

课程编号：3182121321

无线通信安全



第二讲 密码学基础

李晖

lihuill@bupt.edu.cn

6G安全与韧性原则

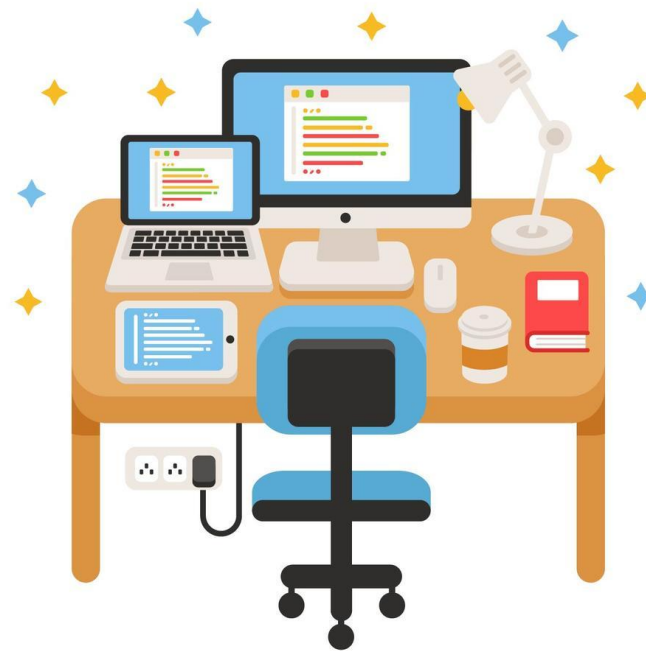
- 全球电信联盟(Global Coalition on Telecoms)的七个政府在**2026年世界移动通信大会(Mobile World Congress)**上发布了一套《**6G安全与韧性原则**》，为下一代移动通信网络的设计、部署与保护建立了早期的政策框架。
- 该框架提出了关于如何防范**网络攻击与物理威胁**、增强供应链韧性，以及确保**持续、可靠服务**的基本要求。
- 6G系统需实现明确且可衡量的安全目标：
 - ✓ 攻击扩散遏制 (Containment)
 - ✓ 数据机密性保护 (Confidentiality)
 - ✓ 数据完整性保护 (Integrity)
 - ✓ 系统韧性保障 (Resilience)
 - ✓ 监管合规保障 (Regulatory Compliance)

Global Coalition on Telecoms set 6G security rules as next-gen networks become critical infrastructure backbone

MARCH 05, 2026



1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. 对称密码体制的概念与分类
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



1. 密码学的基本概念

专业术语

- **发送者和接收者、明文和密文**
 - **密码体制**
 - 所有可能的明文的集合 P ，称为**明文空间**；
 - 所有可能的密文的集合 C ，称为**密文空间**；
 - 所有可能的密钥的集合 K ，称为**密钥空间**；
 - **加密算法**: $E: P \times K \rightarrow C, (m, k) \mapsto E_k(m)$,
 - **解密算法**: $D: C \times K \rightarrow P, (c, k) \mapsto D_k(c)$,
- 对 $\forall m \in P, k \in K$, 有 $D_k(E_k(m)) = m$ 。
- 五元组 (P, C, K, E, D) 称为一个**密码体制**。

1. 密码学的基本概念

密码分析

- 
- **唯密文攻击**（**ciphertext-only attack**）指密码分析者仅根据截获的密文进行的密码攻击。
 - **已知明文攻击**（**know-plaintext attack**）指密码分析者已经掌握了一些相应的明、密文对，根据这些明、密文对对密码体制进行的攻击。
 - **选择明文攻击**（**chosen-plaintext attack**）密码分析者暂时获得对加密机的访问权限，可以选择一些明文，并可取得相应的密文。
 - **选择密文攻击**（**chosen-ciphertext attack**）密码分析者暂时获得对解密机的访问权限，可以选择一些密文，并可取得相应的明文。

1. 密码学的基本概念

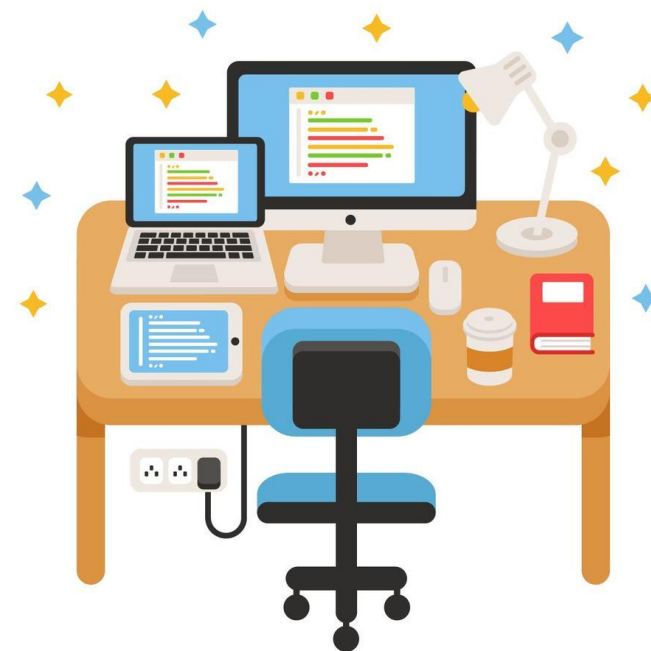
主动攻击

- 中断。如破坏计算机硬件、网络或文件管理系统。
--> 攻击可用性
- 篡改。如修改数据文件中的数据、替换某一程序使其执行不同的功能、修改网络中传送的消息内容等。
--> 攻击完整性
- 伪造。如在网络中插入伪造的消息或在文件中插入伪造的记录。
--> 攻击真实性

被动攻击

- 窃听。如搭线窃听、对文件或程序的非法复制等，以获取他人的信息。
--> 攻击保密性

1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. 对称密码体制的概念与分类
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



2. 古典密码

移位密码 (恺撒密码)

- 加密函数: $E(m) = (m+k) \bmod q$

仿射密码

- 加密函数: $e(x) = ax + b \pmod{m}$

其中: a 和 m 互质, m 是字母数目

维吉利亚密码

置换密码

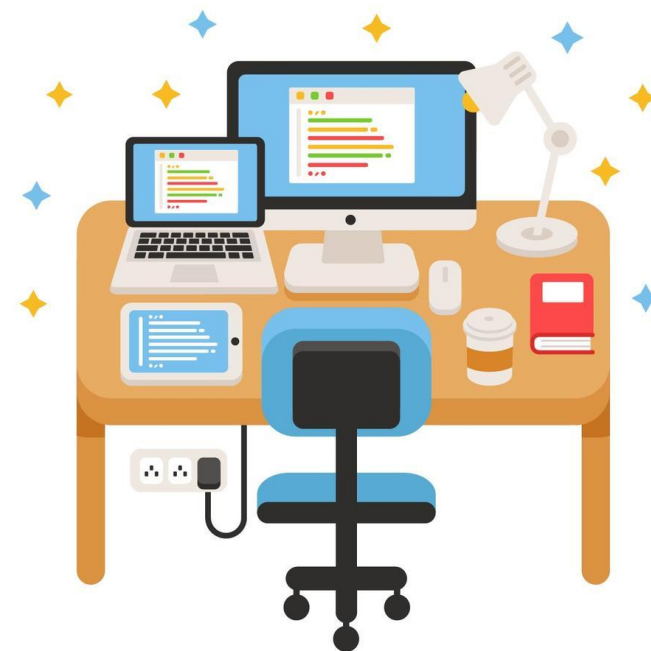
- 根据一定的规则重新排列明文,
以便打破明文的结构特性。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

维吉利亚密码表格

总结: 算法简单, 算法复杂度不高, 难以抵抗穷举搜索攻击

1. 密码学的基本概念
2. 古典密码
3. **密码体制的安全性要素**
4. 对称密码体制的概念与分类
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



3. 密码体制的安全性要素

理论安全性，完善保密性或无条件安全性

- 当攻击者不知道密钥时，知道对应的密文对于估计明文没有任何帮助
- 攻击者具有无穷的計算资源，也无法破解

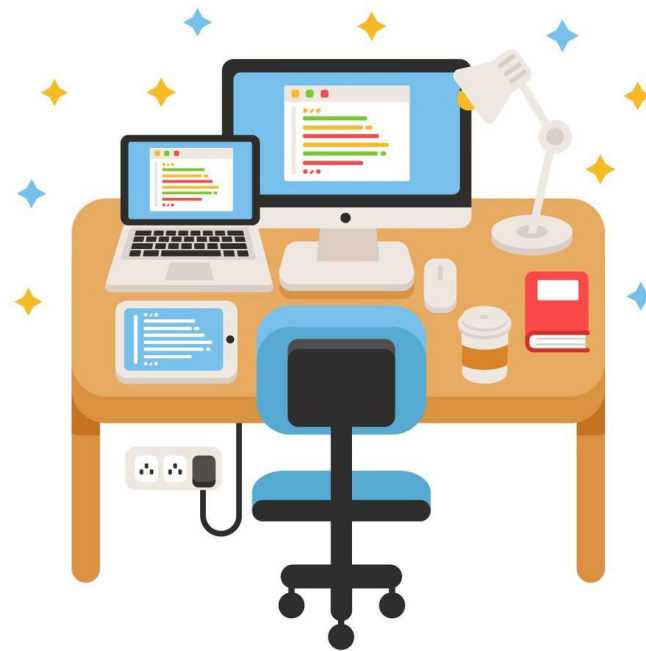
实际安全性，实际的不可破译性

- 不能在希望的时间内或实际可能的条件下求解

一个密码体制的安全性涉及两方面的因素：

- 所使用的密码算法的**保密强度**
- **密码算法**之外的不安全因素

1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. **对称密码体制的概念与分类**
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



4 对称密码体制的概念与分类

密码算法分类

- 按照保密的内容分:
 - **受限制的 (restricted)算法:** 算法的保密性基于保持算法的秘密。
 - **基于密钥 (key-based)的算法:** 算法的保密性基于对密钥的保密。

4 对称密码体制的概念与分类

基于密钥的算法，按照密钥的特点分类：

- **对称密码算法** (symmetric cipher)
 - 又称传统密码算法，或秘密密钥算法或单密钥算法。
 - 加密密钥和解密密钥相同，或实质上等同。
- **非对称密码算法** (asymmetric cipher)
 - 又称**公开密钥算法** (public-key cipher) 。
 - 加密密钥和解密密钥不相同，从一个很难推出另一个。
 - 用一个密钥进行加密，而用另一个进行解密。
 - **公开密钥**(public key)，简称**公钥**，可以公开，用于加密和签名验证；
 - **私人密钥**(private key)，简称**私钥**，必须保密，用于解密和生成签名。

4 对称密码体制的概念与分类

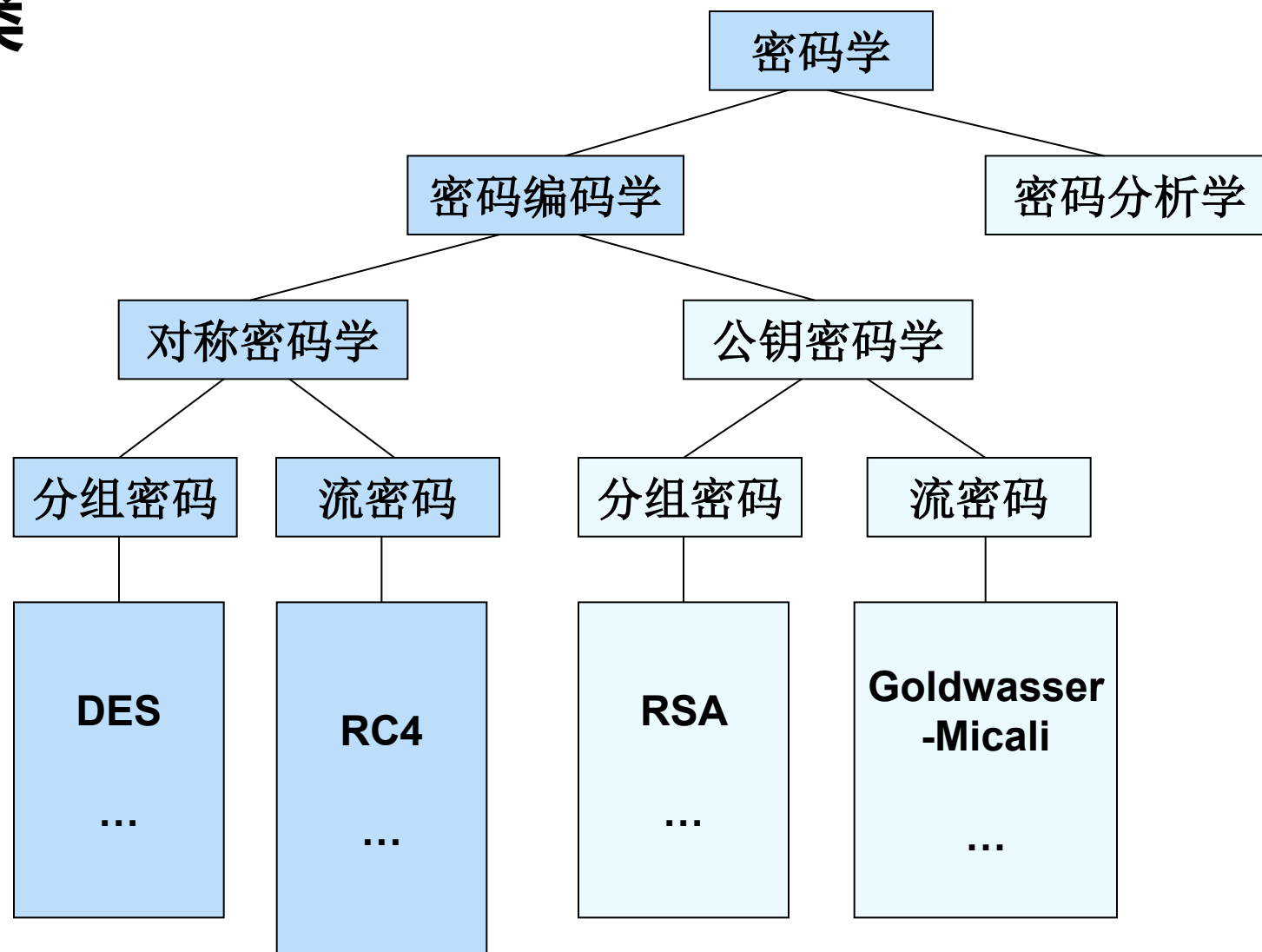
- 按照明文的处理方法：
 - **分组密码 (block cipher)** :将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。
 - **流密码 (stream cipher)** :又称**序列密码**。序列密码每次加密一位或一字节的明文，也可以称为流密码。

序列密码是手工和机械密码吗？

流密码是属于对称密码体制，还是非对称密码体制？

4 对称密码体制的概念与分类

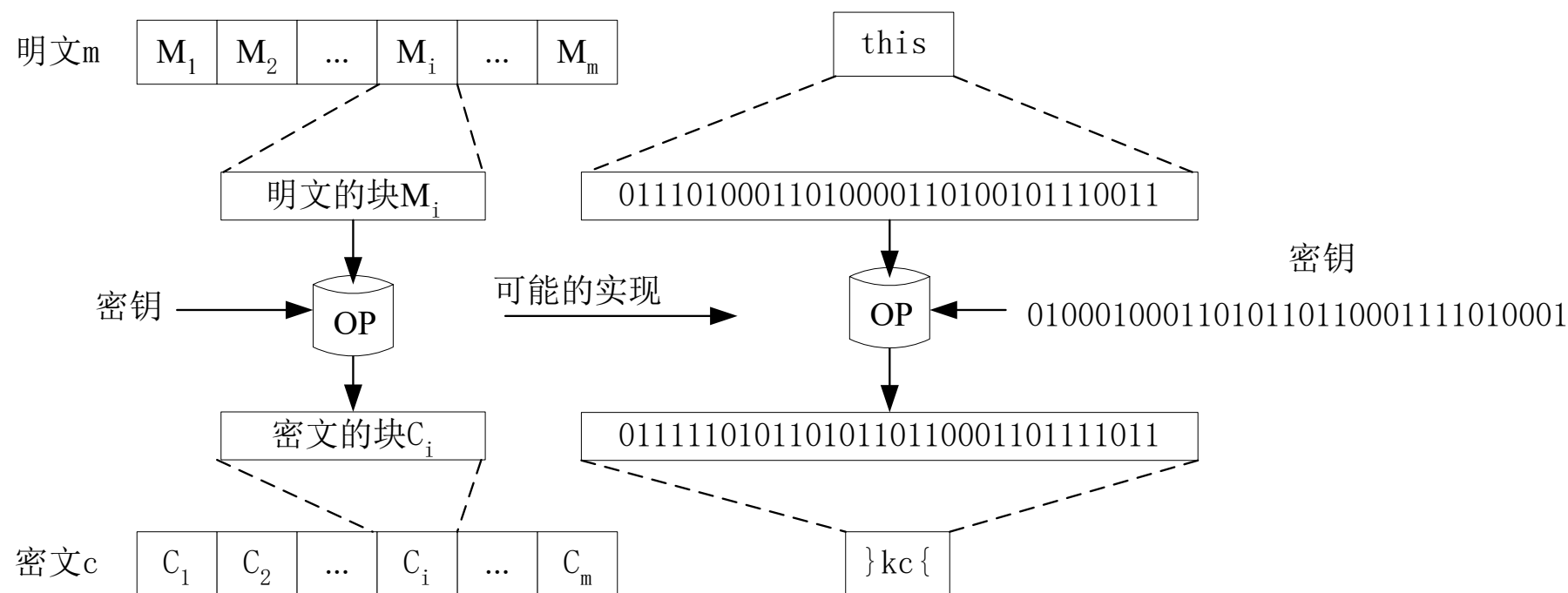
密码算法分类



4 对称密码体制的概念与分类

分组密码的概念

分组密码（Block Cipher），也称之为**块密码**，将明文消息编码表示后的数字序列，划分成固定大小的组（或位块），各组分别在密钥的控制下变换成等长的输出数字序列。



4 对称密码体制的概念与分类

分组密码分类

- 加密方式的不同，分组密码又可分为三类：
 - 代替密码
 - 移位密码
 - 乘积密码
- 根据加密和解密密钥是否相同，分为：
 - 对称分组密码
 - 非对称分组密码

4 对称密码体制的概念与分类

流密码的定义

流密码又称为**序列密码**，是指明文消息按字符（如二元数字）逐位地加密的一类密码算法。

- 与它对应的是分组密码，是指将明文消息（含多个字符），逐组地进行加密。
- 流密码算法：RC4，A5，SEAL，PKZIP...

