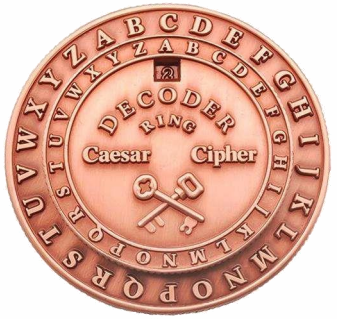
西安电子科技大学
XIDIAN UNIVERSITY
计算机科学与技术学院
School of Computer Science and Technology

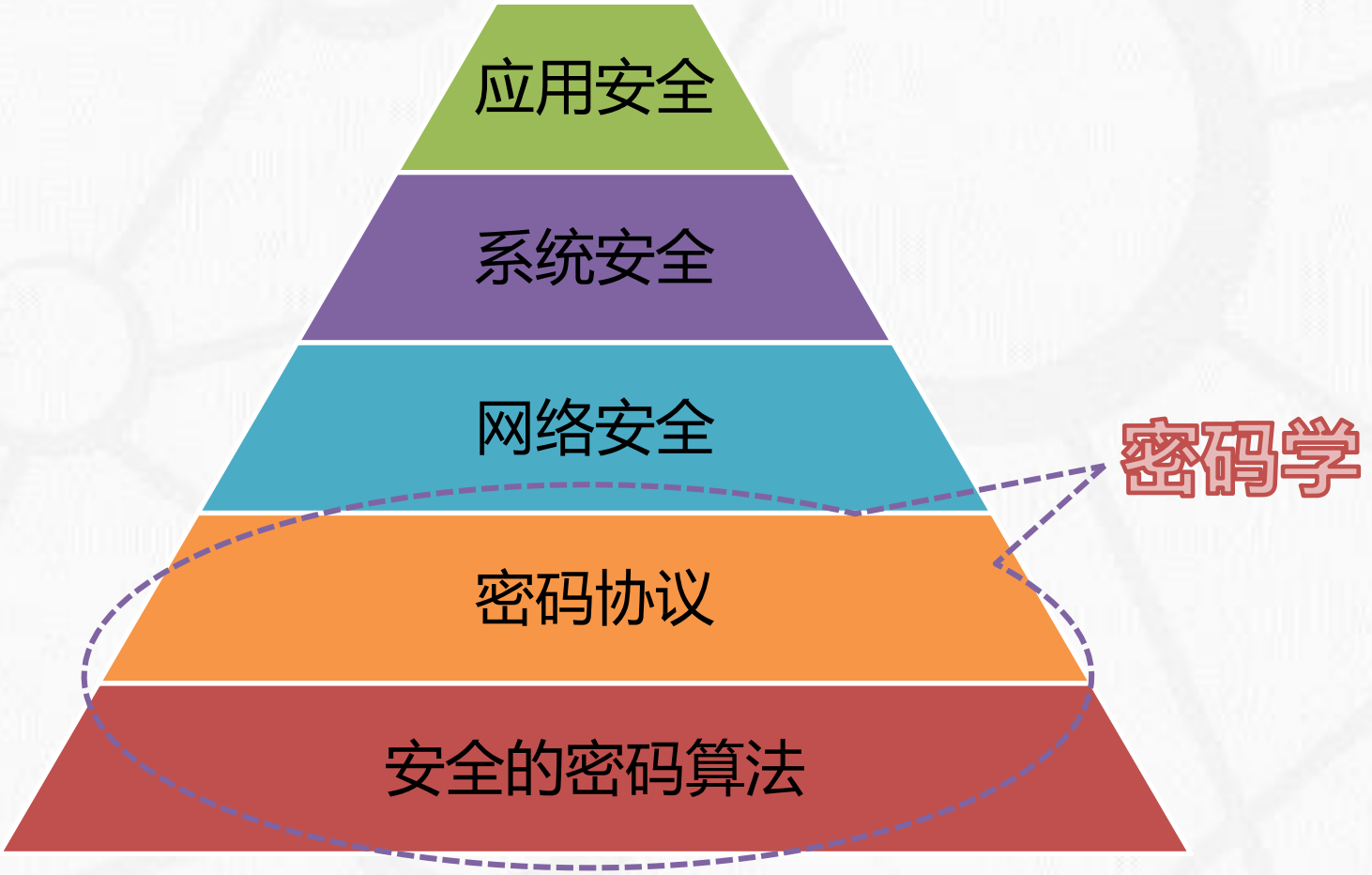
第二章 数据安全基础

彭延国

ygpeng@xidian.edu.cn



第二章 数据安全基础 - 基石



§2 数据安全基础 - 内容提要

§2.1 现代密码学基础(基础工具)

§2.2 公钥基础设施(系统架构)

§2.3 网络安全协议(具体应用)

古典密码、现代密码

§2.1 现代密码学基础

§2.1 现代密码学基础 - 我们从一个故事开始

主观题 1分

设置

XIDIAN UNIVERSITY

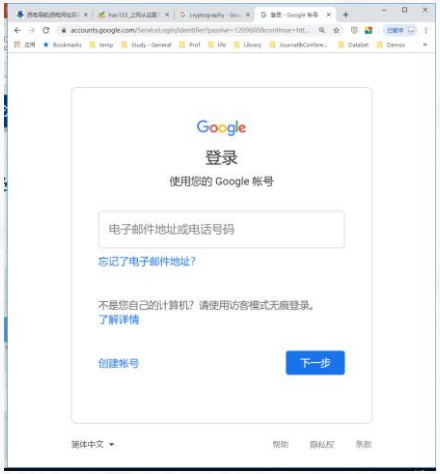
密码学在哪里?

正常使用主观题需2.0以上版本雨课堂

作答

密码学在哪里?

密码学无处不在……



登录

密码锁、指纹锁

移动支付

……

§2.1 现代密码学基础 - Why？(1)

