Classical Ciphers (CS-452)

Week 2

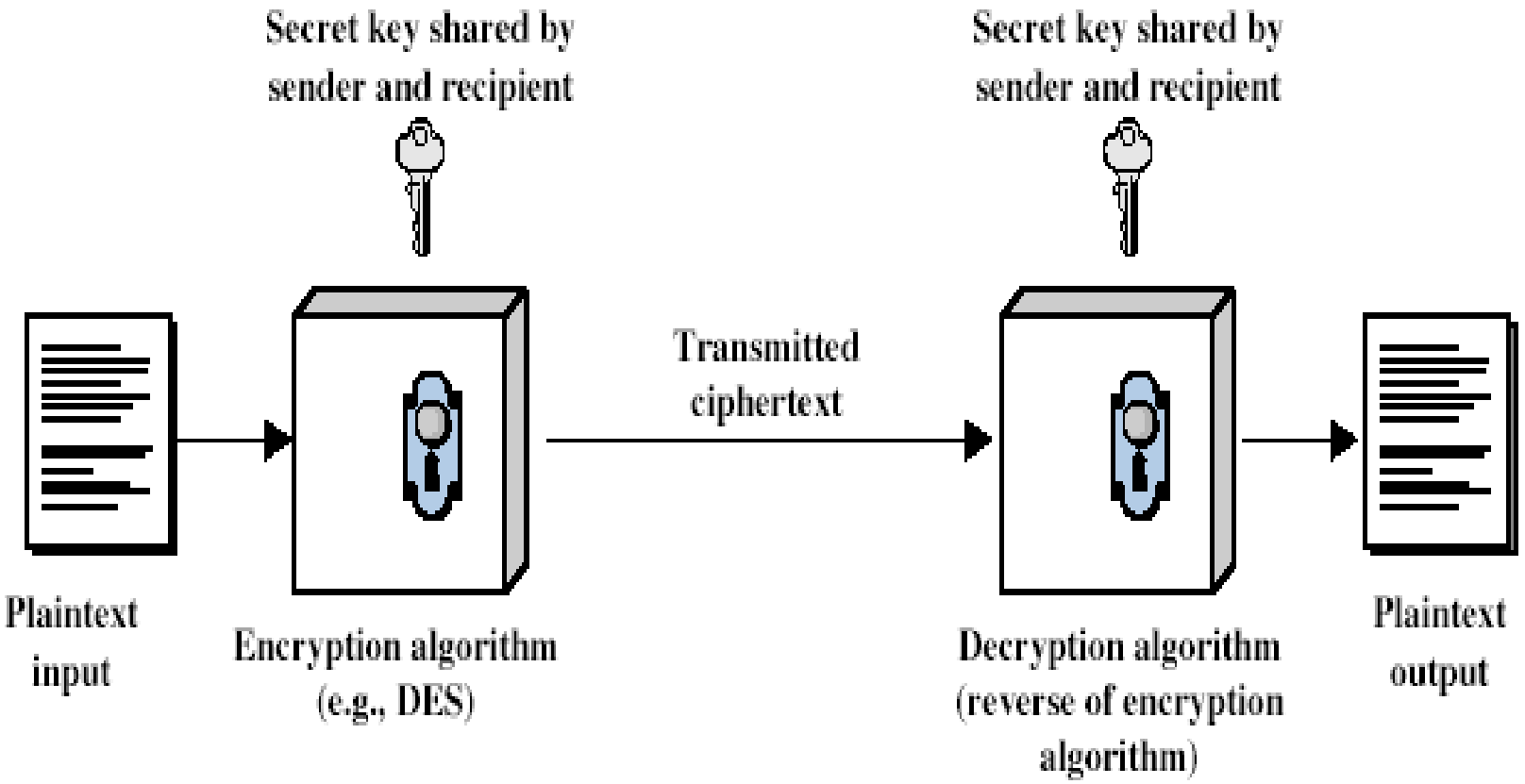
Cryptology Fundamentals and Classical Ciphers

Symmetric Encryption

- A form of cryptosystem in which encryption and decryption are performed using the same key – single-key encryption
- Was only type prior to invention of public-key in 1970's, and by far most widely used