4 对称密码体制的概念与分类

流密码原理

将明文划分成字符（如单个字母），或其编码的基本单元（如0，1数字），分别与密钥流进行加密运算，解密时以同步产生的同样的密钥流实现。

设明文为 $x = x_0x_1x_2\ldots$ $x_i \in GF(2), i \geq 0$

设密钥为 $r = r_0r_1r_2\ldots$ $r_i \in GF(2), i \geq 0$

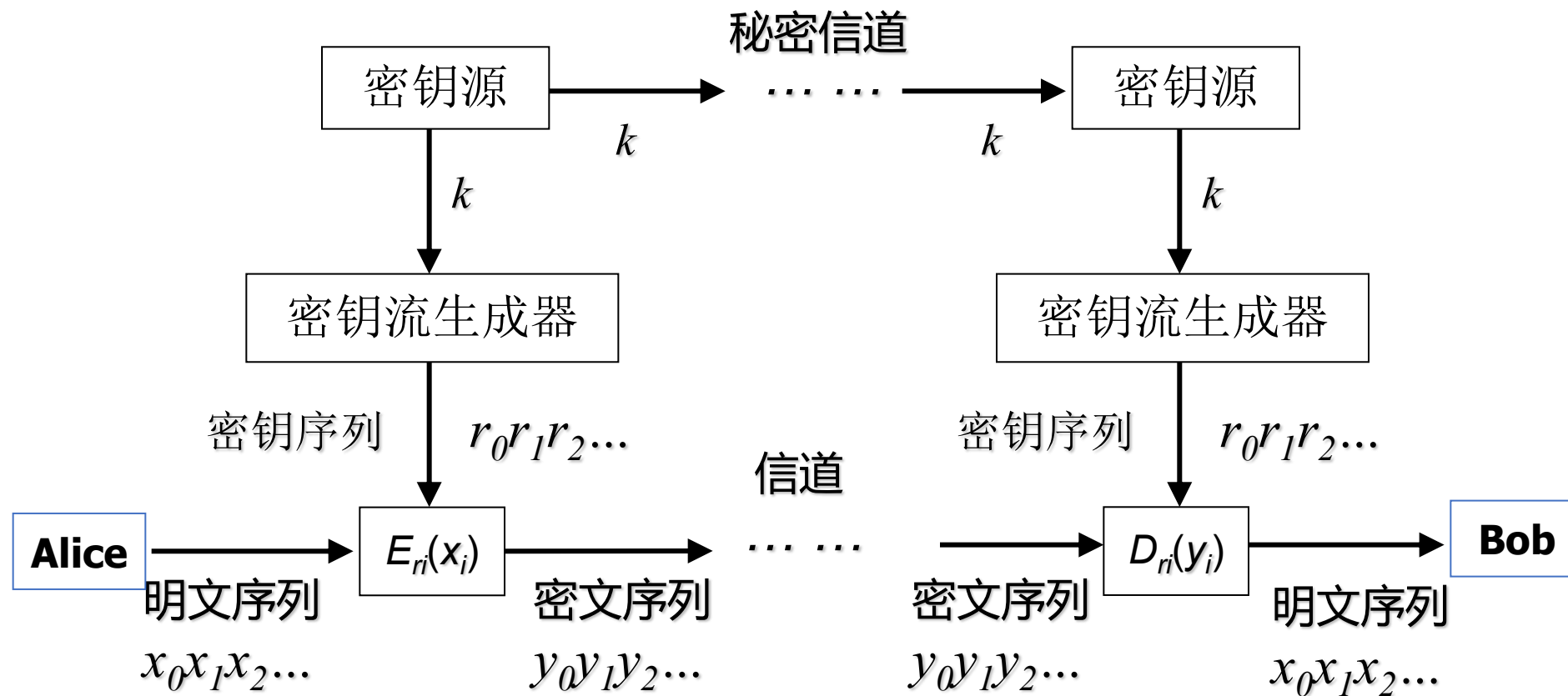
设密文为 $y = y_0y_1y_2\ldots$ $y_i \in GF(2), i \geq 0$

则加密变换为 $y_i = E_{r_i}(x_i) \quad i \geq 0$

则解密变换为 $x_i = D_{r_i}(y_i) \quad i \geq 0$

4 对称密码体制的概念与分类

基于流密码体制的加密通信模型



分组密码的工作模式

- 也称为密码模式，通常是由基本密码算法、一些反馈和一些简单运算组合而成。
- 特点：
 - 其安全性依赖于基本密码
 - 模式的效率将不会明显地低于基本密码
 - 不同的模式有不同的特点，适用于不同场合

4 对称密码体制的概念与分类

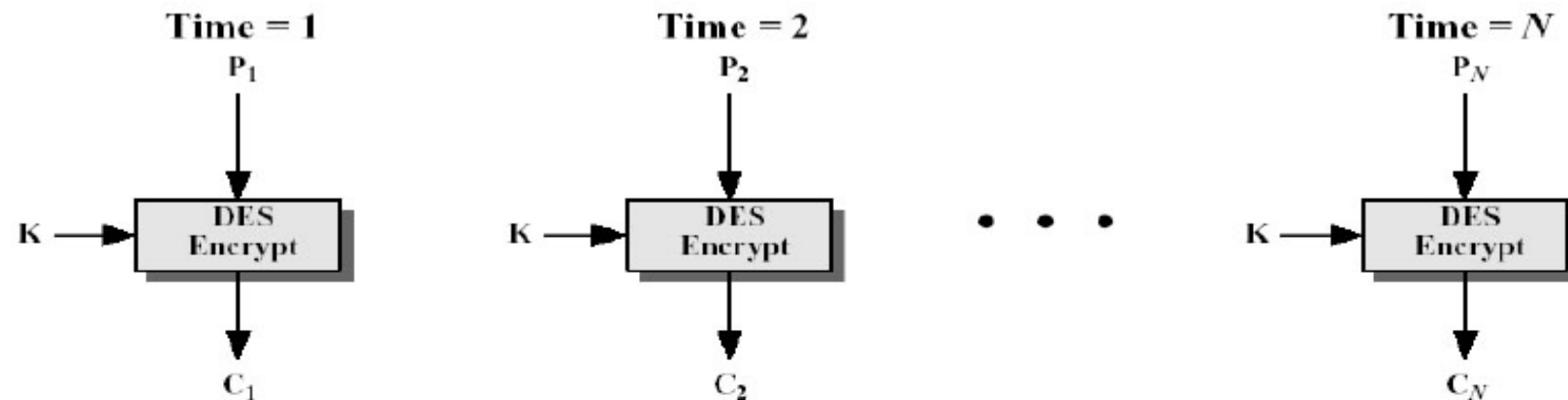
分组密码的工作模式

- 电子密码本ECB (Electronic CodeBook)
- 密码分组链接CBC (Cipher Block Chaining)
- 密码反馈CFB (Cipher FeedBack)
- 输出反馈OFB (Output FeedBack)
- 计数器模式CTR (CouTeR)
- 带偏移的密码本OCB (Offset CodeBook)
- CCM模式 (CTR +CBC-MAC)
- GCM模式 (Galois/Counter Mode)

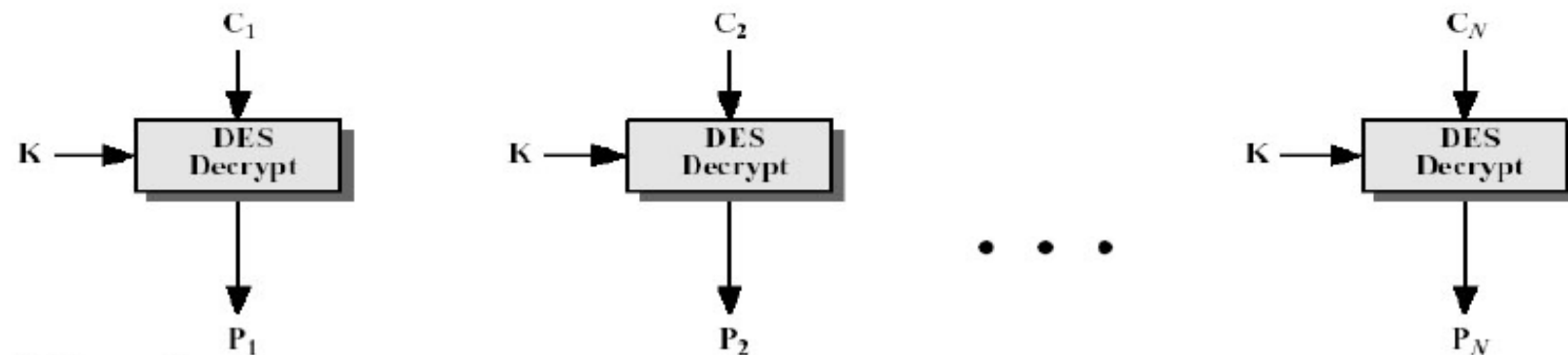
4 对称密码体制的概念与分类

电子密码本ECB

$$C_i = E_K(P_i) \Leftrightarrow P_i = D_K(C_i)$$



(a) Encryption



(b) Decryption

4 对称密码体制的概念与分类

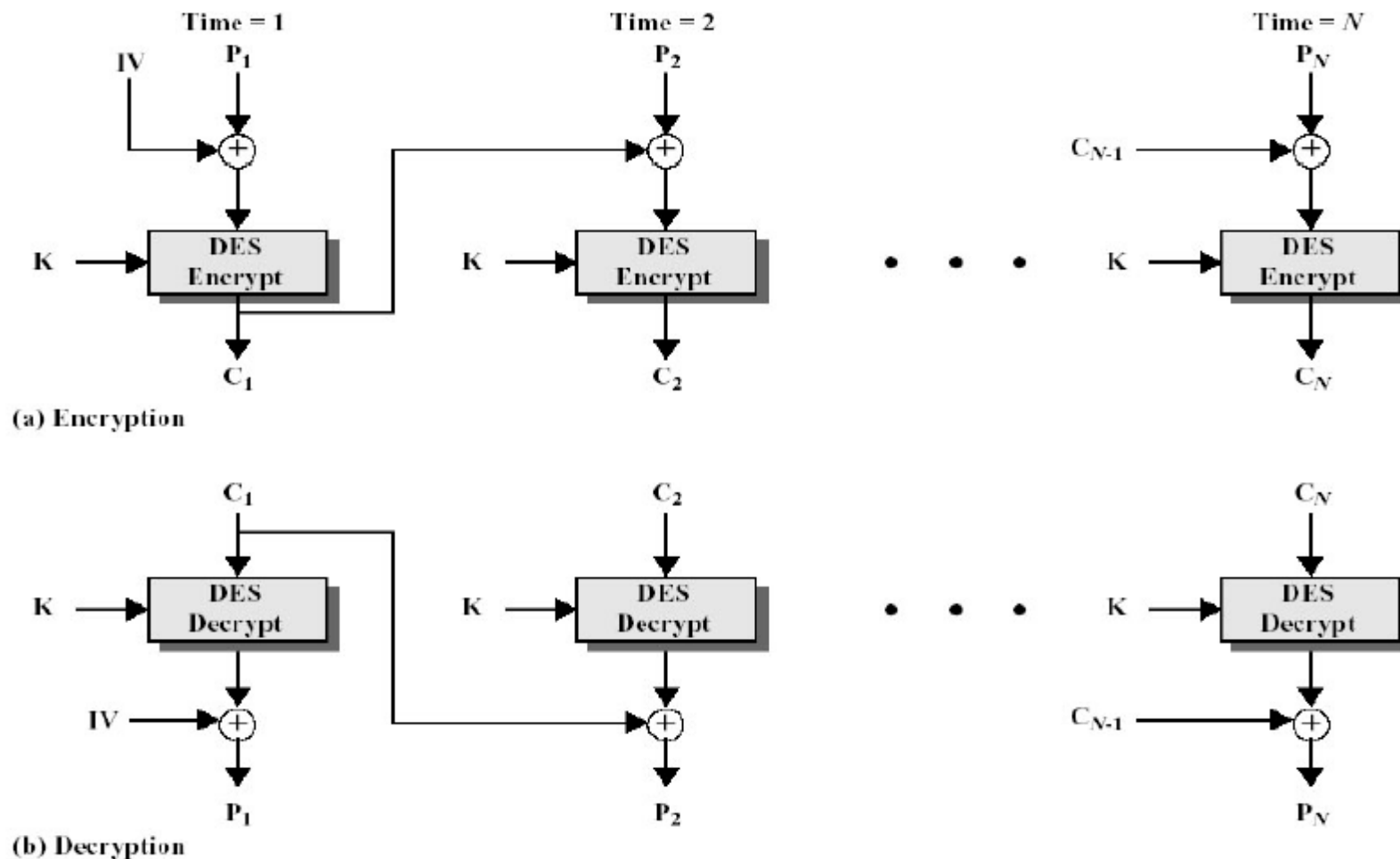
ECB特点

- 简单和有效
- 可以并行实现
- 不能隐藏明文的模式信息
 - 相同明文  相同密文
 - 同样信息多次出现造成泄漏
- 对明文的主动攻击是可能的
 - 信息块可被替换、重排、删除、重放
- 误差传递：密文块损坏  仅对应明文块损坏
- 适合于传输短信息

4 对称密码体制的概念与分类

密码分组链接CBC

$$C_i = E_K(C_{i-1} \oplus P_i) \Leftrightarrow P_i = D_K(C_i) \oplus C_{i-1}$$



4 对称密码体制的概念与分类

CBC特点

- 没有已知的并行实现算法
- 能隐藏明文的模式信息
 - 需要共同的初始向量IV
 - 相同明文 → 不同密文
 - 初始向量IV可以用来改变第一块
 - 定期更换IV（如果需要传递IV，要保证IV的完整性）
- 对明文的主动攻击是不容易的
 - 信息块不容易被替换、重排、删除、重放
 - 误差传递：密文块损坏 → 两明文块损坏
- 安全性好于ECB
- 适合于传输长度大于64位的报文

4 对称密码体制的概念与分类

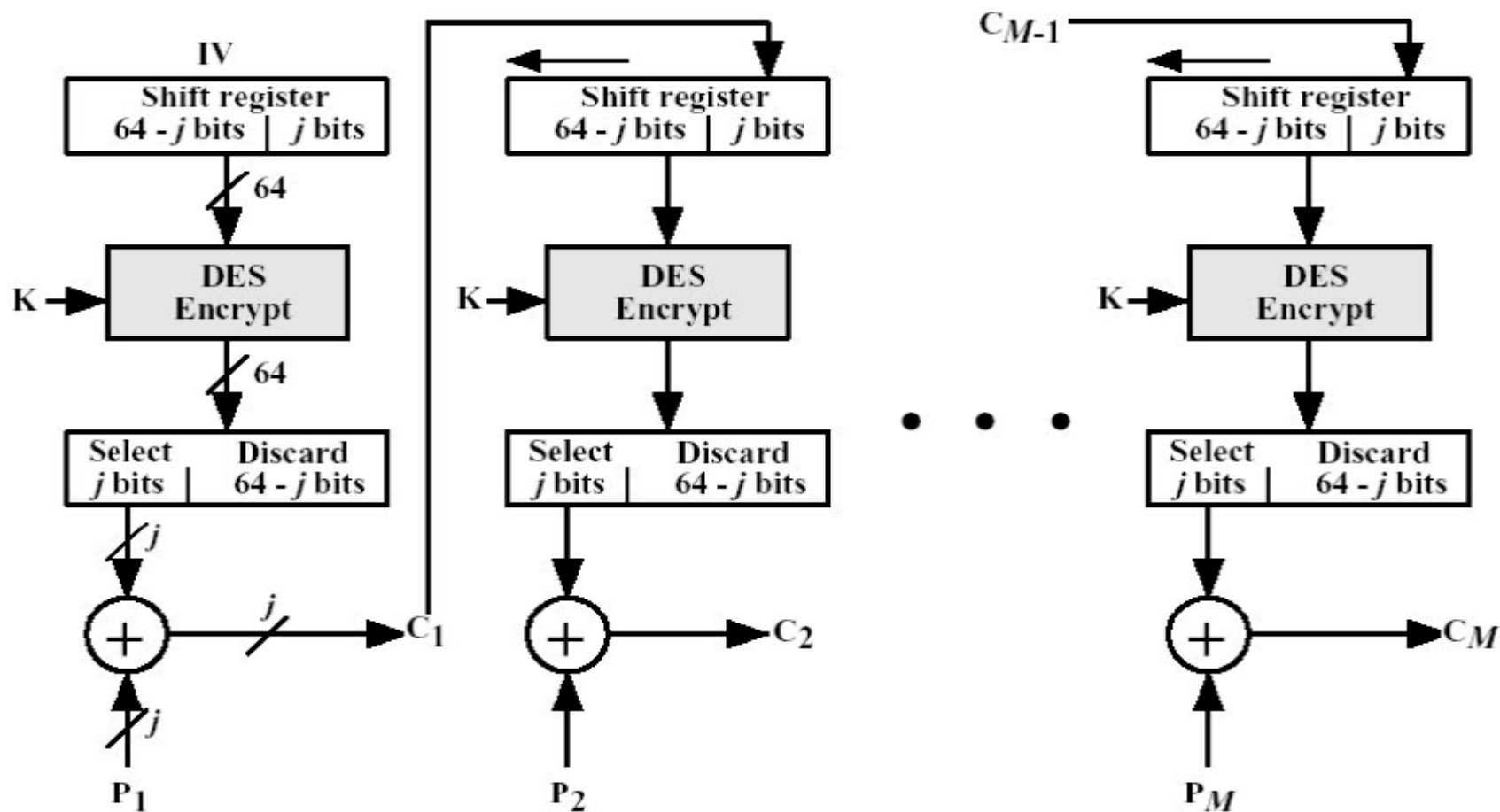
密码反馈CFB

- 分组密码  自同步流密码
- S_i 为移位寄存器, j 为流单元宽度
- 加密:
 - $C_i = P_i \oplus (E_K(S_i) \text{的高} j \text{位})$
 - $S_{i+1} = (S_i \ll j) | C_i$
- 解密:
 - $P_i = C_i \oplus (E_K(S_i) \text{的高} j \text{位})$
 - $S_{i+1} = (S_i \ll j) | C_i$

