西安郵電大學

XI'AN UNIVERSITY OF POSTS & TELECOMMUNICATIONS

2、单表代换密码

主讲人：任方

网络空间安全学院

移位密码

- 移位密码的加密对象为英文字母，移位密码采用对明文消息的每一个英文字母向前推移固定位的方式实现加密。换句话说，移位密码实现了26个英文字母的循环移位。
- 移位密码中，当取密钥k=3时，就得到凯撒密码。

定义1.2.1　移位密码体制

令 $M = C = K = Z_{26}$ 。对任意的 $key \in Z_{26}$，$x \in M$，$y \in C$，定义

$$e_{key}(x) = (x + key) \bmod 26$$

$$d_{key}(y) = (y - key) \bmod 26$$

移位密码

恺撒密码是移位距离为3的移位密码。

一般的移位密码：移位距离可以是任何数字。比凯撒密码复杂，但是仍可以通过尝试法破解。

思考：有多少种可能？

25种！

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	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

假设明文为：

s e c u r i t y

18 04 02 20 17 08 19 24

$e_{key}(x) = (x + 7) \bmod 26$

25 11 09 01 24 15 02 05

z l j b y p c f

$d_{key}(y) = (y - 7) \bmod 26$

18 04 02 20 17 08 19 24

s e c u r i t y

加密

解密

移位密码的密钥空间大小为**26**，其中有一个弱密钥，即**key=0**。

仿射密码

- 仿射密码是移位密码的一个推广，其加密过程中不仅包含移位操作，而且使用了乘法运算。

定义 仿射密码的密码体制

令 $M = C = Z_{26}$ 密钥空间为 $K = \{(k_1, k_2) \in Z_{26} \times Z_{26} : \gcd(k_1, 26) = 1\}$

对任意密钥 $key = (k_1, k_2) \in K$ $x \in M$ $y \in C$

定义：$e_{key}(x) = (k_1 x + k_2) \bmod 26$

$d_{key}(y) = k_1^{-1}(y - k_2) \bmod 26$

假设：明文字符对应的整数为13

仿射密码的密钥为 key=(11, 3)

加密

$$e_{key}(x) = (k_1 x + k_2) \bmod 26$$

$$y = (11 \times 13 + 3) \bmod 26 = 16$$

密文为：16

$$11^{-1} \bmod 26 = 19$$

解密

$$d_{key}(y) = k_1^{-1}(y - k_2) \bmod 26$$

$$x = 19 \times (16 - 3) \bmod 26 = 13$$

在 Z_{26} 中，满足条件：$\gcd(k_1,26)=1$ 的 k_1 只有 12 个不同的值（它们分别是：1,3,5,7,9,11,15,17,19,21,23,25），因此仿射密码的密钥空间大小为 $12\times 26=312$，其中有 12 个弱密钥，即 k_1 取与 26 互素的 12 个数中的一个并且 $k_2=0$。由于仿射密码的密钥空间不大，使用穷举搜索的方式即可破解。

代换密码

定义 代换密码体制：

令 $M=C=Z_{26}$，K 是 Z_{26} 上所有可能置换构成的集合。对任意的置换 $\pi \in K$ $x \in M$ $y \in C$ 定义：

$$e_\pi(x)=\pi(x)$$

$$d_\pi(y)=\pi^{-1}(y)$$

这里 π 和 π^{-1}互为逆置换。

A	B	C	D	E	F	G	H	I	J	K	L	M
q	w	e	r	t	y	u	i	o	p	a	s	d
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
f	g	h	j	k	l	z	x	c	v	b	n	m

假设明文为：security

加密：

itexkozn

解密：

security

例如:古埃及法老坟墓上的文字

思想:代替(substitution)

