第 2 章　密码技术

第 2 章　密码技术

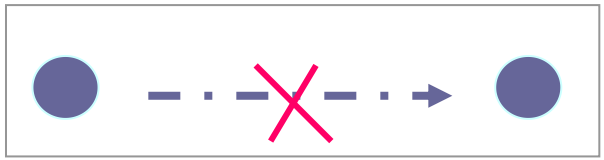
- 2.1　古典密码
- 2.2　对称密码体制
- 2.3　公钥密码体制

2.1 古典密码

- 2.1.0 密码学基本概念
- 2.1.1 古典密码学概述
- 2.1.2 凯撒密码--Caesar
- 2.1.3 单表代换密码--Affine
- 2.1.4 唯密文攻击
- 2.1.5 多字母代换--Playfair
- 2.1.6 多表代换密码--Vegenere，Rotor
- 2.1.7 置换密码

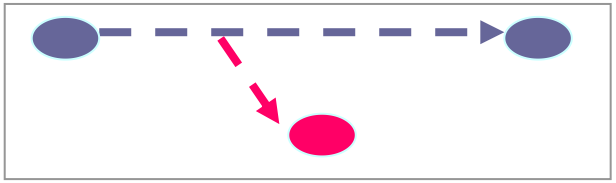
网络通信面临的潜在威胁

中断



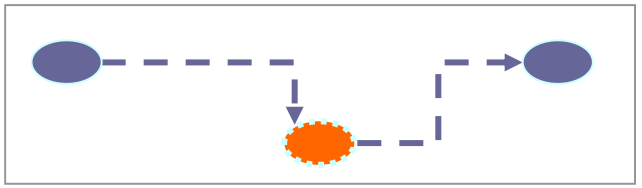
可用性

窃听



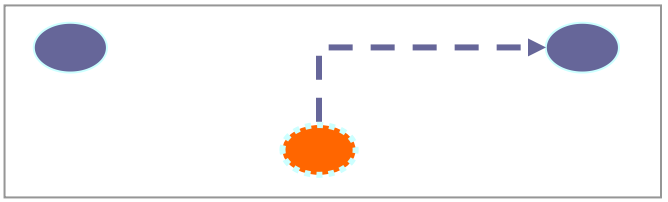
机密性

篡改



完整性

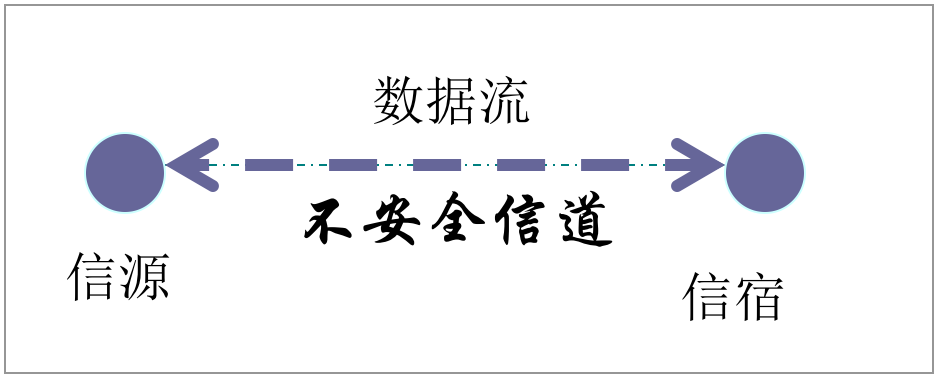
欺骗/
假冒



真实性

密码学的目标

在不安全的信道中实现安全的通信！



2.1.0 密码学基本概念

- 密码学发展史
  - 滚筒密码（人类有记载的第一个密码）
  - 凯撒密码（古罗马古埃及时代）
  - 两次世界大战的密码战（Enigma密码机）
  - 香农1949 “*Communication Theory of Secrecy System*”提出了现代保密通信的模型和发展方向
  - 1976 Diffie-Hellman“*New Direction in Cryptography*”指出用计算复杂度作为设计密码算法的工具（一种密钥交换算法，使双方安全地交换密钥）
  - 1997 美国DES加密标准
  - 商用密码发展
  - 2004年8月28日 “*中华人民共和国电子签名法*”

密码学发展新方向(略)

- **量子密码(Quantum Cryptography)**
  - 诞生于20世纪70年代，量子密码学的理论基础是物理学的量子力学理论
  - 以量子密码学制作密钥，则此**密钥具有不可复制性**。如果不幸被中途撷取，则因为测量过程中会改变量子状态，盗得的会是毫无意义的资料。
  - **安全性由海森堡测不准原理及单量子不可复制定理保证**。**海森堡测不准原理**指观察者无法同时准确地测量待测物的位置与动量。**单量子不可复制定理**指在不知道量子状态的情况下复制单个量子是不可能的，复制单个量子就需要作测量，而测量必然改变量子的状态。

密码学发展新方向(略)

- **DNA密码**(DNA Cryptography)
  - 1994年DNA计算的出现而出现，以**DNA**为信息载体，以**现代生物技术**为实现工具。
  - 利用**DNA计算**的超大规模并行性、超低的能量消耗和超高密度的信息存储能力等优点，实现加密、认证及签名等密码学功能。
  - 不足
    - 缺乏相关的理论支持
    - 实现困难

