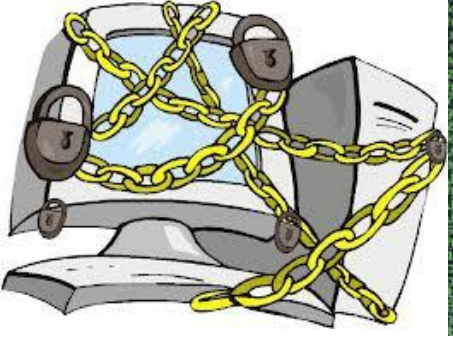



信息系统安全

数据安全保护

机密性保护

陈春华 博士
chunhuachen@scut.edu.cn

2018 春季
华南理工大学 软件学院

大纲

- 数据机密性保护
  - 加密概念
  - 古典加密
  - 现代密码体制
  - 密钥管理
  - 数据隐藏概述

数据安全保护的概念

- 机密性保护
  - 保护数据不为非授权者(用户、实体或者过程)获取或使用
- 完整性保护
  - 保护数据在传输或者存储过程中不受到非授权的篡改或者破坏
- 抗抵赖性保护
  - 指在传输数据时必需携带含有自身特质、别人无法复制的信息，防止数据的发送者或者接受者事后对自己行为的否认。

数据安全保护的概念

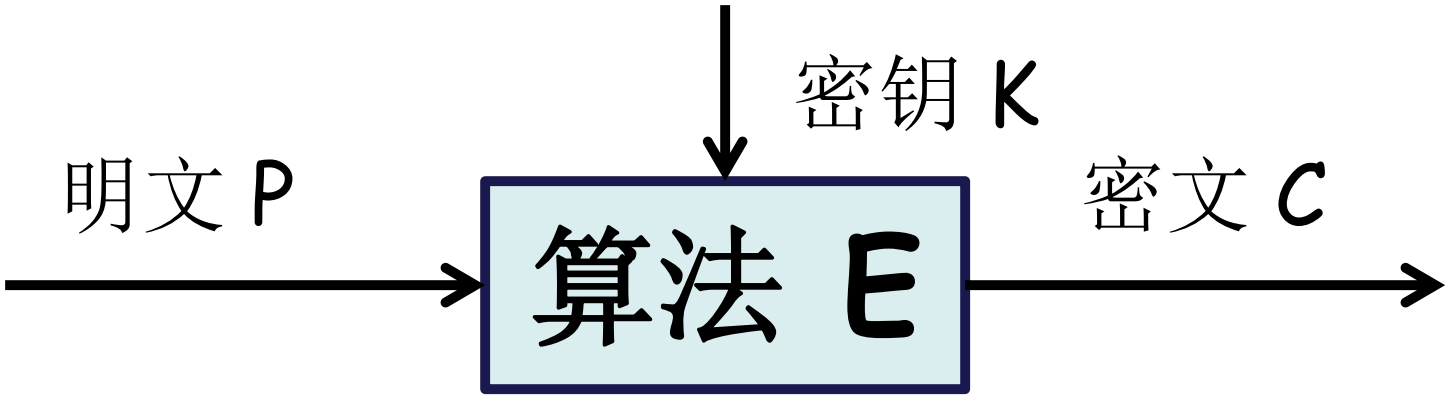
- 可用性保护
  - 保证数据能够正常地使用
- 本讲重点关注数据的机密性保护

