哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

L2: Classical cryptography - II

Lecturer: Zoe L. JIANG

A309
8:00-9:45

Recall

Shift cipher

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

- $k_1 = 3$
- m_1 = b e g i n t h e a t t a c k n o w
- C_1 = E H J L Q W K H D W W D F N Q R Z

- C_2 = O V D T H U F W V Z Z P I S L R L F Z H Y L A O L Y L
- k_2 = ? 7
- m_2 = ?

Brute-force attack
Try all 26 possible keys

Types of Attack	Known to Cryptanalyst
Ciphertext Only Attack (COA)	•Encryption algorithm •Ciphertext

Recall

Mixed monoalphabetic cipher

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

- C_1 = G D O O K V C X E F L G C D
- m_1 = ?

Brute-force attack does not work

Statistical attack works well

Outline

- Steganography隐写术
- Substitution cipher替换密码
  - Monoalphabetic cipher单字母单表密码
    - Caesar cipher (Shift cipher)
    - Mixed alphabetic cipher
    - Morse code
  - Polyalphabetic cipher单字母多表密码
    - Vigenère cipher
  - Multiple letter cipher多字母单表密码
    - Playfair cipher
    - Hill cipher
  - A special substitution cipher
    - One-time pad (OTP)
- Transposition cipher置换密码
- Rotor machine转轮密码机

Exercise

m
K
C

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

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	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
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

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
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

Exercise

- Multiple shift ciphers in sequence
- Encrypt
  - the 1st, 5th, 9th, and so on characters with the shift cipher with k = 3
  - the 2nd, 6th, 10th, and so on characters with the shift cipher with k = 1
  - the 3rd, 7th, and so on characters with the shift cipher with k = 6
  - the 4th, 8th, and so on characters with the shift cipher with k = 5

Polyalphabetic cipher

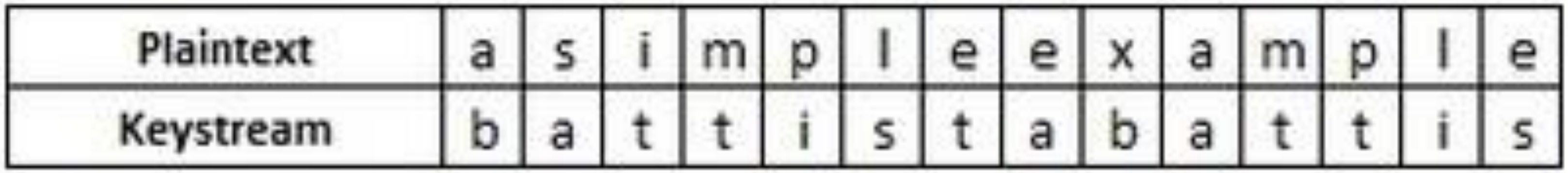
- The substitution rule changes continuously from one character position to the next in the plaintext according to the elements of the encryption key
- Feature: same plaintext character is substituted by different ciphertext characters (i.e., polyalphabetic)

Vigenère cipher

- At the time, and for many centuries since its invention, it was renowned for being a very secure cipher, and for a very long time it was believed to be unbreakable. It was this thought that earned it the nickname "le chiffre indéchiffrable" (French for "the unbreakable cipher")
- Although this is not true (it was fully broken by Friedrich Kasiski in 1863), it is still a very secure cipher in terms of paper and pen methods, and is usable as a field cipher.

Vigenère cipher - Gen

- Choose a keyword (or keyphrase), repeat this keyword over and over until it is the same length as the plaintext. This is called the *keystream*.