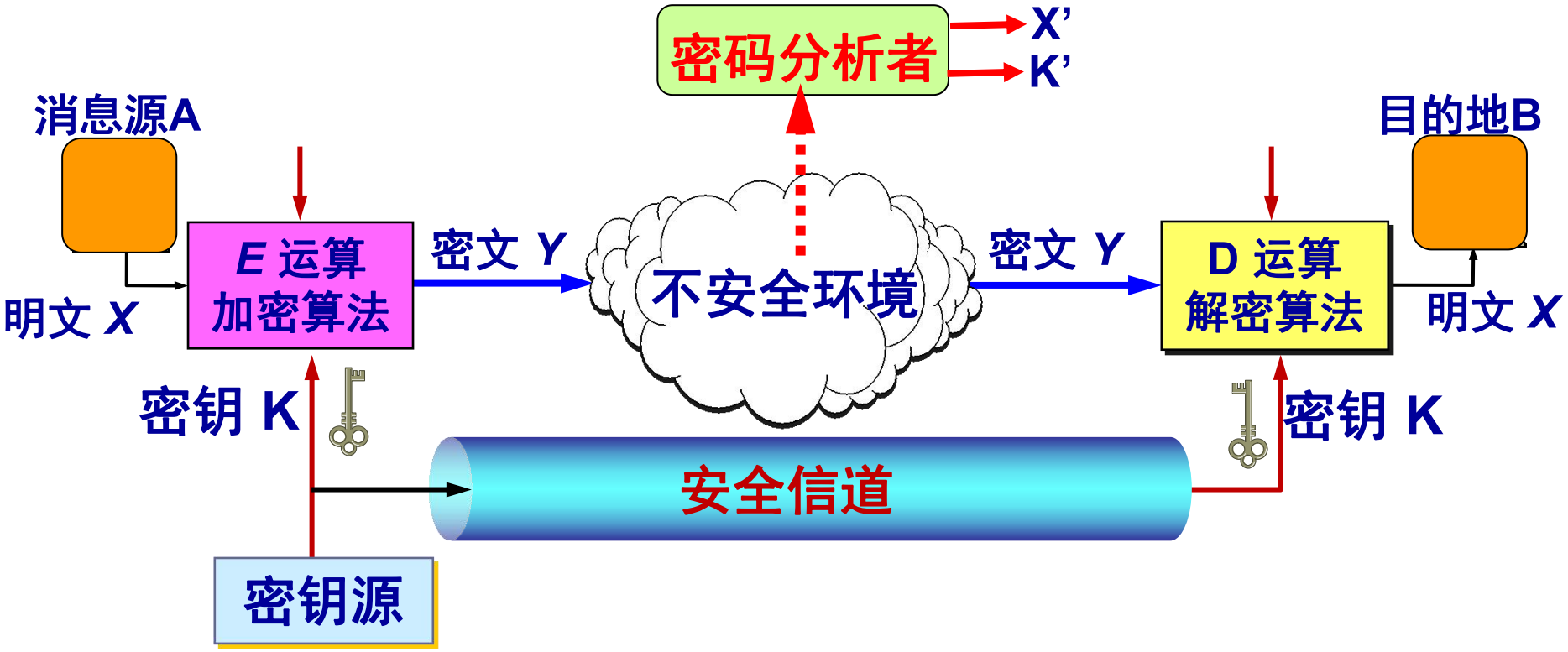
密码学发展新方向(略)

	传统密码	量子密码	DNA密码
发展状况	2000多年前凯撒密码，具有完善的理论体系	20世纪79年代，已经逐渐开始投入使用	1994年，理论处于探索阶段，使用代价高昂
安全性	基于数学不可计算理论，除了一次一密外，仅具有计算安全性	理论上不可破，安全性建立在海森堡测不准定理之上，物理法则保证了安全性	以生物学技术的局限性为安全依据，与计算能能力无关，相关理论有待研究
使用功能	计算使用电子计算机、量子计算机和DNA计算机；传输使用多种介质；存储用光盘、磁介质和DNA等；可实现公私钥加密、身份认证和数字签名等功能。	量子信道传输；适合实时通信，不适合安全存储；不易实现公钥加密、数字签名等功能	物理手段传送；存储用DNA等；可实现公私钥加密、身份认证和数字签名等多种功能

密码学基本概念

- **密码体制**：是密码技术中最核心的概念，一个密码体制被定义为一对数据变换，其中，被隐蔽的数据是**明文[plaintext]**，隐蔽后的数据是**密文[ciphertext]**
- **加密[encryption]**：将**明文**转换为**密文**的过程
- **解密[decryption]**：将**密文**转换为**明文**的过程
- 密码与隐写术不同

密码体制



用户 A 向 B 发送明文 X，通过加密算法 E 运算后，就得出密文 Y。

加密模型的基本组成

- **明文**：原始**可理解**的消息或数据，是算法的输入；
- **加密算法**：对明文进行各种处理（**代替**和**变换位置**）

  $Y=E(K, X)$
- **密钥**：加密算法的输入，**独立于明文和算法**。
- **密文**：算法的输出，依赖于明文和密钥，看起来完全随机且**意义不可理解**。
- **解密算法**：本质上是加密算法的**逆运算**。

