Security

- Network and Internet security
  - Cryptographic techniques
  - Cryptographic algorithms and protocols
    - Symmetric
    - Asymmetric
    - DI algorithms
    - Authentication pls
  - Cryptology
    - Cryptography - Art of devising ciphers
    - +
    - Cryptanalysis - Art of breaking ciphers

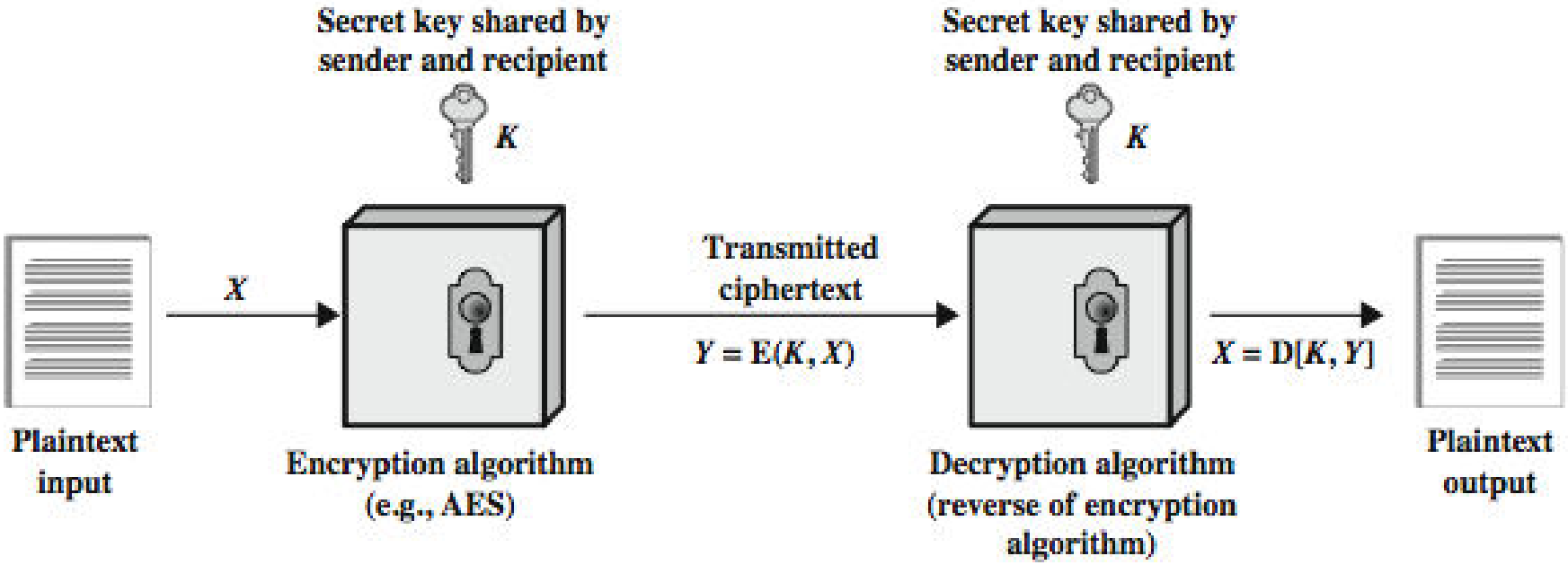
Symmetric Encryption

- conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- only type prior to invention of public-key in 1970's
- most widely used
- m people in a group => m (m-1)/2 keys

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Symmetric Cipher Model



Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically :