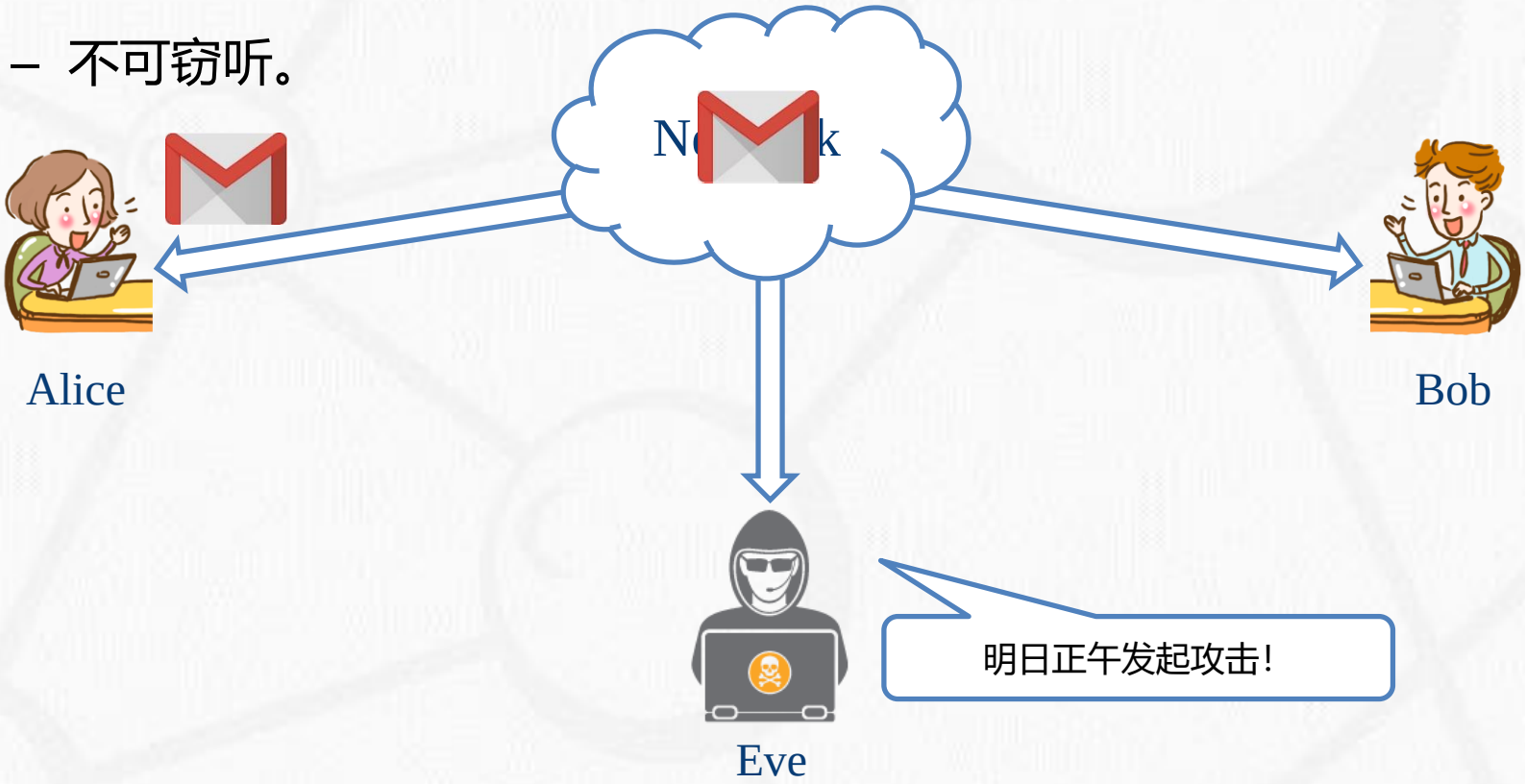
- Alice有一封信件需要邮寄给Bob：

§2.1 现代密码学基础 - Why? (2)

- Alice有一封机密信件需要邮寄给Bob，包含作战计划，需保证：
  - 不可篡改；
  - 不可窃听。

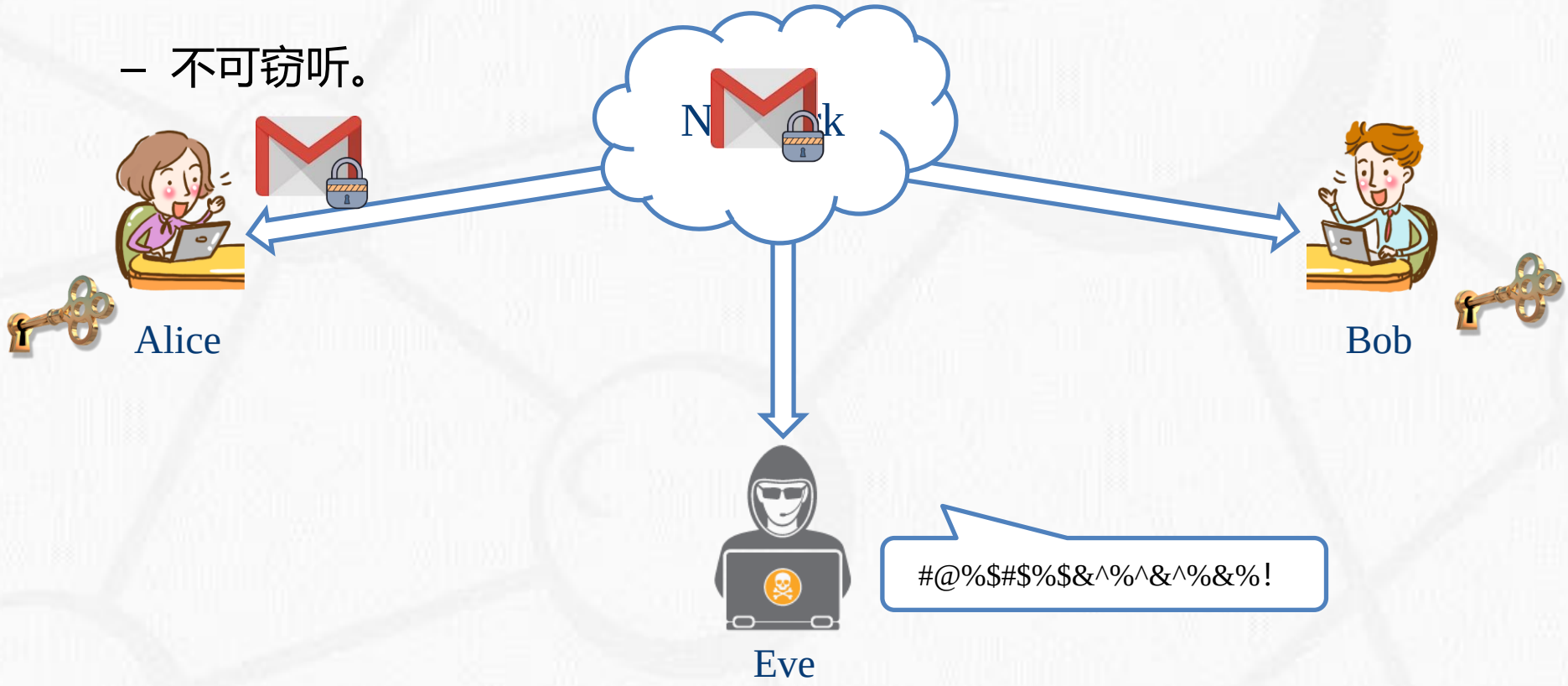
§2.1 现代密码学基础 - Why? (3)

- Alice有一封邮件需要通过网络发送给Bob，包含作战计划，需保证：
  - 不可篡改；
  - 不可窃听。



§2.1 现代密码学基础 - Why? (4)