4 对称密码体制的概念与分类

CFB加密示意图

$$C_i = P_i \oplus (E_K(S_i) \text{的高} j \text{位}); \quad S_{i+1} = (S_i \ll j) | C_i$$

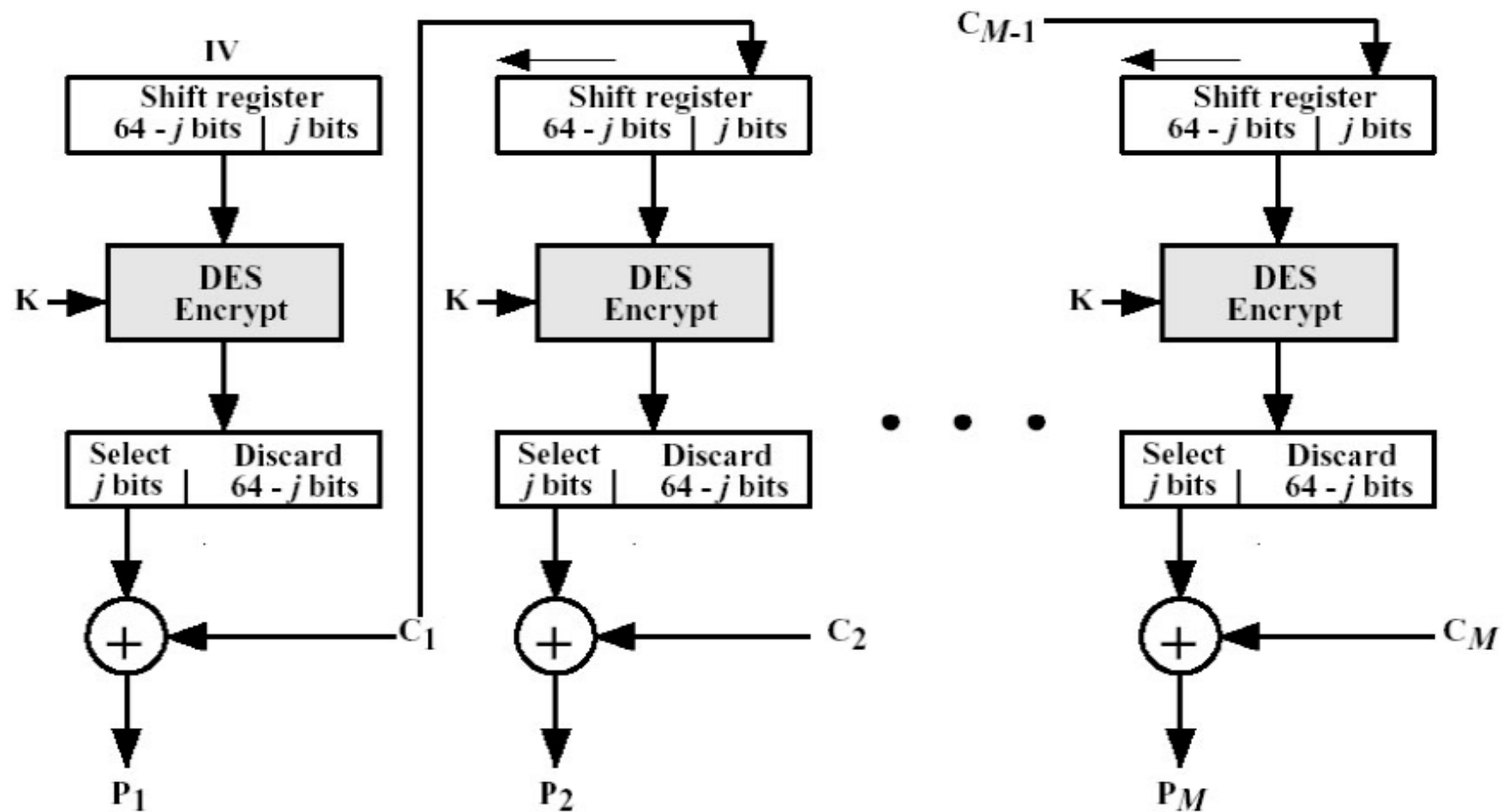


(a) Encryption

4 对称密码体制的概念与分类

CFB解密示意图

$$P_i = C_i \oplus (E_K(S_i) \text{的高} j \text{位}); \quad S_{i+1} = (S_i \ll j) | C_i$$



(b) Decryption

4 对称密码体制的概念与分类

CFB特点

- 分组密码  自同步流密码
- 没有已知的并行实现算法
- 关于IV
 - 为进行正常的加密和解密，发送与接收需要共同IV
 - IV应具有唯一性（即在密钥不变时，每次加密使用不同的IV）
- 优点：隐藏了明文模式
- 缺点：
 - 误差传递，一个单元损坏影响多个单元

4 对称密码体制的概念与分类

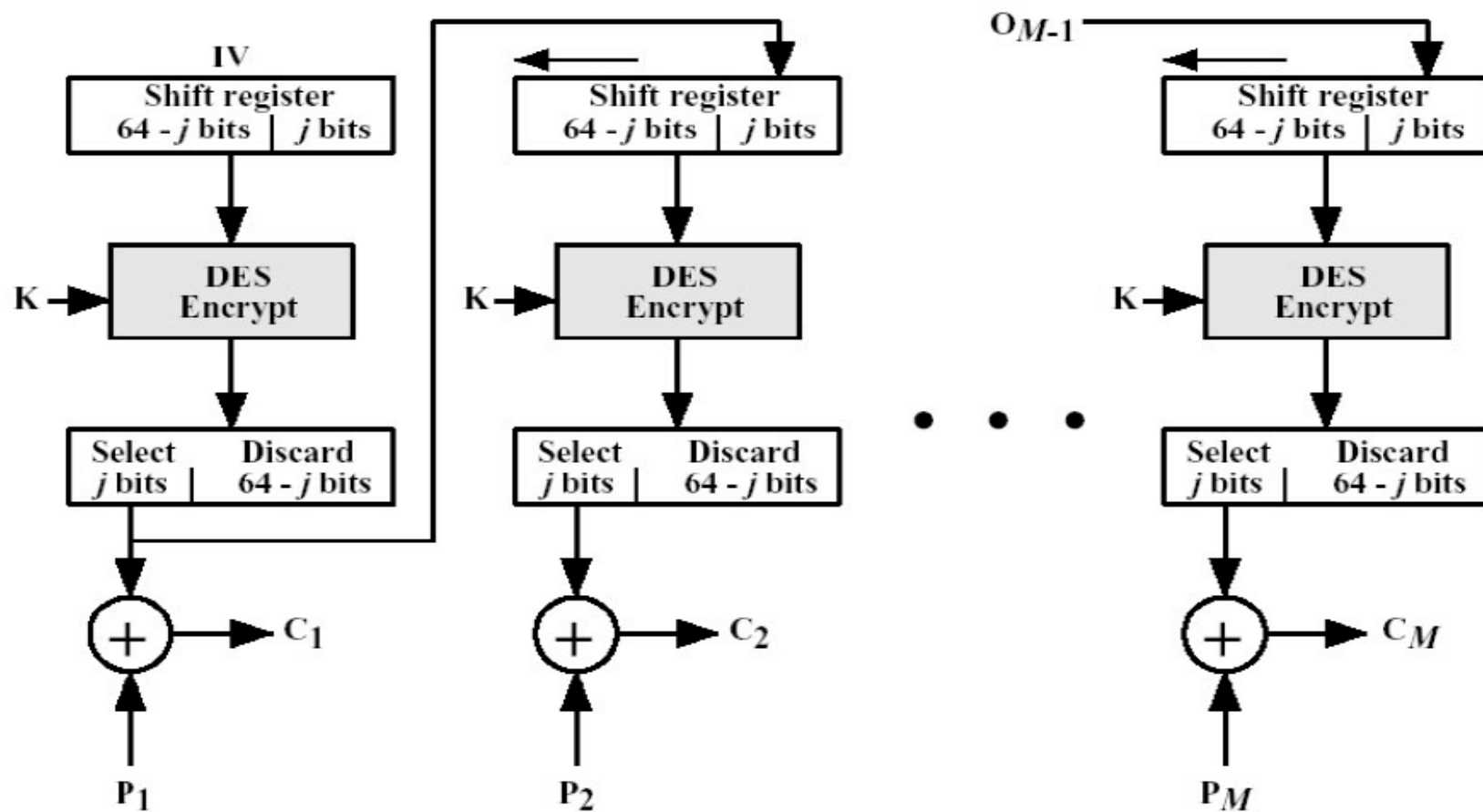
输出反馈OFB

- 分组密码  同步流密码
- S_i 为移位寄存器, j 为流单元宽度
- 加密:
 - $C_i = P_i \oplus (E_K(S_i) \text{的高} j \text{位})$
 - $S_{i+1} = (S_i \ll j) | (E_K(S_i) \text{的高} j \text{位})$
- 解密:
 - $P_i = C_i \oplus (E_K(S_i) \text{的高} j \text{位})$
 - $S_{i+1} = (S_i \ll j) | (E_K(S_i) \text{的高} j \text{位})$

4 对称密码体制的概念与分类

OFB加密示意图

$$C_i = P_i \oplus (E_K(S_i) \text{的高} j \text{位}); \quad S_{i+1} = (S_i \ll j) | (E_K(S_i) \text{的高} j \text{位})$$

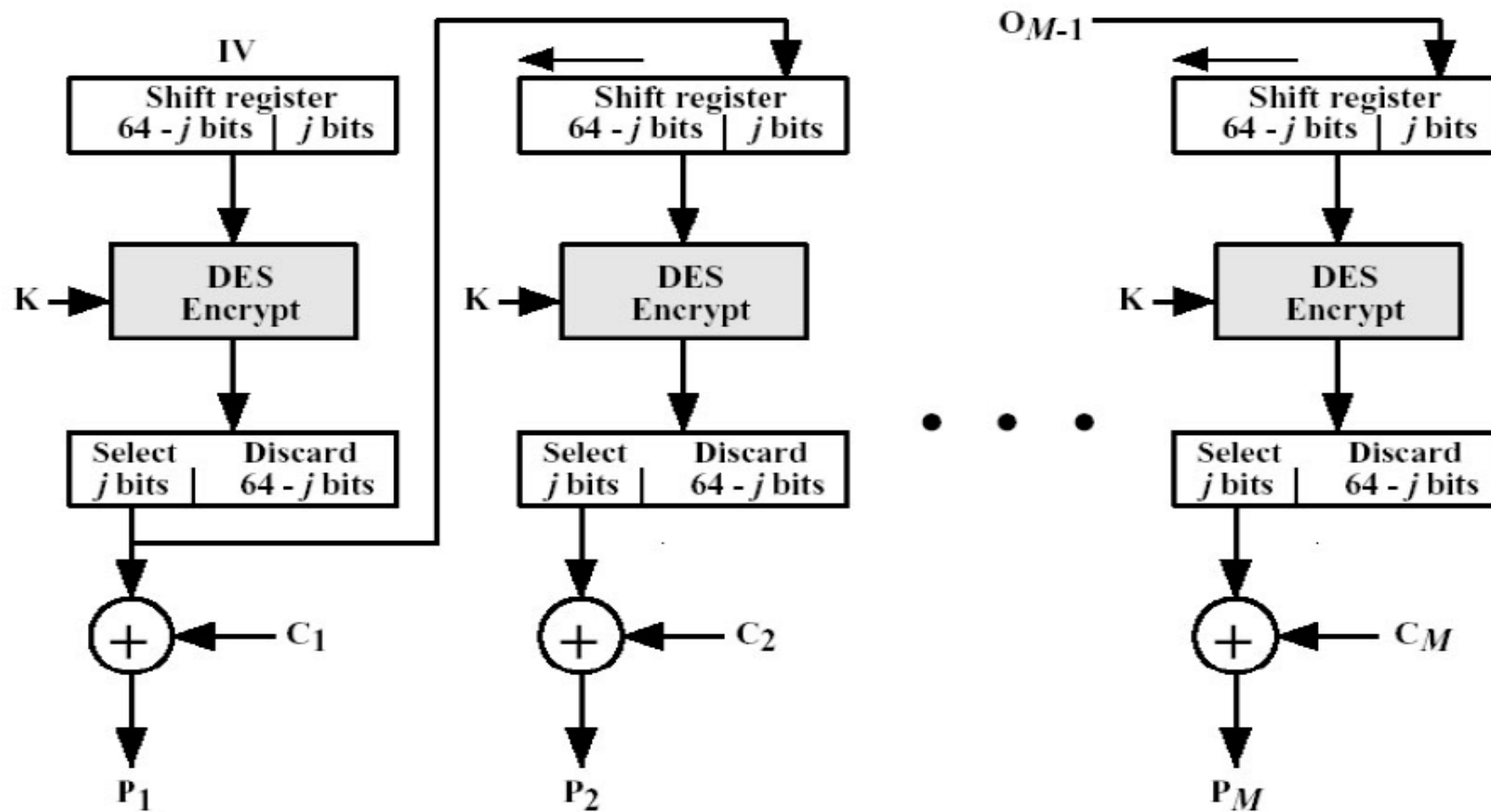


(a) Encryption

4 对称密码体制的概念与分类

OFB解密示意图

$$P_i = C_i \oplus (E_K(S_i) \text{的高} j \text{位}); \quad S_{i+1} = (S_i \ll j) | (E_K(S_i) \text{的高} j \text{位})$$



(b) Decryption

4 对称密码体制的概念与分类

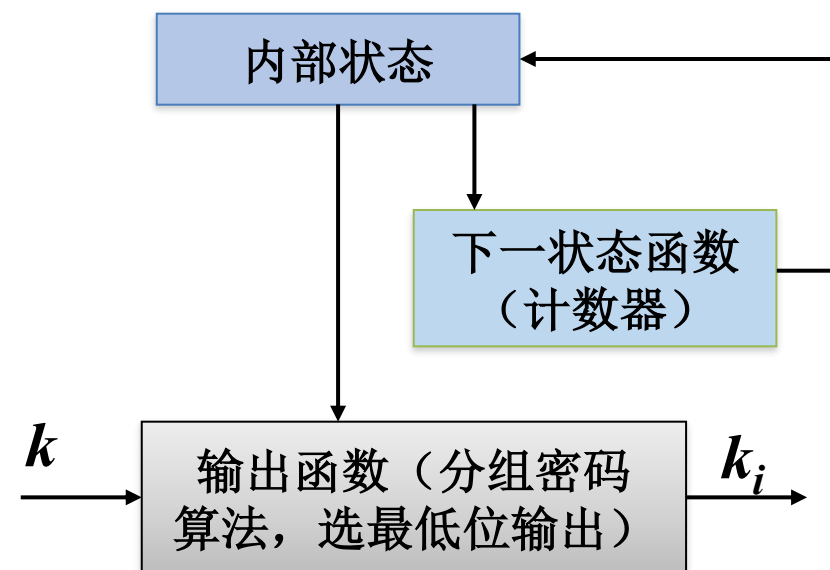
OFB模式特点

- 分组密码  同步流密码
- 没有已知的并行实现算法
- 优点：
 - 隐藏了明文模式
 - 没有误差传递：一个单元损坏只影响对应单元
- 缺点：
 - 不具有自同步能力，要求系统要保持严格的同步
 - 重新同步时需要新的IV，IV可以用明文形式传送
- 对明文的主动攻击是可能的
 - 信息块可被替换、重排、删除、重放
- 安全性较CFB差

4 对称密码体制的概念与分类

计数器模式(Counter Mode)

- Diffie等人在1979年提出
- 将一个计数器输入到寄存器中。每一个分组完成加密后，计数器都要增加某个常数，典型值是1。
- 该模式的同步和错误扩散特性同OFB模式完全一样。
- 可直接生成第 i 个密钥比特 k_i ；保密随机访问数据文件时是非常有用



4 对称密码体制的概念与分类

CTR模式

➤ 特点

- 硬件效率：允许同时处理多块明/密文
- 软件效率：允许并行计算
- 预处理
- 随机访问
- 可证明安全性：能够证明CTR至少和其他模式一样安全
- 简单性：只需要实现加密算法
- 无填充：可以高效地作为密钥流使用。

4 对称密码体制的概念与分类

OCB模式

- OCB模式通过使用同一个密钥对数据的一次处理，同时提供了加密和数据完整性检测。
- WPA2.0中使用基于128位的AES在OCB（offset CodeBook）模式，实现WRAP中的数据机密性与完整性保护机制。
- OCB模式优点：
 - 并行处理
 - 非常高效
 - 可以证明是可靠的

