密 码 学

第二章 密码学的基本概念

网络空间安全学院
朱 丹
zhudan@nwpu.edu.cn

网 络 空 间

Cyberspace

在信息化时代，人们生活和工作在物理世界、人类社会和信息空间(Cyberspace) 组成的三元世界中

2008 年，美国第54 号总统令对Cyberspace 进行了定义："Cyberspace 是信息环境中的一个全球域，由独立且互相依存的IT 基础设施和网络组成，包括互联网、电信网、计算机系统，以及嵌入式处理器和控制器。"

在国内，Cyberspace 一词有多种翻译：信息空间、网络空间、网电空间、数字世界等。有的甚至直接译音，称为赛博空间

网络空间特征

Characteristics of 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

信息安全要素

Elements of Information Security

机密性 (Confidentiality)

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

完整性 (Integrity)

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

可用性 (Availability)

保证合法用户对信息和资源的使用不会
被不正当地拒绝

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

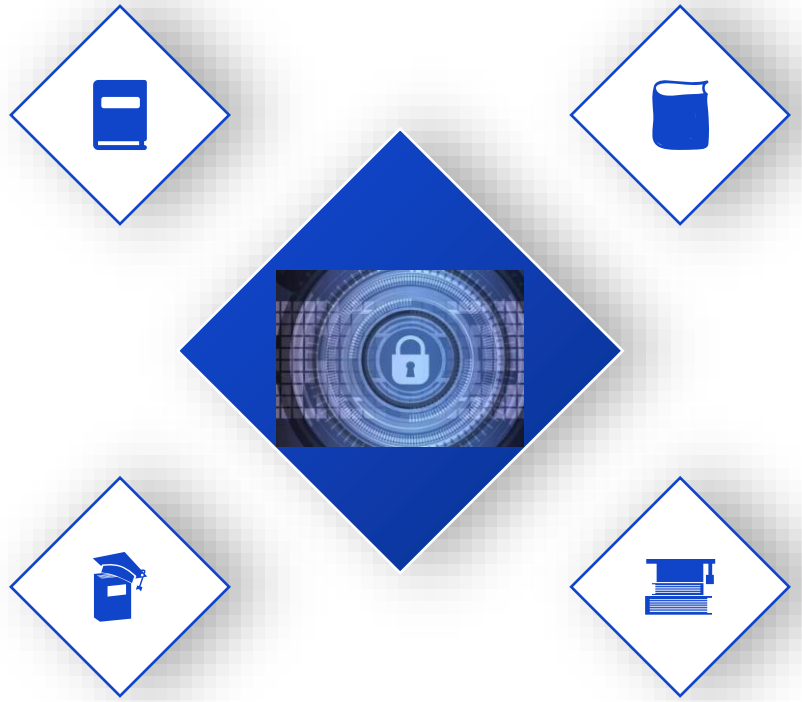
The Role of Cryptography

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

章节安排

Outline

密码学的基本概念

密码学发展史

密码体制的安全性

密码编码的基本方法

替代密码的统计分析

章节安排

Outline

密码学的基本概念

密码学发展史

密码体制的安全性

密码编码的基本方法

替代密码的统计分析

Password vs. Cryptography

密码/口令（Password） -- 认证技术

密码学的范畴

Scope of Cryptography

密码学研究什么？

- 密码编码学——主要研究对信息进行编码，实现对信息的隐蔽（机密性）、完整性验证等
- 密码分析学——主要研究加密信息的破译或信息的伪造
- 密钥管理学——主要研究密码应用中的密钥安全性问题