- Alice有一封邮件需要通过网络发送给Bob，包含作战计划，需保证：
  - 不可篡改；
  - 不可窃听。



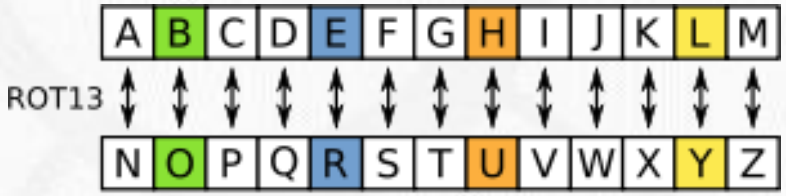
西安电子科技大学
XIDIAN UNIVERSITY

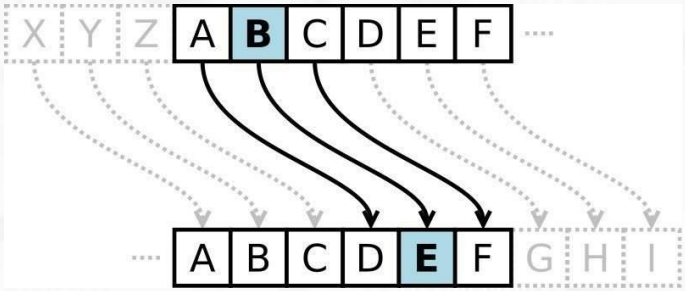
从古典到现代，从艺术到科学

§2.1.1 密码学的发展历程

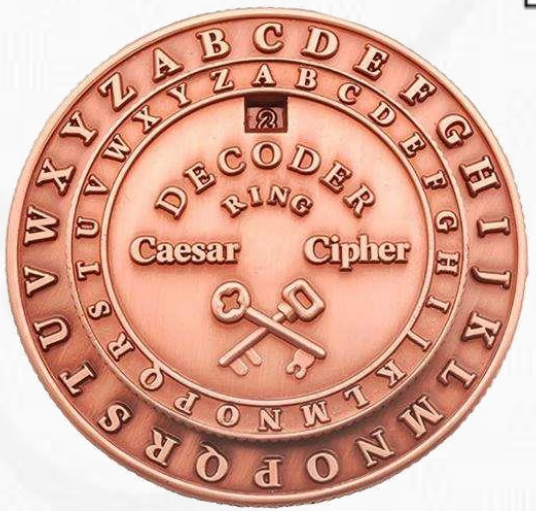
§2.1.1 密码学的发展历程 - 古典密码阶段

- 密码学作为艺术，而不是科学
  - 密码算法的基本手段出现，针对的是字符；
  - 简单的密码分析手段出现；
  - 主要特点：数据的安全基于算法的保密。

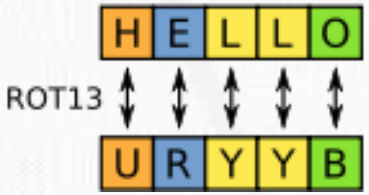




凯撒密码示意图



凯撒密码盘



ROT13密码示意图

§2.1.1 密码学的发展历程 - 密码棒(The scytale)

- 密码棒(The scytale)
  - 古希腊密码(出现在公元前5世纪)
  - 不可知的周期作为密钥，仅发送者和接收者掌握密钥

尝试破解：K T M I O I L M D L O N K R I I R G N O H G W T

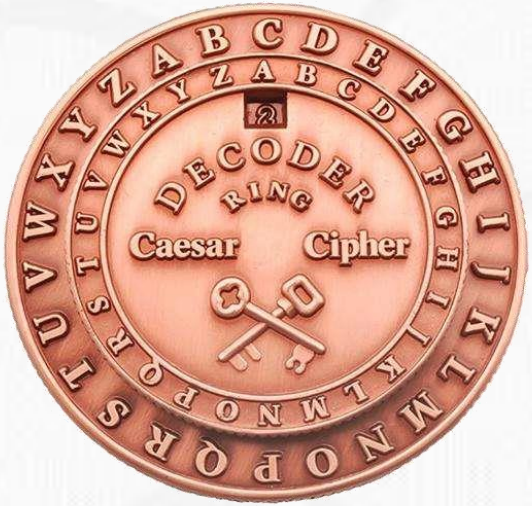
明文：K I L L K I N G T O M O R R O W M I D N I G H T

密文：K T M I O I L M D L O N K R I I R G N O H G W T

明文：K I L L K I N G T O M O R R O W M I D N I G H T

§2.1.1 密码学的发展历程 - 凯撒密码

- 凯撒密码
  - 一种最简单且最广为人知的加密技术
  - 一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。



- 例子：按照字母表向后顺移三个字符位

明文：meet me after the toga party

密文：PHHW PH DIWHU WKH WRJD SDUWB

§2.1.1 密码学的发展历程 - 凯撒密码的数学定义

- 可以定义如下的映射：

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
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

