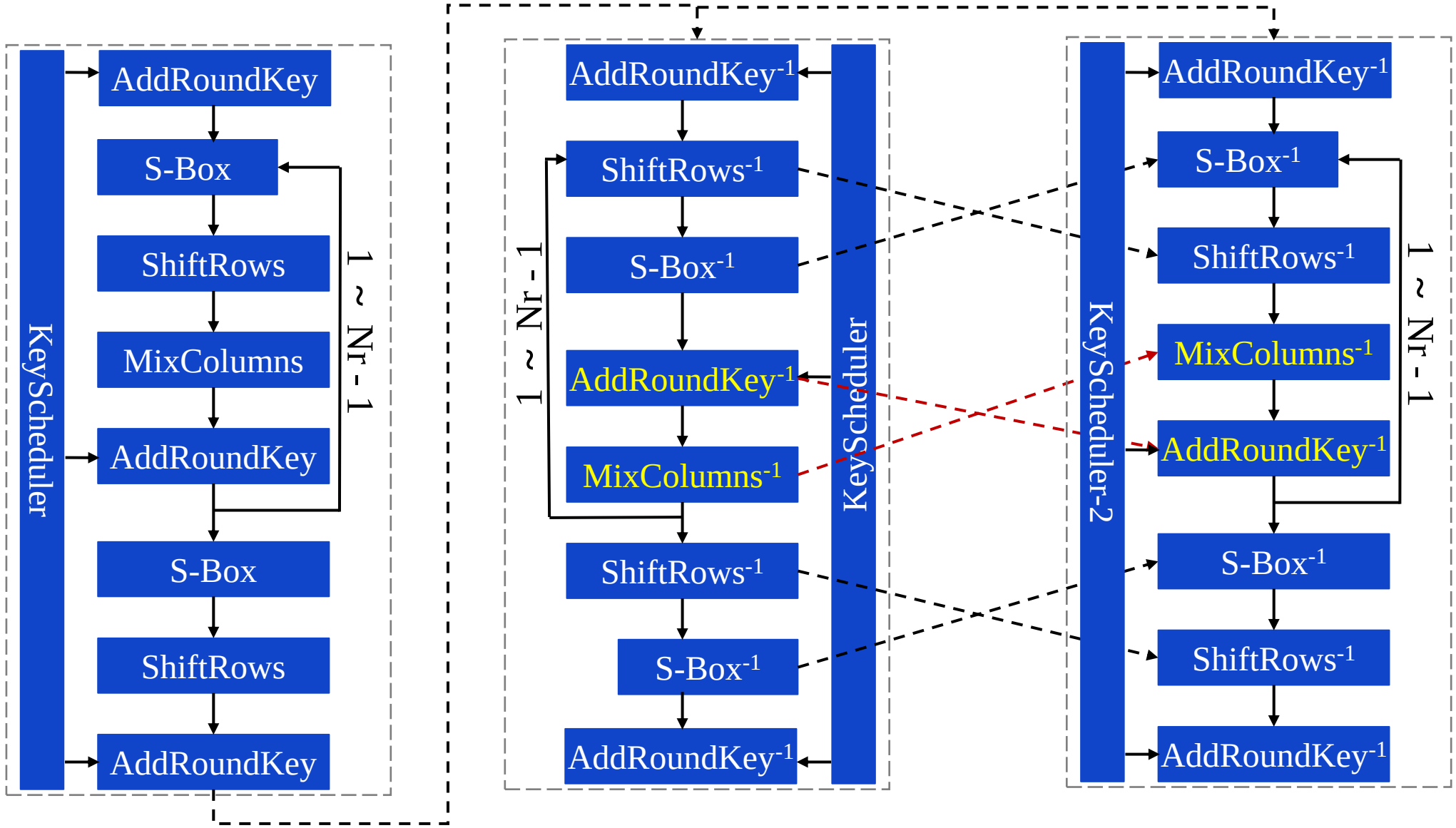
- S盒变换 – S-Box
- 行移位 – ShiftRows
- 列混合 – MixColumns
- 密钥扩展 – KeyScheduler
- 加轮密钥 – AddRoundKey