  $X=D(K, Y)$

密码体制的安全要求

- 加密算法必须是足够强的
- 发送者和接收者必须在某种安全的形式下获得密钥并且必须保证密钥安全

密码学的研究内容

- 密码学包括：密码编码学[Cryptography]和密码分析学[Cryptanalysis]
  - 密码编码学：是密码体制的设计学，寻求提供信息机密性、完整性、真实性和非否认性等方法。
  - 密码分析学：是在未知密钥的情况下从密文推演出明文或密钥的技术，研究加密消息的破译和伪造等破坏密码技术所能提供安全性的方法。
- 密码编码学与密码分析学合起来即为密码学[cryptology]。

密码编码学

- 三个独立的特征
  - 转换明文为密文的运算类型：代替（代换）和置换
  - 密钥个数：一个或多个
  - 处理明文的方法：分组密码（一组元素）和流密码（一个元素）

针对密码的攻击

- **密码分析**
  - 简称密码分析，是从密码算法设计角度出发，评判密码算法安全性的重要方法。
  - 密码分析的目的
    - 完全破译：破译使用者的密钥
    - 部分破译：恢复某些密文对应的明文
- **穷举攻击**
  - 攻击者对一条密文尝试所有可能的密钥直到把它转化为可读的有意义的明文。

针对密码的攻击

- **侧信道攻击**：是一种针对**实现密码算法**的物理攻击方法（参考补充1）
- **密码误用攻击**：由于应用软件开发者未正确**使用密码算法**而产生（加密模式误用、初始向量误用、加密算法误用等）漏洞进行攻击（参考补充2）

密码分析

- 密码分析种类
  - 唯密文攻击：分析者有一个或n个用同一个密钥加密的密文
  - 已知明文攻击：分析者有1/n个待破解密文+some明文和对应的密文
  - 选择明文攻击：分析者可得到所需要的任何明文对应的密文，这些密文和待破解的密文是用同一密钥加密
  - 选择密文攻击：分析者可得到所需要的任何密文对应的明文，这些密文和待破解的密文是用同一密钥加密

密码分析

攻击类型	密码破译者已知的信息
唯密文 [Ciphertext Only]	• 加密算法、要解密的密文（攻击难度最大，一般算法均可抵御）
已知明文 [Known Plaintext]	• 加密算法、要解密的密文 • 一个或多个用密钥产生的明文-密文对 （一般要求加密算法能抵抗该类攻击）
选择明文 [Chosen plaintext]	• 加密算法、要解密的密文 • 破译者选定的明文消息，以及使用密钥产生的对应密文
选择密文 [Chosen ciphertext]	• 加密算法、要解密的密文 • 破译者选定的密文，以及使用密钥产生的对应的解密明文
选择文本 [Chosen text]	• 加密算法、要解密的密文 • 破译者选定的明文消息，以及使用密钥产生的对应密文 • 破译者选定的密文，以及使用密钥产生的对应的解密明文

密码分析

- 如果不论截取者获得了多少密文，但在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为**无条件安全的，**或称为**理论上是不可破的。**
- 如果密码体制中的密码不能被可使用的计算资源破译，则这一密码体制称为在**计算上是安全的。**满足以下两个条件之一：
  - 破解密文的代价超出被加密信息的价值
  - 破解密文需要的时间超出信息的有用寿命

2.1.1 古典密码学概述

- 古典密码算法特点
  - 计算强度小
  - 以字母表为主要加密对象
  - 数据安全基于算法的保密
  - 密码分析方法基于明文的可读性以及字母和字母组合的频率特性
  - 代换技术和置换技术

古典密码学

- 典型类型
  - 代换密码(Substitution)：代换是古典密码中用到的最基本的处理技巧，所谓代换，就是将明文中的一个字母用其他字母、数字或符号替代的一种方法。
    - 单表代换密码：凯撒密码、仿射密码、单表代换密码
    - 多表代换密码
  - 置换密码(Permutation)：将明文字符按照某种规律重新排列而形成密文的过程。

相关说明

- 古典密码部分，被加密文本均假设为26个英文字母，算法描述中，常常用数字表示字母，对照关系表如下：

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

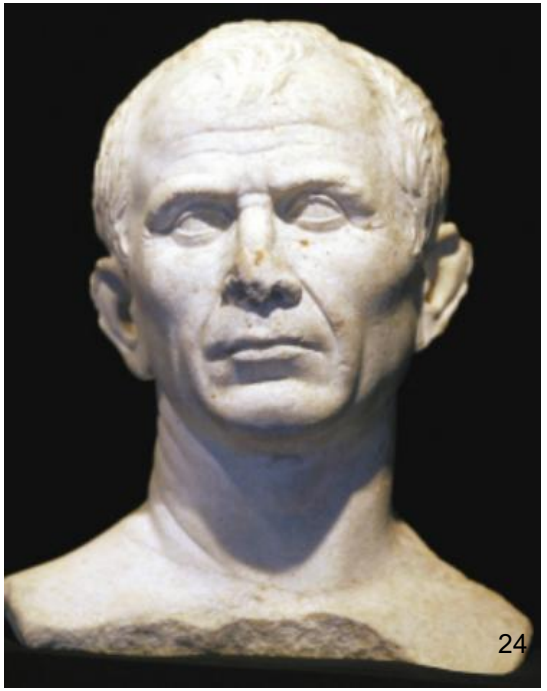
2.1.2 凯撒密码(Caesar Code)

- 已知最早的代换密码，又称**移位密码**
- 代换表（密钥，**k=3**）

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

明文：Caesar 密文：Fdhvdu



凯撒密码(Caesar Code)