4 对称密码体制的概念与分类

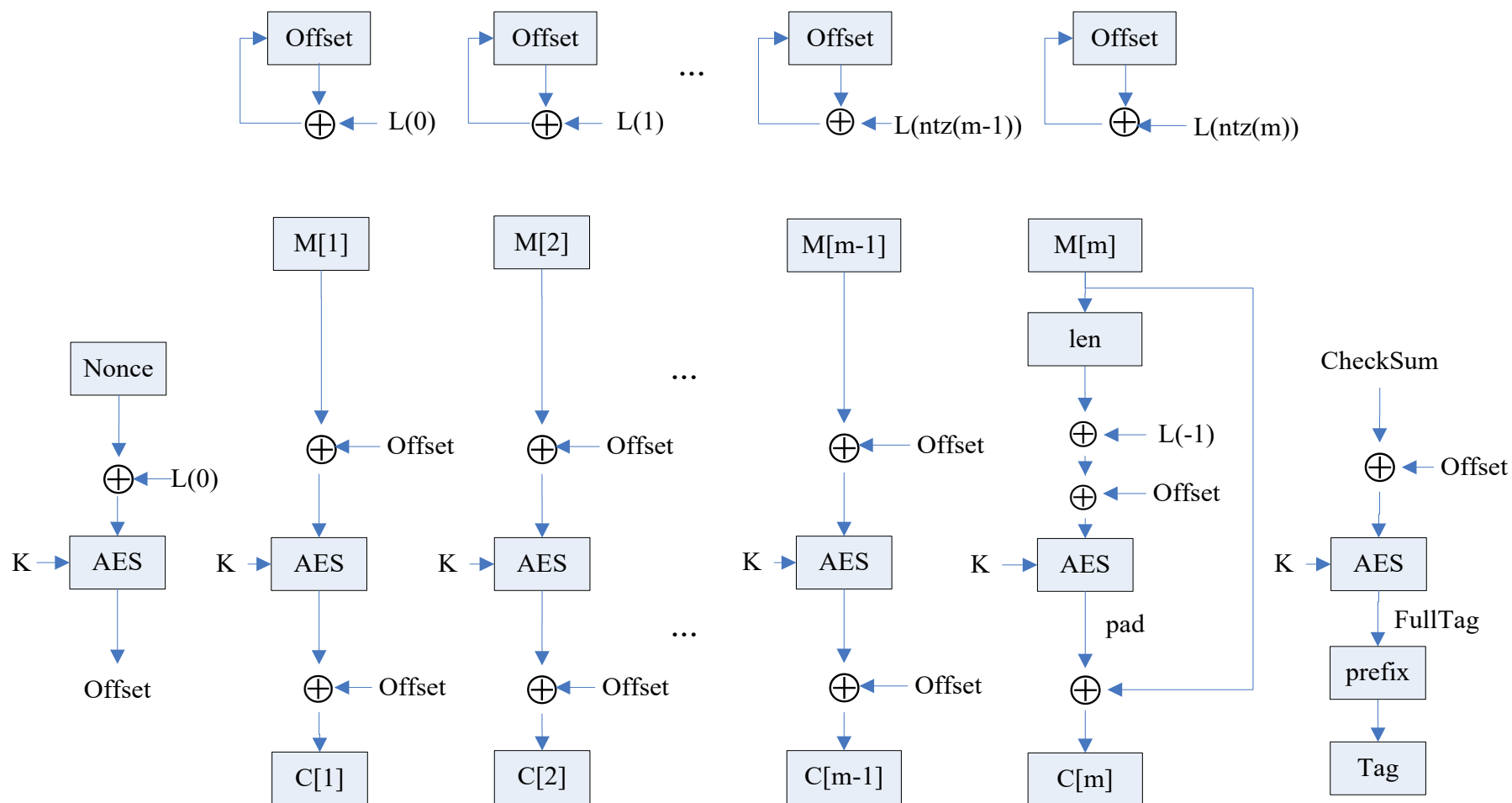
OCB模式

➤ 加密

预先计算: 1) $L(0) = E_k(0)$;

2) $L(-1) = lsb(L(0))?(L(0) \gg 1) \oplus const43 : (L(0) \gg 1)$;

3) For $i > 0$, $L(i) = lsb(L(i-1))?(L(i-1) \ll 1) \oplus const87 : (L(i-1) \ll 1)$;

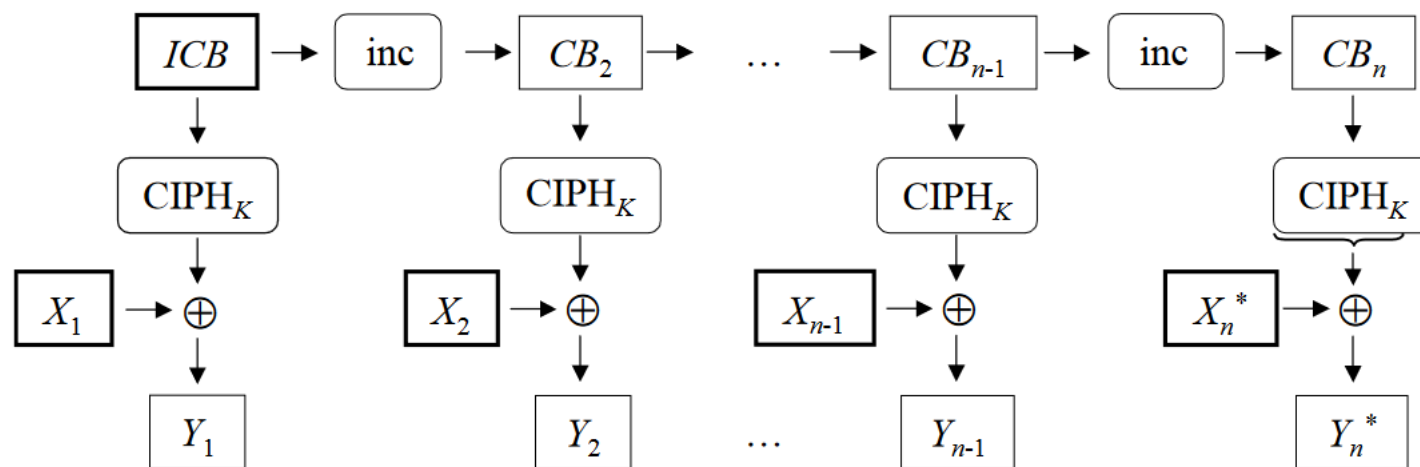
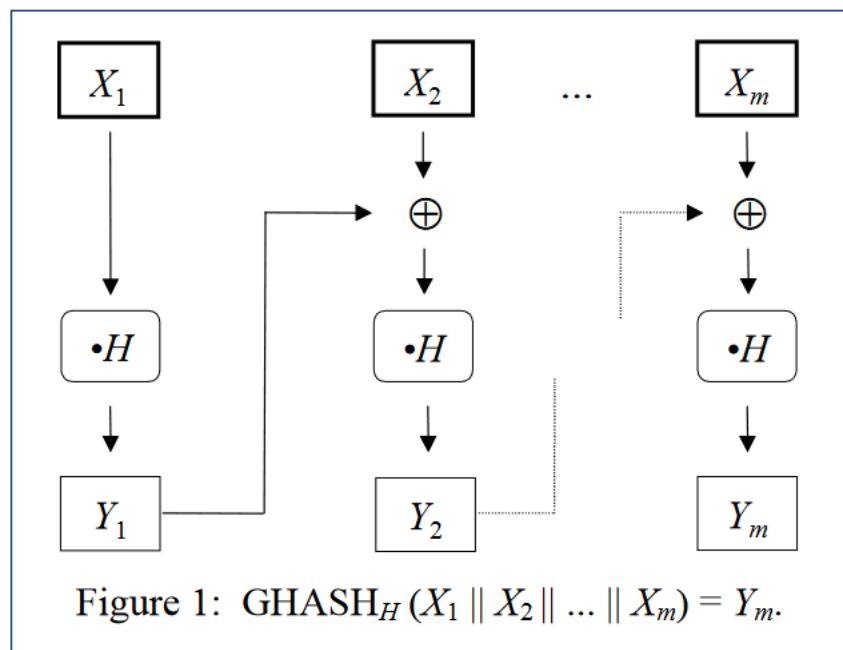


4 对称密码体制的概念与分类

GCM模式

➤ 基础算法

- GHASH: 利用“伽罗瓦域算法”计算比特串X的HASH值;
- $\text{GCTR}_K(\text{ICB}, X)$: 对比特串X和初始分组ICB利用密钥K计算其密文;
- $\text{CIPH}_K(X)$: 对于密钥为K, 分组为X的分组密文的输出。



4 对称密码体制的概念与分类

GCM模式

➤ 发送方流程

GCM加密算法的输入:

1. 初始化向量IV
2. 明文P
3. 关联数据A
4. 密钥K

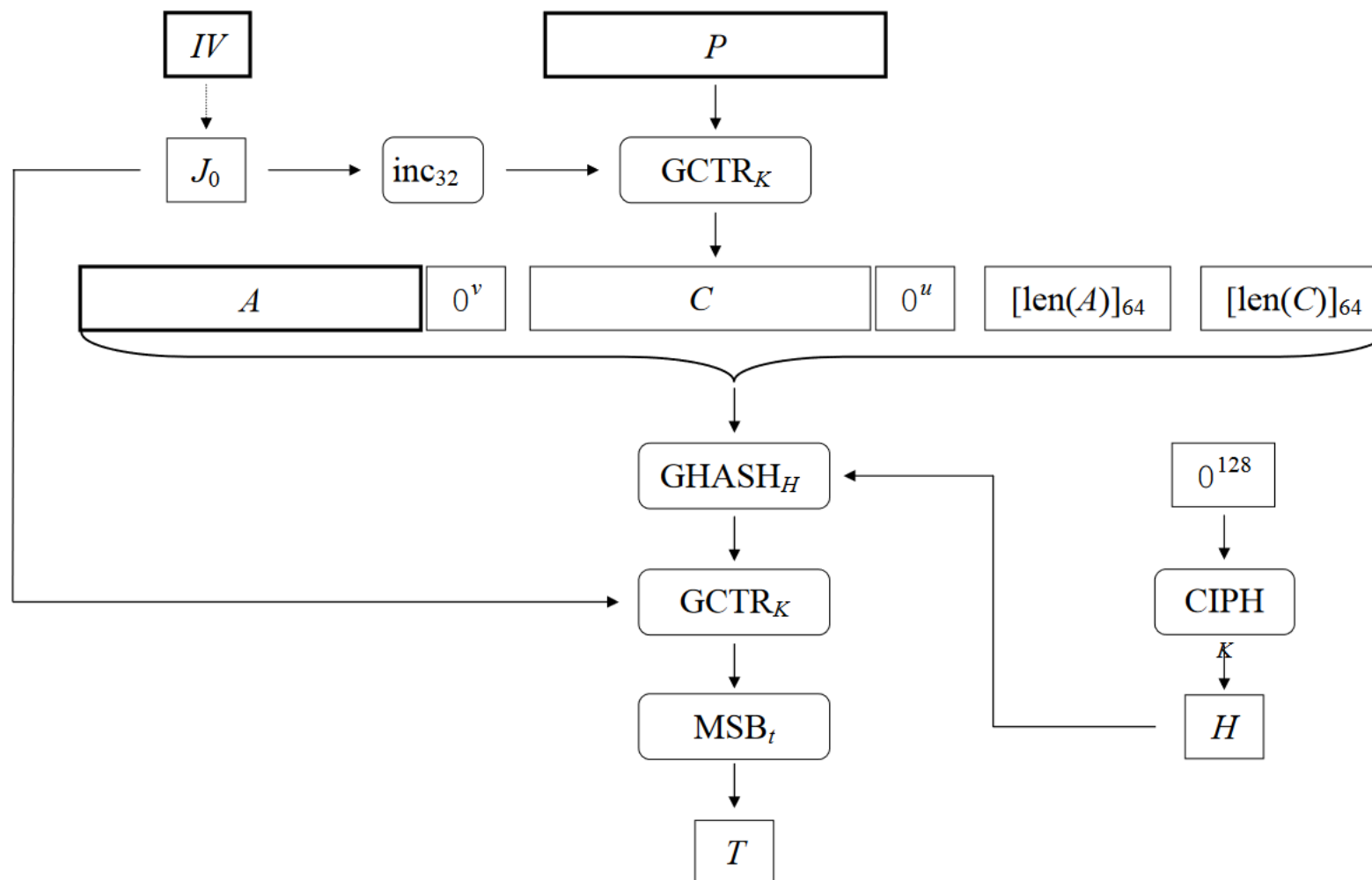
GCM加密算法的输出:

1. 密文C
2. 校验值T

IV生成 J_0 :

If $\text{len}(IV)=96$, then let $J_0 = IV \parallel 0^{31} \parallel 1$.

If $\text{len}(IV) \neq 96$, then let $s = 128 \lceil \text{len}(IV)/128 \rceil - \text{len}(IV)$, and let $J_0 = \text{GHASH}_H(IV \parallel 0^{s+64} \parallel [\text{len}(IV)]_{64})$.



4 对称密码体制的概念与分类

GCM模式

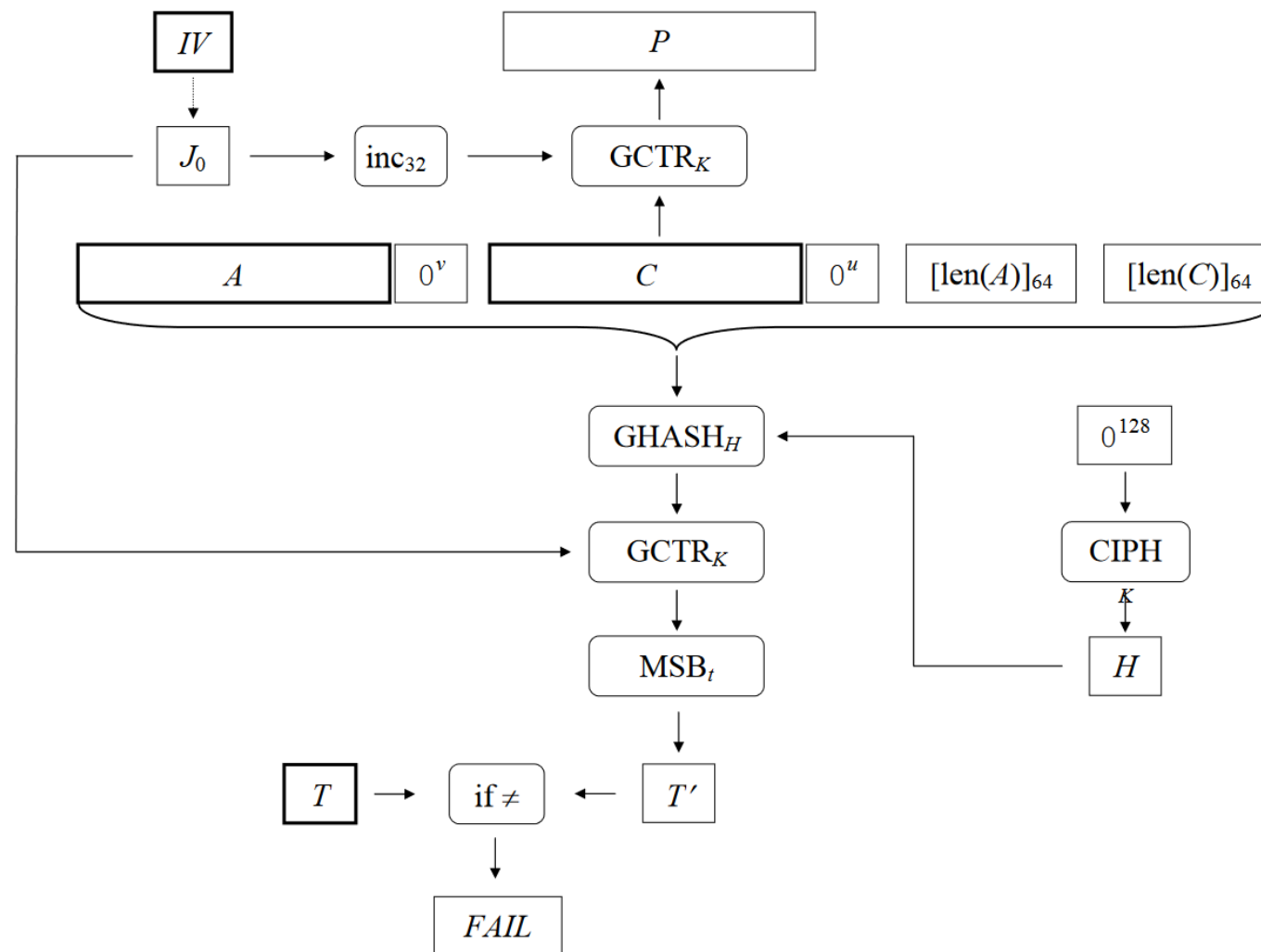
➤ 接收方流程

GCM解密验证算法的输入:

1. 初始化向量IV
2. 密文C
3. 关联数据A
4. 认证值T
5. 密钥K

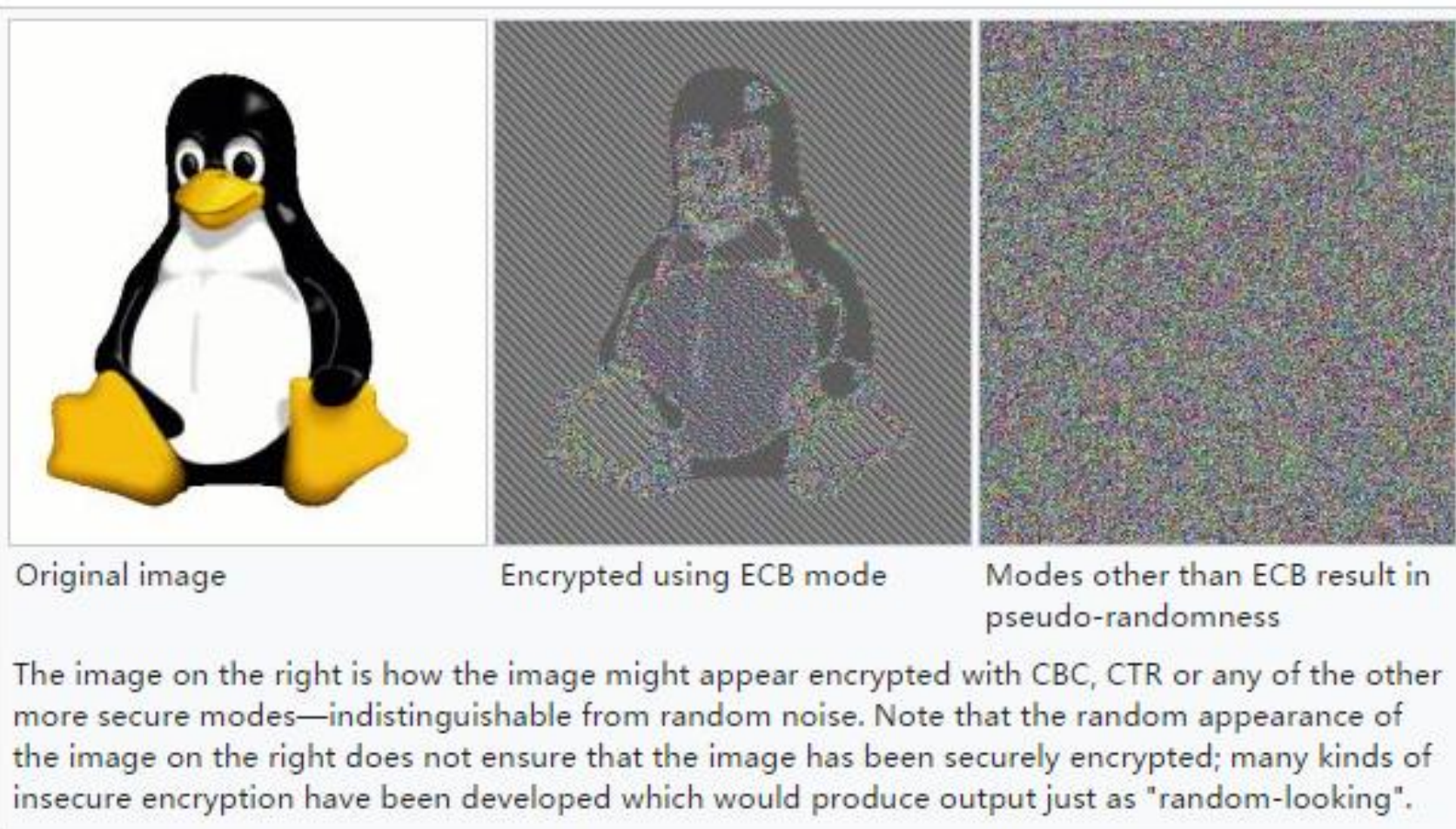
GCM加密算法的输出:

1. 明文P(或者验证失败*FAIL*)



4 对称密码体制的概念与分类

不同模式加密图片的例子



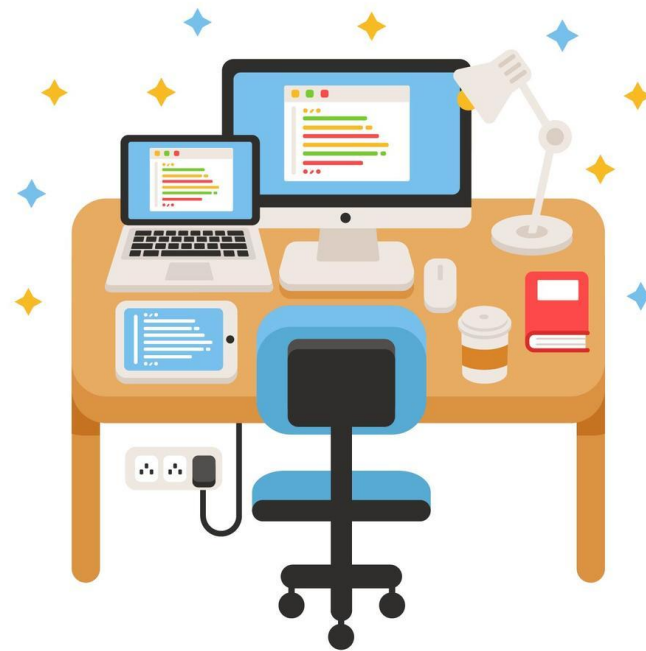
4 对称密码体制的概念与分类

工作模式选用原则

- **CBC,CFB,OFB,CTR**的选择取决于实用特殊考虑;
- **ECB模式**, 简单、高速, 但最弱, 易受重发攻击, 一般不推荐;
- **CBC**适用于文件加密, 但较ECB慢, 且需要另加移存器和组的异或运算, 但安全性加强。软件加密最好选用此种方式;
- **OFB**和**CFB**较**CBC**慢许多, 每次迭代只有少数bit完成加密。若可以容忍少量错误扩展, 可选**CFB**。否则, 可选**OFB**或**CTR**;
- 在字符为单元的流密码种多选**CFB**模式, 如终端和主机间通信。而**OFB**或**CTR**用于高速同步系统, 不容忍差错传播。
- **OCB**模式通过使用同一个密钥对数据的一次处理, 同时提供了加密和数据完整性检测, 适合保护长数据。

本讲内容

1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. 对称密码体制的概念与分类
5. **非对称密码体制**
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



5 非对称密码体制

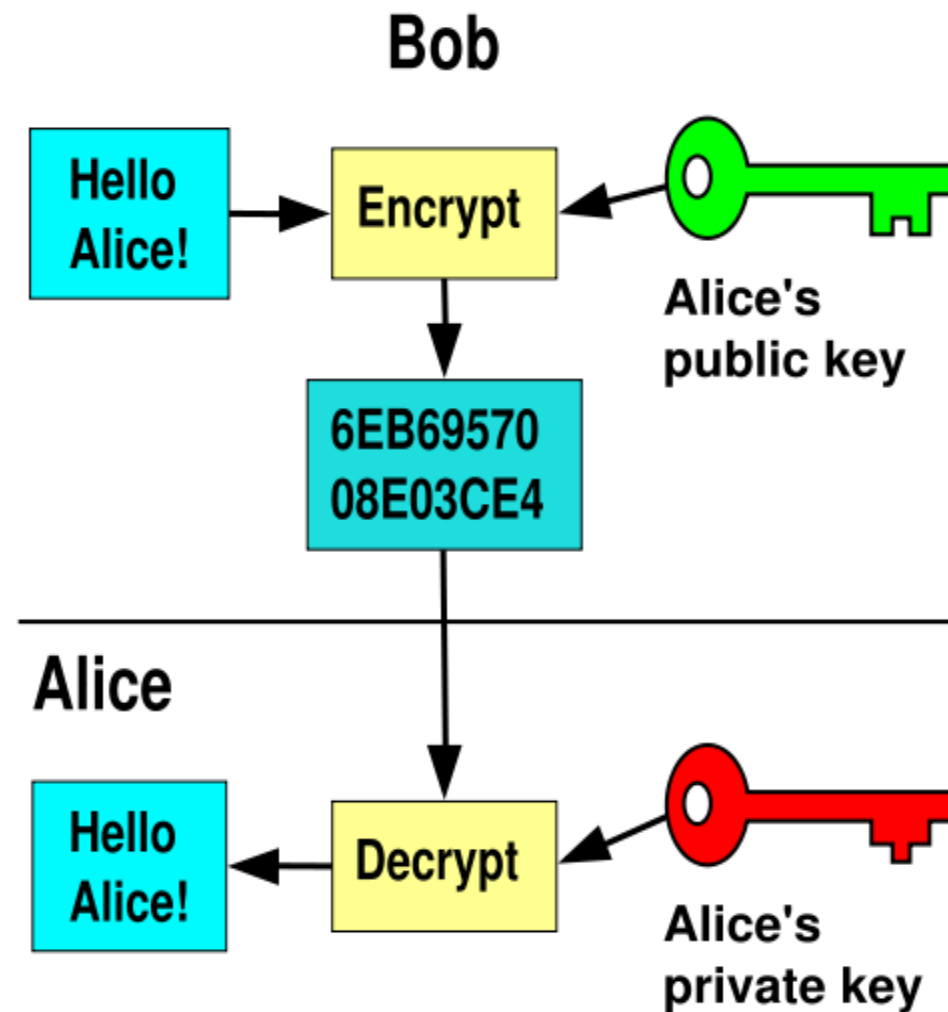
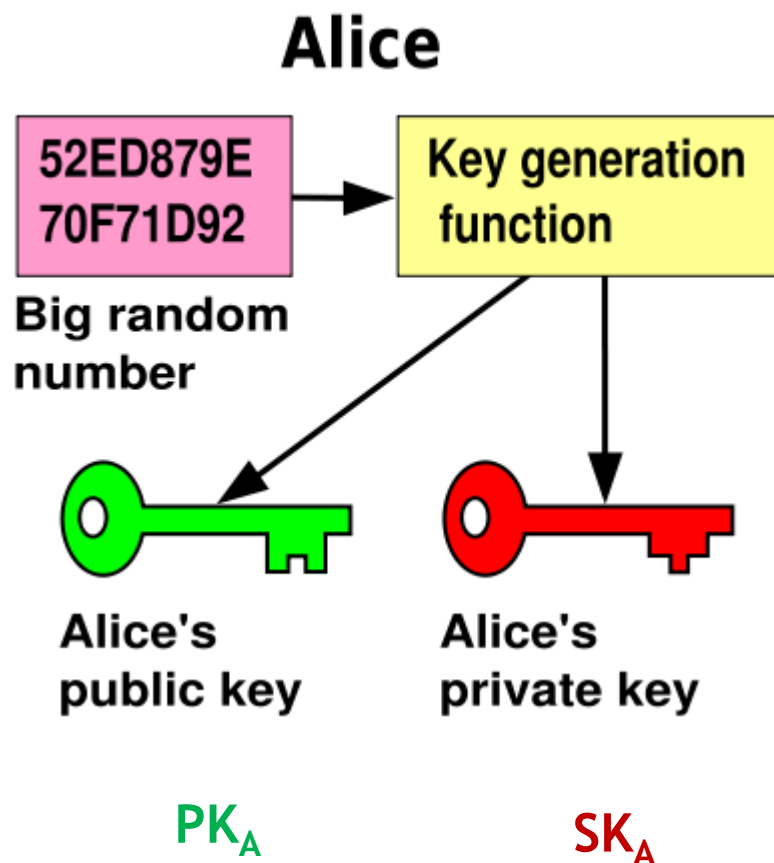
对称密码体制的缺陷

- 密钥管理问题：在有多个用户的网络中，任何两个用户之间都需要有共享的秘密钥，当网络中的用户 n 很大时，需要管理的密钥数目是非常大 $n(n-1)/2$ ；而公钥体制只需要 n 对公/私钥；
- 无签名功能 当主体A收到主体B的电子文档（电子数据）时，无法向第三方证明此电子文档确实来源于B。
- 邮箱的例子
 - 任何人可以向邮箱投举报信
 - 用户（审计人员）才能打开邮箱，读信的内容



5 非对称密码体制

公钥加密模型



5 非对称密码体制

参数生成过程:

- 要求接收消息的端系统，产生一对用来加密和解密的密钥，如图中的接收者A，产生一对密钥 PK_A ， SK_A ，其中 PK_A 是公开密钥， SK_A 是秘密密钥。
- 接收者A将加密密钥（图中的 PK_A ）予以公开，另一密钥被保密（图中的 SK_A ）。

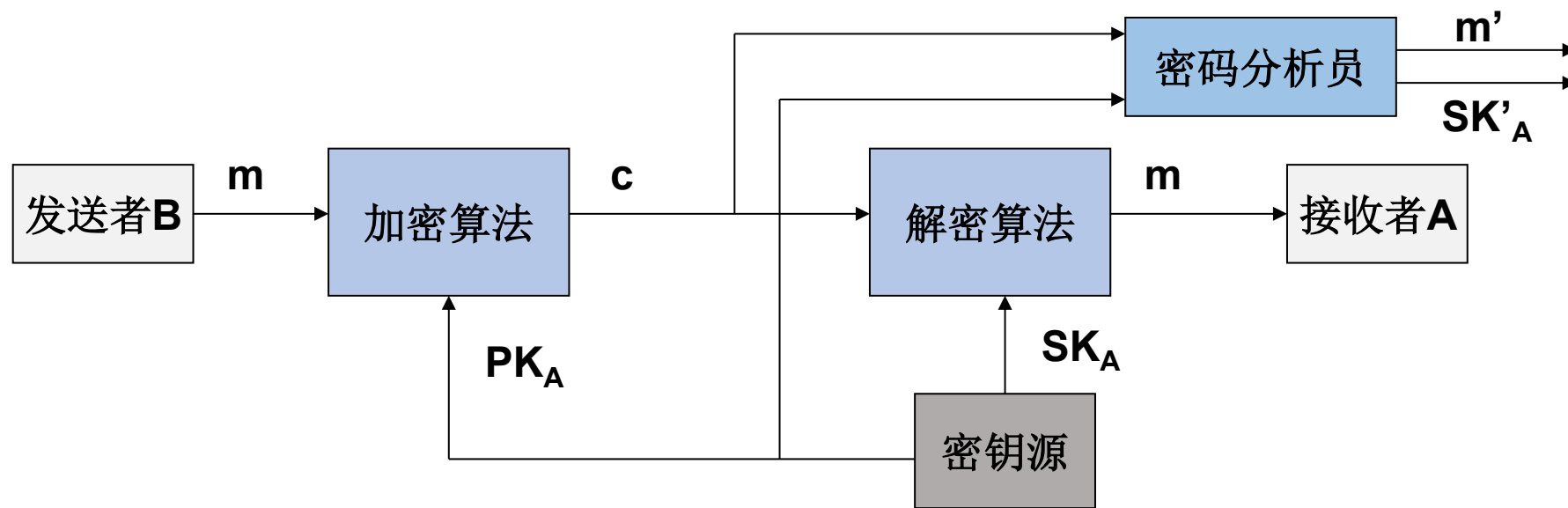
参数生成需满足的要求:

- 由私钥及公开参数容易计算出公开密钥;
- 由公钥及公开参数推导私钥是困难的;

5 非对称密码体制

加解密过程

- B要想向A发送消息 m ，则使用A的公开钥 PK_A 加密 m ，表示为 $c=E_{PK_A}[m]$ ，其中 c 是密文， E 是加密算法。
- A收到密文 c 后，用自己的秘密钥 SK_A 解密，表示为 $m=D_{SK_A}[c]$ ，其中 D 是解密算法。



公钥加密体制框图

5 非对称密码体制

加解密算法需满足要求

- 利用公钥及公开参数加密明文容易计算；
- 利用私钥及公开参数解密密文容易计算；
- 只利用公钥解密密文困难；
- 加、解密次序可换，即

$$E_{PKA}[D_{SKA}(m)] = D_{SKA}[E_{PKA}(m)]$$

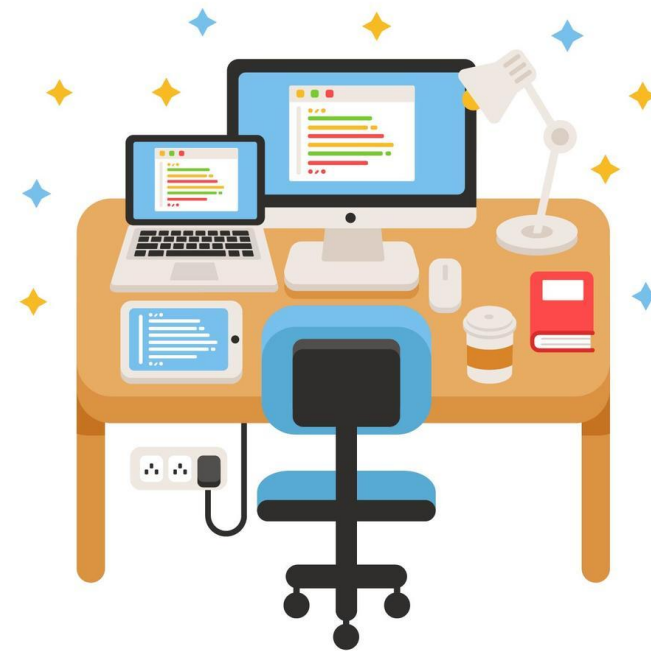
- 这一条虽然非常有用，但不是对所有的算法都作要求。

典型公钥密码算法

- RSA算法、ElGamal算法、椭圆曲线密码算法等

本讲内容

1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. 对称密码体制的概念与分类
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



传统签名的基本特点:

- 能与被签的文件在物理上不可分割
- 签名者不能否认自己的签名
- 签名不能被伪造
- 容易被验证

数字签名是传统签名的数字化，基本要求:

- 能与所签文件“绑定”
- 签名者不能否认自己的签名
- 签名不能被伪造
- 容易被验证

6 数字签名

➤ 基本流程

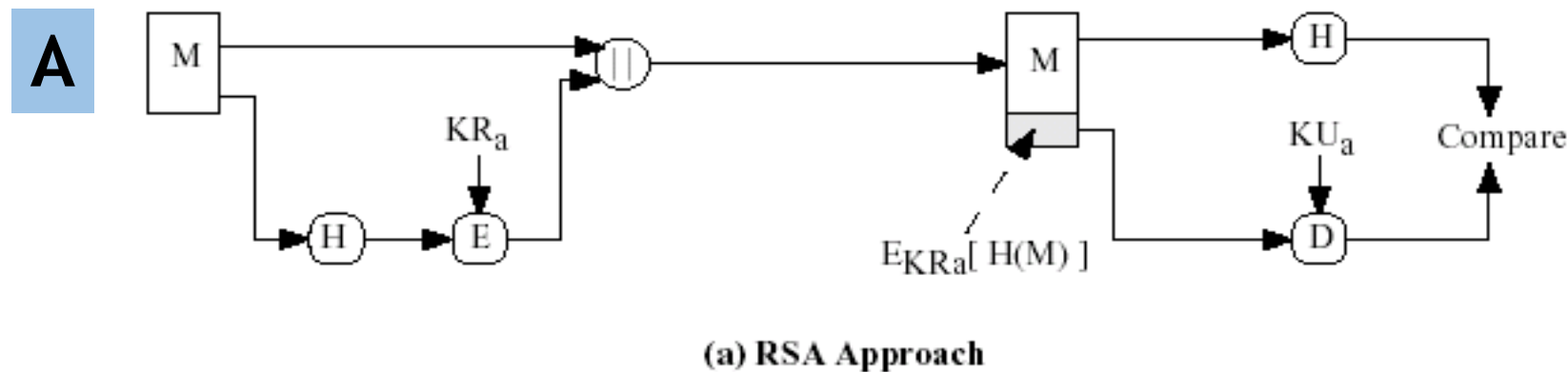
- 先对消息 M 作一个摘要 $H(M)$
- 然后发送方用自己的私钥对 $H(M)$ 进行加密，得到签名 $E_{K_{Ra}}(H(M))$
- 连同消息 M 一起，发送出去
- B收到复合的消息之后，把签名提取出来
- B用A的公钥对签名解密得到 H'
- B计算所收到消息的摘要 $H(M')$
- 如果 $H'=H(M')$ ，则消息确实是A产生的

➤ 问题

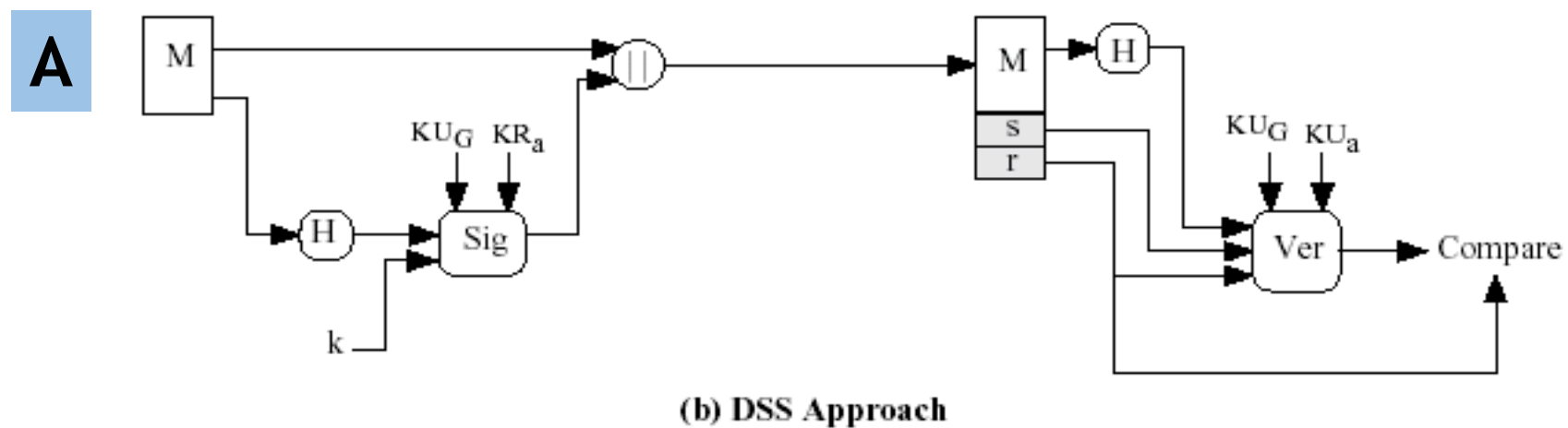
- 公钥的管理，公钥与身份的对应关系
- 签名的有效性，私钥丢失？

6 数字签名

RSA签名方案



DSS签名方案



注: KU_G 全局公共密钥; K 一个随机数



Anamarija Pogorelec, Managing Editor, Help Net Security

March 12, 2026

Share



Wireless vulnerabilities are doubling every few years

Wireless vulnerabilities are being disclosed at a rate that has no precedent in the fifteen-year history of systematic tracking. In 2025, researchers published 937 new wireless-related CVEs, an average of 2.5 per day, according to a threat report from Bastille Networks based on data from the NIST National Vulnerability Database.

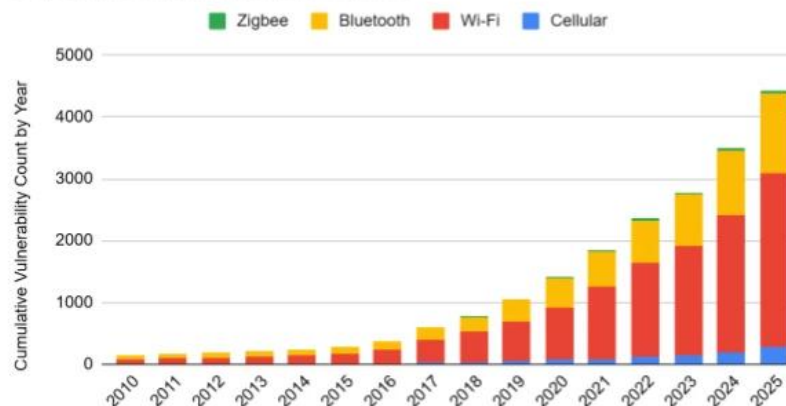
Bastille Networks 发布无线安全报告

- 2025年披露 937个无线相关漏洞（CVE）
- 平均每天2.5个无线漏洞
- 15年增长230倍
- 增长速度是整体漏洞的20倍
- Wi-Fi: 占60%以上
- 漏洞覆盖芯片级和协议

Wireless Threats Increasing 20X Faster than Overall CVE disclosures!

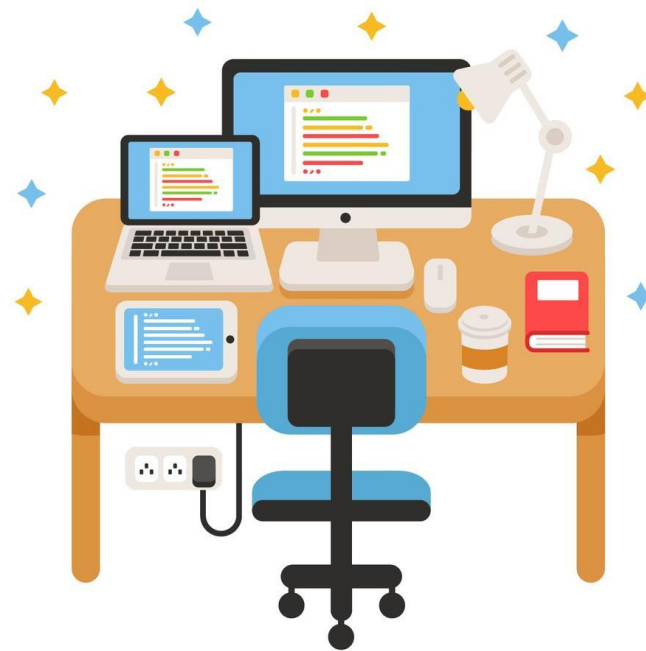
Wireless Threat Growth 2010 - 2025

Source: NIST National Vulnerability Database



- Over the past 15 years, wireless vulnerabilities have grown more than 230X
- Wireless increasing over 20X faster than overall CVE disclosures.
- Wi-Fi and Bluetooth drive most of this growth, while cellular and IoT protocols steadily expand the attack surface.

1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. 对称密码体制的概念与分类
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述

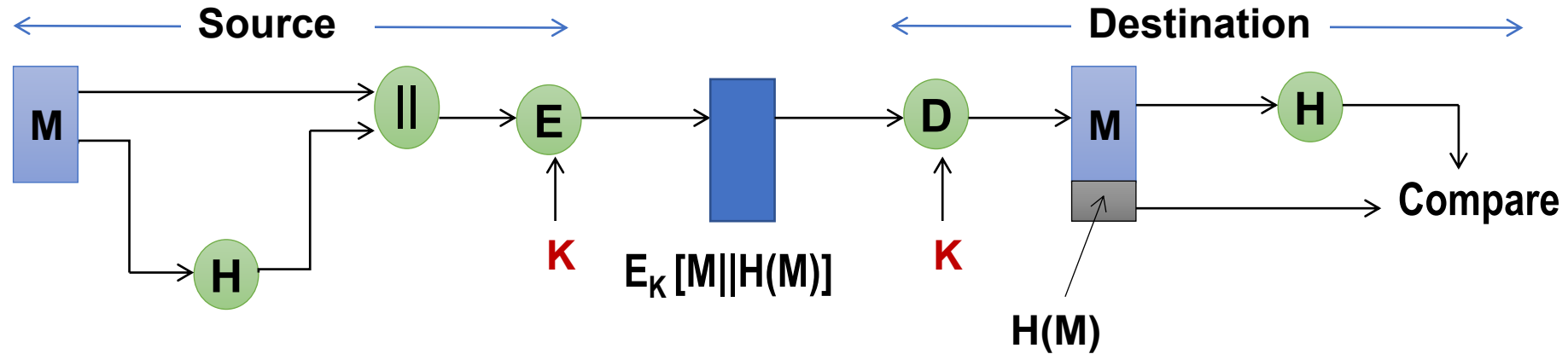


散列函数基本概念

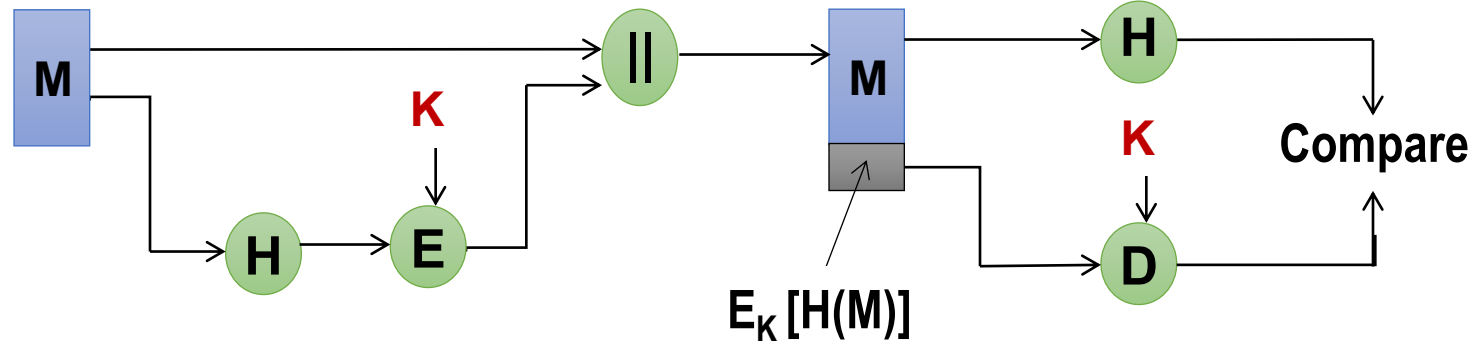
- $H(M)$: 输入为任意长度的消息 M ; 输出为一个固定长度的散列值, 称为消息摘要(MessageDigest)。
- 这个散列值是消息 M 的所有位的函数并提供错误检测能力: 消息中的任何一位或多位的变化都将导致该散列值的变化。
- 又称为哈希函数、数字指纹 (Digitalfinger print)。

7 散列函数

散列函数的基本用法(a、b)



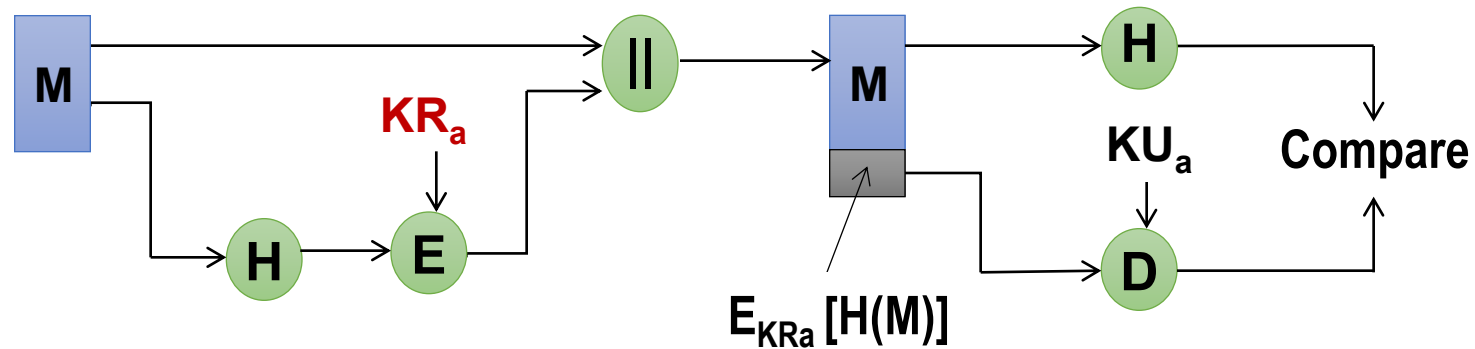
- (a) Provides confidentiality - - only A and B share K
Provides authentication - - $H(M)$ is cryptographically protected



- (b) Provides authentication - - $H(M)$ is cryptographically protected

7 散列函数

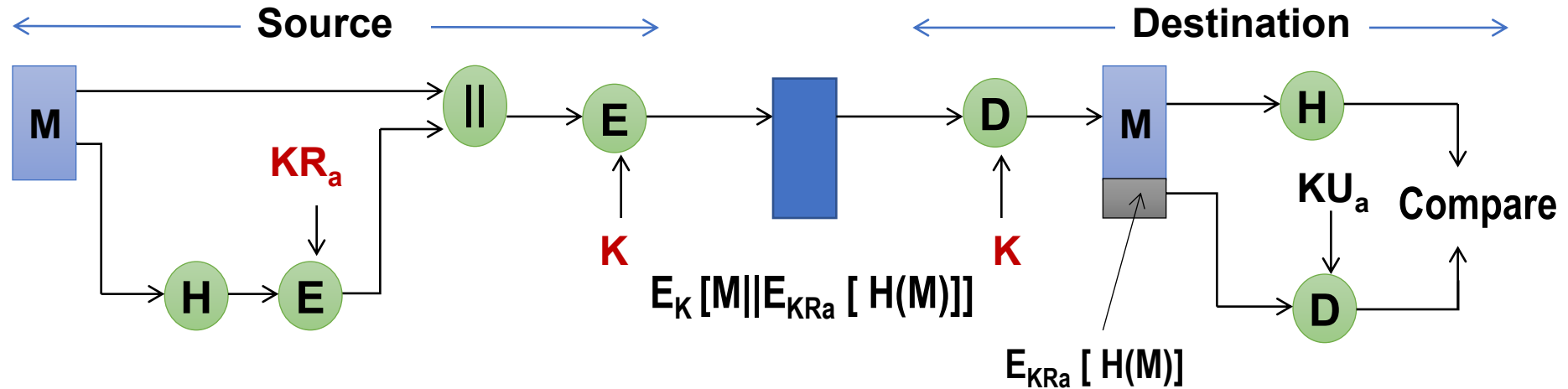
散列函数的基本用法(c)



- (c) **Provides authentication and digital signature**
- $H(M)$ is cryptographically protected
 - only A could create $E_{KR_a}[H(M)]$

7 散列函数

散列函数的基本用法(d)

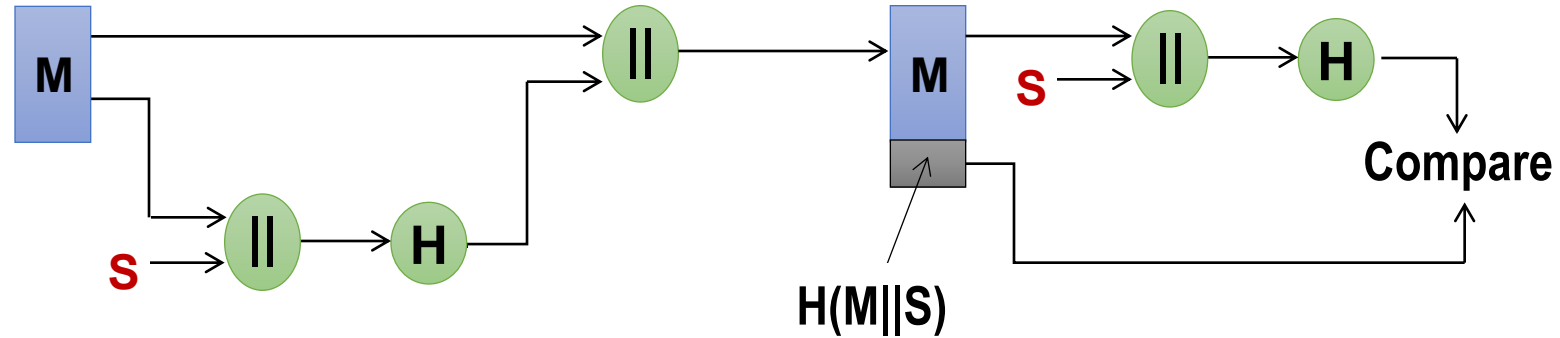


(d) $A \rightarrow B: E_K[M \parallel E_{KR_a}[H(M)]]$

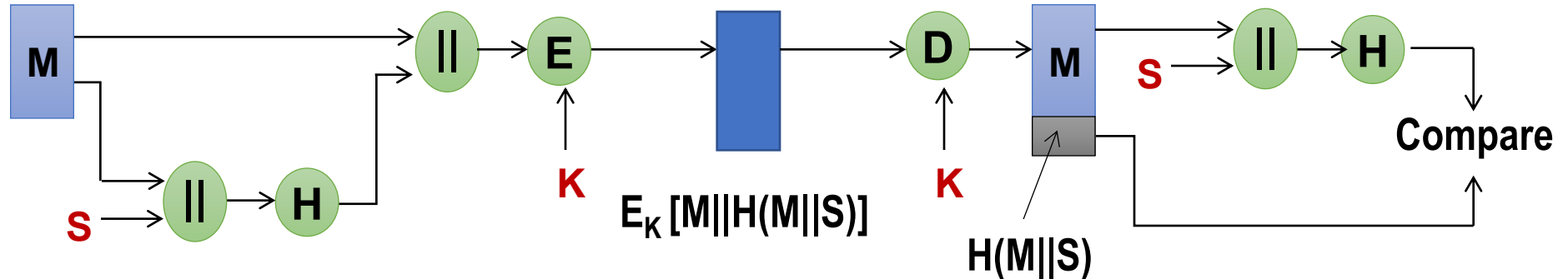
- Provides authentication and digital signature
- Provides confidentiality