数据的机密性保护

- 可读性保护
  - 借助数据加密技术
- 可见性保护
  - 借助数据隐藏技术

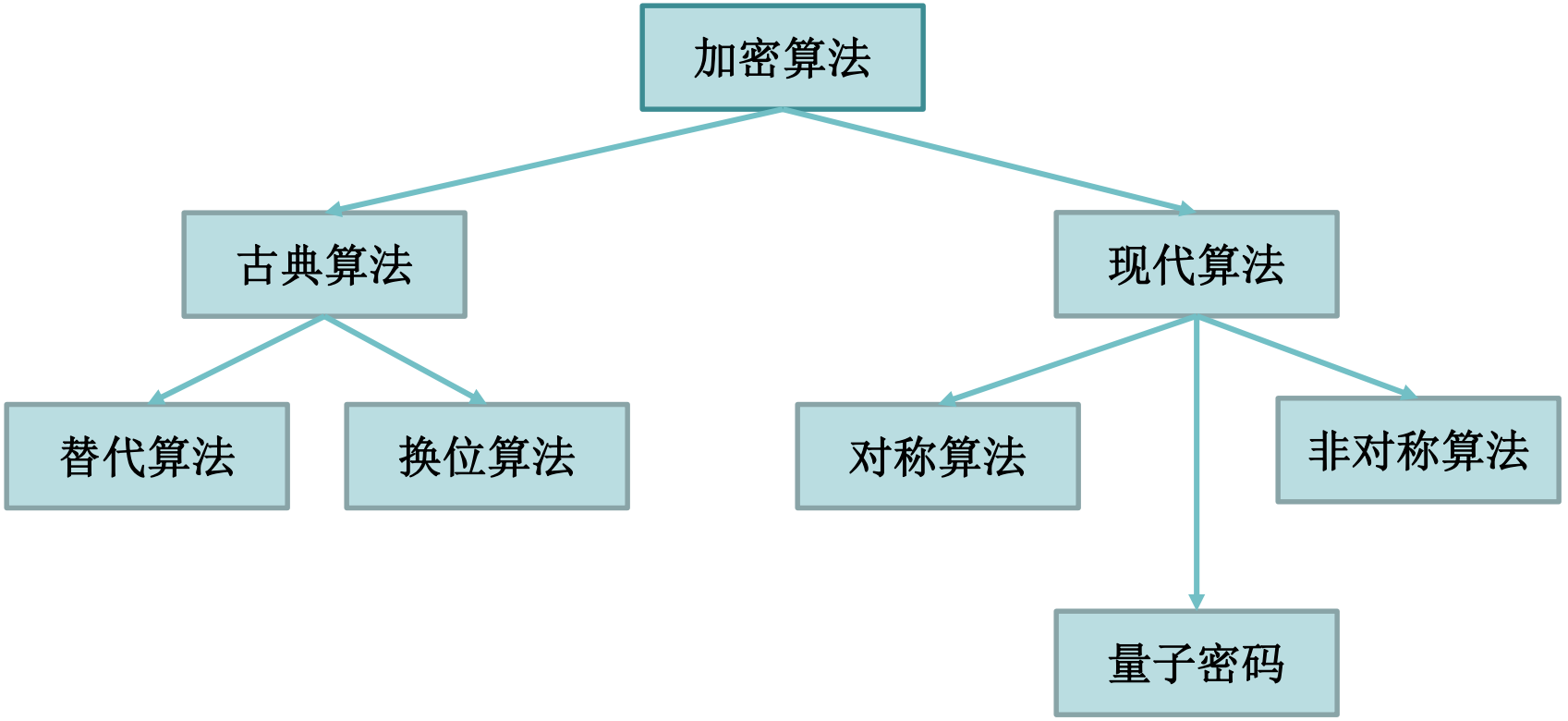
数据加密基础

- 数据加密是隐藏数据的可读性，使得非授权用户不能直接了解数据的内容。

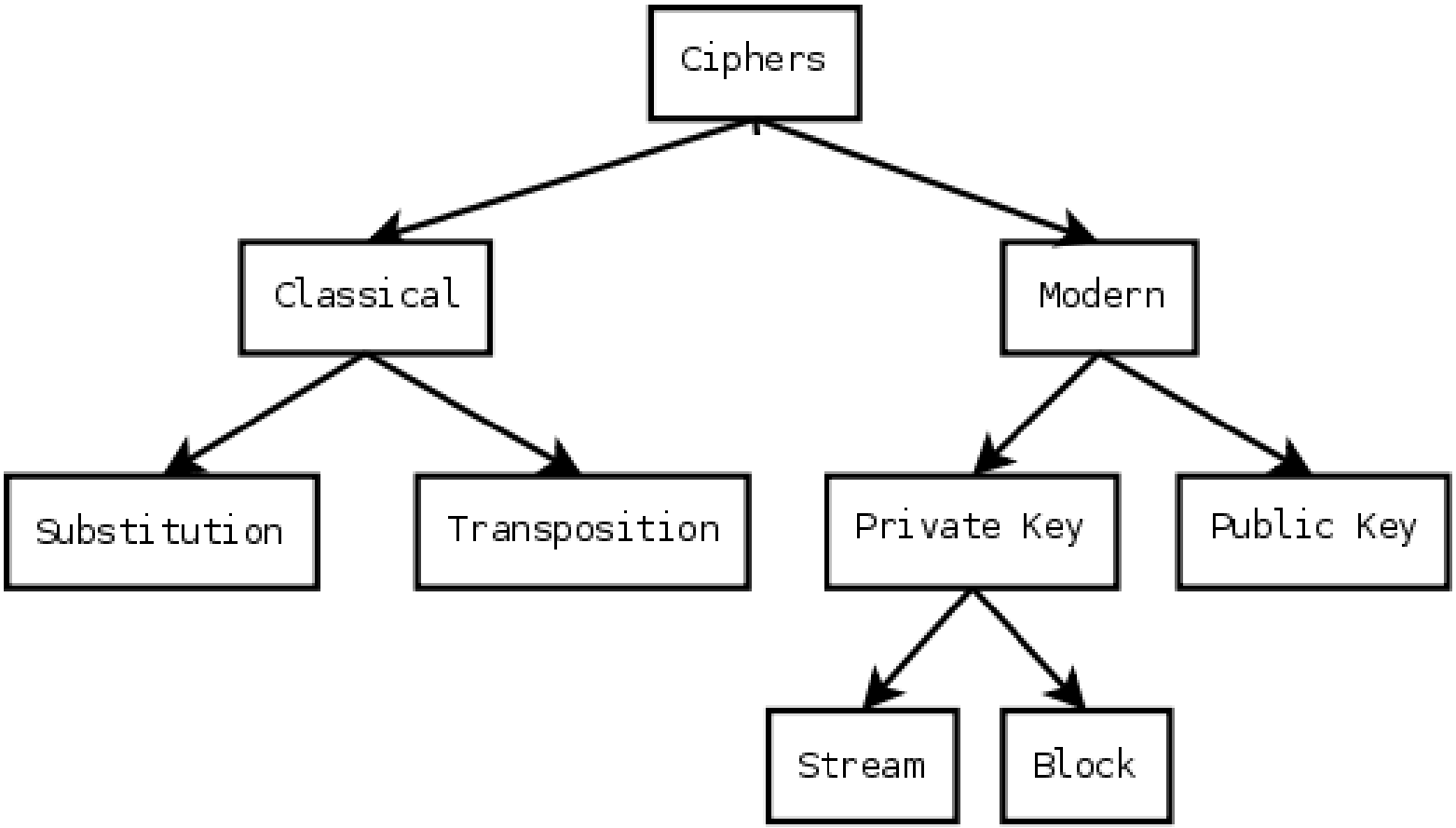


- 加密/密码系统包括：明文空间、密文空间、密钥空间和密码算法

加密算法分类



加密算法分类


Ciphers
Classical
Modern
Substitution
Transposition
Private Key
Public Key
Stream
Block