- **数学描述：**

$$c=E(p)=(p+k) \bmod 26$$

$$p=D(c)=(c-k) \bmod 26$$

其中，明文$p \in Z_{26}$，密文$c \in Z_{26}$，密钥$k \in N$且k取[1,25]

凯撒密码(Caesar Code)

- 思考：如何破解？
- 举例
  - 凯撒希望与安东尼见面，见面地点在Tiber(the river)或Coliseum(the arena)
  - 凯撒派信使送去密信，内容为“EVIRE”
  - 如果安东尼不知道密码key，如何知道真正的见面地点？
- 攻击方法：穷举攻击(攻击者对一条密文尝试所有可能的密钥直到把它转化为可读的有意义的明文)

凯撒密码(Caesar Code)

- 思考：凯撒密码最多需要尝试多少次？
- 尝试次数与什么有关？

  密钥空间
- 凯撒密码密钥空间25个，太小，不安全
- 如何增加破解难度？ 增大密钥空间
- 如何增大密钥空间？

2.1.3 单表代换密码

- 代换表是26个字母的*任意置换*
- 数学描述：

$c=k(p1),(p2),\ldots,(pm),\ldots;$

$p=k^{-1}(c1),k^{-1}(c2),\ldots,k^{-1}(cm),\ldots$

其中，明文$p\in(Z_{26})^m$，密文$c\in(Z_{26})^m$，

密钥$k\in\{\Pi\mid$定义在0，…，25上的置换$\}$

单表代换密码

- 例题：加密函数

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

- 解密函数：

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

s g m a k e x o f h b v q z u j d w l p t c I n r y

- 明文：nice work
- 密文：XWVF RHYE
- 问题：密钥空间是多少？

26！

仿射密码 --Affine

- 凯撒密码的扩展，是一种典型的单表代换密码
- 数学描述：

$$c=E(p)=(a \times p+b) \bmod 26$$

$$p=D(c)=(c-b) \times a^{-1} \bmod 26$$

运用了乘法逆元和模运算，其中，明文$p \in Z_{26}$，密文$c \in Z_{26}$，

密钥k=（a,b），$0 \leqslant a, b \leqslant 25$且$\gcd(a, 26)=1$（a与26互素）

$a^{-1} \cdot a \equiv 1 \mod 26$

举例：a=3, $a^{-1}=9$；　a=5 $a^{-1}=21$；　a=7 $a^{-1}=15$；　a=1 $a^{-1}=1$；　a=9 $a^{-1}=3$；