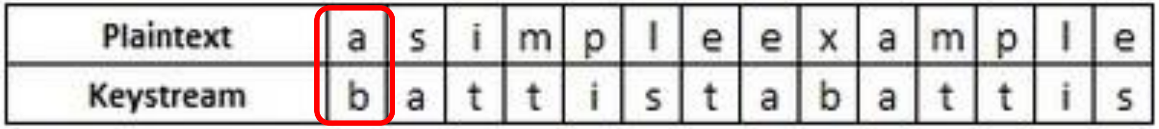


Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

The keystream using the keyword battista

Vigenère cipher - Enc

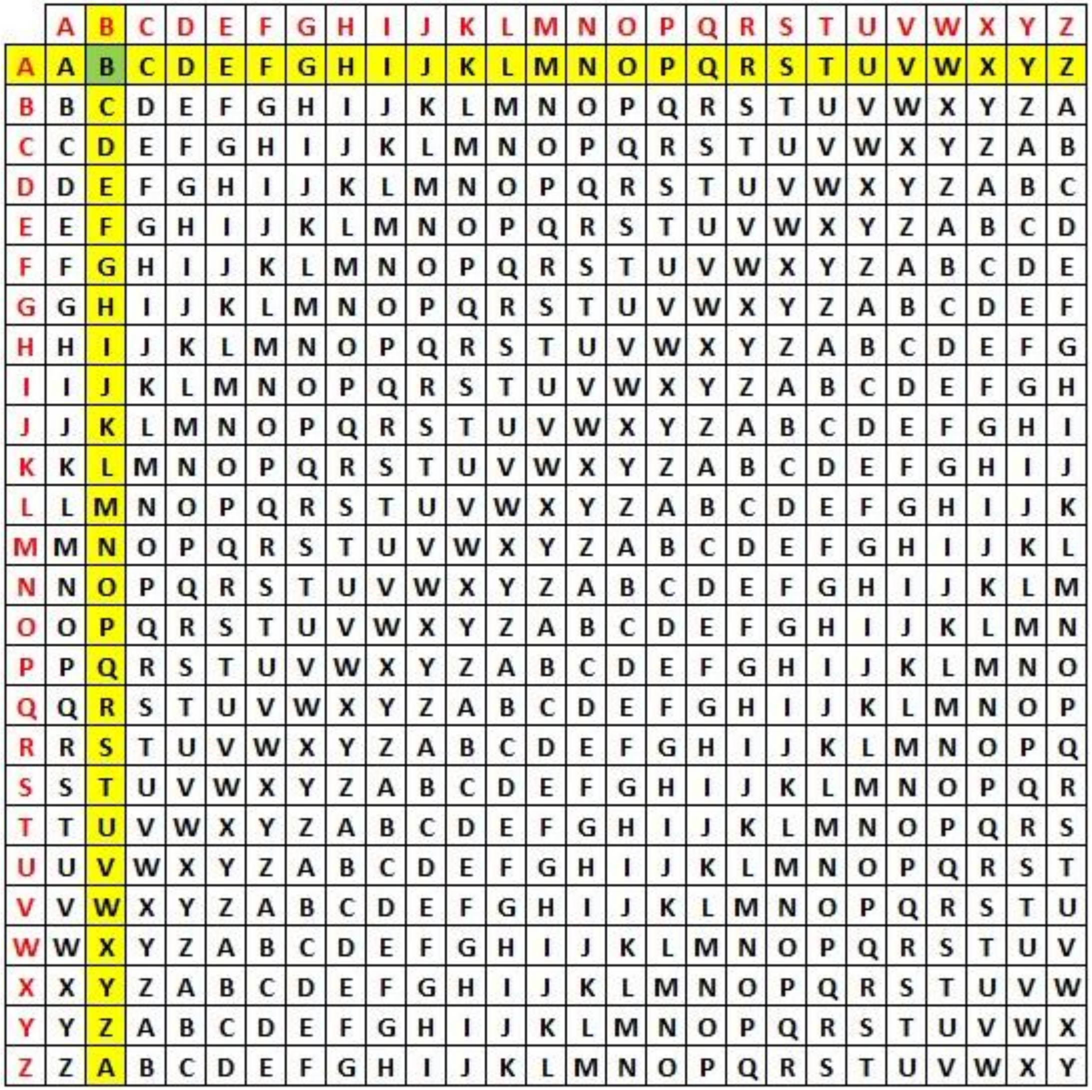
- For each plaintext letter, find the letter down the left hand side of the tabula recta, and take the corresponding letter from the keystream, and find this across the top of the tabula recta. Where these two lines cross in the table is the ciphertext letter you use
- As an example, we shall encrypt the plaintext "a simple example" using the keyword *battista*. First we must generate the keystream, by repeating the letters of the keyword until it is the same length as the plaintext.



Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

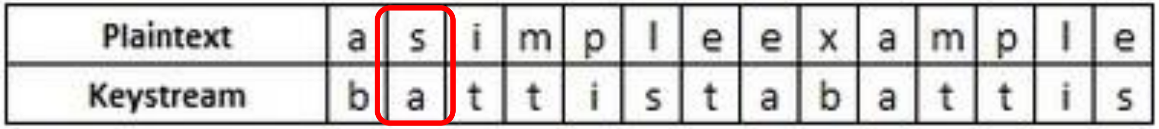
Vigenère cipher - Enc

- The keystream *b* means we choose the column with B at the top, and the plaintext "a" means we choose the row with A at the left. We get the ciphertext "B".



