古典密码学
Classical Cryptography

古典密码学特点

- 密码算法的安全性基于算法的安全性
  - 密码算法本身必须要保密
- 加密算法
  - 字母的代换
  - 顺序的置换

凯撒密码，Caesar’s Cipher

凯撒密码系统：英语的26个字母分别用Z_{26}的元素表示，密钥是3。

$$Enc:\ \forall m \in M, c = (m+3) \bmod 26$$

$$Dec:\ \forall c \in C, m = (c-3) \bmod 26$$

0	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
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

问题：算法和密钥都是确定的。

移位密码，Shift Cipher

移位密码系统：英语的26个字母分别用Z_{26}的元素表示，

$M = C = Z_{26}^{l}$ ， 密钥空间 $K = Z_{26}$

$$Enc: \ \forall m = (m_1, m_2, \ldots, m_l) \in M,$$

$$c = (m_1 + k \bmod 26, m_2 + k \bmod 26, \ldots, m_l + k \bmod 26)$$

$$Dec: \ \forall c = (c_1, c_2, \ldots, c_l) \in C,$$

$$m = (c_1 - k \bmod 26, c_2 - k \bmod 26, \ldots, c_l - k \bmod 26)$$

穷举攻击：例举密钥空间中的25个密钥，解密密文到有意义字符串。

移位密码，Shift Cipher

k=0: OVDTHUFWVZZPISLRLFZHYLAOLYL

k=1: NUCSGTEVUYYOHRKQKEYGXKZNKXK

k=2: MTBRFSDUTXXNGQJPJDXFWJYMJWJ

k=3: LSAQERCTSWWMFPIOICWEVIXLIVI

k=4: KRZPDQBSRVVLEOHNHBVDUHWKHUH

k=5: JQYOCPARQUUKDNGMGAUCTGVJGTG

k=6: IPXNBOZQPTTJCMFLFZTBSFUIFSF

k=7: HOWMANYPOSSIBLEKEYSARETHERE

k=8: GNVLZMXONRRHAKDJDXRZQDSGDQD

k=9: FMUKYLWNMQQGZJCICWQYPCRFCPC

k=10: ELTJXKVMLPPFYIBHBVPXOBQEBOB

k=11: DKSIWJULKOOEXHAGAUOWNAPDANA

k=12: CJRHVITKJNNDWGZFZTNVMZOCZMZ

k=13: BIQGUHSJIMMCVFYEYSMULYNBYLY

k=14: AHPFTGRIHLLBUEXDXRLTKXMAXKX

k=15: ZGOESFQHGKKATDWCWQKSJWLZWJW

k=16: YFNDREPGFJJZSCVBVPJRIVKYVIV

k=17: XEMCQDOFEIIYRBUAUOIQHUJXUHU

k=18: WDLBPCNEDHHXQATZTNHPGTIWTGT

k=19: VCKAOBMDCGGWPZSYSMGOFSHVSFS

k=20: UBJZNALCBFFVOYRXRLFNERGURER

k=21: TAIYMZKBAEEUNXQWQKEMDQFTQDQ

k=22: SZHXLYJAZDDTMWPVPJDLCPESPCP

k=23: RYGWKXIZYCCSLVOUOICKBODROBO

k=24: QXFVJWHYXBBRKUNTNHBJANCQNAN

k=25: PWEUIVGXWAAQJTMSMGAIZMBPMZM

作业

- As on most challenge sites, there are some beginner cryptos, and often you get started with the good old caesar cipher. I welcome you to the WeChall style of these training challenges :)
  Enjoy!