为什么要进行数据加密？

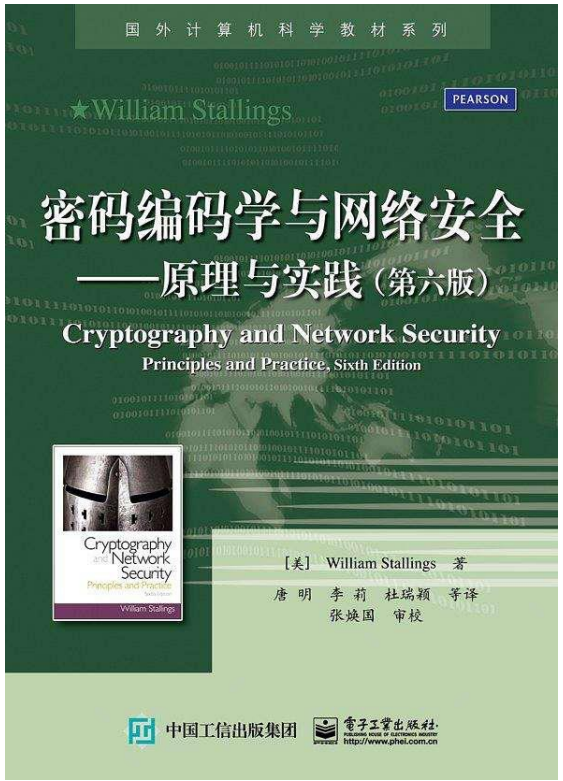
- 为了数据安全！

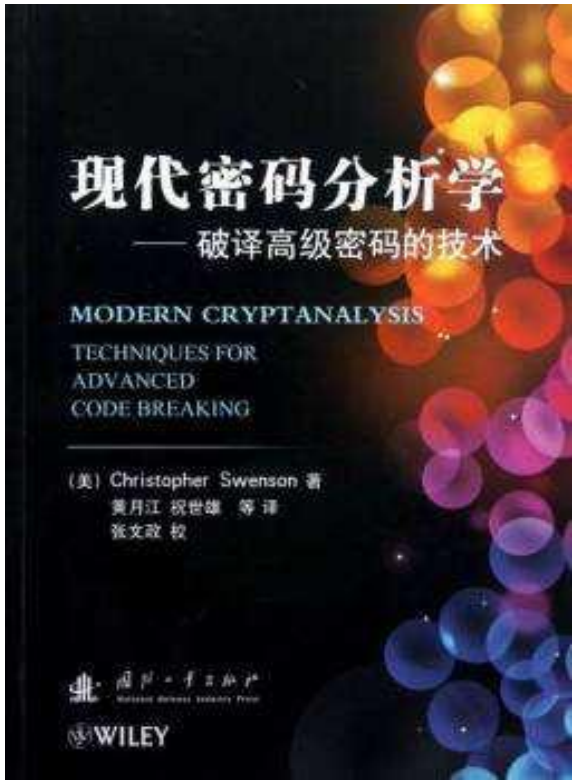
密码学在信息安全中处于什么地位？

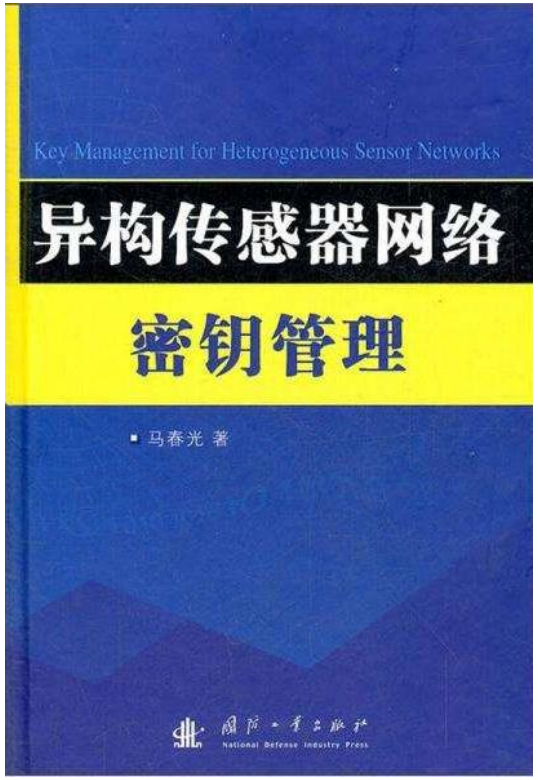
- 信息安全的重要基础技术

密码学的范畴

Scope of Cryptography







密码学解决的问题

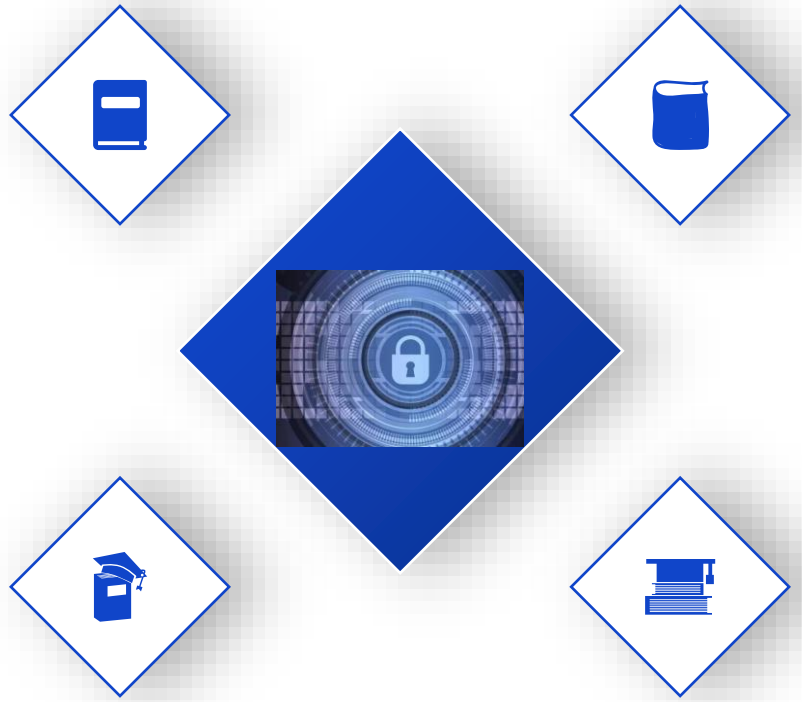
The Role of Cryptography

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

密码体制的组成

明文（Message - m）

密文（Ciphertext - c）

密钥（Key - k）

明文空间（M）

密文空间（C）

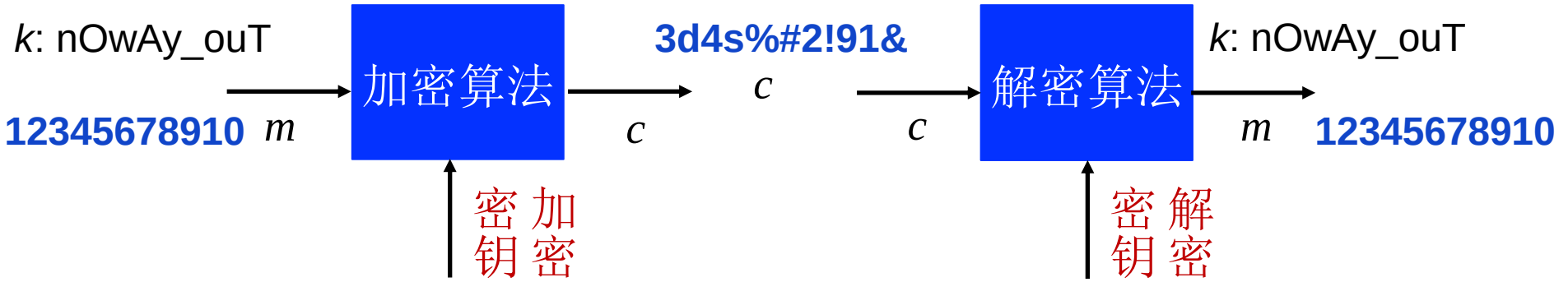
密钥空间（K）

加密算法（Encryption - E_{k_e}）

解密算法（Decryption - D_{k_d}）

对于$\forall m \in M, \forall k \in K$，都有 $\begin{cases} c = E_{k_e}(m) \\ m = D_{k_d}(c) \end{cases}$

加 密 和 解 密



加密和解密算法的操作通常都是在一组密钥的控制下进行的, 分别称为加密密钥(Encryption Key) 和解密密钥(Decryption Key)

保 密 通 信 模 型

Model of Secure Communication

主动攻击

非法接入者

被动攻击

密码分析员

c'

m'

信源

m

加密器

c = E(K1, m)

c

公开信道