  $Y = E(K, X)$

  $X = D(K, Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

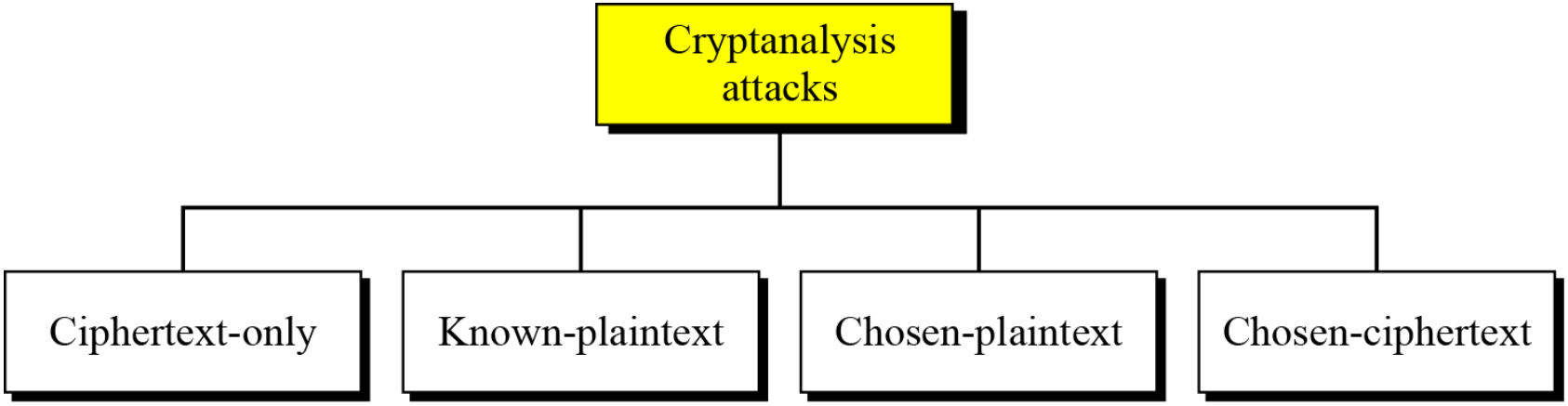
- can characterize cryptographic system by:
  - type of encryption operations used
    - substitution
    - transposition
    - product
  - number of keys used
    - single-key or private
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

Kerckhoff's Principle

- Resistance of the cipher to attack – secrecy of the key
- Guess – difficult
- Key domain - large

Cryptanalysis

As cryptography is the science and art of creating secret codes,
cryptanalysis is the science and art of breaking those codes.



Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext

More Definitions

- **unconditional security**
  - no matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **computational security**
  - given limited computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken

Cryptanalysis

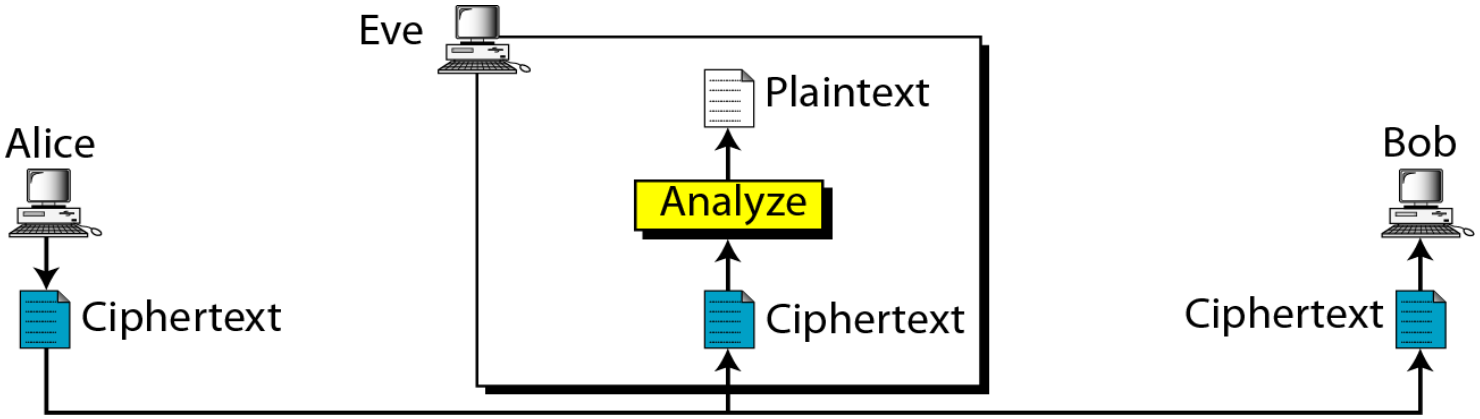
- objective to recover key not just message
- general approaches:
  - Brute-force attack
  - Cryptanalytic attack