- ESP BFTNV MCZHY QZI UFXAD ZGPC ESP WLKJ OZR ZQ NLPDLC LYO JZFC FYTBFP DZWFETZY TD TNSONDLMLOOL

单字母替换， Mono-alphabetic substitution

密码替换：英语的26个字母Z_{26}分别用的元素表示，

$M = C = Z_{26}^{l}$ ， 密钥空间是字母上的所有置换π 。

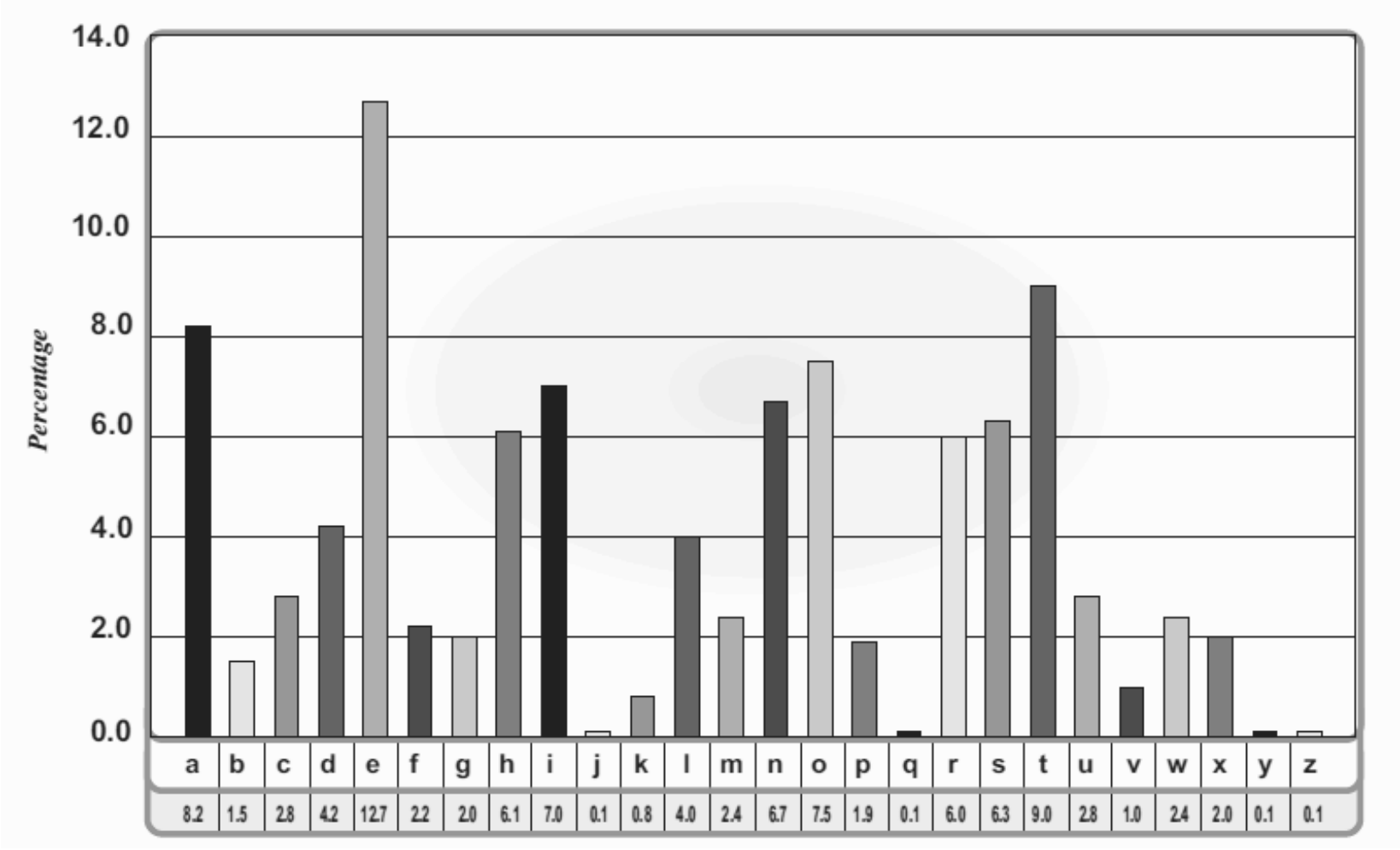
$$Enc: \forall m = (m_1, m_2, ..., m_l) \in M,\ c = (\pi(m_1), \pi(m_2), ..., \pi(m_l))$$

$$Dec: \forall c = (c_1, c_2, ..., c_l) \in M,\ m = (\pi^{-1}(c_1), \pi^{-1}(c_2), ..., \pi^{-1}(c_l))$$

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

密钥空间为：26！-1，约等于2^{88}

单字母替换，Mono-alphabetic substitution



单字母替换，Mono-alphabetic substitution

E的概率大约为0.12

T, A, O, I, N, S, H, R的概率为0.06-0.09

D, L的概率大约为0.04

C, U, M, W, F, G, Y, P, B的概率为0.015-0.023

V, K, J, X, Q, Z的概率小于0.01

常见的两字母组合

TH, HE, IN, ER, AN, RE, DE, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF

常见的三字母组合

THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

维吉尼亚密码，Vigener

维吉尼亚密码：英语的26个字母 Z_{26} 分别用的元素表示，

$M = C = K = Z_{26}^{l}$ 。

$$Enc: \forall m = (m_1, m_2, ..., m_l) \in M, \forall k = (k_1, k_2, ..., k_l) \in K$$

$$c = ((m_1 + k_1 \bmod 26), (m_2 + k_2 \bmod 26), ..., (m_l + k_l \bmod 26))$$

$$Dec: \forall c = (c_1, c_2, ..., c_l) \in M, \forall k = (k_1, k_2, ..., k_l) \in K$$

$$m = ((c_1 - k_1 \bmod 26), (c_2 - k_2 \bmod 26), ..., (c_l - k_l \bmod 26))$$

Plaintext:	the man and the woman retrieved the letter from the post office
Key:	bea dsb ead sbe adsbe adsbeadsb ean sdeads bead sbe adsb eadbea
Ciphertext:	VMF QTP FOH MJJ XSFCS SIMTNFZXF YIS EIYUIK HWPQ MJJ QSLV TGJKGF

维吉尼亚密码，Vigener

例 1.4 假设 $m=6$，密钥字为“CIPHER”，其对应于如下的数字串 $K=(2,8,15,7,4,17)$。要加密的明文为：

thiscryptosystemisnotsecure

将明文串转化为对应的数字，每 6 个为一组，使用密钥字进行模 26 下的加密运算，如下所示：

19	7	8	18	2	17	24	15	19	14	18	24	18	19
2	8	15	7	4	17	2	8	15	7	4	17	2	8
21	15	23	25	6	8	0	23	8	21	22	15	20	1

4	12	8	18	13	14	19	18	4	2	20	17	4
15	7	4	17	2	8	15	7	4	17	2	8	15
19	19	12	9	15	22	8	25	8	19	22	25	19

则相应的密文应该为：

VPXZGIAXIVWPUBTTMJPWIZITWZT

解密时，使用相同的密钥字，进行逆运算即可，这里不再给出。

维吉尼亚密码，Vigener

密钥空间大小为26^m，如当*m*=5时，密钥空间所含密钥的数量是>1.1×10^7。

在一个密钥长度为m的维吉尼亚密码中，一个字母可以被映射为m个字母中的某一个（假定密钥字包含m个不同的字母）

这样的一个密码体制称为多表代换密码体制。

维吉尼亚密码，Vigener

确定长度：

1）Kasiski测试法

- 两个相同的明文段加密成相同的密文段，则这两个明文段之间的间距很大的概率是密钥长度的整数倍。
- 搜索长度至少为3的相同密文段，记下离起始点的那个明文段的距离，假如得到的距离分别是d1,d2,…, 则可以猜测长度m为d1,d2,…最大公因子的因子。

Plaintext:	the	man	and	the	woman	retrieved	the	letter	from	the	post	office		
Key:	bea	dsb	ead	sbe	adsbe	adsbeadsb	ean	sdeads	bead	sbe	adsb	eadbea		
Ciphertext:	VMF	QTP	FOH	MJJ	XSFCS	SIMTNFZXF	YIS	EIYUIK	HWPQ	MJJ	QSLV	TGJKGF		