仿射密码

- 例题：密钥k=(7,3),且gcd(7,26)=1，明文hot

加密：Hot=(7,14,19), a=7, b=3

(7 X 7 +3) mod 26 = 0
(7 X 14 +3) mod 26 = 23
(7 X 19 +3) mod 26 = 6

} 密文：(0, 23, 6)=axg

解密：7^{-1}= 15

(0 - 3) X 15 mod 26 = 7
(23-3) X 15 mod 26 = 14
(6 - 3) X 15 mod 26 = 19

} 明文：(7, 14, 19)=hot

仿射密码

- 练习：密钥k=(9,3),且gcd(9,26)=1，明文hot，求加解密过程。

加密：Hot=(7,14,19), a=9, b=3

(9 X 7 +3) mod 26 = 14

(9 X 14 +3) mod 26 = 25

(9 X 19 +3) mod 26 = 18

} 密文：(14,25,18)=ozs

解密：$9^{-1}=3$

(14-3) X 3 mod 26 = 7

(25-3) X 3 mod 26 = 14

(18-3) X 3 mod 26 = 19

} 明文：(7,14,19)=hot

仿射密码

- 习题

1. 仿射密码的密钥k=(11,23)，对明文the national security agency加密并使用解密变换验证你的结果。

2. 设由仿射变换对一个明文加密得到的密文为

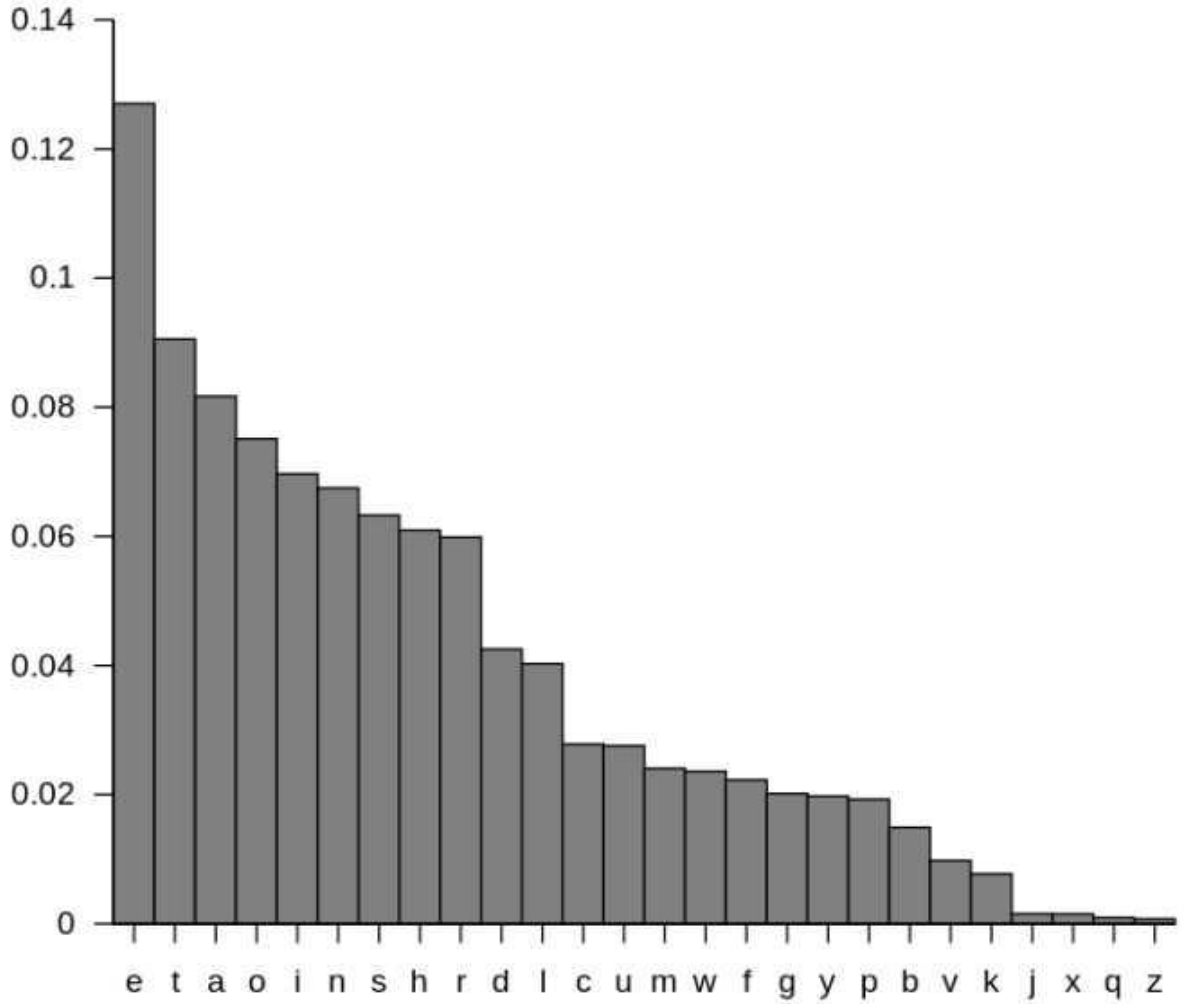
edsgi ckxhu klzve qzvkx wkzuk vcuh

又已知明文的前两个字符是if，对该密文解密(已知明文攻击)

2.1.4 唯密文攻击

- **统计攻击(频率攻击):** 利用明文（未经压缩的英文文本）的属性，利用语言的**统计规律**进行攻击（**唯密文攻击**）
- 人类的语言存在冗余，以英文文档为例：
  - 字母E是使用频率最高的
  - 其次是 T，R，N，I，O，A，S
  - Z，J，K，Q，X出现频率比较低
  - A，I，U很少用在词尾，E、N、R常出现在词尾。E、S、D作为字母结尾字母的单词超过一半，T、A、S、W为起始字母的单词约占一半。

唯密文攻击



A	8.19%	B	1.47%
C	3.83%	D	3.91%
E	12.25%	F	2.26%
G	1.71%	H	4.57%
I	7.10%	J	0.14%
K	0.41%	L	3.77%
M	3.34%	N	7.06%
O	7.26%	P	2.89%
Q	0.09%	R	6.85%
S	6.36%	T	9.41%
U	2.58%	V	1.09%
W	1.59%	X	0.21%
Y	1.58%	Z	0.08%

古典密码的唯密文攻击

- 对于双字母、三字母组合

Double letter	Triple letter
TH	THE
HE	AND
IN	TIO
ER	ATI
RE	FOR
ON	THA
AN	TER
EN	RES

唯密文攻击

- 统计攻击（频率攻击）过程
  - 假设：根据分析假设某些结论
  - 推断：在假设的前提下，推断某些结论
    - 双频、字幕跟随关系、构词规则、词义
  - 验证发展：填上破译出的字母，根据词义、构词规则不断发展
- 单字母代替密码由于带有原始字母使用频率的统计学特征因此容易被攻破

唯密文攻击

- 仿射密码等单表代换密码都没有破坏明文的频率统计规律，可以直接用统计分析法
- 举例：已知用户用移位密码加密，密文为 “KHOOR, HYHUB RQH”，用统计法求密钥和对应明文
- 分析：H—4; O,R—2;其余字母1个
- 推测：
  - H---e
  - e+x=h，即4+x=7, x=3,密钥为3
  - 解密：hello, every one