解密器

m = D(K2, c)

m

信宿

密钥源
K1

安全信道

密钥源
K2

章节安排

Outline

密码学的基本概念

密码学发展史

密码体制的安全性

密码编码的基本方法

替代密码的统计分析

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 – 第一阶段

科学密码学前夜时期（1949年之前）

4000多年前，人类创造的象形文字（最原始的密码方法）

19世纪末，密码的主要标志是手工和机械密码

1949年前，密码技术基本上是一门技巧性很强的艺术

这一阶段最有影响力的密码学论文：1918年，Friedman发表的《重合指数及其在密码学中的应用》

William F. Friedman

https://www.britannica.com/biography/William-F-Friedman

密码学的发展 – 第二阶段

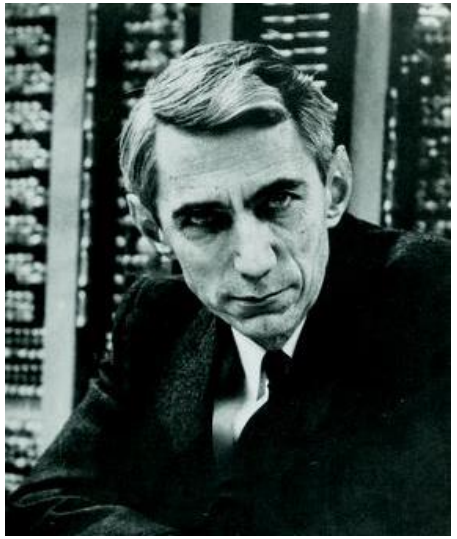
对称密码学早起发展时期（1949– 1975）

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。

密码学的发展 – 第四阶段

后量子密码

量子计算机的高度并行性对基于NP困难数学问题的现代公钥密钥体制的威胁是致命的

尚未发现量子计算机对不依赖于任何困难问题的对称密码和HASH函数等密码算法有多项式时间的攻击算法

目前，量子计算主要威胁公钥密钥体制

把具有量子计算安全的公钥密钥体制称为“后量子公钥密码体制”

密 码 标 准 的 发 展

密 码 计 划

- ✓ 美国1997年启动的NIST计划
- ✓ 欧洲2000年启动的NESSIE计划
- ✓ 欧洲2004年启动的ECRYPT计划
- ✓ 美国2007年启动的SHA-3计划
- ✓ 我国近年来也形成了国密标准体系