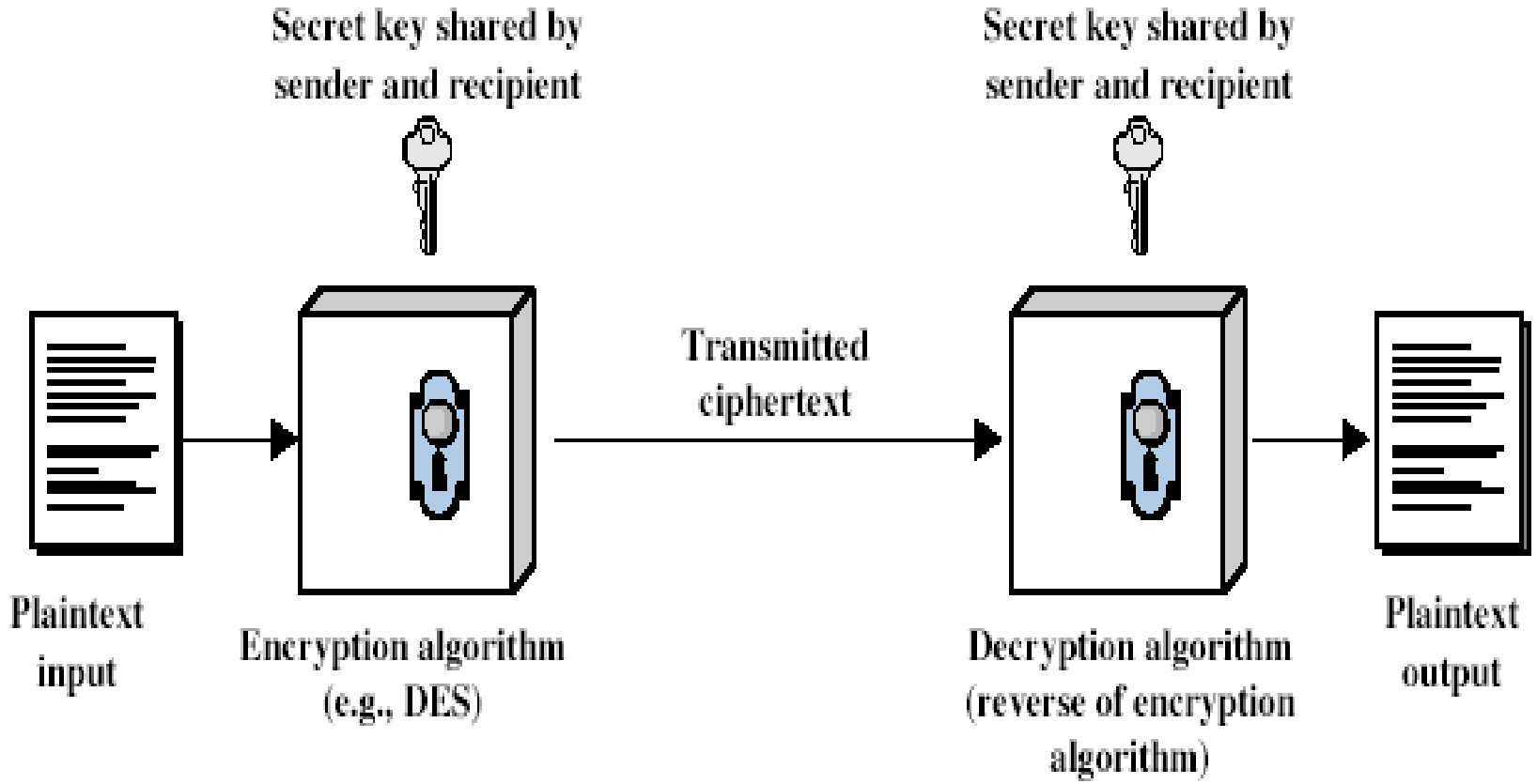
Symmetric Cipher Model

- Encryption algorithm: performs various substitutions and transformation on the plaintext.
- Secret key: the input of encryption algorithm. The key is independent of the plaintext and the alg..



Symmetric Cipher Model

- Decryption algorithm: the ciphertext and the secret key and produces the original plaintext



Requirements

- Two requirements for secure use of symmetric encryption:
  - A strong encryption algorithm: the opponent should be unable to decrypt ciphertext or discover the key even if he/she has a number of ciphertexts and the plaintext that produced each ciphertext
  - Assume encryption algorithm is known
  - Mathematically have:

X: message, K: encryption key, Y: ciphertext

$$Y = E(K,X)$$

$$X = D(K,Y)$$

An opponent can observe Y, but do not have access to K or X.