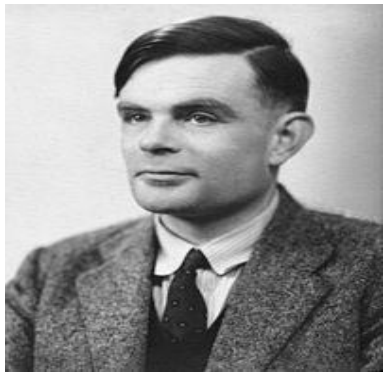
古典密码体制

- 人类很早就使用密码，用于在战争中传递命令等信息，比如凯撒密码等
- 古典密码主要包括如下两种：
  - 替代密码 substitution cipher
  - 换位密码 transposition cipher
  - 在现代计算机的计算能力下，古典密码都是不安全的。
    - 多是因为密钥空间小，难以抵抗穷举密钥攻击

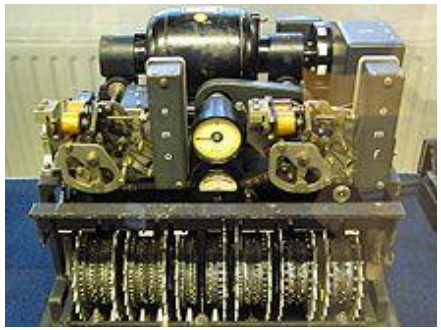
加密设备-简单历史

Battle of France with the Enigma machine

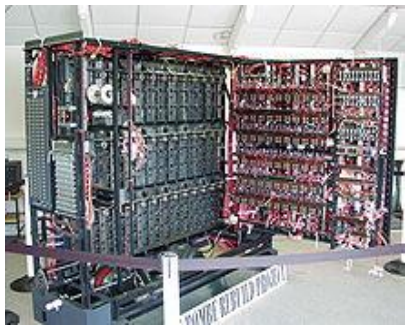
The Enigma machine



Alan Turing



The Lorenz SZ42 machine



The bombe/ Bletchley Park

简单替代密码

- 原理：将明文中每个位置的字母都用其他字母代替
- 凯撒密码算法：
  - 将明文字母替换成字母表中后面的距离为5的字母代替
  - CHINA → HMNSF
- 维吉利亚密码，一种较为复杂的替代密码

简单替代密码-维吉利亚密码

- 维吉利亚方阵：第i行以I开头

明文	a	b	c	d	…	…	v	w	y	x	z
a	A	B	C	D			V	W	Y	X	Z
b	B	C	D	E			W	Y	X	Z	A
.											
i	I	J	K	L	…	…	D	E	F	G	H
.											
z	Z	A	B	C			U	V	W	X	Y

简单替代密码-维吉利亚密码

- 明文：data security; 密钥：basic
- 首先按照密钥长度将明文分解为若干节：

密钥	b	a	s	i	c
明文	d	a	t	a	s
	e	c	u	r	i
	t	y			

简单替代密码-维吉利亚密码

- 第二步：对每一个明文字母，利用密钥basic和维吉利亚方阵进行替换操作
  - 明文首字母"d"对应密钥的"b"列，则选取维吉利亚方阵中的第"b"行"d"列中的字母(E)进行替换
  - C = EALIU FCMZK UY

替代密码

- 比简单替代密码复杂的替代密码还有
  - 多名替换密码 (homophonic substitution cipher)
  - 多字母密码 (poly alphabetic cipher)

换位密码

- 原理：将明文中字母的位置重新排列
- 最简单：将明文倒序输出
- 列换位法：
  - 将明文按密钥长度排列成明文矩阵
  - 按密钥字母在字母表中的顺序，输出明文中的矩阵
  - 例子：密钥 K = computer
  - 明文：WHAT CAN YOU LEARN FROM THIS BOOK

换位密码-列换位法

密钥	C	O	M	P	U	T	E	R
序号	1	4	3	5	8	7	2	6
明文	W	H	A	T	C	A	N	Y
	O	U	L	E	A	R	N	F
	R	O	M	T	H	I	S	B
	O	O	K	X	X	X	X	X

WORO NNSX … …

现代密码体制

加密：$C = E_{EK}(M)$　　解密：$M = D_{DK}(C)$

- 其中，E为加密函数，EK为加密码密钥，D为解密函数，DK为解密密钥；
- 按照EK与DK的关系，现代密码体制可分为
  - **对称密码体制**，又称单钥密码体制
  - **非对称密码体制**，又称公钥密码体制

对称密码体制

- 加密与解密使用相同的密钥，即EK=DK
- 对称密码体制又可分为：
  - 流加密 stream cipher
    - RC4算法等
  - 块加密 block cipher
    - DES算法和AES算法等

非对称密码体制

- 加密使用的密钥和解密使用的密钥不同，即EK!=DK
- 1976年，斯坦福大学科学家Whitfield Diffie and Martin Hellman提出公钥及可利用单向陷门函数构造等概念
- MIT科学家Rivest, Shamir和Adleman提出了第一个可用的公钥算法，即RSA算法

密码体制的安全性分析

- 主要取决于两个方面：
  - 算法安全：算法应该公开，并接受分析与攻击
  - 密钥安全：密钥保密，不能泄露
- 密码体制安全性应当基于密钥的安全性，而不是算法的安全保密。
- 机密性保护-加密的关键是保护密钥的安全

回顾@20160310

- 风险=脆弱性+威胁
- 攻击=威胁的具体实现
- 信息系统安全的概念与内涵
  - 通信安全，信息防御与信息保障
- 信息系统安全体系
  - 安全服务，安全机制，安全策略与安全管理
- 机密性服务与加密机制