- 那么，给定每个字母一个序号：

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

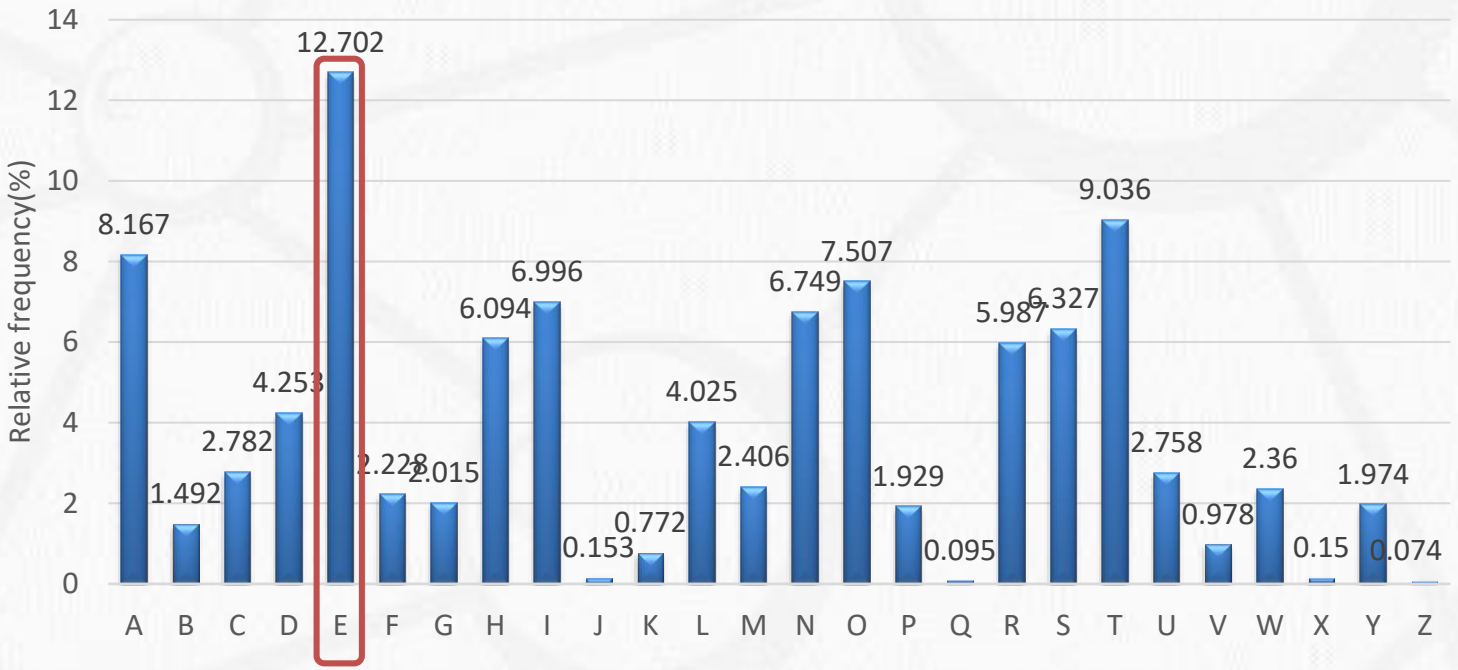
- 凯撒密码可以定义如下：

k就是加解密密钥！！！

  - $C = E(p) = (p + k)\ mod\ (26)$
  - $p = D(C) = (C - k)\ mod\ (26)$

§2.1.1 密码学的发展历程 - 凯撒密码的攻击

- 频率分析法：
  - 每个字母的使用频率皆不相同
  - 根据密文中字母的频率可以进行破解



§2.1.1 密码学的发展历程 - 近代密码阶段(1949~1975)

- 计算机使得基于复杂计算的密码成为可能
  - 1949年Shannon的“The Communication Theory of Secret Systems”；
  - 1971年-1973年IBM Watson实验室的Horst Feistel等几篇技术报告；
  - 主要特点：数据的安全基于密钥而不是算法的保密。
  - 从艺术到科学的蜕变。

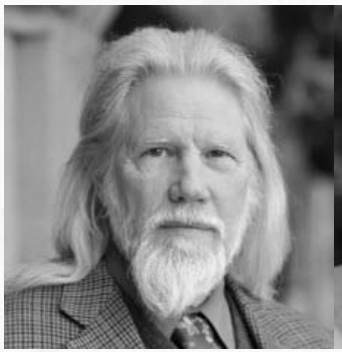
恩尼格玛机

艾伦·麦席森·图灵

电影《模仿游戏》

§2.1.1 密码学的发展历程 - 现代密码阶段(1976至今)

- 公钥密码的崛起
  - 1976年：Diffie & Hellman 的 “New Directions in Cryptography” 提出了公钥密码学思想；
  - 1977年Rivest, Shamir 和 Adleman提出了RSA公钥算法；
  - 90年代逐步出现椭圆曲线等其他公钥算法；
  - 主要特点：公钥密码使得发送端和接收端无密钥传输的保密通信成为可能。



WHITFIELD DIFFIE

MARTIN HELLMAN

2015年图灵奖得主(D-H协议)

RON LINN RIVEST

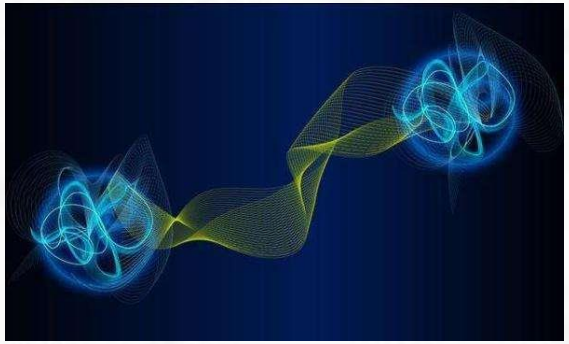
ADI SHAMIR

LEONARD (LEN) MAX ADLEMAN

2002年图灵奖得主(RSA)

§2.1.1 密码学的发展历程 - 现代密码阶段(未来)

- 量子密码时代&后量子密码时代
  - 量子计算机的出现；
  - 传统的数学难解问题不再困难。



量子纠缠现象

墨子号卫星

IBM Q System

西安電子科技大學
XIDIAN UNIVERSITY

密码编码、密码分析、安全模型

§2.1.2 密码学基础

§2.1.2 密码学基础 - 密码学研究分类

- 密码学(Cryptology): 是研究信息系统安全保密的科学.

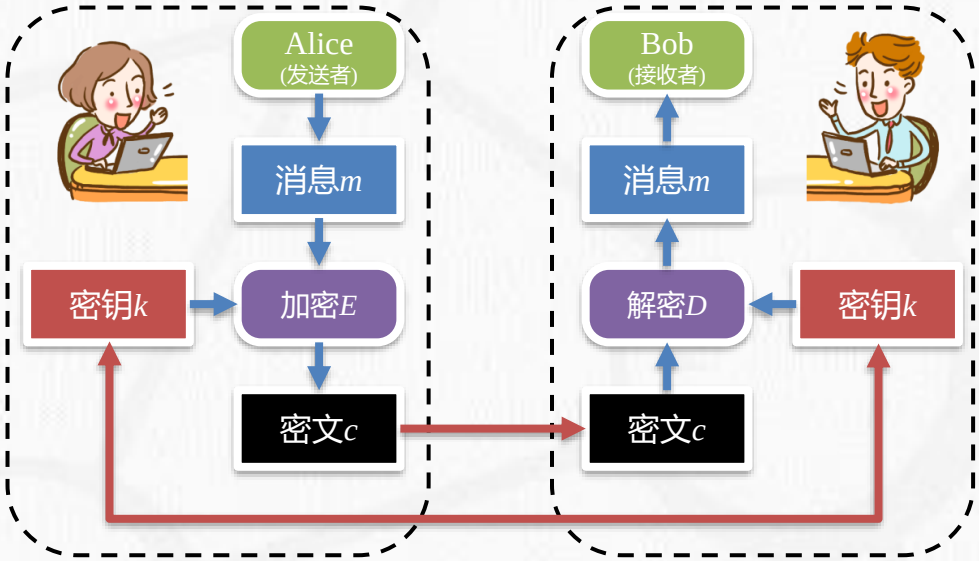
- 密码编码学(Cryptography): 主要研究对信息进行编码,实现对信息的隐蔽.

- 密码分析学(Cryptanalytics):主要研究加密消息的破译或消息的伪造.