Brute Force Search

- Simply try every key until an intelligible translation of the ciphertext into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success - proportional to key size
- DES: 56-bit, triple DES: 168-bit, AES: > 128 bits
- Time required for various key spaces:

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs= 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs= 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs= 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs= 5.9×10^{36} years	5.9×10^{30} years

Brute Force Search

- Simply try every key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success - proportional to key size
- DES: 56-bit, triple DES: 168-bit, AES: > 128 bits
- Time required for various key spaces:

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs= 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs= 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs= 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs= 5.9×10^{36} years	5.9×10^{30} years

Types of Symmetric Ciphers

- Symmetric ciphers are characterized by the techniques they use to transform plaintext to ciphertext:
  - Substitution Ciphers: replace the elements of the plaintext with new elements
  - Transposition Ciphers: Rearrange the elements of the plaintext
  - Product Ciphers: do both (a bridge from classical to modern symmetric ciphers)
- Next, we will study the fundamental techniques of symmetric encryption by looking at some classical ciphers

Substitution Ciphers

Classical Substitution Ciphers

- Letters of plaintext are replaced by other letters or by numbers or symbols

Caesar Cipher

- The earliest known substitution cipher (by Julius Caesar)
- First attested use in military affairs
- Replaces each letter with the letter standing K places further down the alphabet
- When $K = 3$, can define transformation as:

```
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
```

- Example:

```
Plaintext:  meet me after the toga party
```

Caesar Cipher

- The earliest known substitution cipher (by Julius Caesar)
- First attested use in military affairs
- Replaces each letter with the letter standing K places further down the alphabet
- When $K = 3$, can define transformation as:

```
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
```

- Example:

```
Plaintext:  meet me after the toga party
Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

- Mathematically give each letter a number

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

- Then have Caesar cipher as:
  - Plaintext: pt, ciphertext: ct

Encryption: $ct = E(pt) = (pt + k) \bmod 26$

Decryption: $pt = D(ct) = (26 + (ct - k)) \bmod 26$

Cryptanalysis of Caesar Cipher

Cryptanalysis of Caesar Cipher

- A brute force search can be easily performed: simply try all the 25 possible keys - far from security
  - The language of the plaintext is known and easily recognizable
- The input may be compressed, make recognition difficult, e.g., E.g. .zip file

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

Monoalphabetic Cipher

- Allow an arbitrary substitution rather than just shifting the alphabet
- Each plaintext letter maps to a random ciphertext letter

```
Plain: abcdefghIjklmnopqrstuvwxyz
Cipher:DKVQFIBJWPESCXHTMYAUOLRGZN
```

E.g.,

```
If we wish to replace letters
```

Monoalphabetic Cipher

- Allow an arbitrary substitution rather than just shifting the alphabet
- Each plaintext letter maps to a random ciphertext letter

```
Plain: abcdefghIjklmnopqrstuvwxyz
Cipher:DKVQFIBJWPESCXHTMYAUOLRGZN
```

E.g.