回顾@20160310 现代密码体制

加密：$C = E_{EK}(M)$　　解密：$M = D_{DK}(C)$

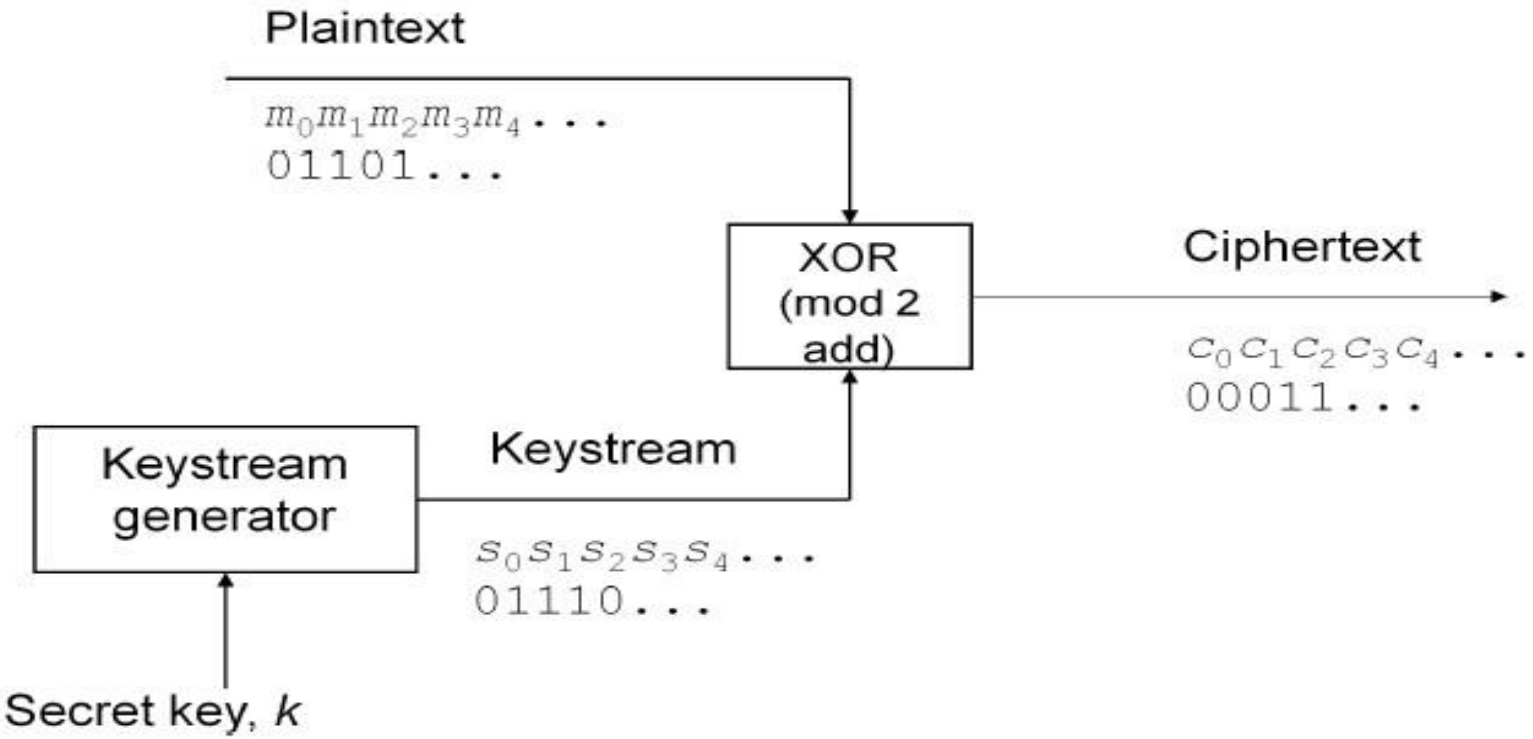
- 其中，E为加密函数，EK为加密码密钥，D为解密函数，DK为解密密钥；
- 按照EK与DK的关系，现代密码体制可分为
  - **对称密码体制**，又称单钥密码体制
  - **非对称密码体制**，又称公钥密码体制

回顾@20160310 对称密码体制

- 加密与解密使用相同的密钥，即EK=DK
- 对称密码体制又可分为：
  - 流加密 stream cipher
    - RC4算法等
  - 块加密 block cipher
    - DES算法和AES算法等

对称体制：流加密

- 通常对明文与**密钥流**进行逐比特位(bit)进行加密操作(异或运算)



chunhuachen@scut.edu.cn

对称体制：流加密

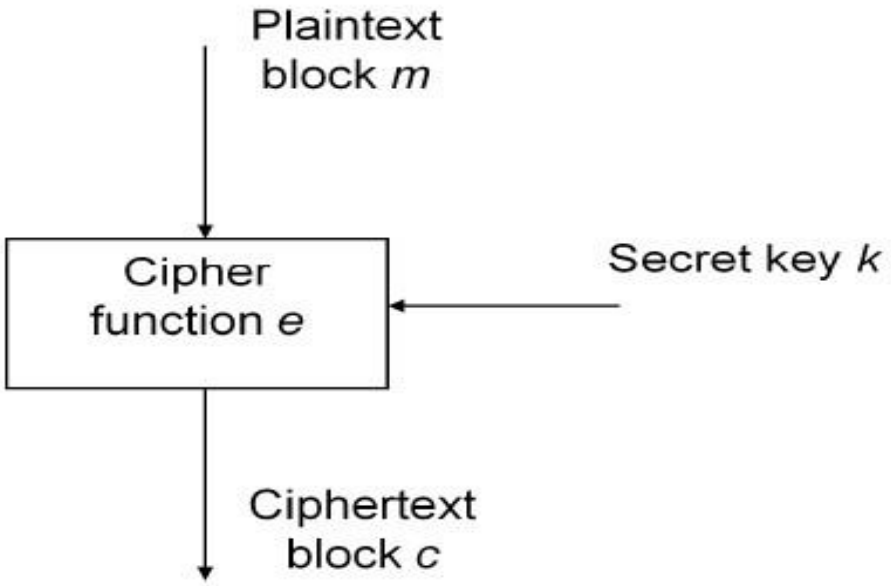
- 密钥流：基于**种子密钥K**，通过**密钥流生成函数**不断产生
- 密钥流(生成函数)安全属性：
  - 具有很长的周期，**伪随机性**等托
  - 通常来说，通过密钥流的一部分去寻找其他部分，在计算上是很困难的
- 种子密钥K通常仅使用在一个通信会话中，不可重复使用，即作为会话密钥。