AES算法结构

Structure model



分组密码工作模式

加密模式		特 点
Electronic Code Book(ECB)	电子密码本模式	简单快速，可并行计算
Cipher Block Chaining(CBC)	密码分组链接模式	仅解密支持并行计算
Cipher Feedback Mode(CFB)	密文反馈模式	仅解密支持并行计算
Output Feedback Mode(OFB)	输出反馈模式	不支持并行运算
Counter (CTR)	计数器模式	支持并行计算

比 较

Comparison

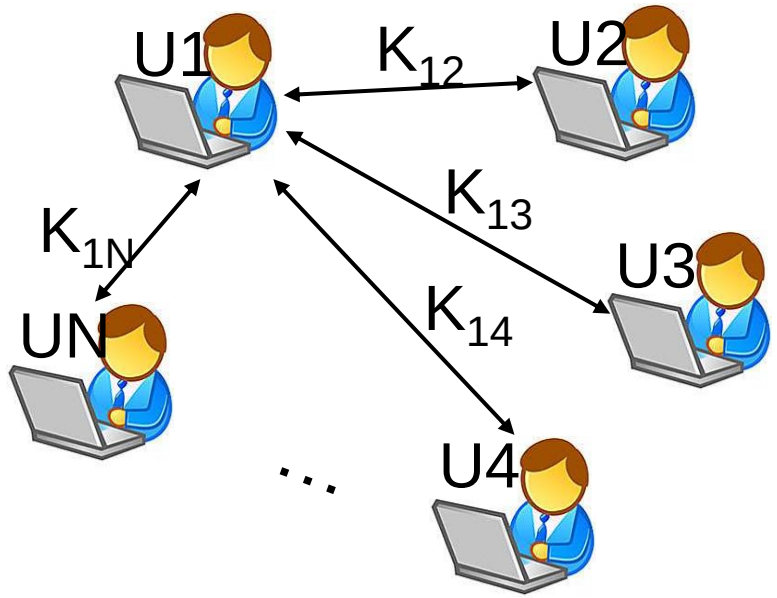
密码算法	DES	AES	SM4	PRESENT
网络结构	Festal网络	S-P网络	滑动窗口	S-P网络
分组长度	64	128	128	64
密钥长度	64	128/192/256	128	80/128
子密钥长度	48	128	32	64
轮数	16	10/12/14	32	31
S盒规模	6进4出	8进8出	8进8出	4进4出
结构特点	对合	对称	对合	非对称

公 钥 密 码

- 公钥密码设计思想
- 典型的数学困难问题
- RSA、DH、ElGamal等算法密码生成流程
- RSA、DH、ElGamal等算法参数选取原则
- RSA、DH、ElGamal等密码安全性分析
- ECC的数学基础

公钥密码的产生背景

- 传统密码体制下密钥难共享
- 密钥难管理
- 难以解决签名和认证问题

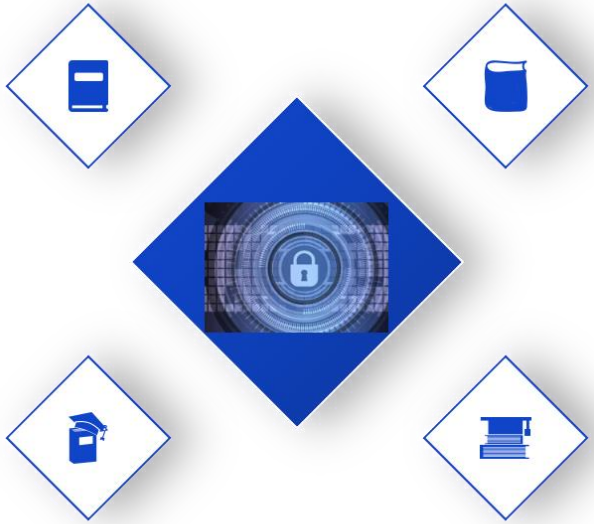


机　密　性

防止敏感信息泄漏

完　整　性

防止关键信息被篡改



真　实　性

防止身份或数据假冒

不可否认性

防止攻击行为抵赖

公钥密码数学问题

- ① 大合数的因子分解问题
- 大素数的乘积容易计算($p \times q \to n$)，而大合数的因子分解困难($n \to p \times q$)