	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

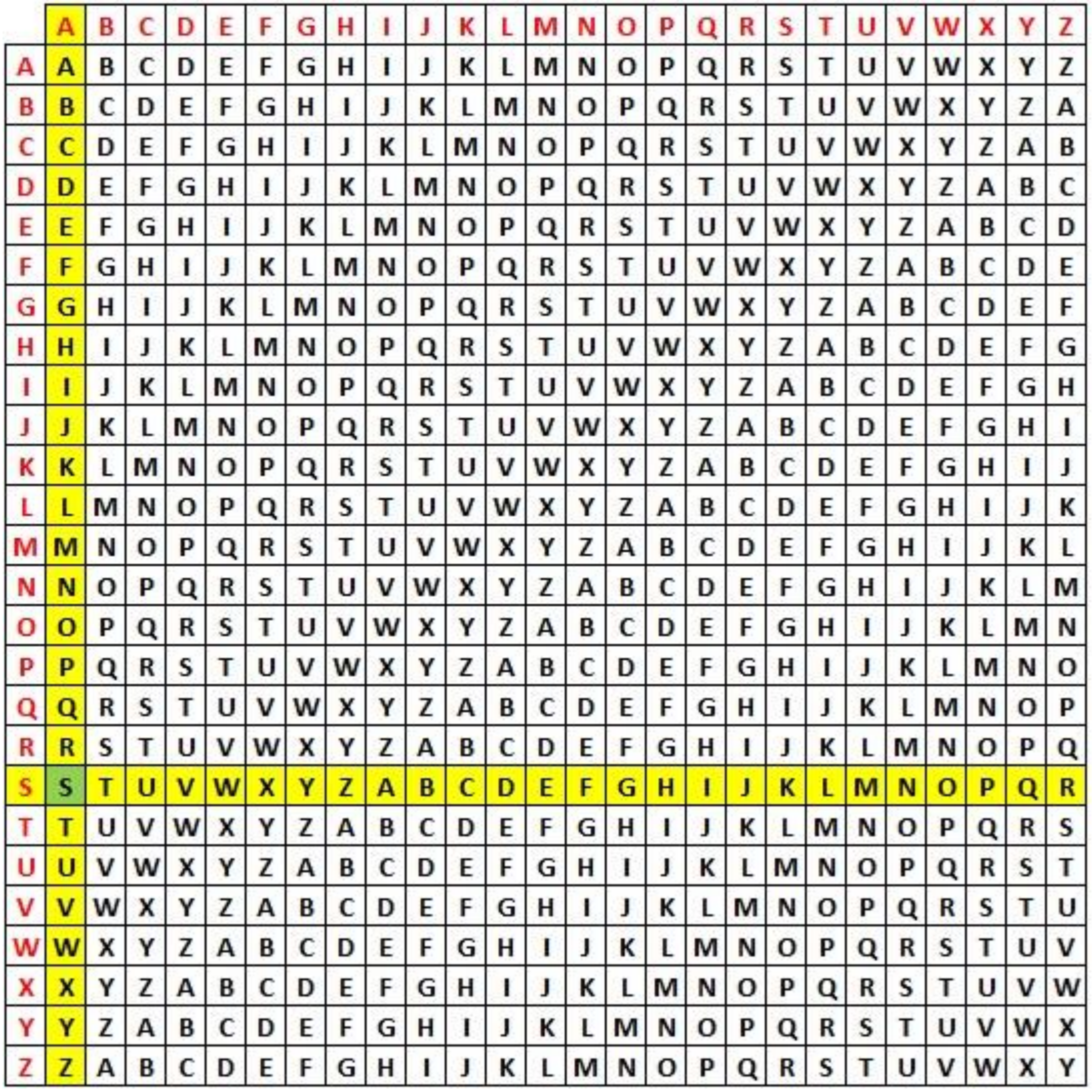
Tabula Recta



Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

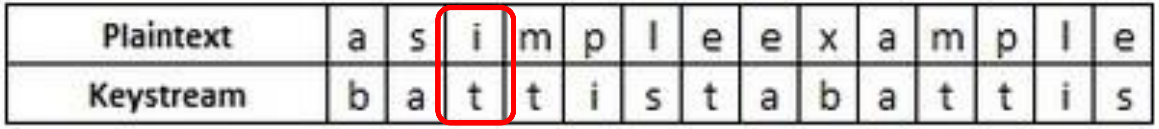
Vigenère cipher - Enc

- For the second plaintext letter "s", we go down to S on the left, and use the keystream *a* to go to A along the top. We get the ciphertext letter "S".



	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

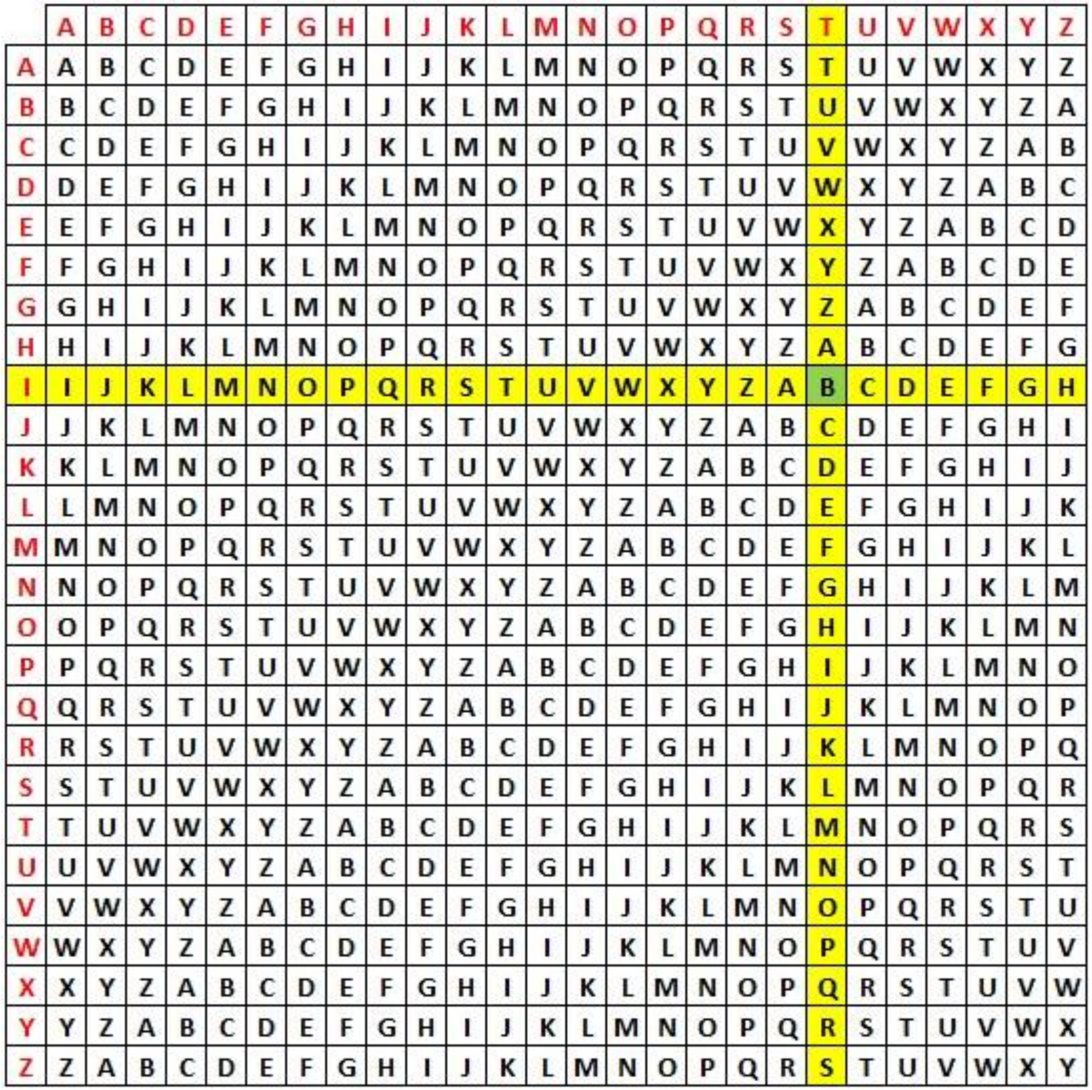
Tabula Recta



Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

Vigenère cipher - Enc

- With the plaintext letter "i", we go down to I on the left, and the keystream letter *t* means we go to T across the top. We get the ciphertext letter "B".