§2.1.2 密码学基础 - 主要角色

- 参与者：
  - 发送者：发送信息的一方；
  - 接收者：接收信息的一方；
  - 窃听者：尝试窃取信息的攻击者。

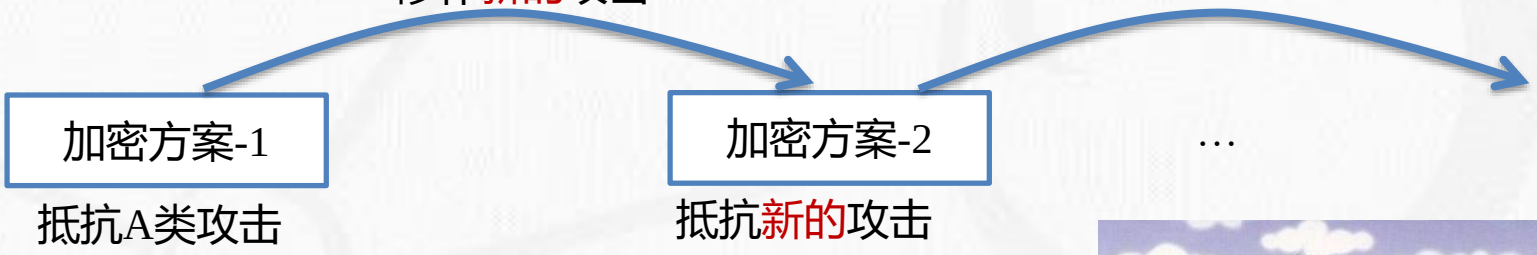
- 主要对象：
  - 消息m：也就是明文，原始消息。
  - 密文c：加密后的消息。
  - 加密E：由明文转变为密文的函数。
  - 解密D：由密文转变为明文的函数。
  - 密钥k：用于加密或解密的钥匙。



1. 如何构造加解密算法
2. 如何生成密钥
3. 如何分配和管理密钥

§2.1.2 密码学基础 - 如何分析安全性?

- 古典密码：
  - 方法：针对每一类攻击进行安全性分析。



  - 缺陷：攻击者可能发现新的攻击。
  - 这就像一场猫捉老鼠的游戏。

- 现代密码：
  - 立足于终止猫捉老鼠的游戏；
  - 证明密码方案能够抵挡某一类攻击者。

安全性证明

§2.1.2 密码学基础知识 - 现代密码学的三原则(1)

- 现代密码学三原则：

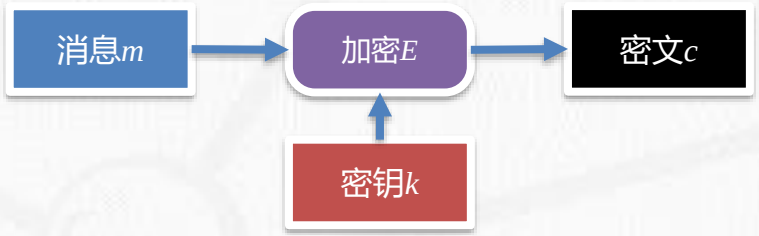
原则1 **形式化安全性定义(Formal security definition)**

原则2 **精确假设(Precise assumptions)**

原则3 **安全性证明(Proofs of security)**

§2.1.2 密码学基础知识 - 现代密码学的三原则(2)

- 原则1：形式化安全性定义
  - 密码方案应该达到怎样的安全属性?



密文隐藏所有明文的语义

- 原则2：精确假设
  - 安全性建立在怎样的假设基础上?

- 原则3：安全性证明
  - 证明：当假设成立时，加密方案满足形式化定义。

§2.1.2 密码学基础知识 - 安全性定义的必要性

有的放矢

安全性定义的必要性

对于方案:

不同的方案达到不同的安全性

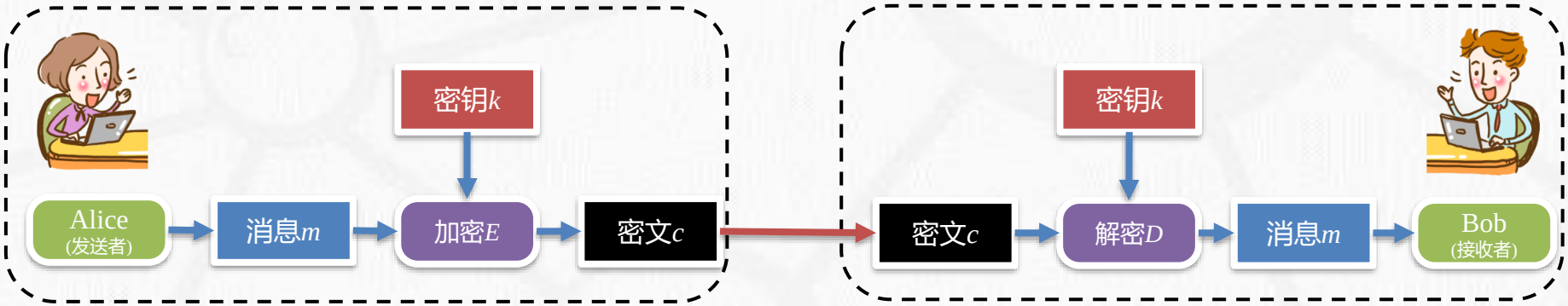
对于证明:

安全性证明仅针对特定的安全性定义有意义

正确的安全性定义是一件极其重要的事情!

§2.1.2 密码学基础知识 - 对称加密

- 对称加密方案是一个三元组(Gen, Enc, Dec)
  - Gen是一个用于生成加解密密钥k的算法。
  - Enc是加密算法。该算法的输入是明文m和密钥k，输出的是密文c。
  - Dec是解密算法。该算法的输入是密文c和密钥k，输出的是明文m。



正确性:

$$Dec(k, c := Enc_k(m)) = m$$

§2.1.2 密码学基础知识 - 安全性的衡量

信息安全保密性的高低是通过破解它的难易程度来衡量的。

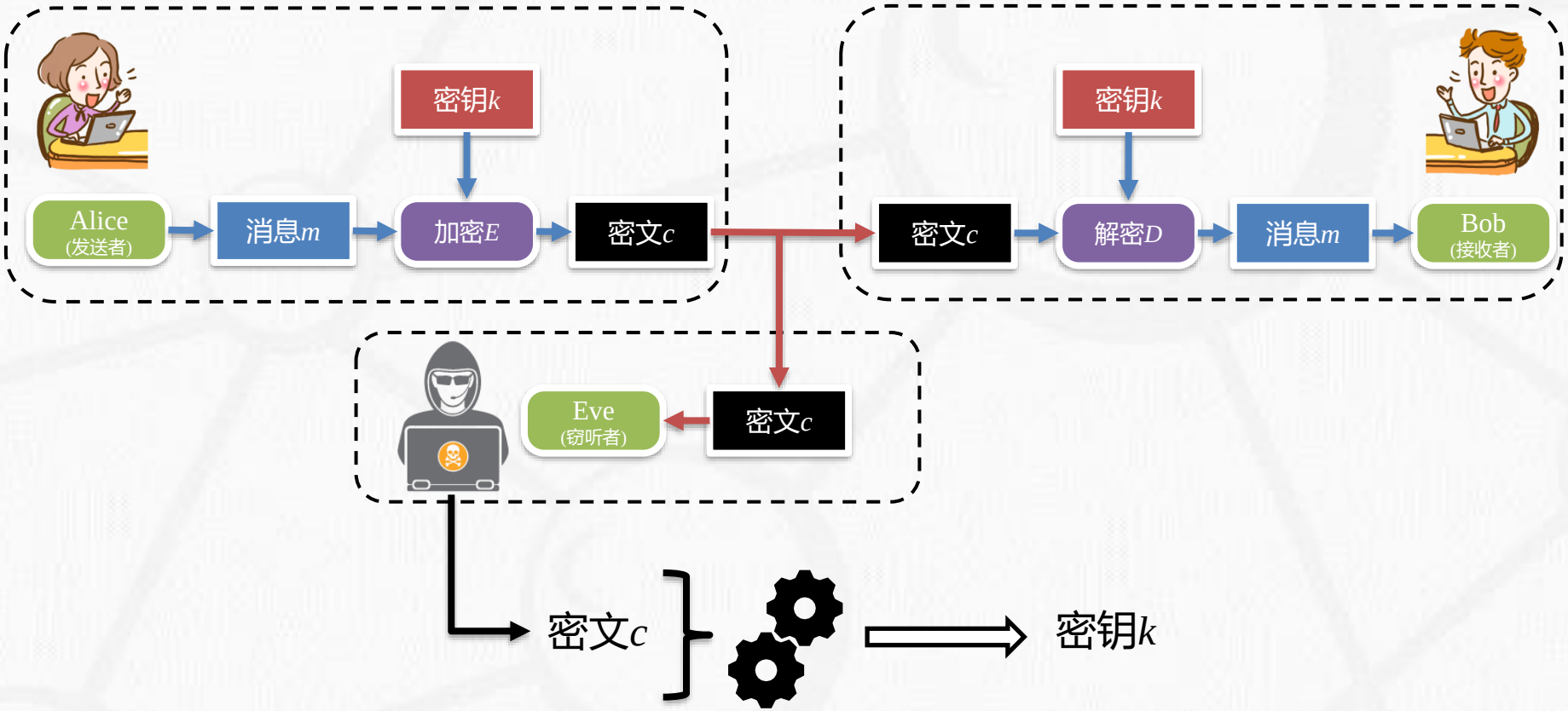
§2.1.2 密码学基础知识 - 怎样定义安全性?

- 1. 威胁模型(攻击者的能力):
  - 描述攻击者的能力，包括攻击者可以获取的、可以做的。
  - 唯密文攻击
  - 已知明文攻击
  - 选择明文攻击
  - 选择密文攻击