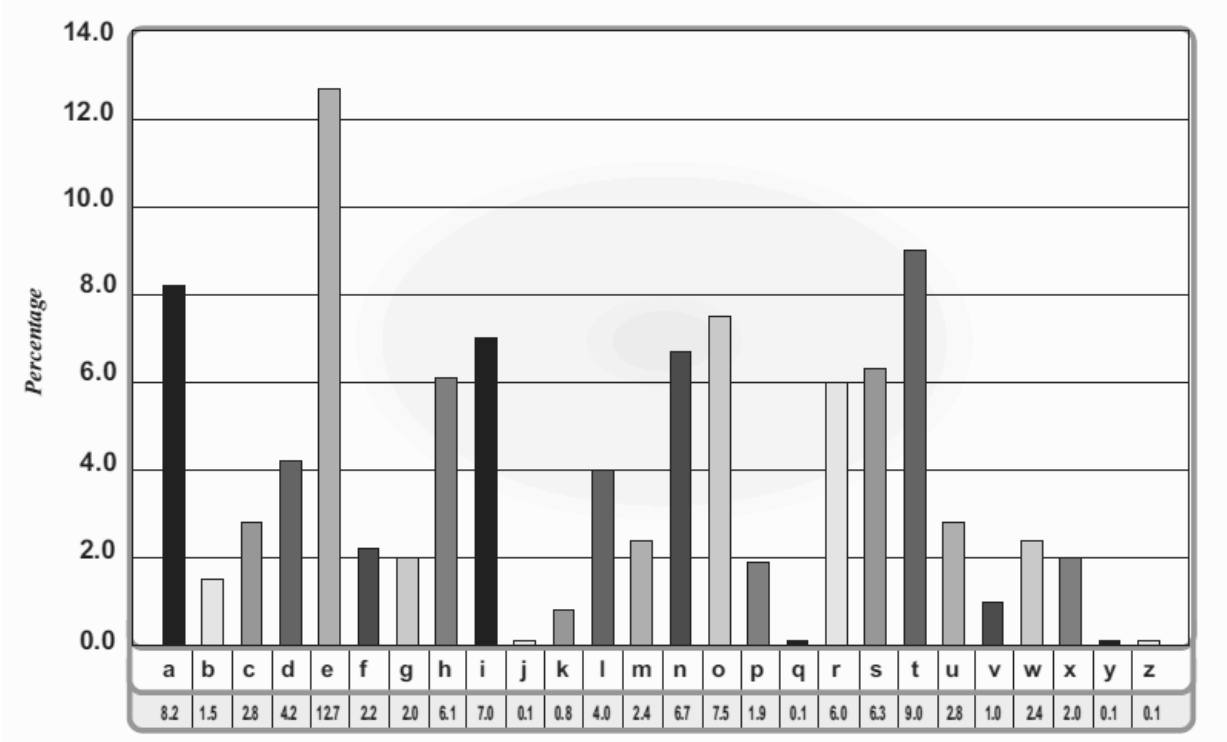
维吉尼亚密码，Vigener

2）重合指数法

设x为英文串，$p_0, p_1 \ldots p_{25}$是$A, B, \ldots, Z$出现的期望概率，则

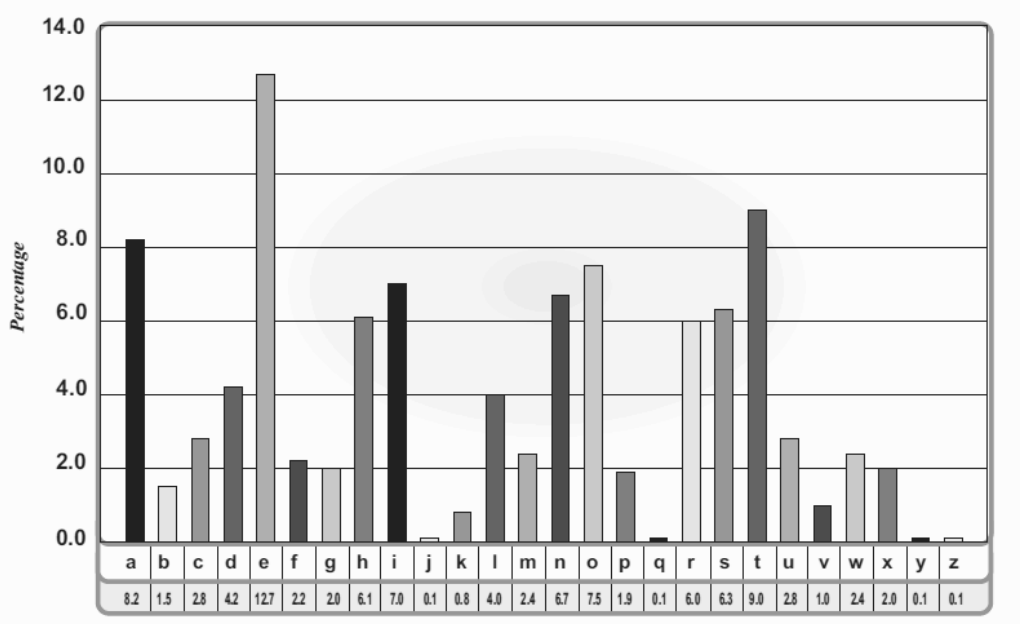
$$I_c(\mathrm{x}) \approx \sum_{i=0}^{i=25} p_i^2 = 0.065$$

$$I_c \approx 26(\frac{1}{26})^2 = 0.038$$



维吉尼亚密码，Vigener

2）重合指数法



8.2	67.24
1.5	2.25
2.8	7.84
4.2	17.64
12.7	161.29
2.2	4.84
2	4
6.1	37.21
7	49
0.1	0.01
0.8	0.64
4	16
2.4	5.76
6.7	44.89
7.5	56.25
1.9	3.61