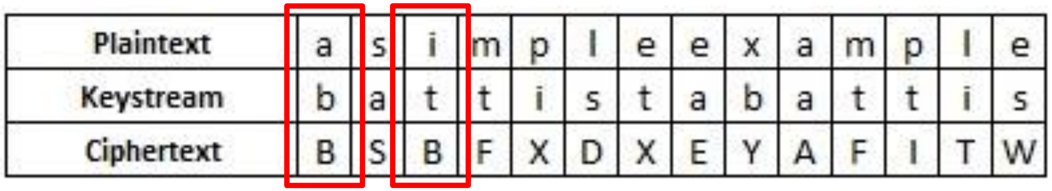


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Tabula Recta

Vigenère cipher - Enc

- Continuing in this way we get the final ciphertext "BSBF XDXEYA FITW“

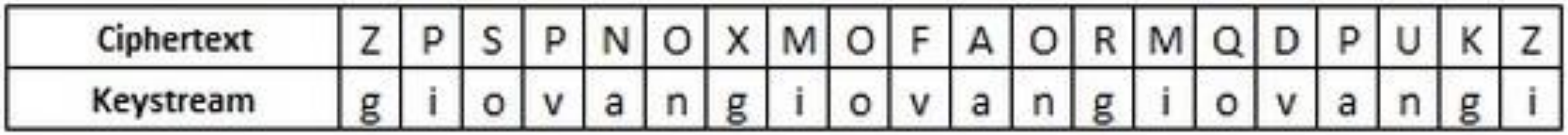


Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s
Ciphertext	B	S	B	F	X	D	X	E	Y	A	F	I	T	W

- Notice that the "a" and "i" both encrypt to "B", and also that the three "e"s that appear encrypt to "X", "E" and "W"

Vigenère cipher - Dec

- To decrypt a ciphertext with the keyword, we first have to generate the keystream by repeating the keyword until we have a keystream the same length as the ciphertext. Then you find the column with the letter of the keystream at the top, and go down this column until you find the ciphertext letter. Now read across to the far left of the table to reveal the plaintext letter
- As an example we shall decipher the ciphertext "ZPSPNOXMOFAORMQDPUKZ" which has been encoded using the keyword *giovan*. We start by generating the keystream.

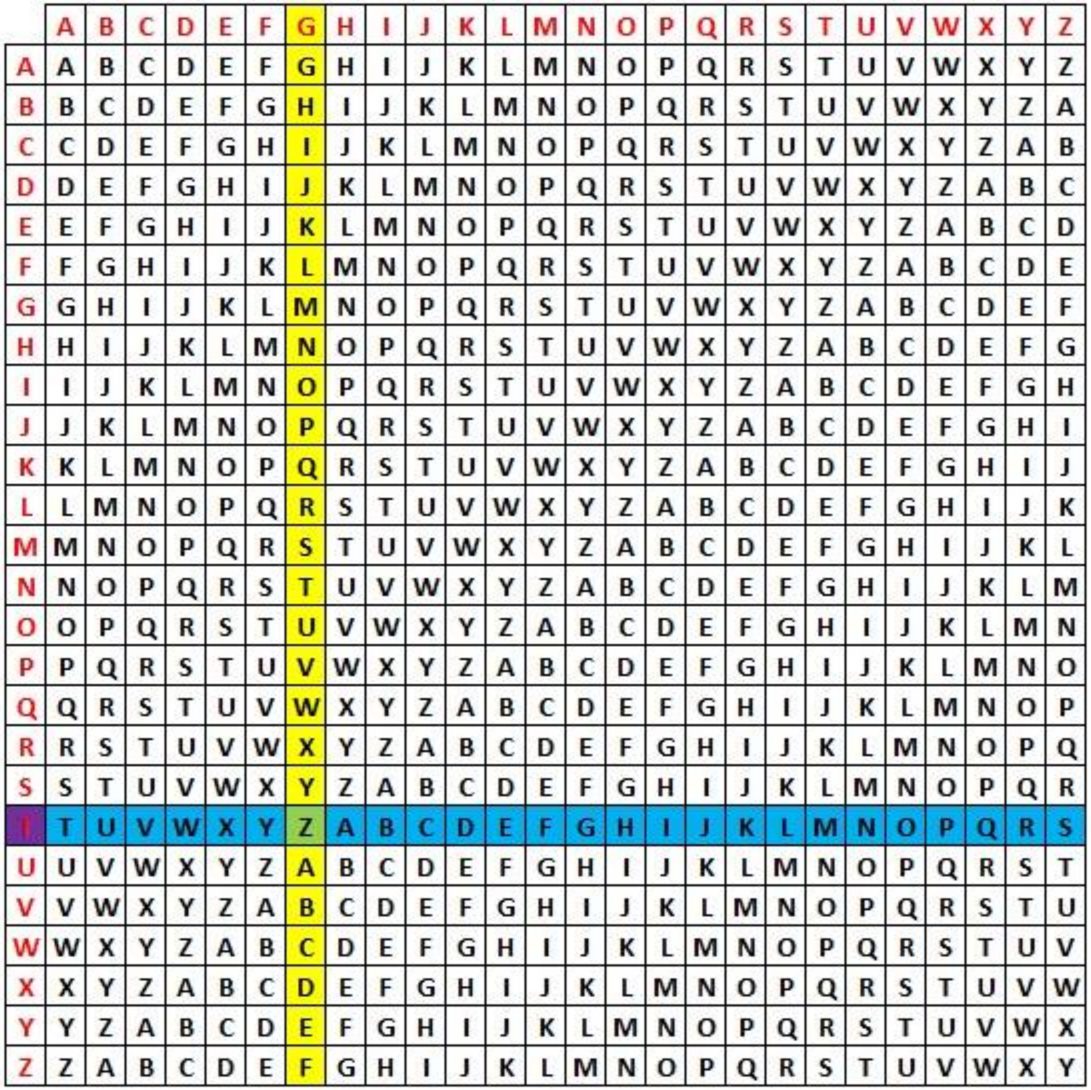


Ciphertext	Z	P	S	P	N	O	X	M	O	F	A	O	R	M	Q	D	P	U	K	Z
Keystream	g	i	o	v	a	n	g	i	o	v	a	n	g	i	o	v	a	n	g	i

Ciphertext	Z	P	S	P	N	O	X	M	O	F	A	O	R	M	Q	D	P	U	K	Z
Keystream	g	i	o	v	a	n	g	i	o	v	a	n	g	i	o	v	a	n	g	i