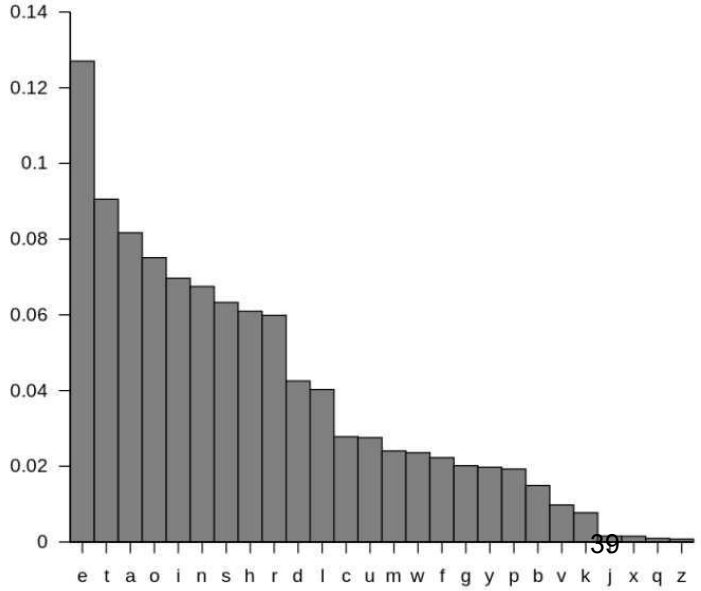
唯密文攻击

- 例题：截取一段仿射密码的密文 c=ap+b mod 26
- 密文

FMXVED KAPHFE RBNDKR XRSREF MOR

UDSDKD VSHVUF EDKAPR KDLYEV LRHHRH

- 统计分析 R(8),D(7), E/H/K(5), S/F/V(4)
- 尝试
  - R=E(e),D=E(t)
  - R=E(e),E=E(t)
  - R=E(e),H=E(t)
  - R=E(e),K=E(t)
  - R=E(t),D=E(a)



唯密文攻击

- R=E(e), D=E(t)

$$\begin{cases} 4a+b=17 \\ 19a+b=3 \end{cases}$$

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

解得 a=6, b=19

由于gcd(6,26)=2>1, 故猜测错误

- R=E(e),E=E(t)　　a=13　X
- R=E(e),H=E(t)　　a=8　　X
- R=E(e),K=E(t)　　a=3,　b=5　　√

则解密函数$p=(c-5)*3^{-1}=9c-19$

明文：alogorithms are quite general definitions of arithmetic processes

其他代换密码

- 单字母代替容易被攻破是由于其带有原始字母使用频率的一些统计学特性
- 改进1：同音词密码—对每个字母提供多种代替（称为同音词）
- 改进2：多字母代换密码—对明文中的多字母一起加密
  - Playfair密码:将明文中的双字母作为一个单元并将其转换为密文的双字母
  - Hill密码:基于矩阵理论，将明文中m个字母一起加密得到m个字母的密文
  - 抗唯密文攻击，但是容易被已知明文攻击破解

其他代换密码

- 改进3：多表代换密码—明文中的字母采用不同的单表代换加密。
  - Vigenere密码:用多个凯撒密码表来代换不同的明文字母
  - 密码周期越长越难破译
- 一次一密
  - 使用与消息一样长、无重复、随机密钥来加密消息，密钥仅使用一次
  - 绝对安全(无条件安全)，理论上不可破，但是实用困难
  - 量子技术可能可以解决这个问题

2.1.5 多字母代换密码--Playfair

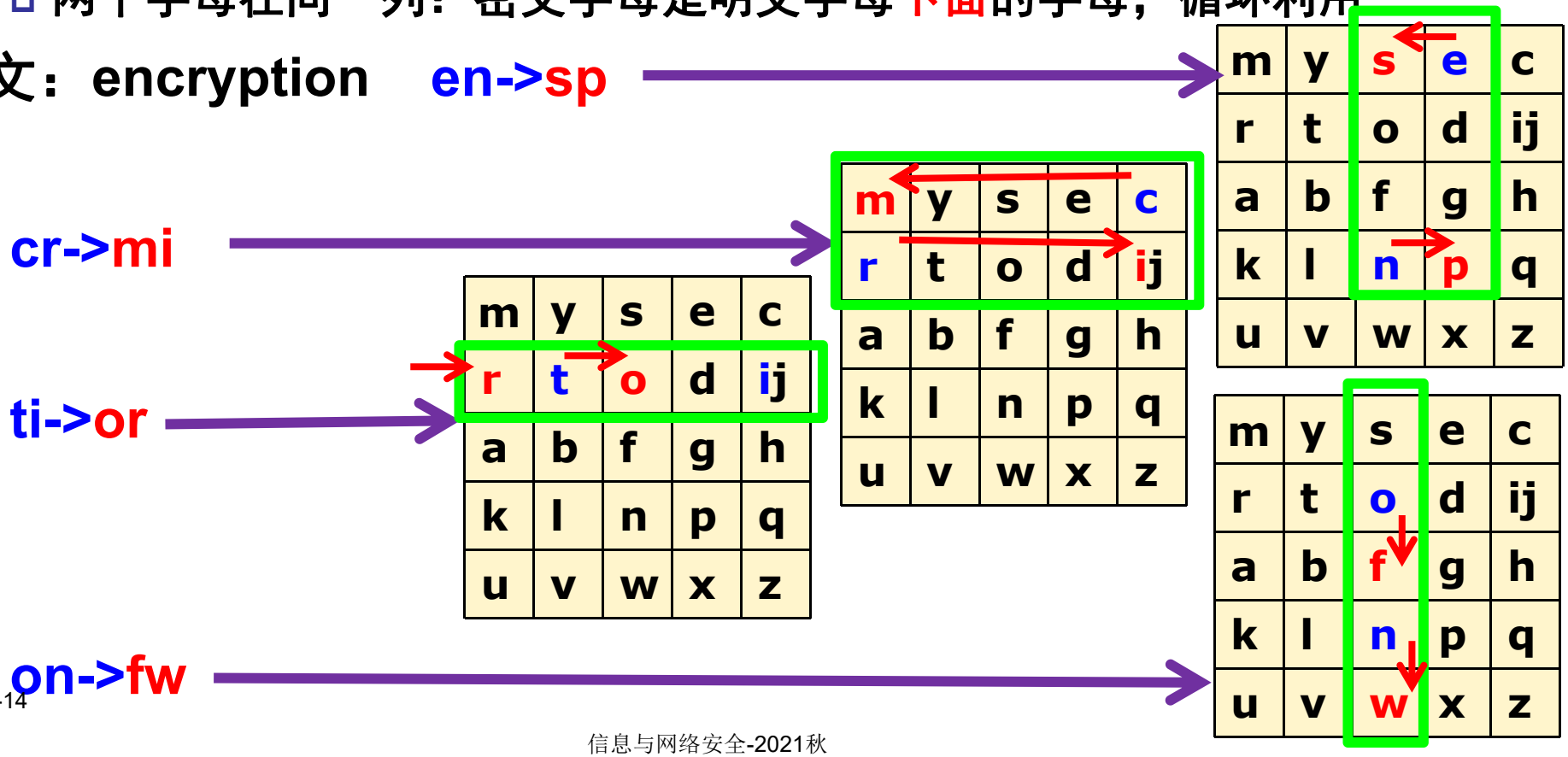
- Playfair密码
  - 最著名的多字母代换密码，一战和二战盟军使用
  - 方法：将明文中的双字母作为一个单元转换为密文中的双字母
  - 操做步骤
    - 选一个密词（去掉其中的重复字母）
    - 构造5*5矩阵密钥表
      - 先填写密词，再填写其余字母
      - 忽略Q或者I和J放在一起