一次一密流加密 (One time pad)

- 密钥流使用**真随机源**产生的比特流(要求无周期性)，且只使用一次进行加密
- 所描述的加密即为一次一密算法，具有信息论意义上的**无条件安全~**
- 真随机源很难实现，密钥管理(保密传输)等很难实现，因此它不具有现实的可用性。
- 现代流加密通常使用**线性反馈移位寄存器结构**构建密钥流生成函数，可以产生具有很长周期密钥流。

对称体制：块加密

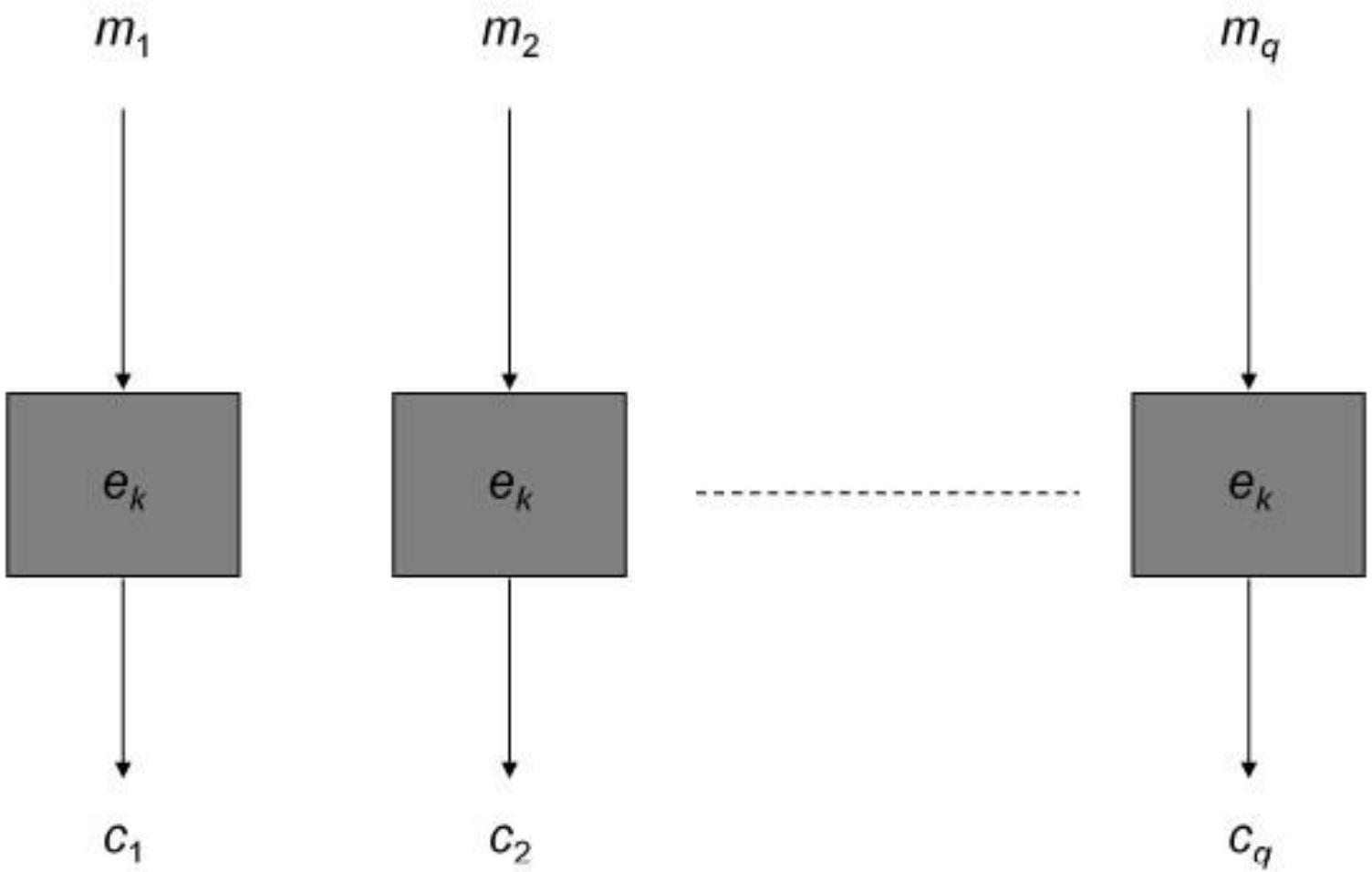
- 将明文编码(如使用0,1编码)，并按照一定长度(m)进行分组，再将各组明文的编码分别在密钥的控制下进行加密