Vigenère cipher - Dec

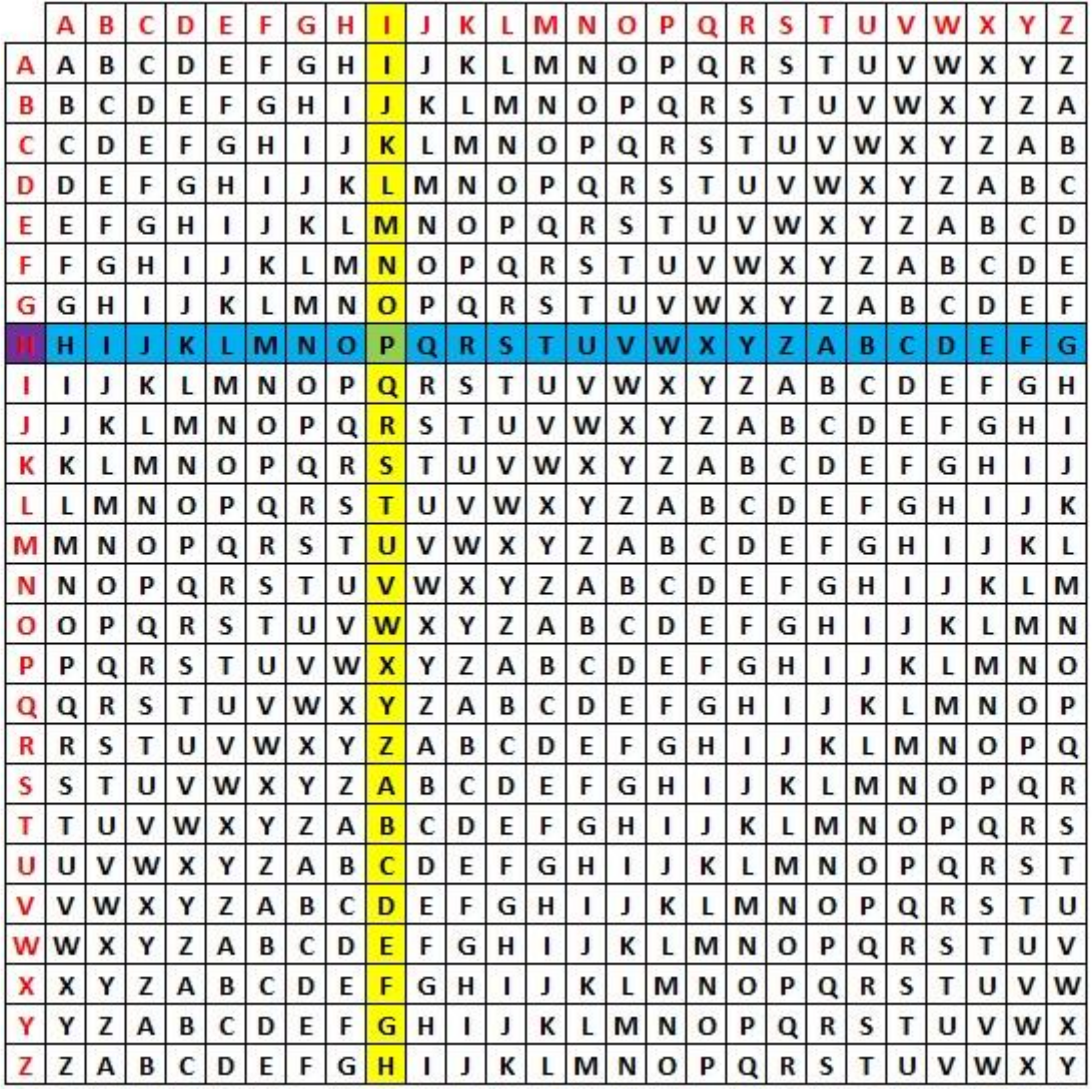
- look along the top row to find the letter from the keystream, G. We look down this column (in yellow) and find the ciphertext letter "Z" (in green). We then go along this row (in blue) to the left hand edge, and the letter here (in purple) is the plaintext letter. In this case it is "t".



	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

Vigenère cipher - Dec

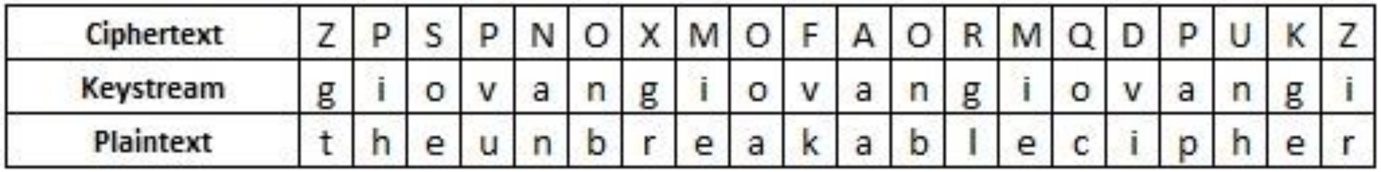
- In the same way as above, we find the keystream letter I, and find the ciphertext letter "P" in this column. We then follow this row to find the plaintext letter "h".



	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

Vigenère cipher - Dec

- Continuing in this way we retrieve the ciphertext "the unbreakable cipher"



Ciphertext	Z	P	S	P	N	O	X	M	O	F	A	O	R	M	Q	D	P	U	K	Z
Keystream	g	i	o	v	a	n	g	i	o	v	a	n	g	i	o	v	a	n	g	i
Plaintext	t	h	e	u	n	b	r	e	a	k	a	b	l	e	c	i	p	h	e	r

- The Vigenère Cipher was the biggest step in cryptography for over 1000 years. The idea of switching between ciphertext alphabets as you encrypt was revolutionary, and an idea that is still used to make ciphers more secure. One of the most famous examples of codes and ciphers in history, the ENIGMA machine, is just a modified polyalphabetic substitution cipher!

Vigenère cipher

- General equation of the encryption process is

$$C_i = (m_i + k_{i \bmod l}) \bmod 26$$

- General equation of the decryption process is

$$m_i = (C_i - k_{i \bmod l}) \bmod 26$$

- Compare the equation with that of the Caesar cipher

$$C = (m + 3) \bmod 26$$

$$m = (C - 3) \bmod 26$$

l: the length of the key words

- Why does Vigenère cipher belong to monoalphabetic cipher?