举例：密词 my secret code is -->mysecrtodi

m	y	s	e	c
r	t	o	d	ij
a	b	f	g	h
k	l	n	p	q
u	v	w	x	z

- 加密操作：将明文消息分解为两个字母一个单元，利用密钥表进行代换。代换过程中遵循如下规则
  - 字母所在行为密文所在行，另一个字母所在列为密文所在列
  - 如果两个字母一样，中间插入Q或X
  - 两个字母在同一行：密文字母是明文字母右边的字母，循环利用
  - 两个字母在同一列：密文字母是明文字母下面的字母，循环利用

明文：encryption　en->sp



Playfair

- Playfair密码安全性分析
  - 与单表替换比较，破解难度增加
  - 打破了字母出现的频率统计规律，利用频率分析更困难

2.1.6 多表代换密码--Vigenere密码

- 多表代换密码
- 步骤
  - (1) 用数字表示字母, a=0, b=1, ..., z=25
  - (2) 密钥是一串字母的组合，如 一个有意义的单词或词组
  - (3) 在明文字母下方循环填充密钥字母进行加密。

多表代换密码--Vigenere密码

- 举例：
  - plaintext ： we meet at river
  - Key: stream

Plaintext	w	e	m	e	e	t	a	t	r	i	v	e	r
Key	s	t	r	e	a	m	s	t	r	e	a	m	s
Cipertext	O	X											

作业1：把剩余的密文补全

Vigenere密码

Plaintext	w	e	m	e
Key	s	t	r	e
Cipertext	o	x		

Plaintext

Key

	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

多表代换密码--Vigenere密码

- 安全性：26个字母表
- 是否一定需要查表加密？
- 直接计算
  - 已知：plaintext w=22, key s=18
  - Encryption: (plaintext+key) mod 26
    =(22+18) mod 26
    =14
    =O ciphertext
  - Decryption: ?

多表代换密码--转子(Rotor)加密

- 基本方法：HELLO -> PA???