- ② 有限域上的离散对数问题
- 有限域上大素数的幂乘容易计算($a^b \to c$)，而对数计算困难($\log_a c \to b$)

- ③ 椭圆曲线离散对数问题
- 设d是正整数，G是解点群的基点，计算$dG = Q$是容易的，而由Q求出d是困难的

RSA公钥密码算法

- 加解密算法
  - 随机地选择两个大素数p和q，而且保密
  - 计算$n = p * q$，将n公开
  - 计算$\varphi(n) = (p-1) * (q-1)$，对$\varphi(n)$保密
  - 随机地选取一个正整数e，$1 < e < \varphi(n)$且$(e, \varphi(n)) = 1$，将e公开
  - 根据$ed = 1 \bmod \varphi(n)$，求出d，并对d保密
  - 加密运算：$C = M^e \bmod n$
  - 解密运算：$M = C^d \bmod n$
  - 公开密钥$K_e = <e, n>$，保密密钥$K_d = <p, q, d, \varphi(n)>$

RSA公钥密码算法

- 在计算上由公开的加密钥不能求出解密钥
  - 公开密钥$K_e = <e, n>$
  - 保密密钥$K_d = <p, q, d, \varphi(n)>$
  - 假设攻击者截获密文C，*需恢复明文*

属于哪类攻击?

$$n = pq$$

$$\varphi(n) = (p - 1)(q - 1)$$

$$ed \equiv 1 \bmod \varphi(n)$$

$$M \equiv C^d \bmod n$$

$$C$$

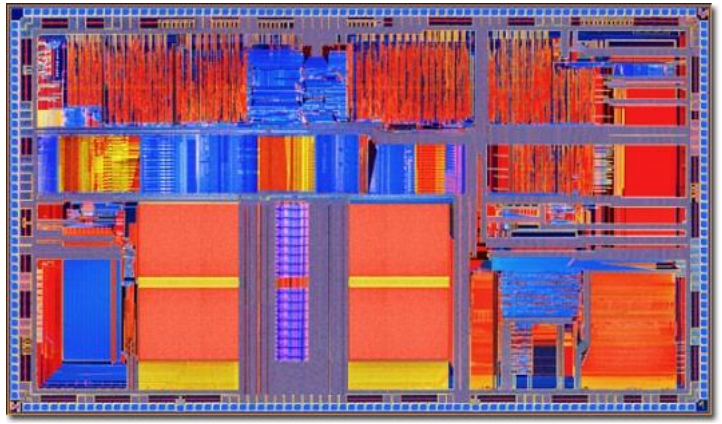
密码算法比较

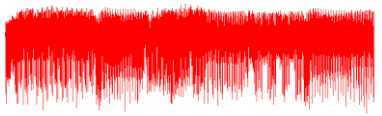
Comparsion

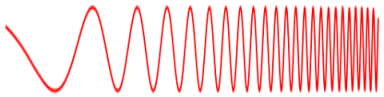
	序列密码算法	分组密码算法	非对称密码算法
算法代表	ZUC	AES、SM4	RSA
设计思想	高质量随机序列	混淆、扩散	数学困难问题
加密部件	移位、模加	S盒、P盒	模幂
密钥长度	128	128	1024+
应用场景	移动通信	批量数据加密	密钥交换、签名

密 码 分 析

- 时间侧信道分析
- 能量侧信道分析
- 能量泄漏模型
- 故障注入分析








感谢聆听!
THANK YOU FOR YOUR ATTENTION!