7 散列函数

散列函数的基本用法(e、f)



(e) Provides authentication -- only A and B share S



(f) Provides authentication -- only A and B share S
Provides confidentiality -- only A and B share K

7 散列函数

Hash函数要求

Hash函数: $h=H(x)$, 要求:

- 定长输出: 可作用于任何尺寸数据且均产生定长输出
- 快速计算: $H(x)$ 能够快速计算
- 单向性: 给定 h , 找到 x 使 $h=H(x)$ 在计算上不可行
- 弱抗冲突**Weak Collision Resistance(WCR):**
给定 x , 找到 $y \neq x$ 使 $H(x)=H(y)$ 在计算上不可行
- 强抗冲突**Strong Collision Resistance(SCR):**
找到 $y \neq x$ 使 $H(x)=H(y)$ 在计算上不可行

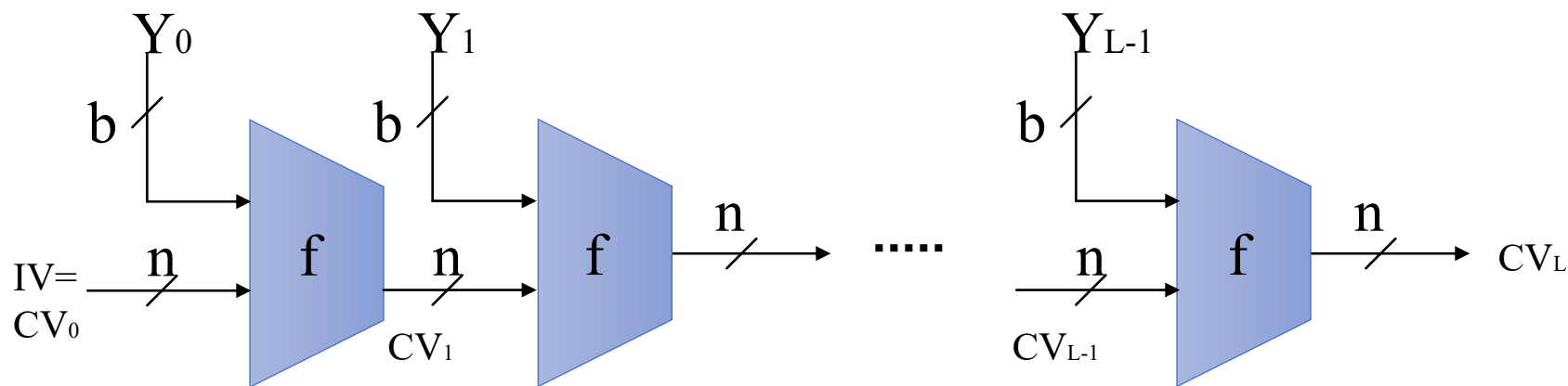
7 散列函数

hash函数通用模型

- 由Merkle于1989年提出
- 几乎被所有hash算法采用
- 具体做法：
 - 把原始消息M分成一些固定长度的块 Y_i
 - 最后一块padding并使其包含消息M的长度
 - 设定初始值 CV_0
 - 压缩函数 f , $CV_i = f(CV_{i-1}, Y_{i-1})$
 - 最后一个 CV_i 为hash值

7 散列函数

hash函数模型图



IV = initial value 初始值

CV = chaining value 链接值

Y_i = i th input block (第 i 个输入数据块)

f = compression algorithm (压缩算法)

n = length of hash code (散列码的长度)

b = length of input block(输入块的长度)

$CV_0 = IV =$ initial n -bit value
 $CV_i = f(CV_{i-1}, Y_{i-1})$ ($1 \leq i \leq L$)
 $H(M) = CV_L$

7 散列函数

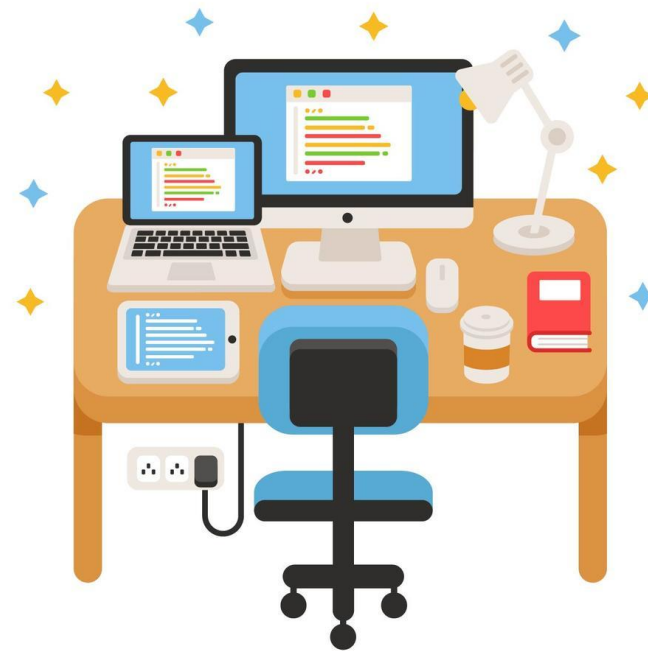
Hash函数例子

- **MD5报文摘要算法**
- **安全散列算法SHA (Secure Hash Algorithm)**
 - SHA-1
 - SHA-2(SHA-224、SHA-256、SHA-384 和 SHA-512)
- **RIPEMD-160报文摘要算法**
- **HMAC**

密码算法: 结论

- **我们通常假设核心密码算法是安全的，需要关注加密算法的使用细节**
 - 进行机密性保护的模式是否正确使用？
 - 加密多次是否反而会泄露信息？
- **简单的应用方式更能保证方案的安全性等同于密码算法的安全性，
越复杂≠越安全。**
- **必须明确使用密码算法的目的。**

1. 密码学的基本概念
2. 古典密码
3. 密码体制的安全性要素
4. 对称密码体制的概念与分类
5. 非对称密码体制
6. 数字签名
7. 散列函数
8. 认证理论与技术概述



8. 认证理论与技术概述

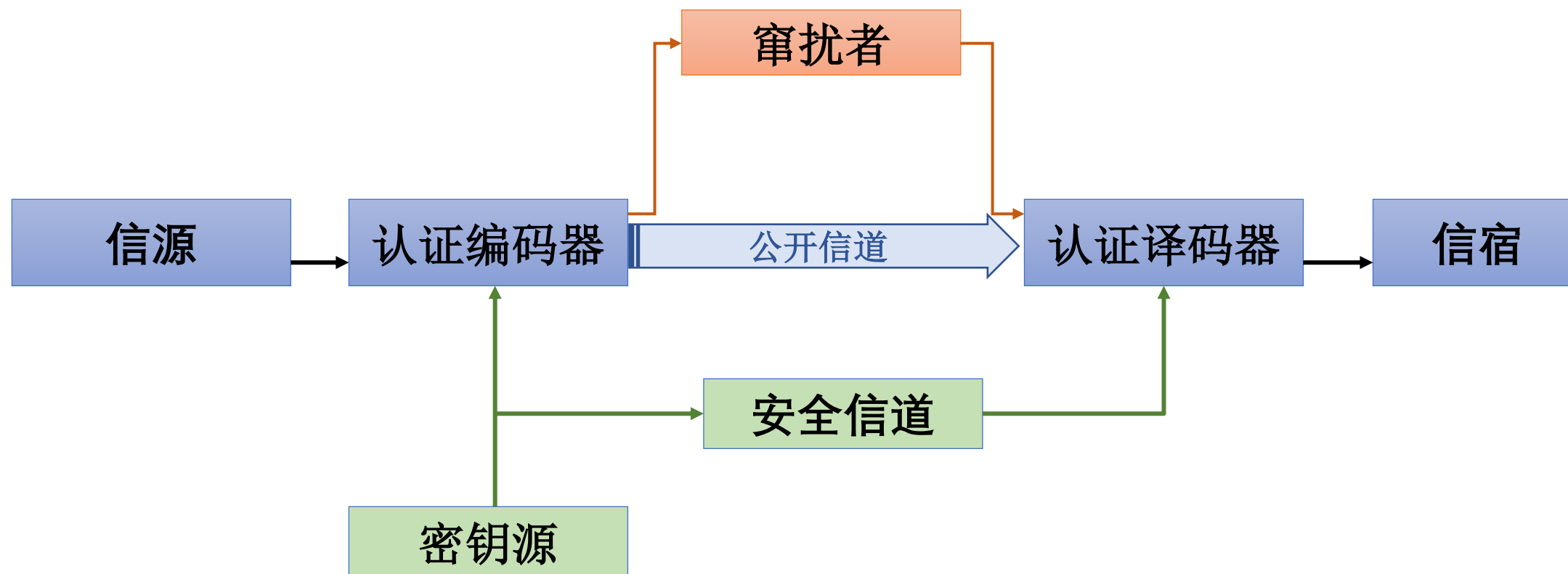
认证概念

- 认证或鉴权（**authentication**）
 - 防止主动攻击
- 认证的**目的**:
 - **实体认证（entity authentication）**：验证信息的发送者/接收者是真正的，而不是冒充的，此为信源/信宿识别；
 - **消息源认证（origin authentication/message authentication）**：验证信息的来源，验证消息在传送或存储过程中未被篡改，重放或延迟等。
- 保密和认证同时是信息系统安全的两个方面，但它们是两个不同属性的问题，认证不能自动提供保密性，而保密性也不能自然提供认证功能。

8. 认证理论与技术概述

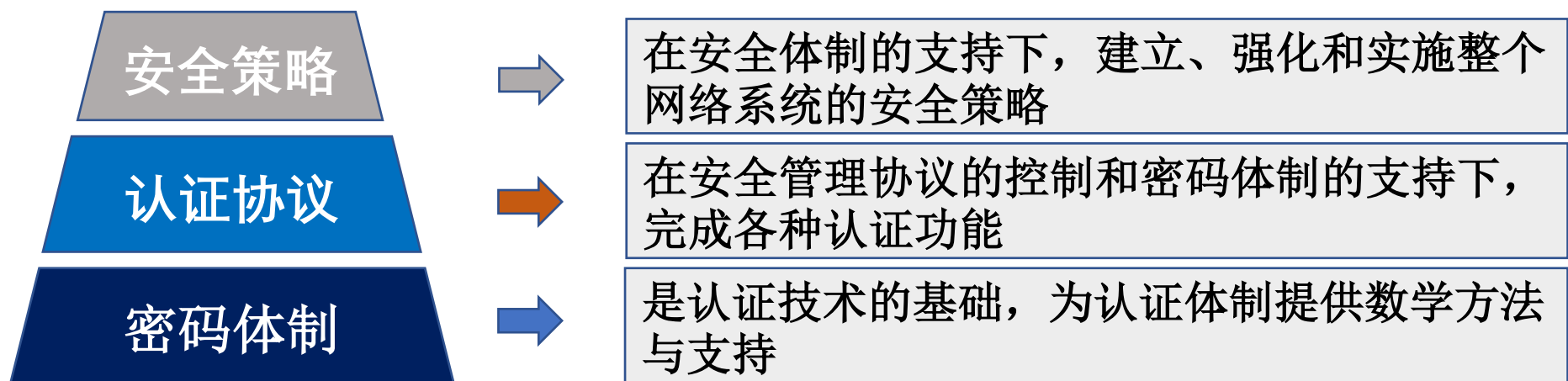
认证系统基本模型

➤ 一个纯认证系统的模型如下图所示：



8. 认证理论与技术概述

认证技术的三个层次



一个安全的认证系统

- ▶ 首先选择恰当的**认证函数**
- ▶ 然后给出合理的**认证协议**(Authentication Protocol)。
- ▶ 最后制定理想的**安全策略**

8. 认证理论与技术概述

认证函数

可用来做认证的函数分为三类：

(1) 信息加密函数(Message encryption)

用完整信息的密文作为对信息的认证。

(2) 信息认证码MAC(Message Authentication Code)

是对信源消息的一个编码函数。

(3) 散列函数(Hash Function)

是一个公开的函数，它将任意长的信息映射成一个固定长度的信息。

8. 认证理论与技术概述

安全协议

- 协议的定义：两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。
- 安全协议：具有安全性功能的协议称为安全协议，也称作密码协议。
- 所谓协议是安全的，意味着非法用户不可能从协议中获得比协议自身所体现的更多的、有用的信息。
- 安全协议分类
 - 密钥建立协议（Key Establishment Protocol）
 - ✓ 建立共享密钥
 - 认证建立协议（Authentication Protocol）
 - ✓ 向一个实体提供对他想要进行通信的另一个实体的身份的某种程度的确信
 - 认证的密钥建立协议（Authenticated Key Establishment Protocol）
 - ✓ 与另一身份已被或可被证实的实体之间建立共享秘密

8. 认证理论与技术概述

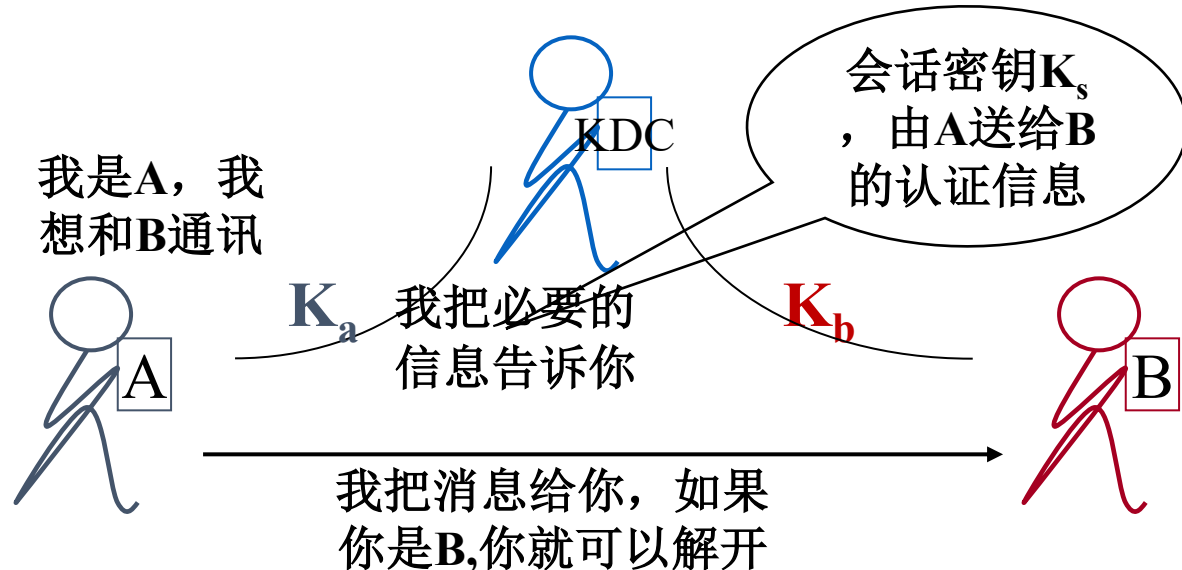
例1：采用单钥体制的密钥建立协议

- 假设A和B要进行通讯，A和B与KDC各有一个共享密钥 K_a 和 K_b ，如何利用这两个密钥进行认证，并且商定一个会话密钥 K_s

1. $A \rightarrow KDC: (ID_A || ID_B || N_1)$
2. $KDC \rightarrow A: E_{K_a}[K_s || ID_B || N_1 || E_{K_b}(K_s, ID_A)]$
3. $A \rightarrow B: E_{K_b}(K_s, ID_A) || E_{K_s}(M)$