动作方向

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

多表代换密码--转子(Rotor)加密

- 利用多层加密能够增加密码破译的难度

动作方向

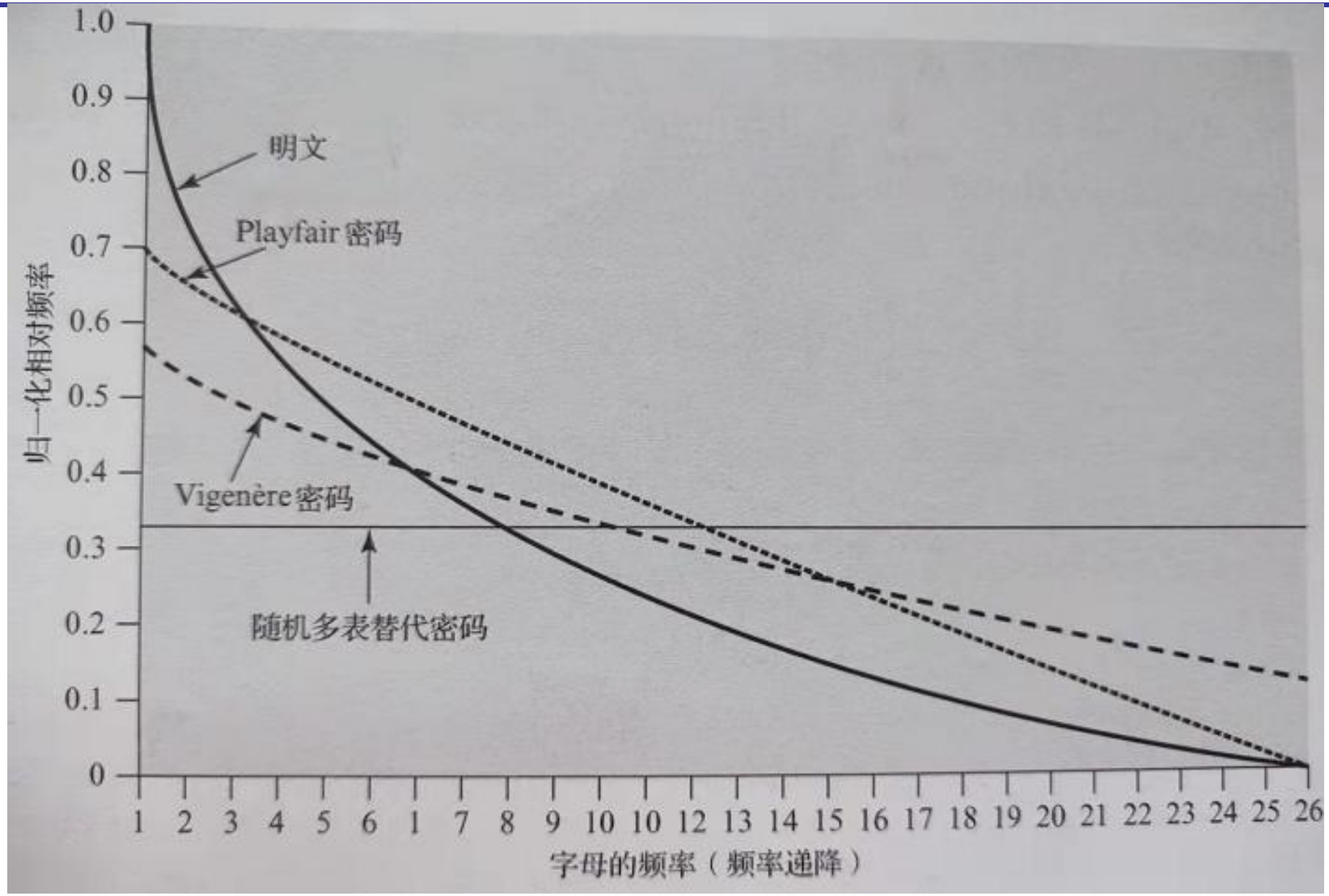
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Fast	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	21	3	15	1	19	10	14	26	20	8	16	7	22	4	11	5	17	9	12	23	18	2	25	6	24	13

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

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

- 3个转子，26^3=11,567个字母表

代换密码的字母频率分布情况



自动加密装置

- **转轮机**：机械转轮用线连接起来实现通常的密码置换
  - 有一个键盘和一系列转轮
  - 每个转轮实现一种简单代换
  - 转轮的输出栓连接到相邻的输入栓
  - 转轮移动后，下一次的代换将变化
- **恩尼格码机Enigma**: 二战德军使用

2.1.7 置换密码

- 数学描述：

$$c=(p_{\Pi(1)},p_{\Pi(2)},\cdots,p_{\Pi(m)}) \bmod 26;$$

$$p=(c_{\Pi^{-1}(1)},c_{\Pi^{-1}(2)},\cdots,c_{\Pi^{-1}(m)}) \bmod 26$$

其中，明文$p\in(Z_{26})^m$，密文$c\in(Z_{26})^m$，

密钥$k\in\{\Pi \mid$定义在0，…，25上的置换$\}$

置换密码

- 例题：密钥

x	1	2	3	4	5	6
∏(x)	3	5	1	6	4	2
x	1	2	3	4	5	6
$\prod^{-1}(x)$	3	6	1	5	2	4

- 明文：she sells sea shells by the sea shore
- 分组：shesel lsseas hellsb ythese ashore
- 置换：EESLSH SALSES LSHBLE HSYEET HRAEOS
- 多次置换：破译难度较大

置换密码

练习题

- 明文：nice work

x	1	2	3	4
∏(x)	2	4	1	3

- 求：密文和逆置换

思考

- 为什么要将密码算法与密钥分开？
  - 希望重复使用已经开发出来的密码算法
  - 重复使用会增加风险
- 保密密码算法更安全吗？
- 对于古典密码算法加密的密文，如何破译（唯密文攻击）？
  - 判断可能使用的加密算法是什么
  - 对于单表代换密码，采用统计分析

滚筒密码

滚筒密码是最古老的一种密码体制

破译以下密文

猜猜看？

信，方成安息息息深式为全安化
技刻，世的全发术地推界研保展
的改动性究障的发变着问和能当
展了社题发力务与人会。展也之
广们文加，是急泛的明速加我。
应生，信强国 用活已息信信

滚筒密码

信，方成安息息
息深式为全安化
技刻，世的全发
术地推界研保展
的改动性究障的
发变着问和能当
展了社题发力务
与人会。展也之
广们文加，是急
泛的明速加我。
应生，信强国
用活已息信信

信，方成安息息息深式为全安化技刻，世的全发术地推界研保展的改动性究障的发变着问和能当展了社题发力务与人会。展也之广们文加，是急泛的明速加我。应生，信强国 用活已息信信

滚筒密码

信，方成安息息
息深式为全安化
技刻，世的全发
术地推界研保展
的改动性究障的
发变着问和能当
展了社题发力务
与人会。展也之
广们文加，是急
泛的明速加我。
应生，信强国
用活已息信信

信息技术的发展与广泛应用，深刻地改变了人们的生活方式，推动着社会文明，已成为世界性问题。加速信息安全的研究和发展，加强信息安全保障能力也是我国信息化发展的当务之急。

关键参数：m(11) ， n(7)