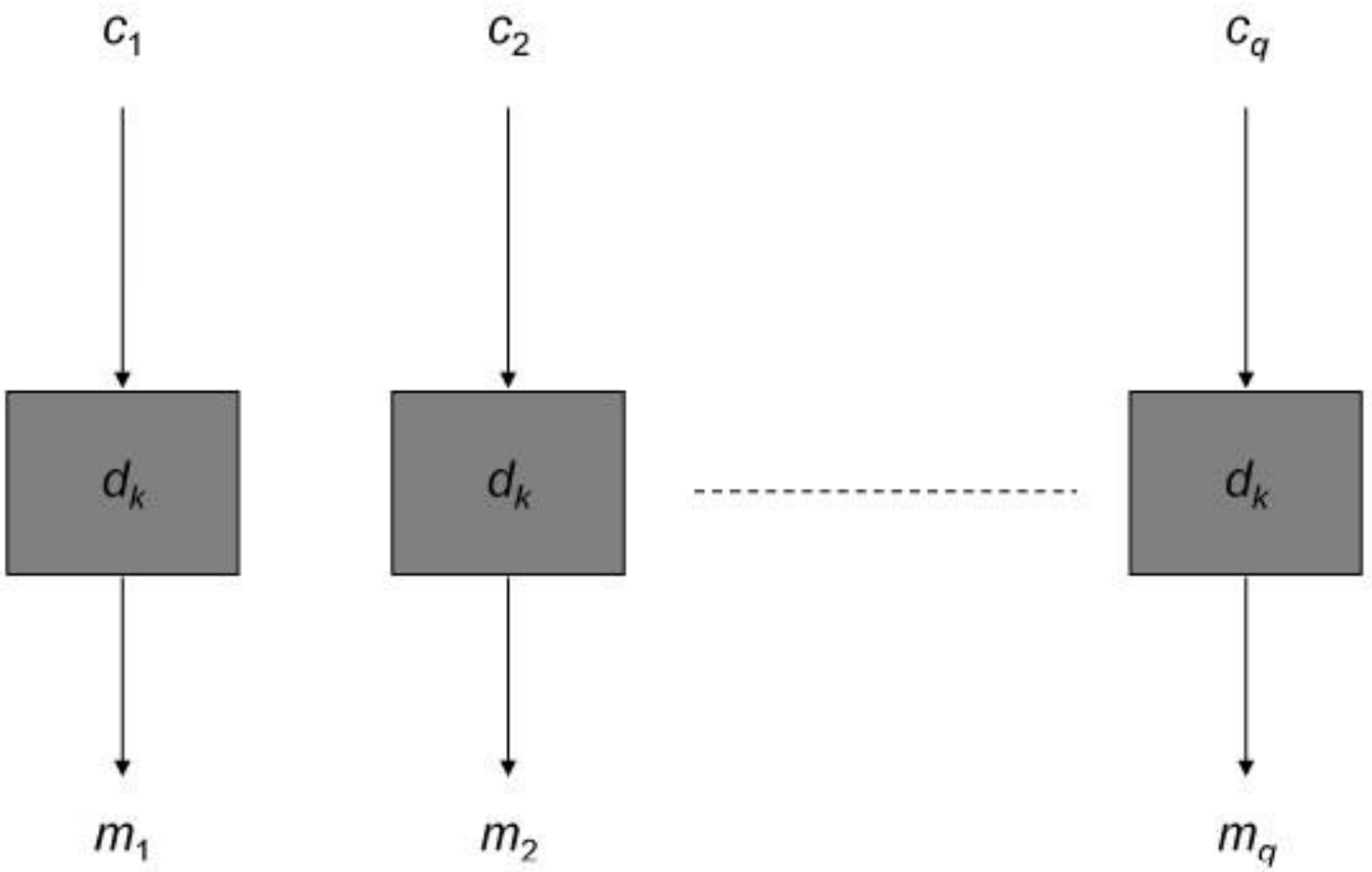
块加密操作模式 mode of operation

- 块加密算法可以在不同的**操作模式**下对明文进行加密
- 推荐的标准操作模式有
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - …, etc