古埃及的原始密码（左方是密文，右方是相应的明文）

单表代换密码

代换密码总体来讲比移位密码难破解的多。

所有可能的置换非常之多（26！）

移位密码和这里的代换密码均属于所谓单表代换密码。

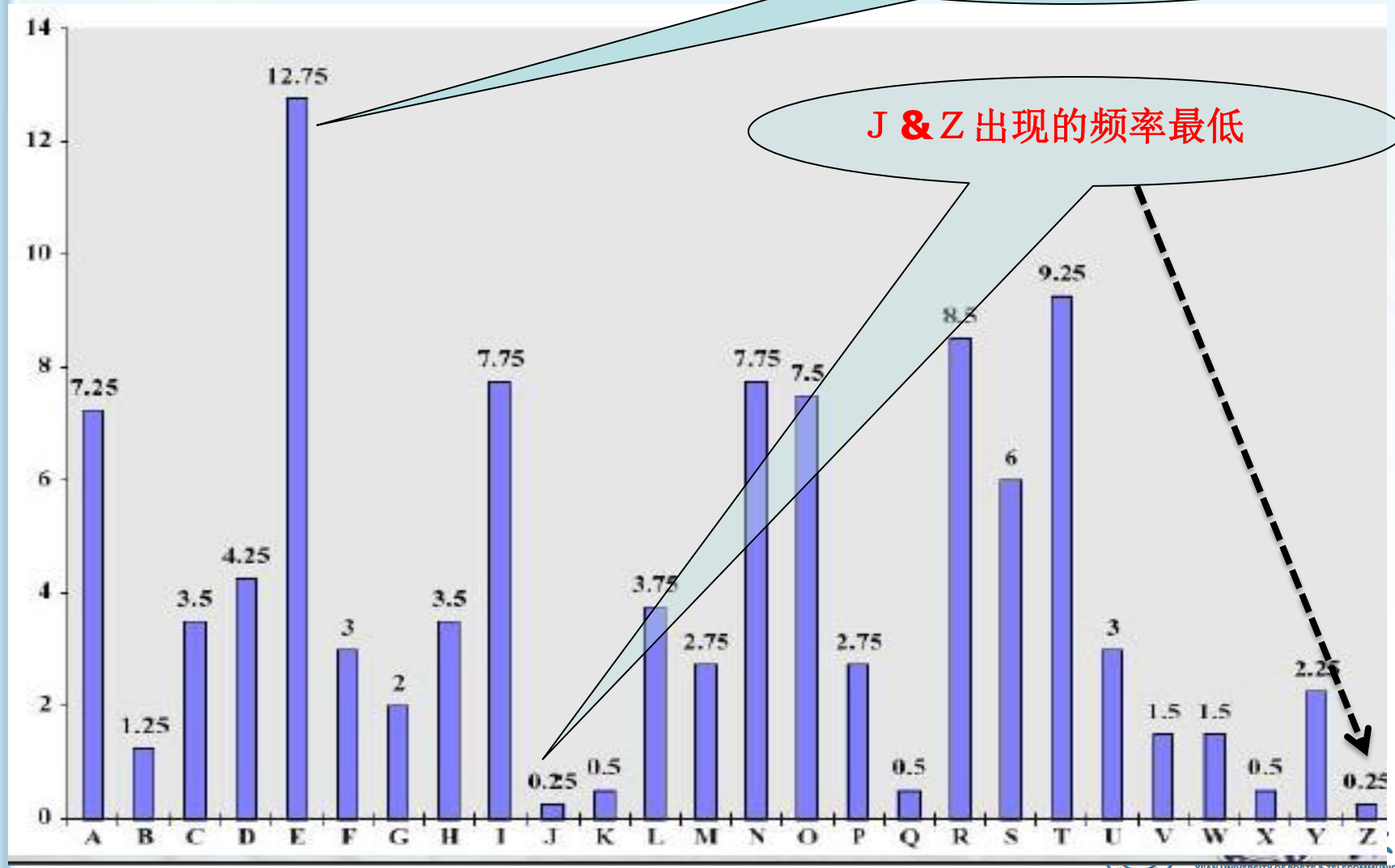
9世纪，阿拉伯的阿尔.金迪提出频度分析的方法来解密，通过分析计算密文字符出现的频率来破译密码。

几乎可以破译所有的单表代换密码！

字母使用的

字母E出现的频率最高

J&Z出现的频率最低



The End !