Security analysis

- The relative frequency distribution becomes obscured, but not totally lost
- Obviously, the longer the encryption key, the greater the masking of the structure of the plaintext
- How to break it? Cha1.3, P14-16
- **Autokey system**: The best possible key is as long as the plaintext message and consists of a purely random permutation of the 26 letters of the alphabet, which is labeled “Random polyalphabetic”

Outline

- Steganography隐写术
- **Substitution cipher替换密码**
  - Monoalphabetic cipher单字母单表密码
    - Caesar cipher (Shift cipher)
    - Mixed alphabetic cipher
    - Morse code
  - **Polyalphabetic cipher单字母多表密码**
    - **Vigenère cipher**
  - **Multiple letter cipher多字母单表密码**
    - **Playfair cipher**
    - **Hill cipher**
  - **A special substitution cipher**
    - **One-time pad (OTP)**
- **Transposition cipher置换密码**
- **Rotor machine转轮密码机**

Multiple letter cipher

- How about destroying some of the statistic characters in monoalphabatic cipher by mapping multiple characters at a time to ciphertext characters?
  - Encrypt multiple letters of plaintext: multiple letter cipher

Playfair KeyGen

- a 5*5 matrix of letters based on a keyword
- fill in letters of keyword first
- fill rest of matrix with other letters in sequence
- eg. using the keyword MONARCHY

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

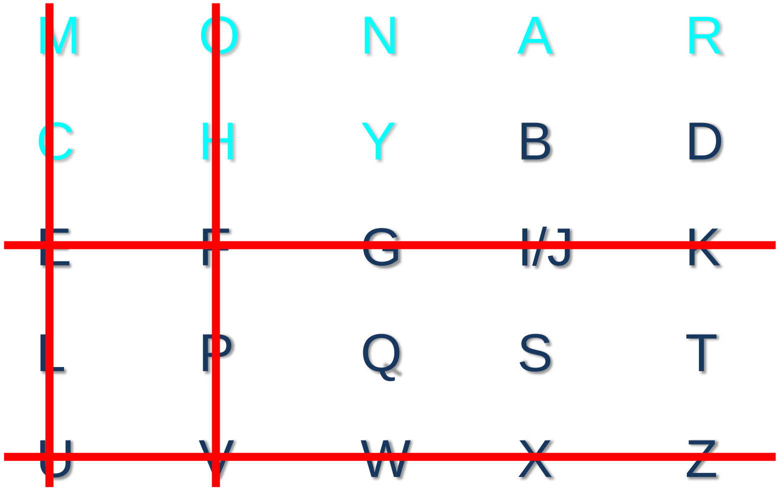
Key Matrix

Playfair Encryption

- plaintext is encrypted two letters at a time
- if a pair is a repeated letter, insert filler like ‘x’
- if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
- if both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
- otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Playfair Encryption Example

- Message = `Move forward`
- Plaintext = `mo ve fo rw ar dx`
- Here `x` is just a filler, message is padded and segmented
- Encryption:
  - `mo` → `ON`; `ve` → `UF`;
  - `fo` → `PH`, etc.



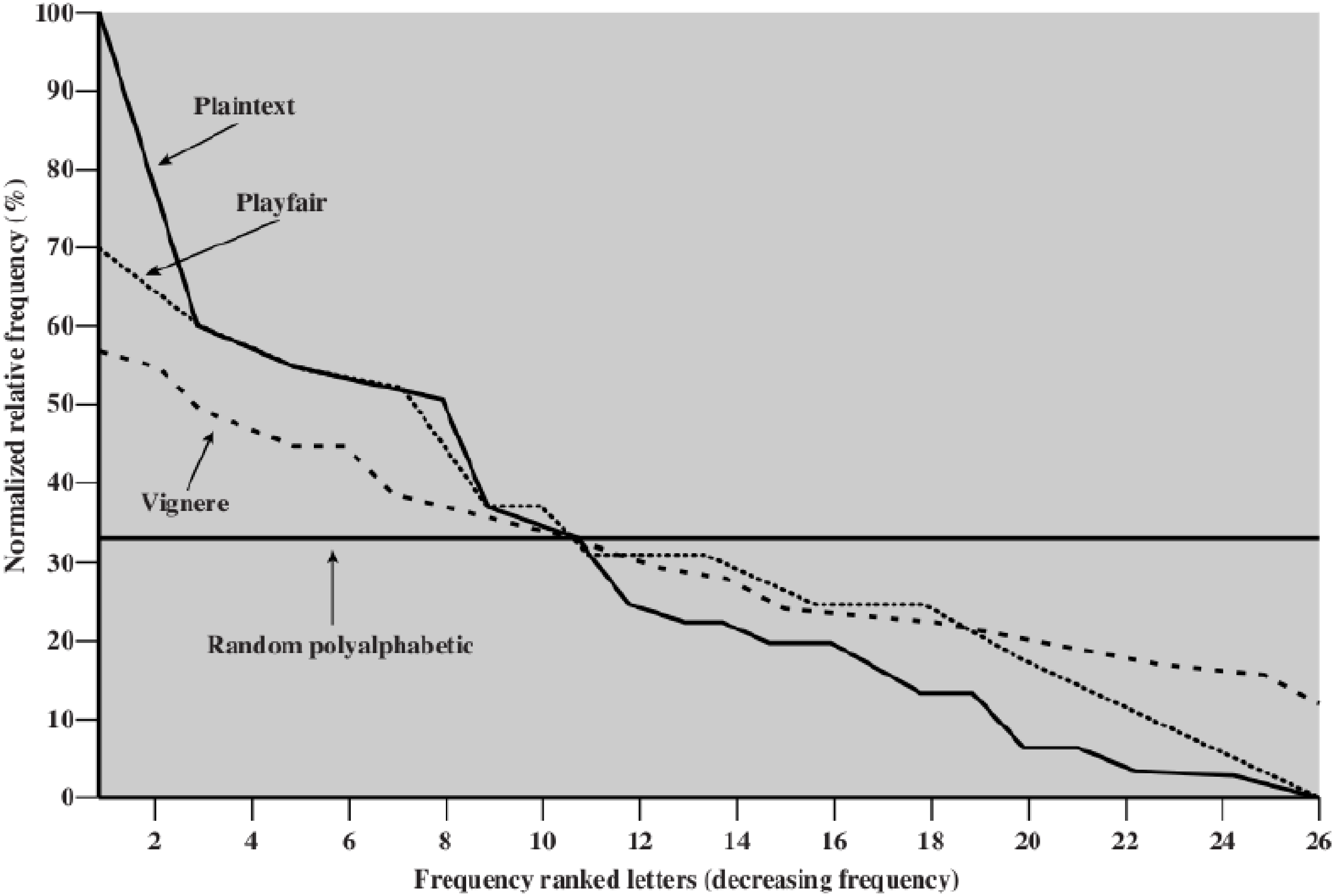
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- Ciphertext = ON UF PH NZ RM BZ

How secure is the Playfair cipher?