密 码 举 例

最早的有记载的加密文字：

公元前19世纪古埃及第十二王朝

尼罗河畔Menet Khufu镇一位贵族的碑文

目的是为了保持神秘和神圣

密 码 举 例

最早的密码 – 斯巴达密码

公元前405年的古希腊

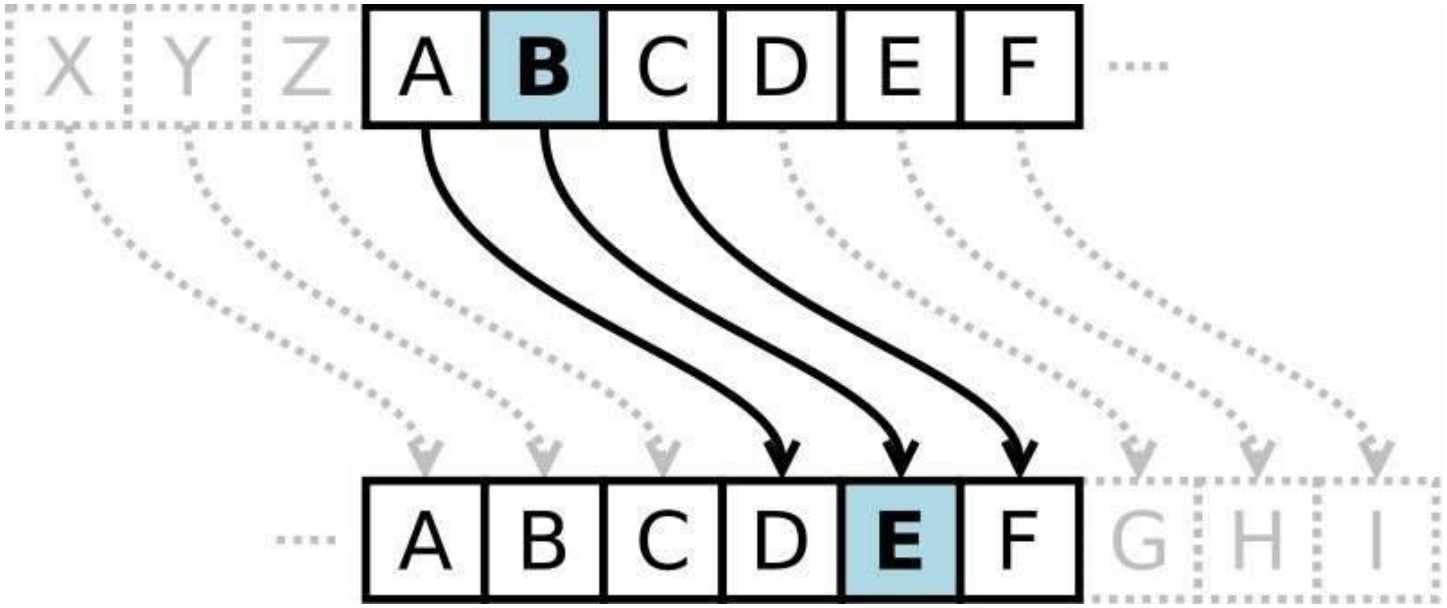
雅典间谍的腰带情报，是世界上最早的密码情报

目的是为了通信保密

密 码 举 例

凯撒密码 - 移位密码

古罗马时代，凯撒发明



明文	密文
ATTACK NOW	DWWDFN QRZ

密 码 举 例

波利比奥斯密码

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

明文	密文
POLYBIUS	3534315412244543

密 码 举 例

斯巴达人“天书”密码

波利比奥斯密码

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

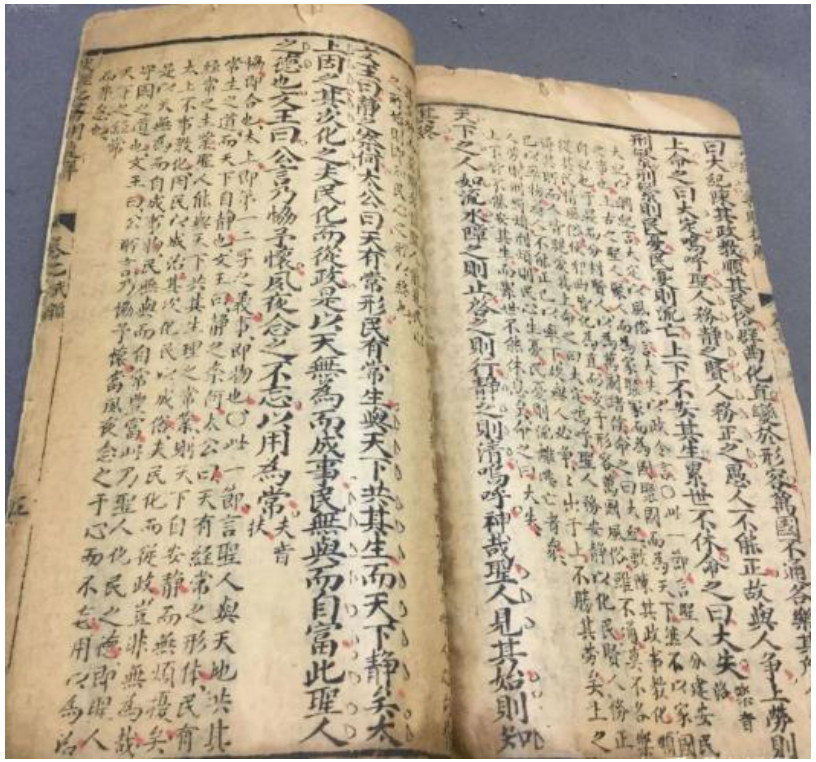
艾伯蒂密码圆盘

转轮密码机 ENIGMA