Brute Force Attack

- CT only attack
- A communicates with B and E is the Intruder
- Exhaustive key search attack
- always possible to simply try every key
- most basic attack, proportional to key size
- assume – intruder knows the alg and key domain

Statistical Attack

- CT only attack



- E uses the inherent characteristics of PT language
- Eg. Letter e occurs frequently

Pattern Attack

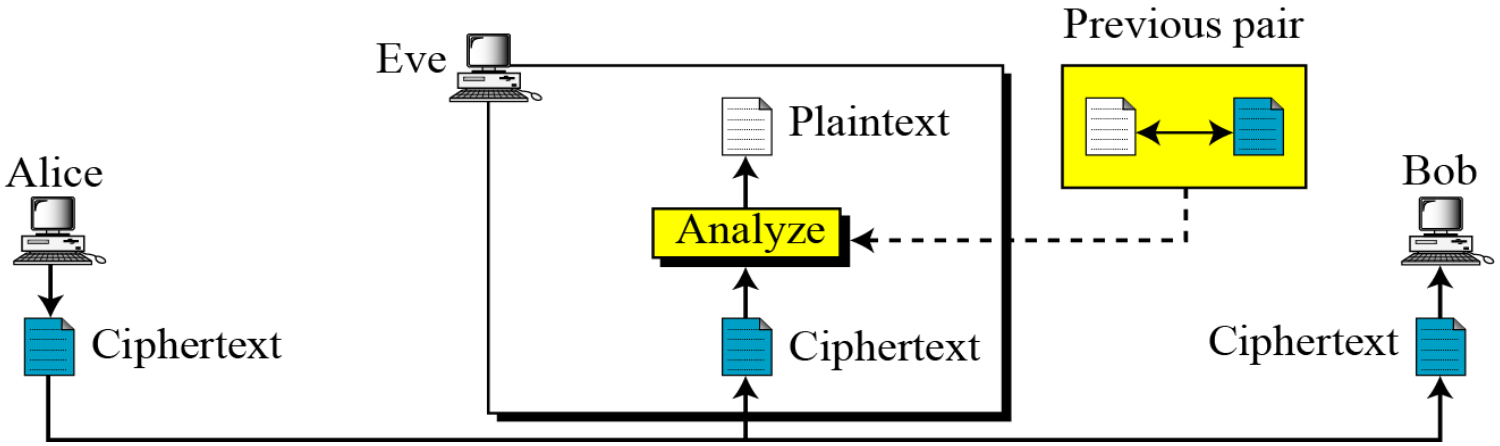
- CT only attack
- E uses the inherent characteristics of PT language
- Hide the chars of the language
- THE
- WKH
- Randomize alg