```
If we wish to replace letters
WI RF RWAJ UH YFTSDVF SFUUFYA
```

Monoalphabetic Cipher Security

- The cipher line can be any permutation of the 26 alphabetic characters
  - $26! = 4*10^{26}$ mappings
- With so many mappings, might think is secure

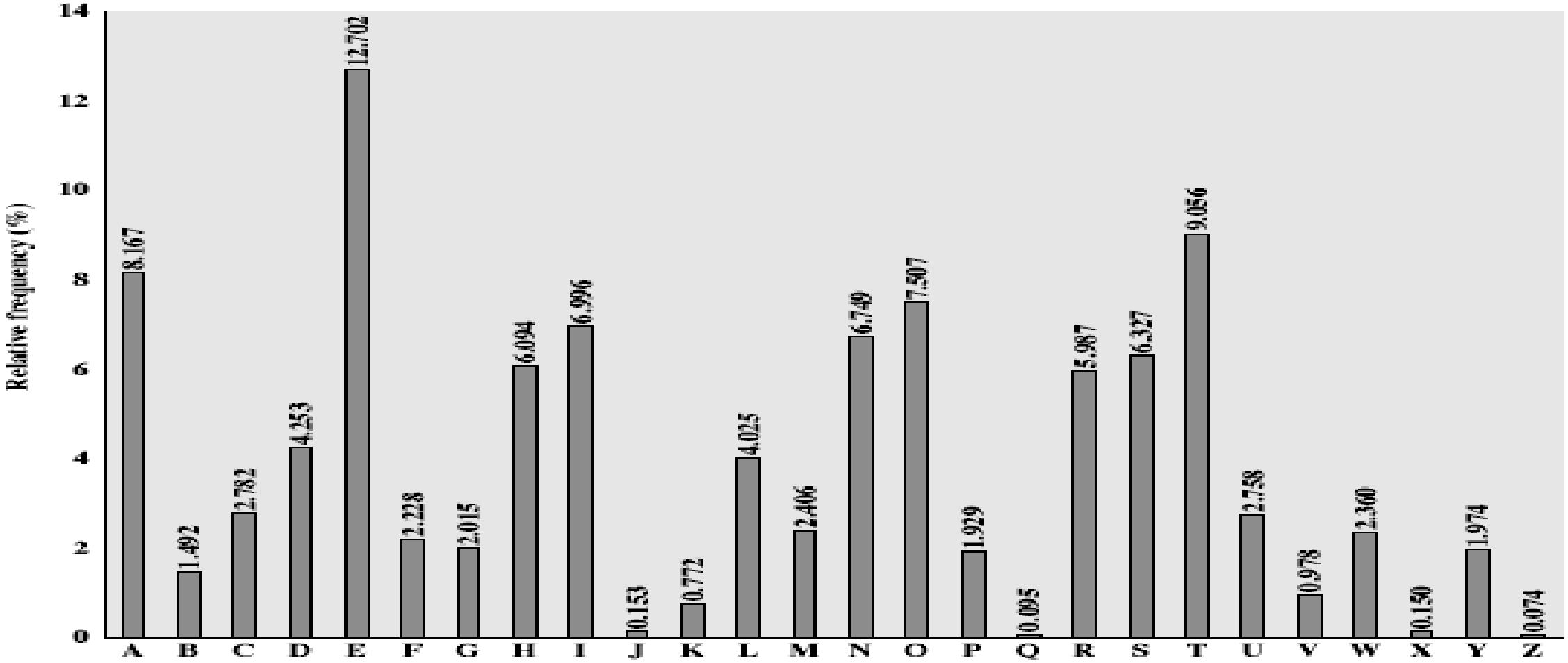
Monoalphabetic Cipher Security

- The cipher line can be any permutation of the 26 alphabetic characters
  - $26! = 4*10^{26}$ keys
- With so many keys, might think is secure
- But would be WRONG – if the cryptanalyst knows the nature of the plaintext (e.g., noncompressed English text), then the analyst can exploit the regularities (frequency of letters) of the language

Language Redundancy and Cryptanalysis

- Human languages are redundant. Letters are not equally commonly used
- In English E is by far the most common letter, followed by T,A,O,I,N,S,R, other letters like Z,J,K,Q,X are fairly rare
  - If the message is long enough, this technique alone may be sufficient

English Letter Frequencies



Use in Cryptanalysis

- Main concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- Calculate letter frequencies for ciphertext
- Compare counts/plots against known values

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQ
  UZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQ UZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔ e

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQ UZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔ e, Z ➔ t

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQ UZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQ
  UZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}
- Most common pair: ZW ➔ and hence ZWP ➔ , ZWSZ ➔

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQU ZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}
- Most common pair: ZW ➔ th and hence ZWP ➔ , ZWSZ ➔

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVP QUZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}
- Most common pair: ZW ➔ th and hence ZWP ➔the, ZWSZ ➔

Example

- UZQSOVUOHXMOPVGPOZPEVAGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTS VPQUZWYMXUZUHSXEPYEPOPDZSUFPOMBZWPFUPZHMDJUDTMOGMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	Tt 2.50	J 0.83	N 0.00
O 7.50	X 4.17	A 1.67	I 0.83	R 0.00
M 6.67				

- P ➔e, Z ➔ t, {S,U,O,M,H} ➔ {a,h,i,n,o,r,s}
- Most common pair: ZW ➔ th and hence ZWP ➔the, ZWSZ ➔ that
- Finally: it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the Viet Cong in Moscow

Playfair Cipher

- Not even the large number of mappings ($4*10^{26}$ mappings) in a monoalphabetic cipher provides security
- One approach to improving security is to encrypt multiple letters – e.g., Playfair Cipher

Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword
- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom
- Fill rest of matrix with other letters
- Eg. using the keyword MONARCHY
- I and j count as one lette

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

Playfair Cipher: Encryption

- Plaintext is encrypted two letters at a time
  - If a pair is a repeated letter, insert filler x, e.g., bolloon ➔ bo lx lo on
  - If both letters fall in the same row, replace each with letter to right with the first element of the row circularly following the last, e.g. ar ➔ rm
  - If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), e.g. mu ➔ cm

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

Playfair Cipher: Encryption

- Plaintext is encrypted two letters at a time
  - Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair, e.g., hs → bp, ea → im (or jm)

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

Playfair Cipher: Encryption

- Plaintext is encrypted two letters at a time
  - Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair, e.g. hs ➔ bp, ea → im (or jm)

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

Playfair Cipher: Decryption

- To decrypt, use the inverse of the encryption rules and drop any extra x that does not make sense in the final message.
  - Decrypts two letters at a time
  - If both letters fall in the same row, replace each with letter to left, e.g., rm ➔ ar
  - If both letters fall in the same column, replace each with the letter above it, e.g., cm ➔ mu

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

Playfair Cipher: Decryption

- Plaintext is encrypted two letters at a time
  - Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair
  - E.g. bp ➔ hs, im → ea

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

Security of Playfair Cipher

- Security much improved over monoalphabetic
- Would need a 676 (26*26) entry frequency table to analyse (verses 26 for a monoalphabetic)
- Was widely used for many years
  - eg. by US & British military in WW1
- It is relatively easy to break because it still leaves much of the structure of the plaintext language intact

Polyalphabetic Ciphers

- Improve security using multiple monoalphabetic substitutions
- Features
  - A set of related monoalphabetic substitution rules is used
  - A key determines which particular rule is chosen for a given transformation
- Vigenère Cipher: Simplest polyalphabetic substitution cipher

Modern Vigenère Tableau

		Plaintext																								
		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**
Key	*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

The set of related monoalphabetic substitution rules consists of 26 Caesar ciphers

		Plaintext																								
		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
Key	*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

- Each Ceasar cipher is denoted by a key letter
- A normal alphabet for the plaintext runs across the top

		Plaintext																								
		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
Key	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

Given a key letter x and a plaintext letter y, the ciphertext letter is at the intersection of row labeled x and the column labeled y ➔ the ciphertext is v

Key \ Plaintext	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

- Write the plaintext out, write the keyword repeated above it
- E.g., using keyword *deceptive*

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
```