密 码 举 例

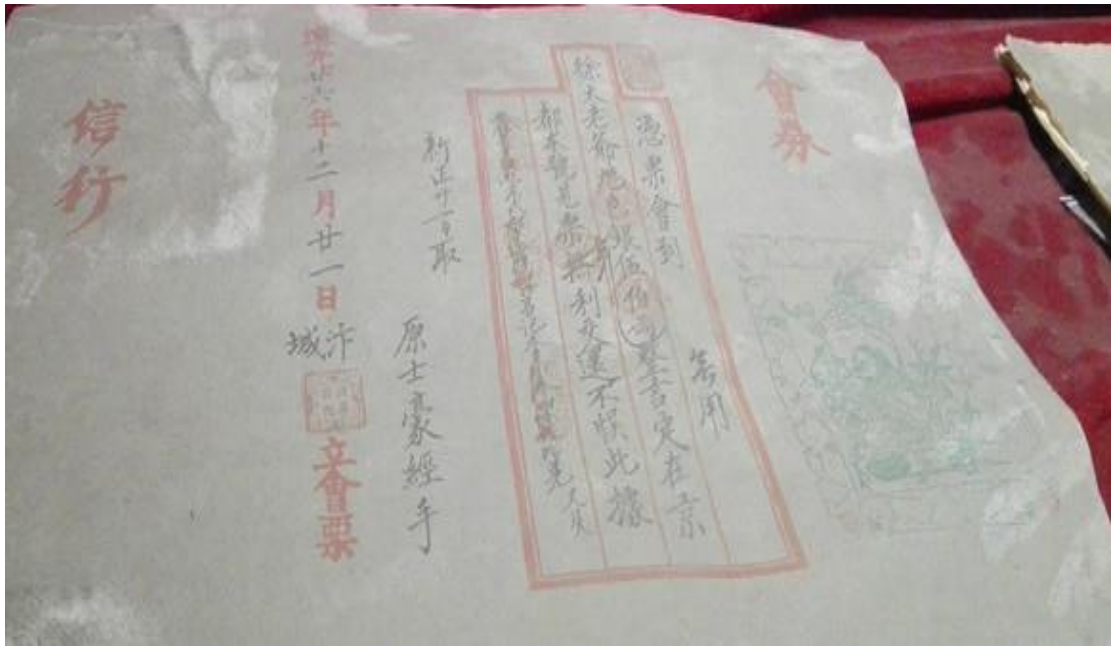
Examples

中国古代兵书《六韬》中的《龙韬•阴符》篇讲述了君主如何在战争中与在外的将领进行保密通信。书中对“阴符”的描写如下：“阴符共有八种：一种长一尺，表示大获全胜，摧毁敌人；一种长九寸，表示攻破敌军，杀敌主将；一种长八寸，表示守城的敌人已投降，我军已占领该城；一种长七寸，表示敌军已败退，远传捷报；一种长六寸，表示我军将誓死坚守城邑；一种长五寸，表示请拨运军粮，增派援军；一种长四寸，表示军队战败，主将阵亡；一种长三寸，表示战事失利，全军伤亡惨重。”



隐写术（Steganography）

加密押的日昇昌银票　　安全机制：多表替代密码 + 认证技术（字迹、水印、密押）



密 码 举 例

豪密•1931（周恩来总理）

豪密，由中国共产党初期领导人之一周恩来亲自编制，以周恩来党内化名“伍豪”命名

“豪密”所用的密码从不重复，简单好记，却难以破译，直到1949年中国国民党垮台，都没有被破译出来

豪密很可能由两部分组成：书名与册码；页码、行数与字序，能够在电报中实现“同字不同码，同码不同字”