- 分析：

- 安全性依赖于KDC的安全性；
- KDC成为影响系统性能的瓶颈；



8. 认证理论与技术概述

例2: Merkle协议

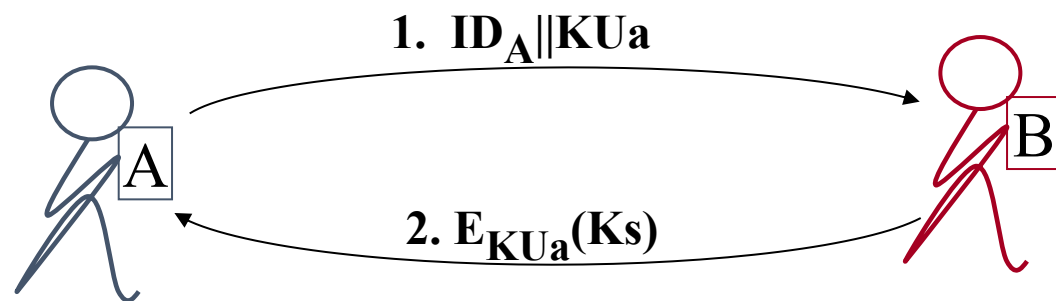
➤ 采用双钥体制的密钥建立协议

➤ 协议描述

- A生成 $\{KU_a, KR_a\}$, $A \rightarrow B: (ID_A, KU_a)$
- B生成随机密钥 K_s , $B \rightarrow A: E_{KU_a}(K_s)$
- A解密 $E_{KU_a}(K_s)$ 得到 K_s : $DKR_a(E_{KU_a}(K_s))$
- A丢弃 $\{KU_a, KR_a\}$, B丢弃 KU_a

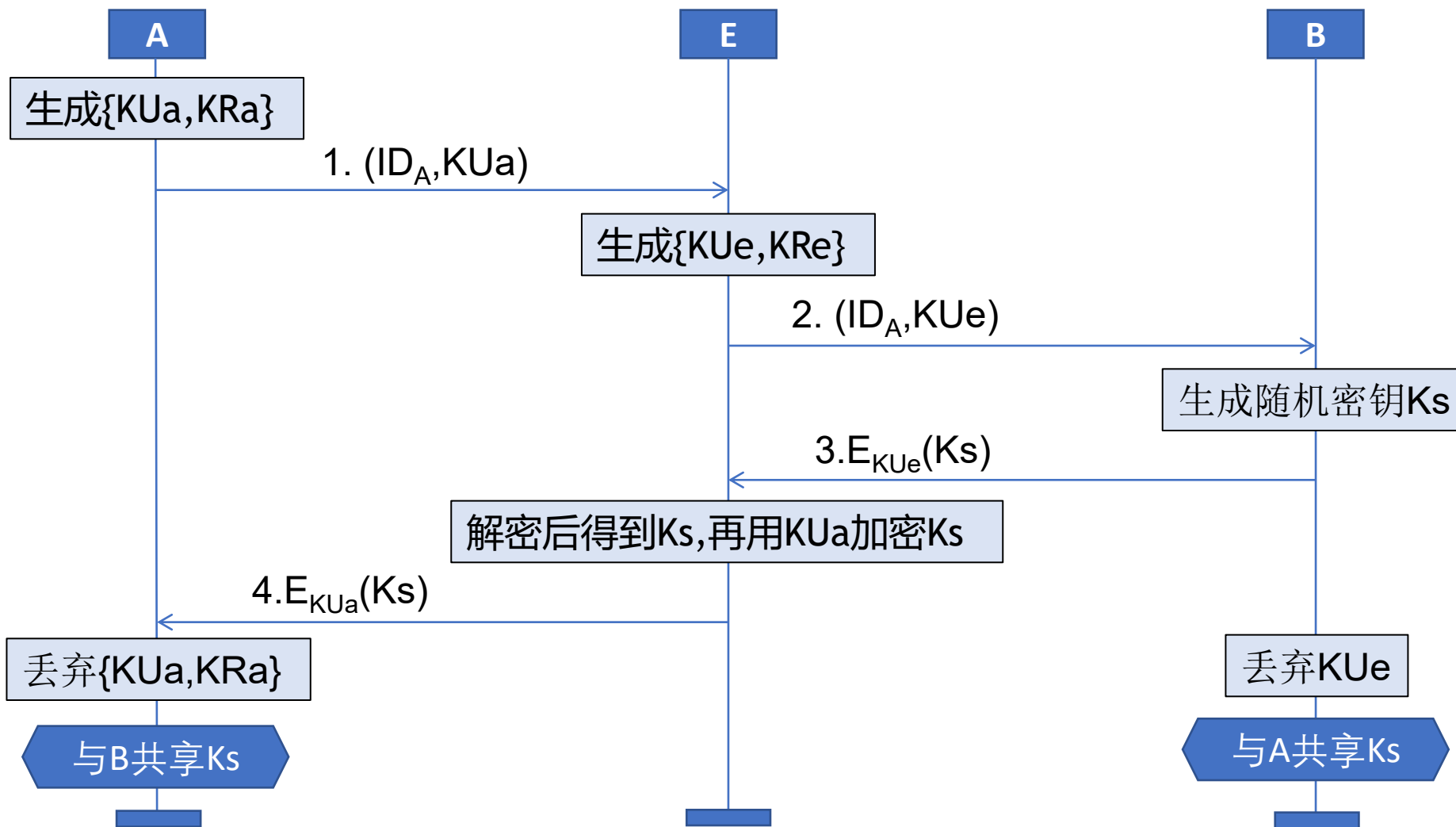
➤ 分析

- 通讯前不需存在密钥, 通讯后也不存在密钥
- 无法防止中间人攻击, 原因是Alice和Bob没有办法来验证他们正在与另一方会话。



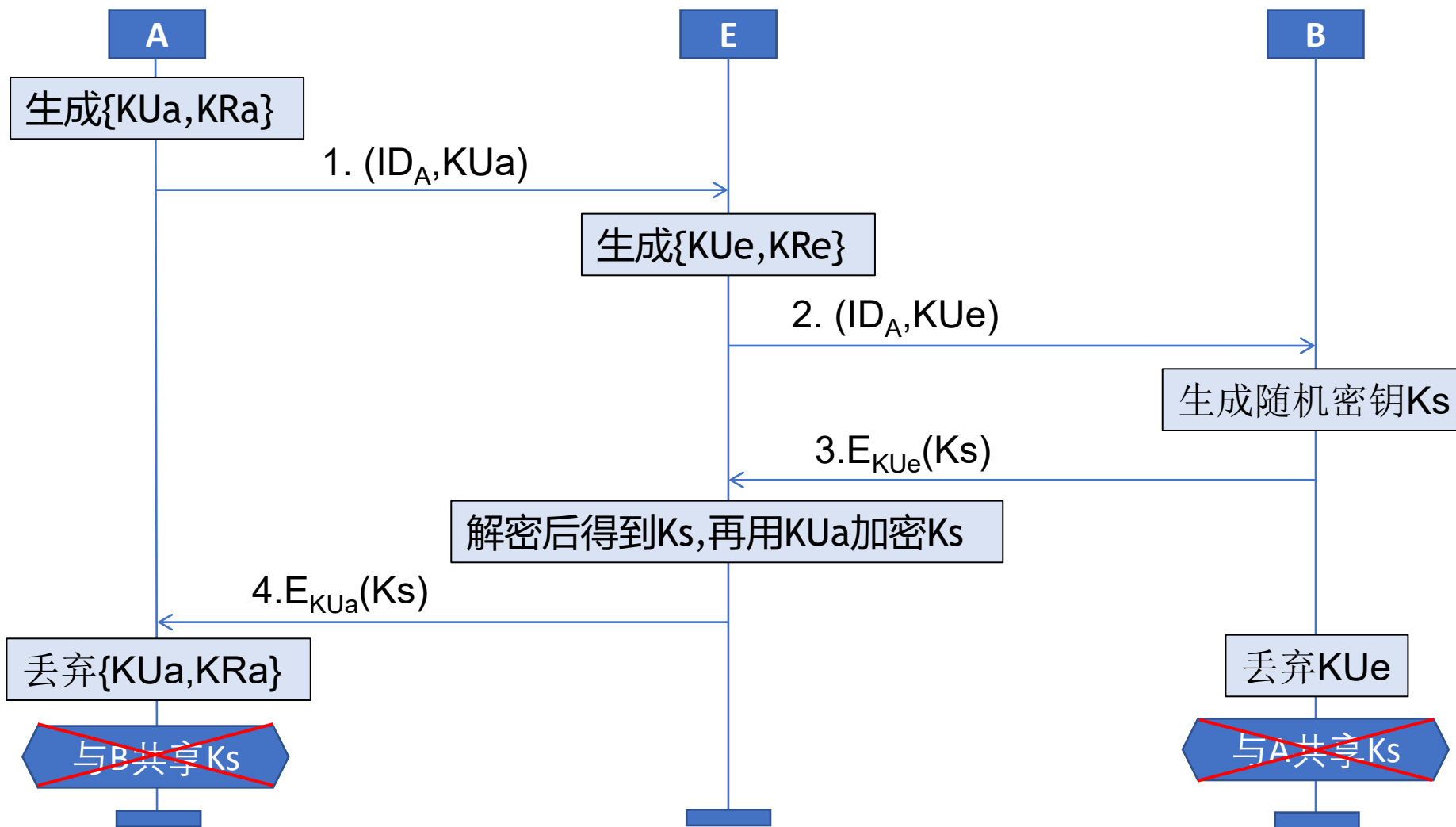
8. 认证理论与技术概述

例2: Merkle协议的中间人攻击



8. 认证理论与技术概述

例2: Merkle协议的中间人攻击



8. 认证理论与技术概述

例3: Diffie-Hellman密钥交换协议

- 允许两个用户可以安全地交换一个秘密信息，用于后续的通讯过程
- 算法的安全性依赖于计算离散对数的难度
- 协议描述：
 - 双方选择素数 p 以及 p 的一个[原根](#) r
 - A选择 $x < p$, 计算 $X_A = r^x \bmod p$, $A \rightarrow B: X_A$
 - B选择 $y < p$, 计算 $Y_B = r^y \bmod p$, $B \rightarrow A: Y_B$
 - A计算: $(Y_B)^x \equiv (r^y)^x \equiv r^{xy} \bmod p$
 - B计算: $(X_A)^y \equiv (r^x)^y \equiv r^{xy} \bmod p$
 - 双方获得一个共享密钥($r^{xy} \bmod p$)
- 素数 p 以及 p 的原根 r 可由一方选择后发给对方

8. 认证理论与技术概述

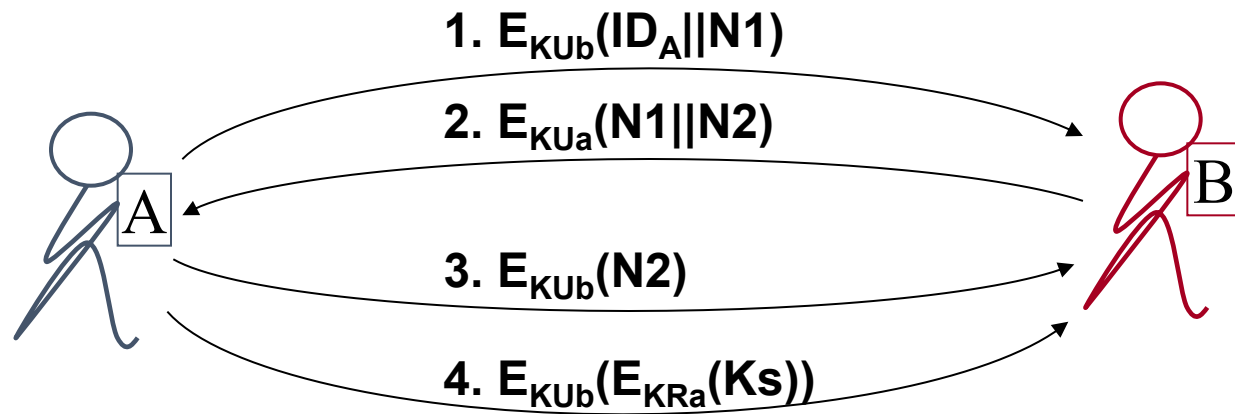
认证建立协议

- 采用单向函数的认证协议
 - Alice向主机发送她的口令
 - 主机计算该口令的单向函数值；
 - 主机将计算得到的单向函数值与预先存储的值进行比较

- 问题
 - 上述协议的前提条件？
 - 上述协议要抵御的威胁？

8. 认证理论与技术概述

认证的密钥建立协议



假定**A**和**B**已经获得了双方的公钥:

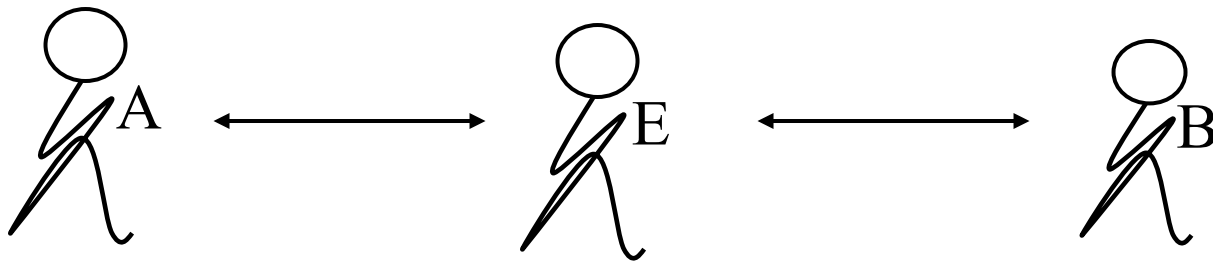
基于公钥的**NS**协议

1. **A** $\rightarrow$ **B**: $E_{KU_b}(ID_A, N1)$
2. **B** $\rightarrow$ **A**: $E_{KU_a}(N1, N2)$
3. **A** $\rightarrow$ **B**: $E_{KU_b}(N2)$
4. **A** $\rightarrow$ **B**: $Y = E_{KU_b}(E_{KR_a}(Ks))$
5. **B**解密 Y 获得会话密钥 $Ks = D_{KU_a}(D_{KR_b}(Y))$

8. 认证理论与技术概述

针对认证协议的一些常见攻击手段和相应对策

- 中间人攻击(MITM, man in the middle)

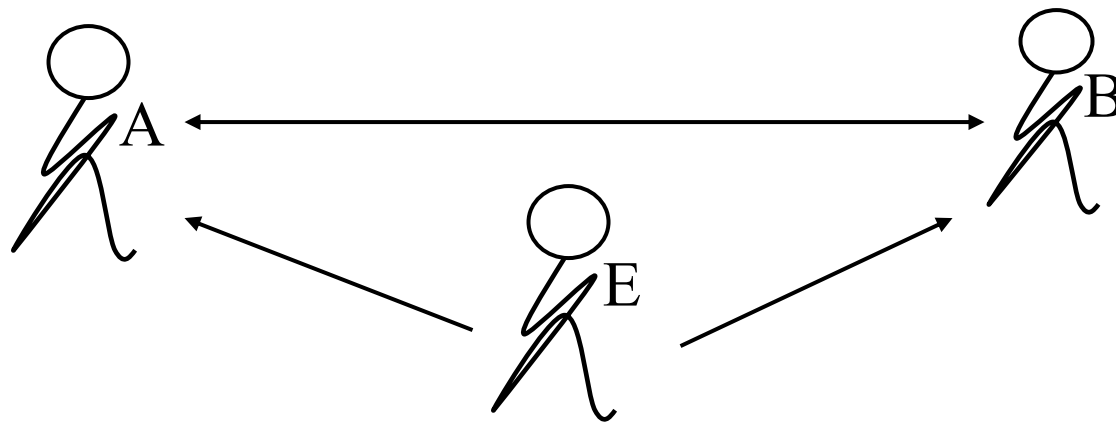


- 如果通讯双方没有任何先决条件，那么这种攻击总是存在的
- A和B的协商过程很容易受到这一类攻击
- 对策：
 - 增加A和B之间的先决知识

8. 认证理论与技术概述

针对认证协议的一些常见攻击手段和相应对策

➤ 重放攻击(replay attacks)



➤ 偷听者可以记录下当前的通讯流量，以后在适当的时候重发给通讯的某一方，达到欺骗的目的

➤ 对策：

- 序列号机制
- 时间戳机制
- 挑战-应答机制

8. 认证理论与技术概述

针对认证协议的一些常见攻击手段和相应对策

➤ 字典攻击

- 通过尝试可能的密码（单词或短语）的攻击方式
- 与暴力破解不同
- 攻击前提

- 了解协议过程
- 拥有比较全面的口令集

➤ 对策

- 选择强壮的口令（长度足够、含有各种字母、数字等各种类型）；
- 频繁更新口令
- 协议设计：
 - 口令的使用过程中，不要泄露口令
 - 在密文中增加口令以外的额外信息

8. 认证理论与技术概述

认证协议中的常见技术

➤ 时间戳

➤ A收到一个消息，根据消息中的时间戳信息，判断消息的有效性

- 如果消息的时间戳与A所知道的当前时间足够接近

➤ 这种方法要求不同参与者之间的时钟需要同步

- 在网络环境中，特别是在分布式网络环境中，时钟同步并不容易做到
- 一旦时钟同步失败
 - 要么协议不能正常服务，影响可用性(availability)，造成拒绝服务(DOS)
 - 要么放大时钟窗口，造成攻击的机会

➤ 时间窗大小的选择应根据消息的时效性来确定

8. 认证理论与技术概述

认证协议中的常见技术

➤ 询问/应答方式(Challenge/Response)

➤ A期望从B获得一个条件

- 首先发给B一个随机值(challenge)
- B收到这个值之后，对它作某种变换，得到response，并送回去
- A收到这个response，可以验证B符合这个条件

➤ 在有的协议中，这个challenge也称为nonce

- 可能明文传输，也可能密文传输

➤ 这个条件可以是知道某个口令，也可能是其他的事情

- 变换例子：用密钥加密，说明B知道这个密钥；
简单运算，比如增一，说明B知道这个随机值

1. 在AES分组密码中，若密文出现1比特差错，分析不同工作模式（ECB、CBC、CFB、OFB、CTR）下的差错传播特性（即影响的比特数），并说明无线信道加密中应如何选择合适的模式及其原因。
2. 请按照课件第75页PPT的示例形式，给出针对DH密钥交换协议的一种攻击。
3. 请分析基于公钥的NS协议（PPT第78页）的安全性，指出其存在的问题，并给出改进协议或建议。

Any Questions?