Key	Plaintext																								
	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

- Write the plaintext out, write the keyword repeated above it
- Eg using keyword *deceptive*

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Vigenère Cipher: Decryption

Vigenère Cipher: Decryption

- Decryption:
  - The key letter identifies the row
  - The position of the ciphertext letter in that row determines the column
  - The plaintext letter is at the top of that column

Cryptoanalysis of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter. Hence letter frequencies are obscured
- But not totally lost
- Suppose that the opponent believes that the ciphertext was encrypted using Vigenère Ciphers
  - If two identical sequences of plaintext occur at a distance that is an integer * length of keyword, they will generate identical ciphertext sequences.

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Security of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter. Hence letter frequencies are obscured
- But not totally lost
- Suppose that the opponent believes that the ciphertext was encrypted using Vigenère Ciphers
  - If two identical sequences of plaintext occur at a distance that is an integer * length of keyword, they will generate identical ciphertext sequences.

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Cryptoanalysis of Vigenère Ciphers

- How can we make the Vigenère cipher a bit more resilient to cryptoanalysis?

- Vigenère with Autokey! (next slide)

Autokey Cipher: Encryption

- Ideally want a key as long as the message
- Vigenère proposed the autokey cipher
- A keyword is concatenated with the plaintext itself providing a running key
- E.g., given key deceptive

```
key:        deceptivewearediscoveredsav
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
```

How to decrypt a ciphertext?

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:        deceptive
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext:
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:        deceptive
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: w
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:        deceptivew
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: w
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:        deceptivew
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: we
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:        deceptivewe
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: we
```

Autokey Cipher: Decryption

- E.g., given
  - key deceptive
  - Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

```
key:        deceptivewearediscoveredsav
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
plaintext: wearediscoveredsaveyourself
```

Transposition Ciphers

- Consider classical transposition or permutation ciphers
- Hide the message by rearranging the letter order without altering the actual letters used

Transposition Ciphers

- Consider classical transposition or permutation ciphers
- Hide the message by rearranging the letter order without altering the actual letters used
- Can recognize these since have the same frequency distribution as the original text

Rail Fence cipher

- Write message letters out diagonally over a number of rows
- Then read the letters row by row
- E.g., Encrypt the message "meet me after the toga party" with a rail fence of depth 2

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

  - Ciphertext: **MEMATRHTGPRYETEFETEOAAT**

- Think: how to encrypt the above message using rail fence cipher of depth 3?

Rail Fence cipher

- Write message letters out diagonally over a number of rows
- Then read the letters row by row
- E.g., Encrypt the message "meet me after the toga party" with a rail fence of depth 3