章节安排

Outline

密码学的基本概念

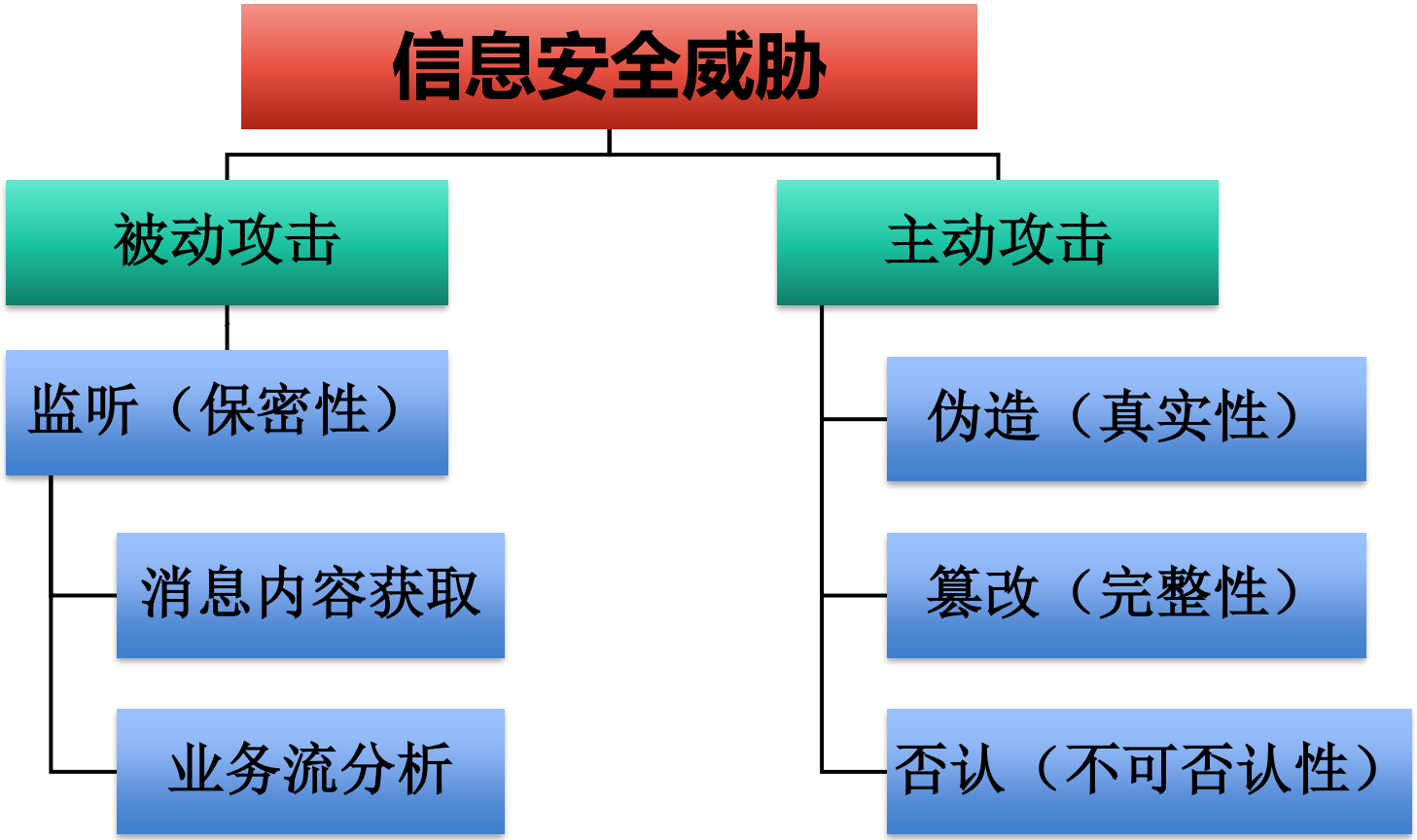
密码学发展史

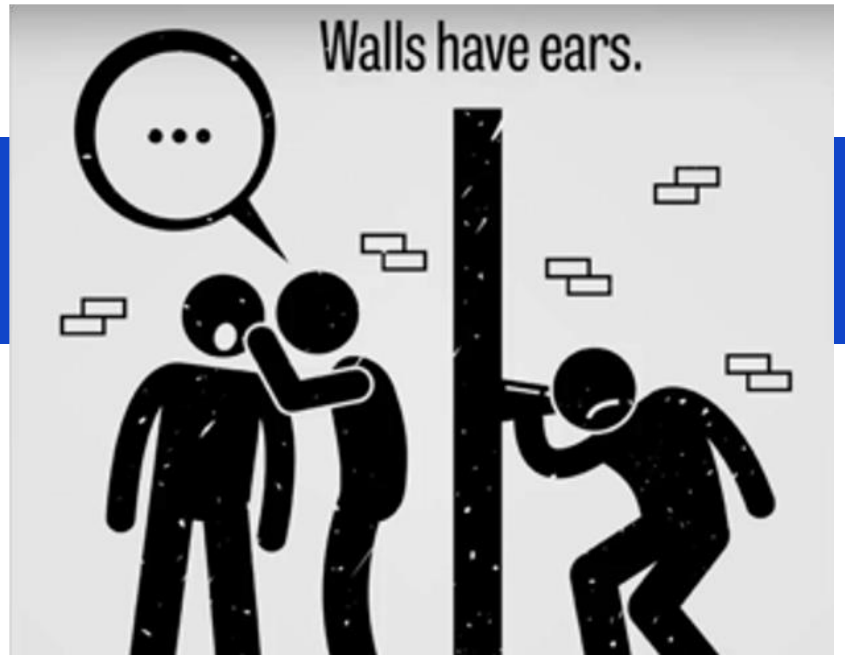
密码体制的安全性

密码编码的基本方法

替代密码的统计分析

信 息 安 全 威 胁



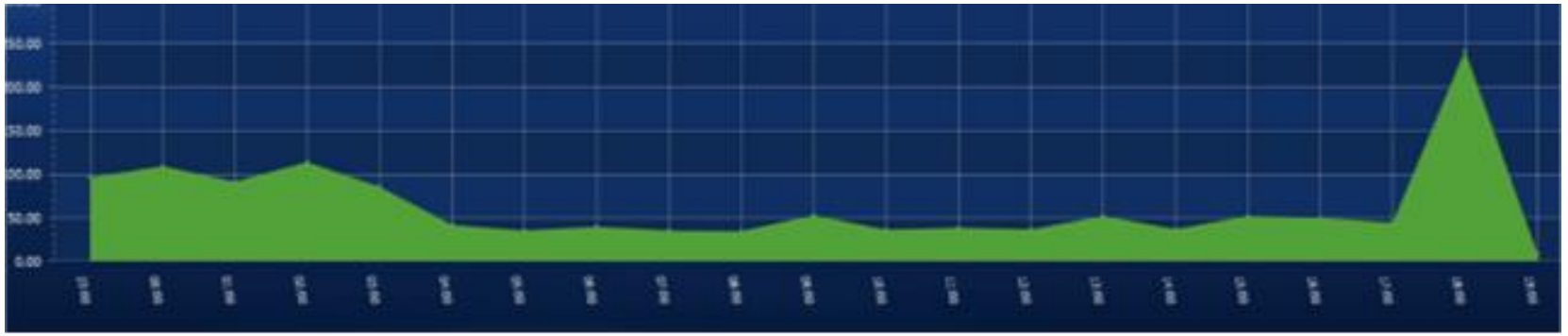


被 动 攻 击

被动攻击试图了解或利用系统的信息，但不影响系统资源

- ✓ 目标通常是获取敏感信息
- ✓ 窃听和流量分析是最常见的被动攻击

流量分析：监测通信双方（信源和信宿）之间的流量模式（如通信频度）



主动攻击：主动攻击包括对数据流进行篡改或伪造数据流

伪装：某实体假装别的实体

重放：将获得的信息再次发送，以产生非授权的效果

篡改：修改合法消息的一部分，或延迟消息的传输，或改变消息的顺序

否认：用户否认曾经对消息的生产、签发、接收等行为

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

“一切秘密寓于密钥之中”

柯克霍夫斯（Kerckhoffs）原则

即使密码系统中的算法为密码分析者所知，也难以从截获的密文推导出明文或密钥

密码体制的安全性仅应依赖于对密钥的保密，而不应依赖于对算法的保密

只有在假设攻击者对密码算法有充分的研究，并且拥有足够的计算资源的情况下仍然安全的密码才是安全的密码系统

密码体制安全性

Security of A Crypto System

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

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

2

可证明安全

把密码体制的安全性规约位某个经过深入研究的数学难题

1

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

破译密码需要N步，N非常大（如$N = 2^n$，$n = 128$）

或破译密码需要大量的存储空间

$$2^{128} \approx 3.4 * 10^{38}$$

中文名	全球超级计算机500强	第一名	美国橡树岭国家实验室的Frontier
外文名	The top 500 -- a respected list of the world's most p	第二名	日本“富岳” [8]
	owerful computers	第三名	芬兰“LUMI” [8]
		第四名	美国“顶点” [8]

美国能源部下属橡树岭国家实验室开发的超算“前沿”运算峰值速度超过每秒100亿亿次

神威　太湖之光

(9.3亿亿次/秒)

https://www.top500.org/

可证明安全：把密码体制的安全性规约位某个经过深入研究的数学难题

RSA – 大数因子分解困难问题

ECC – 有限域上的离散对数困难问题

截至2020年，已成功分解829比特位的整数（RSA-250 ）

https://wikimili.com/en/RSA_Factoring_Challenge
https://wikimili.com/en/RSA_Secret-Key_Challenge
https://wikimili.com/en/Integer_factorization_records
https://wikimili.com/en/RSA_numbers