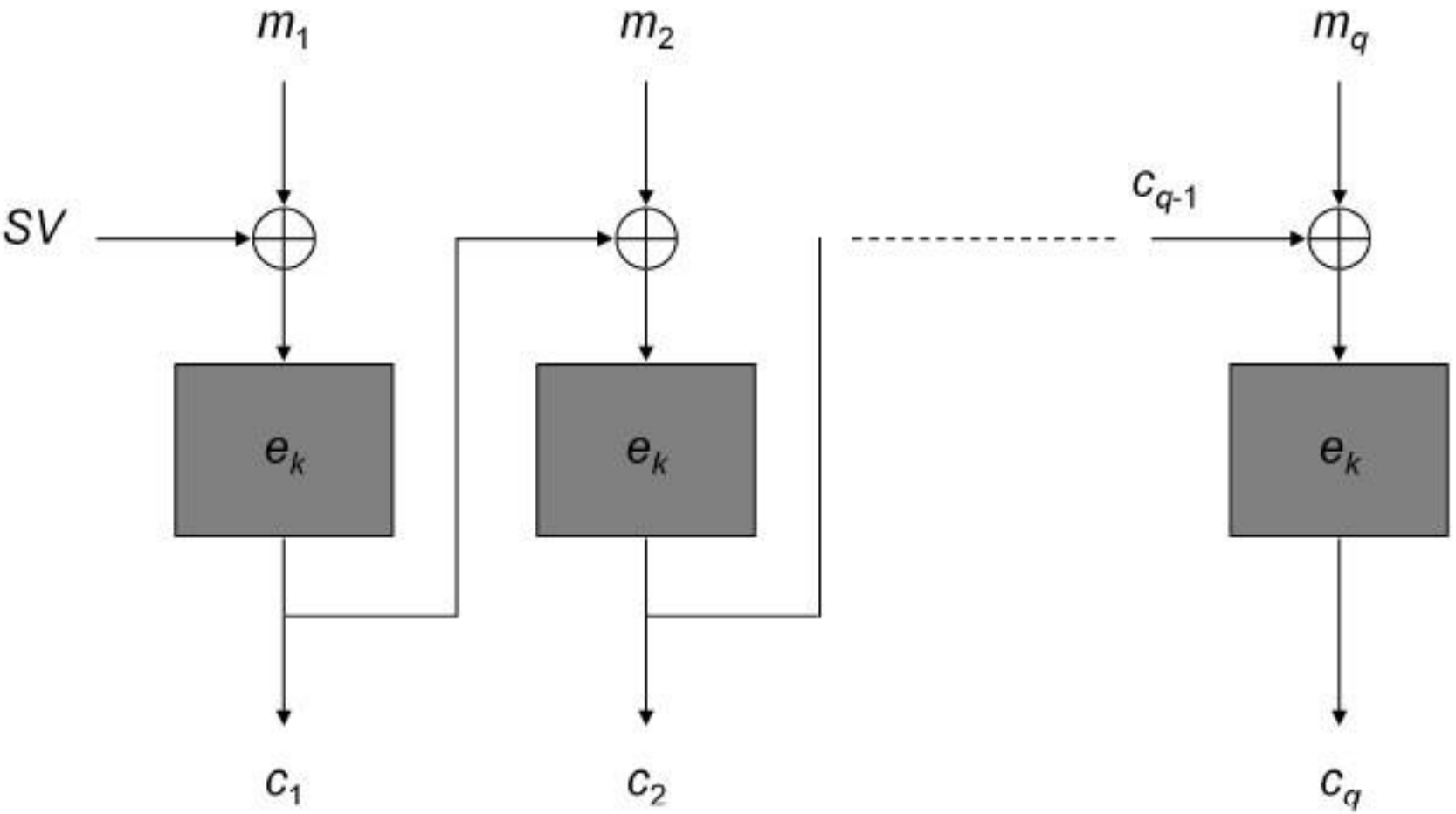
ECB encryption



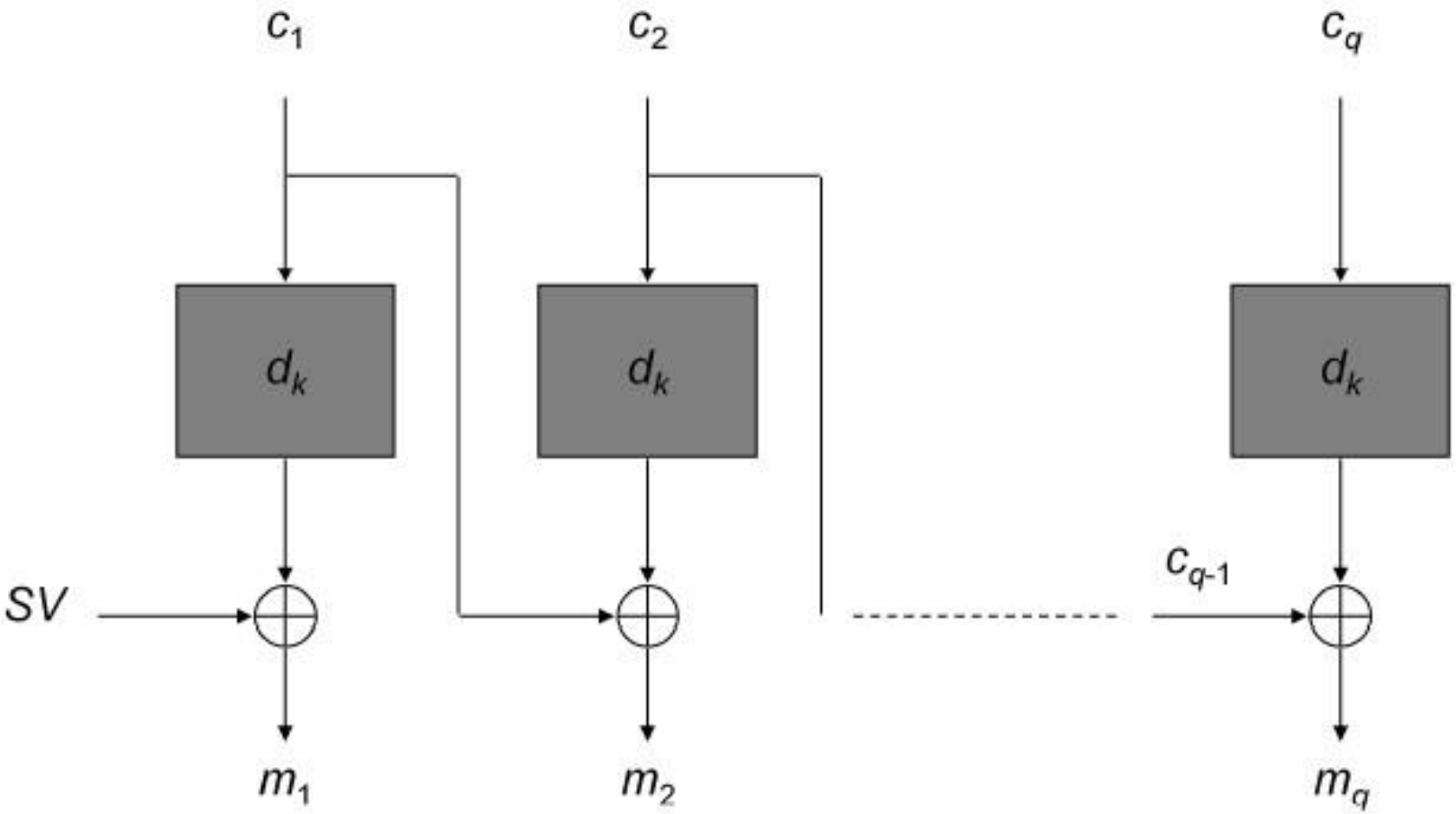
ECB decryption



CBC encryption



CBC decryption



对称体制：块加密

- 块加密具有非常广泛的使用，除加密外，还可以用来构造**消息认证码**算法
- 明文块的长度对安全具有至关重要的影响
  - 至少64bit，推荐128bit或以上，用于抵抗字典攻击
- 块加密中的密钥是否应当作为会话密码使用，取决于所使用的操作模式
  - ECB模式中，应当作为会话密钥