- Playfair was thought to be unbreakable for many decades
- It was used as the encryption system by the British Army in World War I. It was also used by the U.S. Army and other Allied forces in World War II
- As expected, the cipher does alter the relative frequencies associated with the individual letters, but not sufficiently

Relative frequency of occurrence of letters



This figure is from Chapter 2 of William Stallings: "Cryptography and Network Security", Fifth Edition, Prentice-Hall.

Outline

- Steganography隐写术
- Substitution cipher替换密码
  - Monoalphabetic cipher单字母单表密码
    - Caesar cipher (Shift cipher)
    - Mixed alphabetic cipher
    - Morse code
  - Polyalphabetic cipher单字母多表密码
    - Vigenère cipher
  - Multiple letter cipher多字母单表密码
    - Playfair cipher
    - Hill cipher
  - A special substitution cipher
    - One-time pad (OTP)
- Transposition cipher置换密码
- Rotor machine转轮密码机

Another multi-letter cipher: The Hill Cipher

- The Hill cipher takes a very different (more mathematical) approach to multi-letter substitution:
- Mathematically give each letter a number

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
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

- The encryption key, **K**, consists of a 3 × 3 matrix of integers:

$$\mathbf{K} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{31} & k_{31} \end{pmatrix}$$

- Plaintext **m** is represented by

$$\begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$$

Another multi-letter cipher: The Hill Cipher

- Transform three letters at a time from plaintext $\mathbf{m}$

$$
\begin{aligned}
C_1 &= (k_{11}m_1 + k_{12}m_2 + k_{13}m_3) \bmod 26 \\
C_2 &= (k_{21}m_1 + k_{22}m_2 + k_{23}m_3) \bmod 26 \\
C_3 &= (k_{31}m_1 + k_{32}m_2 + k_{33}m_3) \bmod 26
\end{aligned}
$$

- Express in terms of row vectors and matrices:

$$
\mathbf{C} = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{31} & k_{31} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}
$$

- Encryption: $\mathbf{C} = \mathbf{Km} \bmod 26$
- Decryption: $\mathbf{m} = \mathbf{K}^{-1}\mathbf{C} \bmod 26 = \mathbf{K}^{-1}\mathbf{Km} = \mathbf{m}$

The Hill cipher example

- Plaintext: `paymoremoney`
- Encryption key:

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

- `pay` are represented by the vector $\mathbf{m} = \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$
- $\mathbf{Km} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$
- Ciphertext: `LNS`

The Hill cipher example

- Calculate the inverse of the matrix **K**

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- $\mathbf{K}^{-1}\mathbf{C} \bmod 26 = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$
- Please finish the exercise by yourself

How secure is the Hill cipher?

- A 3 × 3 Hill cipher hides not only single-letter but also two-letter frequency information
- Against ciphertext-only attack
- Broken with known plaintext attack

Types of Attack	Known to Cryptanalyst
Ciphertext Only Attack (COA)	•Encryption algorithm •Ciphertext
Known Plaintext Attack (KPA)	•Encryption algorithm •Ciphertext •One or more plaintext-ciphertext pairs formed with the secret key

Cryptanalytic Attacks

Types of Attack	Known to Cryptanalyst
Ciphertext Only Attack (COA)	•Encryption algorithm •Ciphertext
Known Plaintext Attack (KPA)	•Encryption algorithm •Ciphertext •One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext Attack (CPA)	•Encryption algorithm •Ciphertext •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext Attack (CCA)	•Encryption algorithm •Ciphertext •Ciphertext chosen by cryptanalyst, together with its decrypted plaintext generated with the secret key

Outline

- Steganography隐写术
- **Substitution cipher替换密码**
  - Monoalphabetic cipher单字母单表密码
    - Caesar cipher (Shift cipher)
    - Mixed alphabetic cipher
    - Morse code
  - **Polyalphabetic cipher单字母多表密码**
    - **Vigenère cipher**
  - **Multiple letter cipher多字母单表密码**
    - **Playfair cipher**
    - **Hill cipher**
  - **A special substitution cipher**
    - **One-time pad (OTP)**
- **Transposition cipher置换密码**
- **Rotor machine转轮密码机**

One-time Pad (OTP)

- A truly random key as long as the message is used
- Unbreakable since ciphertext bears no statistical relationship to the plaintext
- The security of OTP is entirely due to the randomness of the key
- Disadvantage in practice
  - Large quantities of random keys
  - Key distribution and protection
- OTP is the only cryptosystem that achieves *perfect secrecy*

Outline

- Steganography隐写术
- **Substitution cipher替换密码**
  - Monoalphabetic cipher单字母单表密码
    - Caesar cipher (Shift cipher)
    - Mixed alphabetic cipher
    - Morse code
  - **Polyalphabetic cipher单字母多表密码**
    - **Vigenère cipher**
  - **Multiple letter cipher多字母单表密码**
    - **Playfair cipher**
    - **Hill cipher**
  - **A special substitution cipher**
    - **One-time pad (OTP)**
- **Transposition cipher置换密码**
- **Rotor machine转轮密码机**

Transposition cipher

- Hide the message by rearranging the letter order
- Permuting the plaintext
- The cipher can be made more secure by performing multiple rounds of permutation