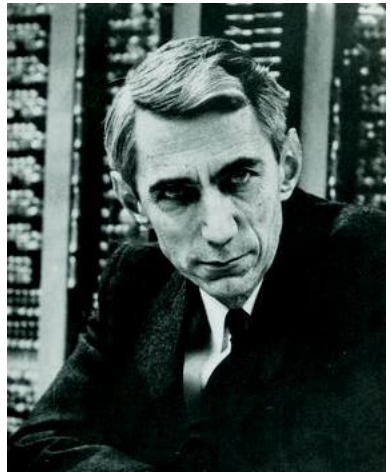
无条件安全：密码分析者具有无限的计算能力，密码体制也不能破译

无条件安全与信息论有关

通过信息论来证明传递过程中无信息泄露

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

该文创立的信息论为密码学奠定了理论基础



Claude E. Shannon

密 码 体 制 安 全 性

完全破译：攻击者可以得到密钥

部分破译：攻击者可以得到部分密文对应的明文

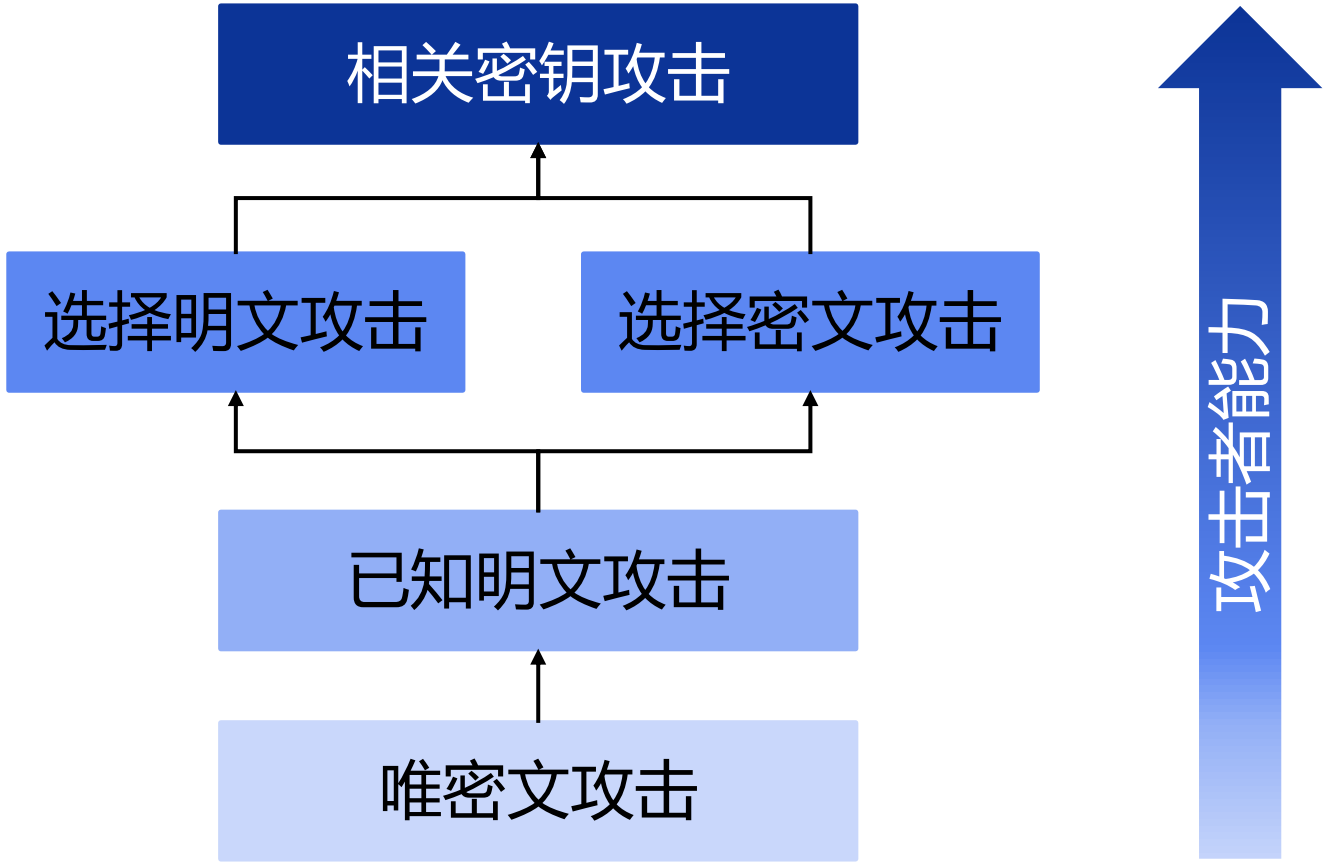
密文区分：攻击者可以以超过50%的概率确定

任意给定两组明文和密文，攻击者可以确定对应关系

给定任意一个明文和对应的密文，以及一些和密文等长的随机串，攻击者可以判断出哪个是正确的密文

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：



已知密文攻击

攻击者掌握足够多使用同一密钥加密的密文

攻击的目的是破译出使用的密钥或对应的明文

已知明文攻击

攻击者具有已知密文攻击的条件

攻击者还掌握足够多使用同一密钥加密的密文及对应的明文

攻击的目的是破译出使用的密钥或其他密文对应的明文

选择明文攻击

攻击者具有已知明文攻击的条件

攻击者还可任意选择对密码破译有利的足够多的明文，并得到相应的密文

攻击的目的是破译出使用的密钥或其他密文对应的明文

分组密码分析中，多采用已知明文或选择明文攻击

选择密文攻击

攻击者具有已知明文攻击的条件

攻击者还可任意选择对密码破译有利的足够多的密文，并得到相应的明文

攻击的目的是破译出使用的密钥或其他密文对应的明文

主要用于攻击公钥密码算法，特别是签名算法

相关密钥

对密码破译有利

与实际密钥有一定内在联系的密钥

已知明文攻击

具有选择明文和选择密文攻击的条件

还能得到由所求密钥的相关密钥对其他任意明文加密所得的密文

例如，设k是待求的密钥，$P_1, P_2, \ldots, P_n$是n个公开的数据，则

$$k \oplus P_1, k \oplus P_2, \ldots, k \oplus P_n$$

就是相关密钥，同时利用由他们加密的明文和密文发起对密钥k的攻击就是一种相关密钥攻击。

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

参 考 阅 读 和 课 后 作 业

After-class Readings and Homework

https://www.huawei.com/cn/trust-center/post-quantum-cryptography

https://baike.baidu.com/item/%E8%B1%AA%E5%AF%86/1076450?fr=ge_ala

搜集一个与密码有关的案例（包括密码的发展、应用、攻击等），用浅显易懂的语言把案例描述清楚，并对案例进行简要的分析。

分析中要体现自己的理解和观点！

Word或PDF文档格式，以学号_姓名命名发送给助教


感谢聆听!
THANK YOU FOR YOUR ATTENTION!