块加密：DES加密算法

- Data Encryption Standard (DES), 即数据加密标准
  - IBM & 美国国家安全局 (NSA)
  - 块长度：64位；有效密钥长度：56位
  - 含有机密设计元素 (S盒/NSA后门?)
- 1976年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），随后在国际上广泛流传开来

安全性：DES加密算法

- 56位的有效密钥长度，密钥空间(2^{56})太
- 攻击：
  - 微分密码分析
  - 线性密码分析
  - 暴力穷举破解 -依次尝试所有可能的密钥
- DES可以被暴力攻击
  - 2008年，SciEngines的 RIVYERA机器，时间少于1天！！

安全性：3DES加密算法

- 在当前攻击下DES安全性不足，已经被**AES加密算法**取代
- 为了应对密钥太短的弱点，人们提出了3DES加密算法；其中一种使用2个密钥，按如下结构进行加密
  - $c = e_{k1}(d_{k2}(e_{k1}(m)))$，其中e/d为DES加密和解密
- 3DES虽然不是标准，但是美国国家标准技术研究所确认3DES在2030年以前均可用于敏感政府信息的加密

实验@DES加解密算法编程实现

- 时间，待安排

块加密：AES加密

- Advanced Encryption Standard，即高级数据加密标准
  - Joan Daemen和Vincent Rijmen设计，又称Rijndael加密法
  - 固定块长度：128位；可变密钥长度：128/192或者256位
- 2002年称为美国联邦政府标准；目前是对称密钥加密中最流行的算法之一

对称体制：共享密钥问题

- 对称体制的潜在假设：**通信双方共享一个用于加密/解密的密钥K**
- 在一个规模为n的通信群体中
  - 如果任意两个实体共享一个密钥，则每个实体需要保密持有(n-1)个密钥，群体共需要n(n-1)个密钥 (复杂度 $O(n^2)$)
  - 通常使用密钥分配中心(KDC)，每个实体仅与KDC共享密钥，用于降低密钥复杂度
- 在规模庞大时，密钥管理困难

非对称体制的基本思想

- 特点：加密与解密使用不同的密钥EK!=DK
- 每个通信实体生成一个密钥对，满足
  - 两个密钥具有某种数学联系
  - 仅知道其中一个密钥，求解对应的另外一个密钥，**在计算上是困难的**
  - 用其中一个密钥进行加密，可以用对应的另一个密钥进行解密
- 通信时，实体将自己加密密钥公开，又称公钥PK; 将解密密钥保密持有，又称私钥SK。
- 在一个规模为n的通信群体中
  - 每个实体仅需一个公私密钥对
  - 密钥规模相对对称体制要小

非对称密码体制(~历史)

- 1976年，斯坦福大学科学家Whitfield Diffie and Martin Hellman提出公钥概念及可利用单向陷门函数构造的基本原理。
- 单向陷门函数多依赖于数学难题
  - 离散对数难题
  - 大整数素因子分解难题
- 1977年，MIT科学家Rivest, Shamir和Adleman提出了第一个可用的公钥算法，即RSA算法。

RSA公钥加密算法

- RSA：安全性依赖于大整数素因子分解难题。
- RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准。
- 为提高保密强度，一般推荐使用1024位，或者更高的2048位。
- 在分布式计算和量子计算机理论日趋成熟的今天，RSA加密安全性受到了挑战。

实验@深入了解RSA算法基本原理

- 时间，待安排

对称与非对称体制比较

- 假设A与B要进行保密通信
- 对称加密
  - A (B)生成密钥，需要通过一个安全信道传送给B；如果密钥泄密，A与B均遭受损失。
  - 运算效率高，使用方便，加密效率高
- 非对称加密
  - A(和B)各自产生自己的一对密钥(即公钥PK和私钥SK)，A(B)将PK在公开信道传送给B(A)，A(B)保密SK。
  - 用对方的公钥加密明文，进行保密传输
  - 运算效率低~~ 通常用来加密对称密钥

密钥管理

- 现代密码体制中，密码算法公开，一切安全依赖于密钥
  - 安全，不是弱密钥
  - 保密，没有泄露
- 密钥管理是信息系统安全至关重要的工作，包括密钥的生成，分配，使用，更新，撤销和销毁等一系列过程

密钥管理

- 密钥生成：生成好的密钥，密钥越长，强度就越大
  - 对称密钥：伪随机比特，随机性要好
  - 公私钥对，需要满足某种数学特征，比如如何产生大素数**(课外阅读)**
- 密钥分配：主要涉及密钥发送与验证
  - 网外分配：可使用秘密信使携带密钥分配
  - 网内分配：用户之间直接分配或者通过KDC分配，涉及密钥分配协议**(后续课程)**

密钥管理

- 密钥控制使用
  - 限制密钥的主权人、合法使用期限、预定用途、预定算法等
- 密钥的保护与存储
  - 不以明文方式、物理安全
  - 秘密共享**(课外阅读)**
- 密钥的停用与更新 **(后续课程)**
- 密钥的销毁

Further Reading:

安全协议

- 参考：
  - 4.2.2节@《基于案例的网络安全技术与实践》，朱宏峰等，清华大学出版社
  - 上课使用板书