0.1	0.01
6	36
6.3	39.69
9	81
2.8	7.84
1	1
2.4	5.76
2	4
0.1	0.01
0.1	0.01
99.9	0.065508

维吉尼亚密码，Vigener

例子，密文如下

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE

CHR共出现5次，其距离分别为165,235,275和285，可以猜测长度为5。

当长度为5时，5个子串的重合指数分别为0.063,0.068,0.069, 0.061,0.072。

维吉尼亚密码，Vigener

维吉尼亚密码采用分治法，被分成了若干个移位密码

如长度猜对，密文字母概率平方和等于明文字母概率平方和

设x为英文串，$p_0, p_1 \ldots p_{25}$是$A, B, \ldots, Z$出现的期望概率，则

$$I_c(\mathrm{x}) \approx \sum_{i=0}^{i=25} p_i^2 = 0.065$$

如长度猜错，统计密文字母出现的概率平方和的期望如下：

$$I_c \approx 26(\frac{1}{26})^2 = 0.038$$

维吉尼亚密码，Vigener

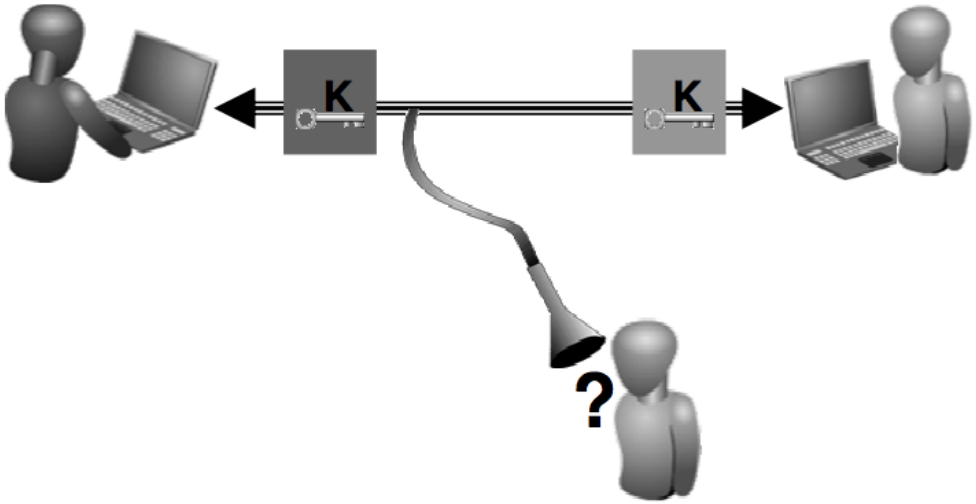
i	value of $M_g(\mathbf{y}_i)$								
1	.035	.031	.036	.037	.035	.039	.028	.028	.048
	.061	.039	.032	.040	.038	.038	.045	.036	.030
	.042	.043	.036	.033	.049	.043	.042	.036	
2	.069	.044	.032	.035	.044	.034	.036	.033	.029
	.031	.042	.045	.040	.045	.046	.042	.037	.032
	.034	.037	.032	.034	.043	.032	.026	.047	
3	.048	.029	.042	.043	.044	.034	.038	.035	.032
	.049	.035	.031	.035	.066	.035	.038	.036	.045
	.027	.035	.034	.034	.036	.035	.046	.040	
4	.045	.032	.033	.038	.060	.034	.034	.034	.050
	.033	.033	.043	.040	.033	.029	.036	.040	.044
	.037	.050	.034	.034	.039	.044	.038	.035	
5	.034	.031	.035	.044	.047	.037	.043	.038	.042
	.037	.033	.032	.036	.037	.036	.045	.032	.029
	.044	.072	.037	.027	.031	.048	.036	.037	

现代密码学特点

- 方案公开
  - 社会工程学
  - 逆向工程
  - 等等

The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

敌手模型



加密算法

- 四种常见的攻击场景
  - 唯密文攻击
  - 已知明文攻击
  - 选择明文攻击
  - 选择密文攻击

- 敌手能力由弱到强
- 设计安全的密码算法难度由易到难

现代密码学

- 1. 有严格而明确的安全定义
- 2. 算法安全性依靠尽可能少的数学假设
- 3. 附有严格的安全性证明