- 2. 攻击模型(安全目标):
  - 一个攻击者攻破加密方案后的含义。

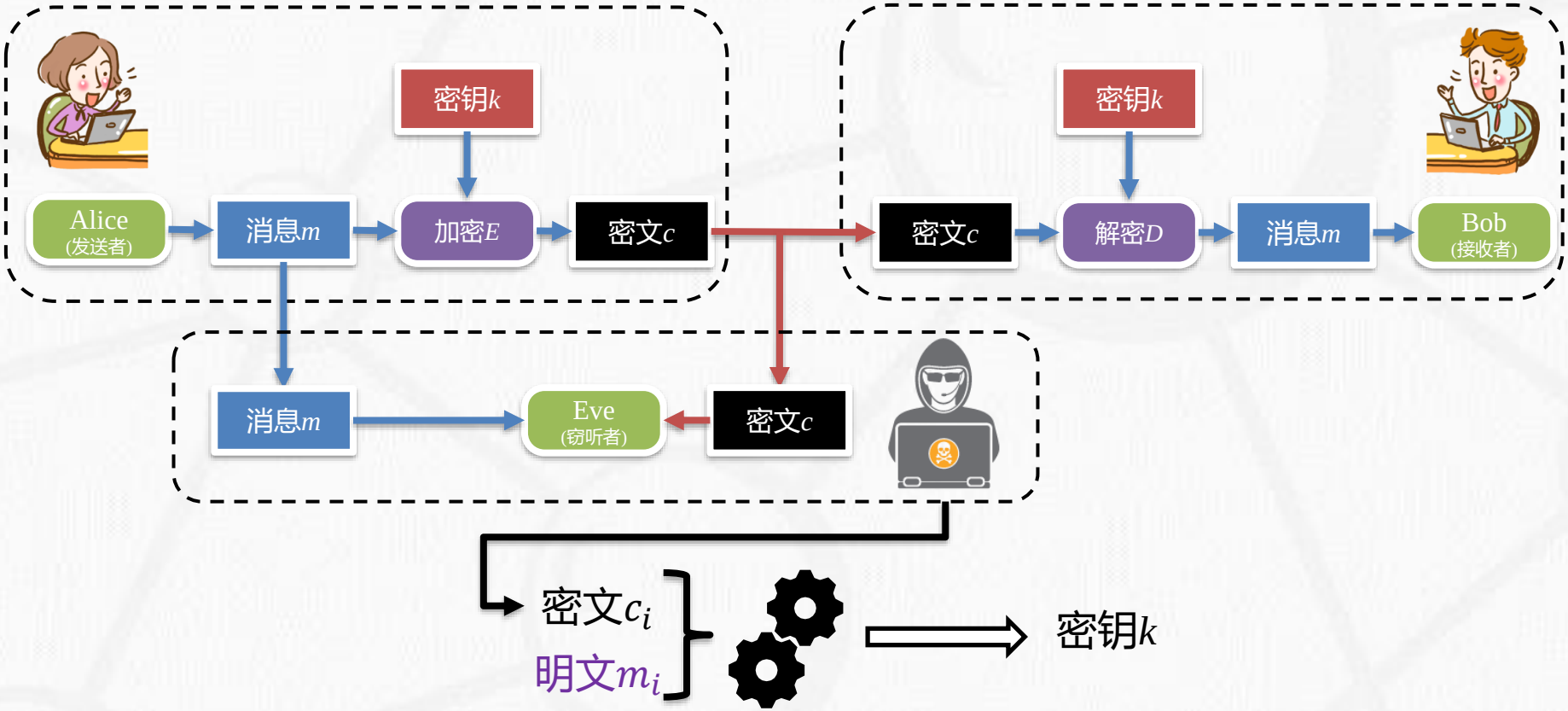
§2.1.2 密码学基础知识 - 惟密文攻击

- 惟密文攻击(COA: Ciphertext-Only Attack)
  - 攻击者可以获得密文c



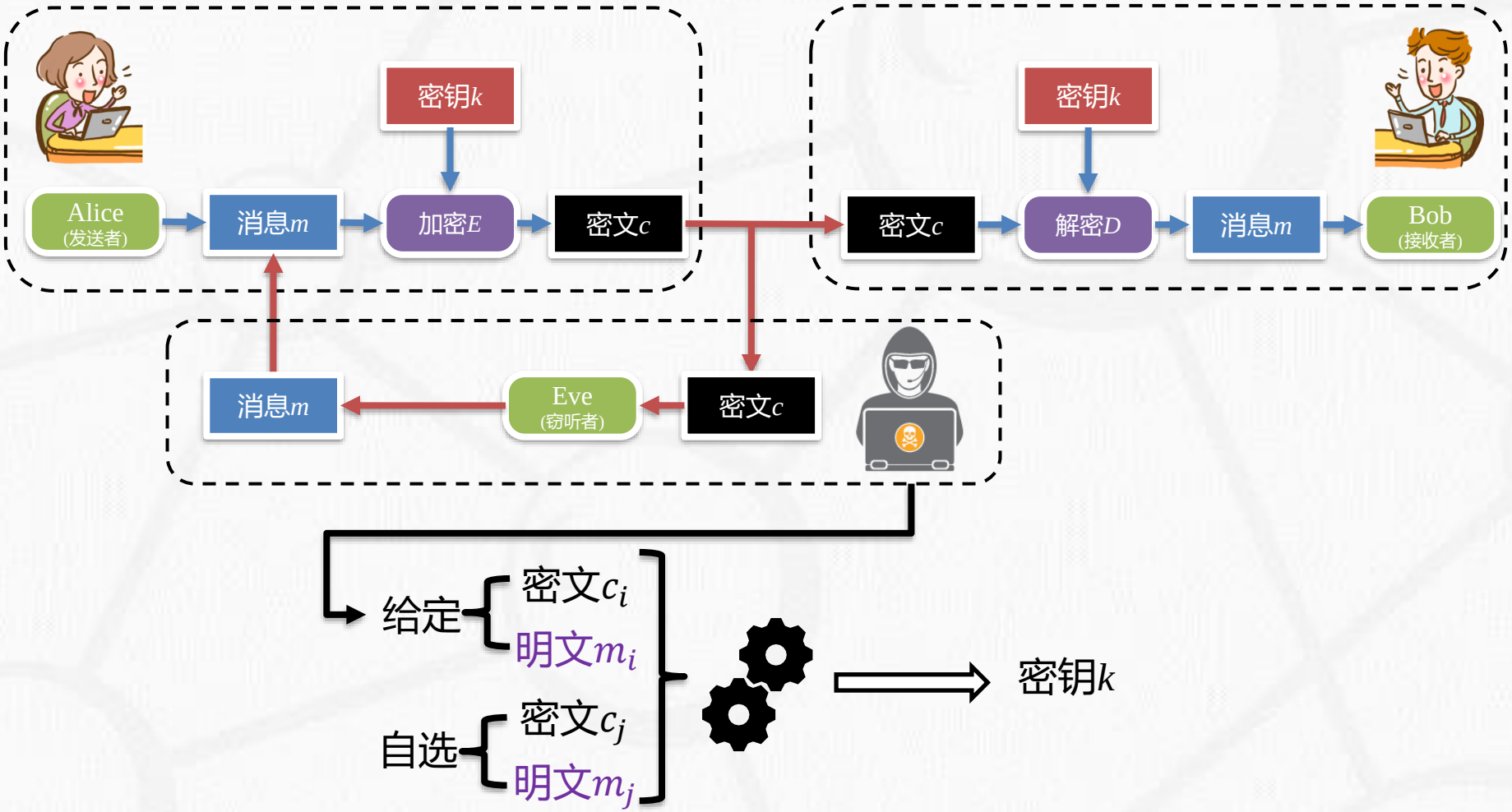
§2.1.2 密码学基础知识 - 已知明文攻击

- 已知明文攻击(KPA: Known-Plaintext Attack)
  - 攻击者可以获得一定数量的明密文对(m_i, c_i)