```
m   t   a   e   h   o   p   t
 e   m   f   r   e   g   a   y
   e   e   t   t   t   a   r
```

  - Ciphertext: **MTAEHOPTEMFREGAYEETTTAR**
  - Think: how to decrypt a ciphertext

ciphertext: CPEERYOURCIMTSUT

Rail Fence cipher: Decryption

- How to decrypt a ciphertext
  - Let |**row**| be the number of rows
  - Compute the length of the ciphertext |**cipher**|
  - Compute the number of letters of each row
  - Write down the ciphertext row by row
  - Read the ciphertext diagonally

Rail Fence cipher: Decryption

- Example:

  ciphertext: **CPEERYOURCIMTSUT**

  |row| = 3

  ❖ **|cipher| = 16**

  ❖ **16/3= 5, 16 mod 3 = 1 ➔**

  1st row: 5+1 = 6 letters

  2nd row: 5 letters, 3rd row: 5 letters

  C P E E R Y

  O U R C I

  M T S U T

  ➔ Plaintext: **computersecurity**

Rail Fence cipher: Decryption

- Example:

  ciphertext: **CPEERYOURCIMTSUT**

  |row| = 3

  - **|cipher| = 16**
  - **16/3= 5, 16 mod 3 = 1 ➔**

    1st row: 5+1 = 6 letters

    2nd row: 5 letters, 3rd row: 5 letters

    C P E E R Y

    O U R C I

    M T S U T

  ➔ Plaintext: **computersecurity**

Steganography

- Cryptography: make the message unintelligible.
- Steganography: Conceal the existence of the message.
- Example:

"Dear George;

Greetings to all at Oxford. Many thanks for your letter and for the summer examination package. All Entry Forms and Fees Forms should be ready for final dispatch to the Syndicate by Friday 20th or at the very latest, I'm told by the 21st. Admin has improved here, thought there's room for improvement still, just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos."

Steganography

Example:

"PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY. "

Steganography

Example:

"PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY. "

PERSHING SAILS FROM NY JUNE I

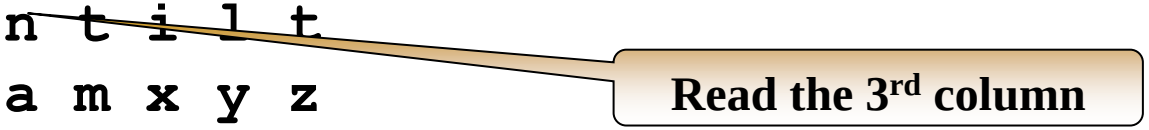
Steganography

- Modern Examples:
  - Encoding hidden message in the pixels of the image
  - Encoding hidden messages in the bits of sound files
- Advantage: useful to parties who are more concerned with hiding the fact of their secret communication, rather than the contents of messages
- Drawbacks:
  - Significant overhead to hide a small amount of information
  - Once the scheme is known, the system is useless

Row Transposition Ciphers

- A more complex transposition
- Write letters of message out in rows over a specified number of columns
- Then reorder the columns according to some key before reading off the columns

```
Key:        3 4 2 1 5 6 7
Plaintext:  a t t a c k p
            o s t p o n e
            d u n t i l t
            w o a m x y z
```




```
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- Think: how to decrypt a ciphertext?
  ciphertext: ATHNIERIPTSISORPNSOCX

Row Transposition Ciphers: Decryption

- How to decrypt a ciphertext?

  ciphertext: ATHNIERIPTSISORPNSOCX

  - |cipher| = 21, |key| = 7 ➔ |row| = 3

```
Key:          3 4 2 1 5 6 7
Ciphertext:   T R A N S P O
              S I T I O N C
              I P H E R S X
Plaintext:    transpositionciphers
```

Product Ciphers

- Ciphers using substitutions or transpositions are not secure because of language characteristics
- Hence consider using several ciphers in succession to make harder
  - Two substitutions make a more complex substitution
  - Two transpositions make a more complex transposition
  - But a substitution followed by a transposition makes a new much harder cipher
    - This is bridge from classical to modern ciphers

Additional References

- http://www.eventid.net/docs/desexample.htm
- http://www.iusmentis.com/technology/encryption/des/
- http://www.research.ibm.com/journal/rd/383/coppersmith.pdf

Acknowledgement

- Some slides are borrowed from Dr. Ping Yang