Rail Fence cipher

- Write plaintext letters out diagonally over a number of rows
- Read off cipher row by row
- E.g. plaintext: `meet me after the toga party`
- Write plaintext out as:

```
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`

Column Transposition Cipher

- Write letters of plaintext out in rows over a specified number of columns
- Reorder the columns according to some key before reading off the columns
- Read the plaintext in the column order specified by the key
- E.g. plaintext: **`attack postponed until two am`**
- Key:
- Plaintext:

4	3	1	2	5	6	7
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`**

Product Ciphers

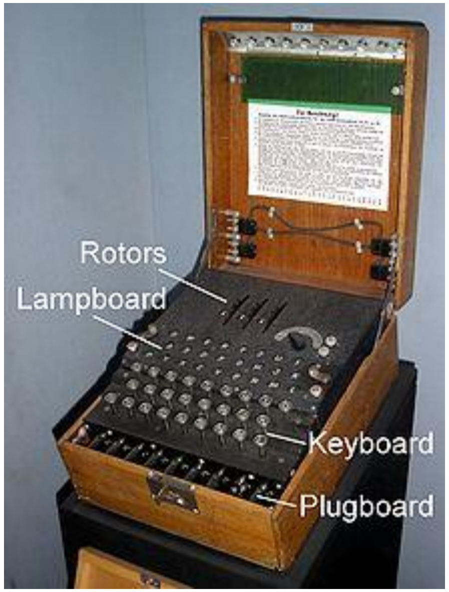
- Ciphers using substitutions or transpositions are not secure because of language characteristics
- Using several ciphers in succession to make harder
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - a substitution followed by a transposition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

Rotor Machines

- Before modern ciphers, rotor machines were most common complex ciphers in use
- Widely used in WWII
  - German Enigma, Allied Hagelin, Japanese Purple
- Implemented a very complex, varying substitution cipher
- Used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted
- With 3 cylinders have 26^3=17576 alphabets

Enigma

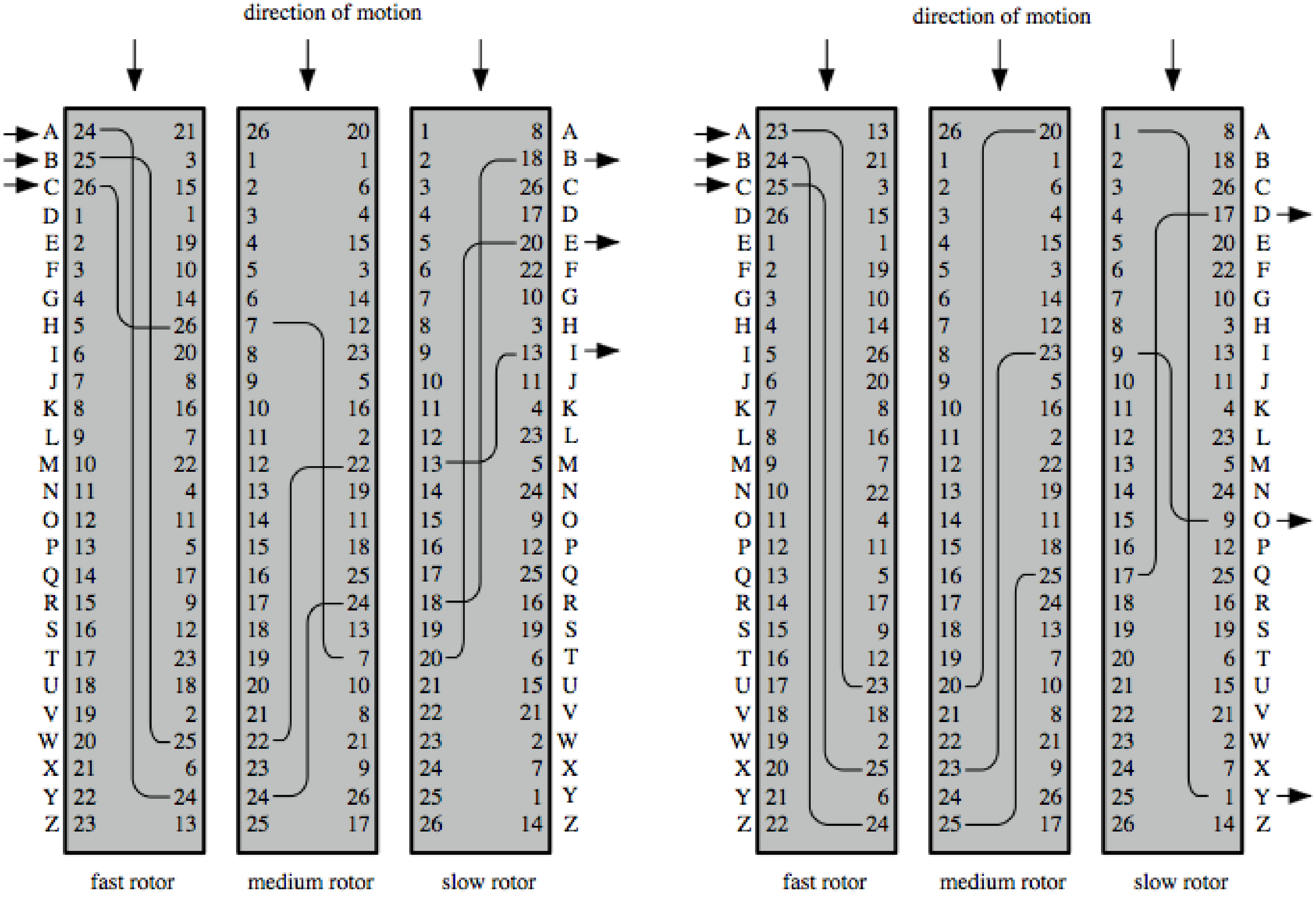
V
U
T
S
R
Q
P
O
L
K
J
I
H
G
F
E
D
C
B
A
Z
Y
X



http://en.wikipedia.org/wiki/Enigma_machine

This figure is from Chapter 2 of William Stallings: “Cryptography and Network Security”, Fifth Edition, Prentice-Hall.

Rotor Machine Principles



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

(a) Initial setting

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

(b) Setting after one keystroke

References

[1] **Stallings William**. Chapter 2, Cryptography and Network Security: Principles and Practice, 5th Edition. Prentice Hall, 2011

[2] http://crypto.interactive-maths.com/vigenegravere-cipher.html