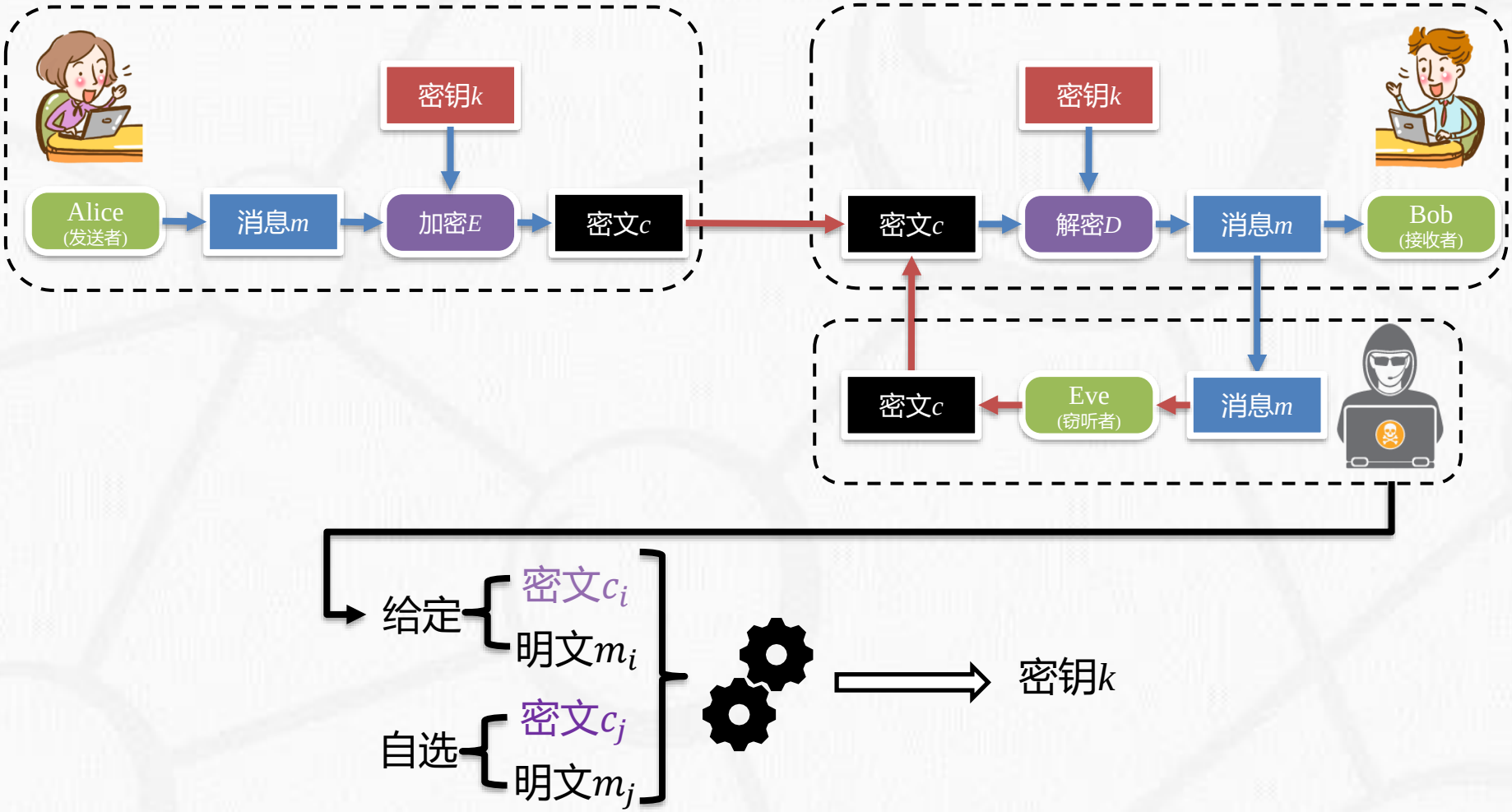
§2.1.2 密码学基础知识 - 选择明文攻击

- 选择明文攻击(CPA: Chosen-Plaintext Attack)
  - 攻击者自主选择明文m_i，并获得对应的密文c_i



§2.1.2 密码学基础知识 - 选择密文攻击

- 选择密文攻击(CCA: Chosen-Ciphertext Attack)
  - 攻击者自主选择密文c_i，并获得对应的明文m_i



§2.1.2 密码学基础知识 - 密码分析的类型

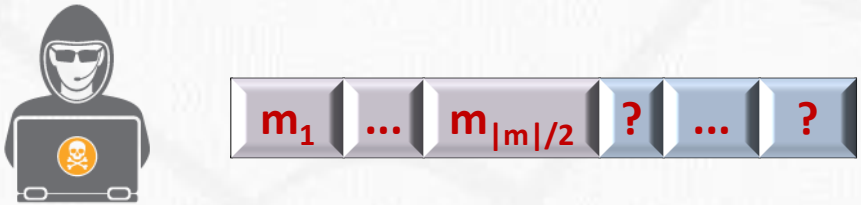
- 密码分析是研究在不知道密钥的情况下来恢复明文的科学。
- 根据所具有的知识和掌握情报的不同，可以将密码分析分为：
  - 唯密文攻击
  - 已知明文攻击
  - 选择明文攻击
  - 选择密文攻击

攻击类型	密码破译者已知的东西
唯密文	• 加密算法 • 待破译的密文
已知明文	• 加密算法 • 待破译的密文 • 由密钥形成的一个或多个明文-密文对
选择明文	• 加密算法 • 待破译的密文 • 由破译者选择的明文消息，连同对应的由密钥生成的密文
选择密文	• 加密算法 • 待破译的密文 • 由破译者选择的猜测性密文，连同它对应的由密钥生成的已破译明文

§2.1.2 密码学基础知识 - 攻击模型(1)

- 安全目标1：攻击者不能计算出完整明文

- 存在问题：
  - 泄露部分明文信息，有的时候也很关键！

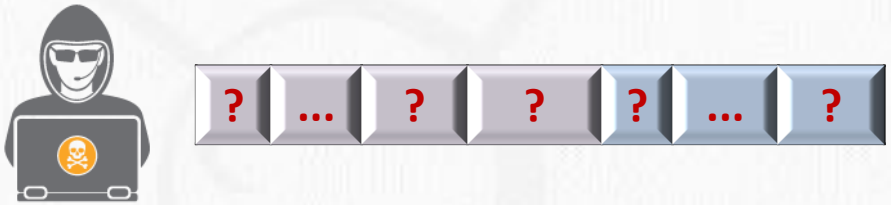


  - 例子：必然泄露明文的大小。对于工资而言，可能泄露工资数大于10万的员工信息。

§2.1.2 密码学基础知识 - 攻击模型(2)

- 安全目标2：攻击者不能计算出明文的任何有意义信息

- 存在问题：
  - 什么是有意义的信息？没有严格的定义。



§2.1.2 密码学基础知识 - 攻击模型(3)

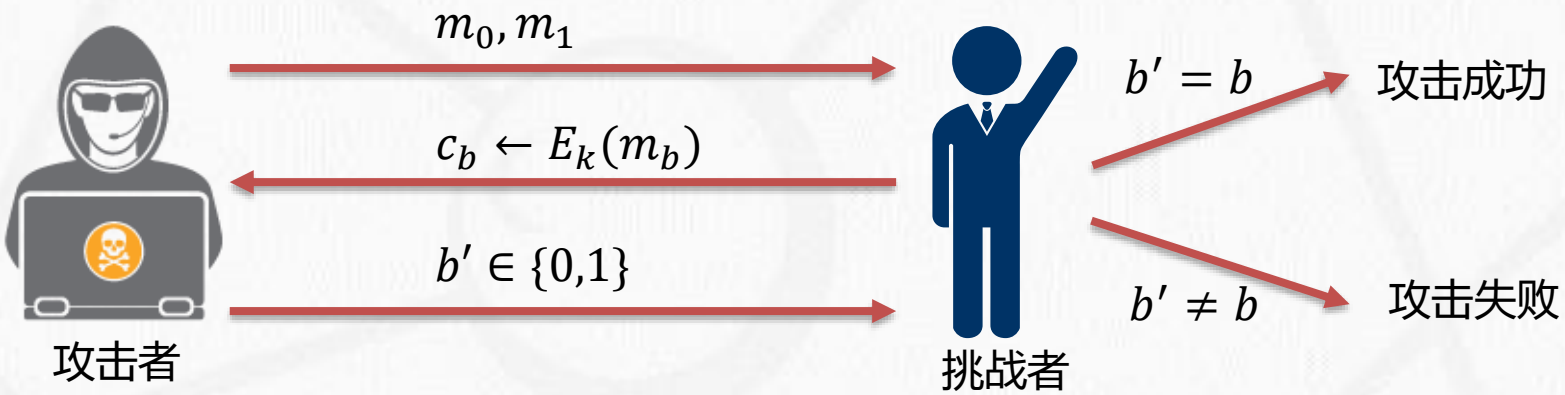
- 最终安全目标：不能从密文中计算出任何关于明文的函数

- 等价于：
  - 攻击者不能从密文中计算出任何信息。

- 采用不可区分性(Indistinguishability)定义最终安全目标。

§2.1.2 密码学基础知识 - 不可区分性

- 不可区分性(Indistinguishability)
  - 攻击者(Adversary)对两个明文m_0和m_1进行挑战。挑战者(Challenger)随机选择其中的一个明文用给定的加密方案加密得到密文c_b，并发送给攻击者。攻击者对猜测$b' \in \{0,1\}$，若满足下式则称该加密方案是不可区分安全的：
    - $|\Pr[b = b'] - \frac{1}{2}| \leq negl(n)$。



§2.1.2 密码学基础知识 - 不可区分安全

- 不可区分安全性：
  - IND-COA：惟密文攻击下的不可区分性。
  - IND-KPA：已知明文攻击下的不可区分性。
  - IND-CPA：选择明文攻击下的不可区分性。
  - IND-CCA：选择密文攻击下的不可区分性。

} 实用的安全性定义

- 新型密码的不可区分性安全：
  - IND-OCPA、PEKS-IND-CPA等。

§2.1.1 & §2.1.2 小结

- 内容回顾
  - 密码学的发展历程
  - 现代密码学的三原则
  - 不可区分性的定义

- 掌握
  - 现代密码学三原则的内涵
  - 密码学中常用的威胁模型
  - 不可区分性的深入解读

Thanks!
Questions & Advices!