Known PT Attack

- E uses the relationship b/w the previous pair to analyse the current CT

  Eg. If ABBA then BABA

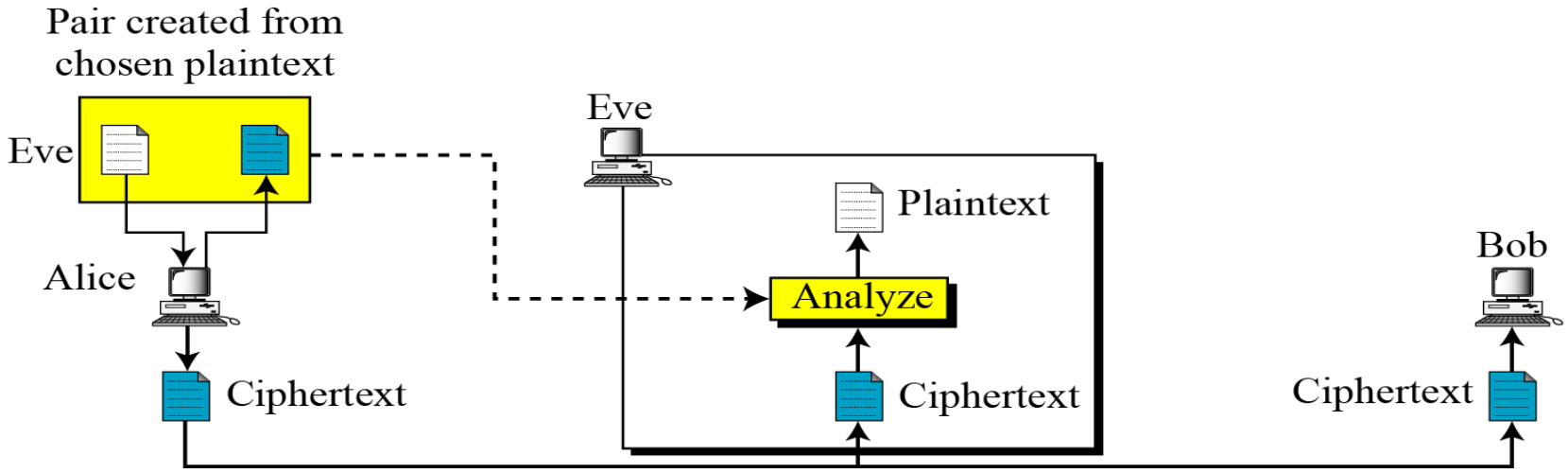
  DEED EDED



- Prevention – A need to use a different key

Chosen PT Attack

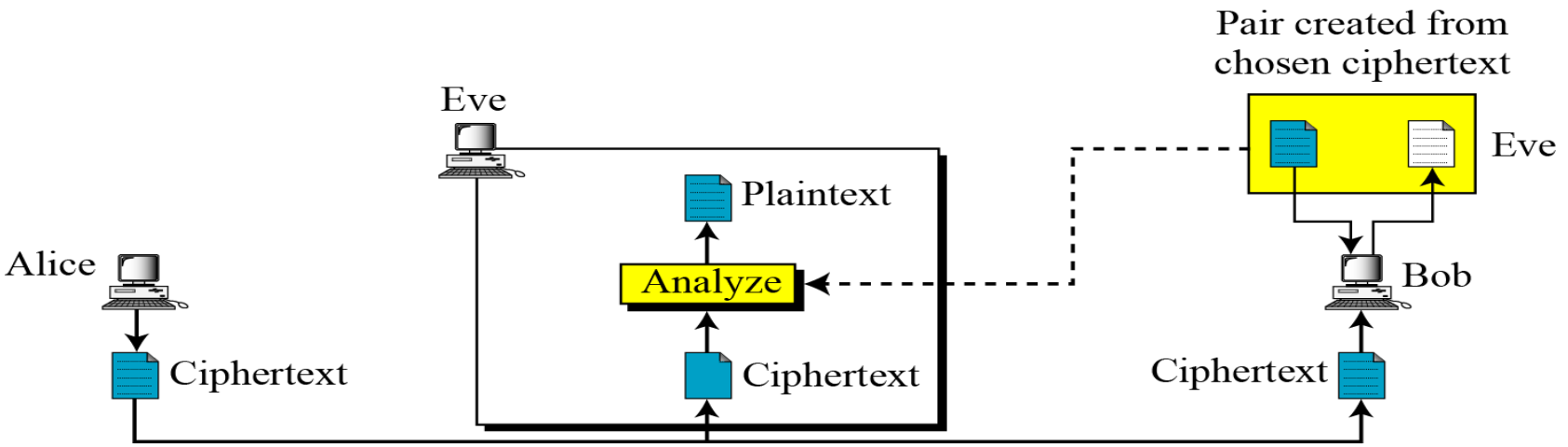
- Similar to KPTA but PT/CT pairs chosen by E
- E has access to A's computer



- Less likely to happen

Chosen CT Attack

- Similar to KPTA
- But E chooses same CT and decrypts it from a CT/ PT pair



- Can happen when E has access to B's computer - Less likely

Categories of Traditional Ciphers

- Substitution Cipher
  - Replace one symbol in PT with another
  - Monoalphabetic Cipher
  - Polyalphabetic Cipher
- Transposition Cipher
  - Reorder the position of symbols in PT

Monoalphabetic Substitution Ciphers

- In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
- letters of plaintext are replaced by other letters or by numbers or symbols

Additive /Shift / Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter
- example:

```
meet me after the party
PHHW PH DIWHU WKH SDUWB
ABBA                ABBA
DEED                QWWQ
```

Caesar Cipher

- 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

- 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

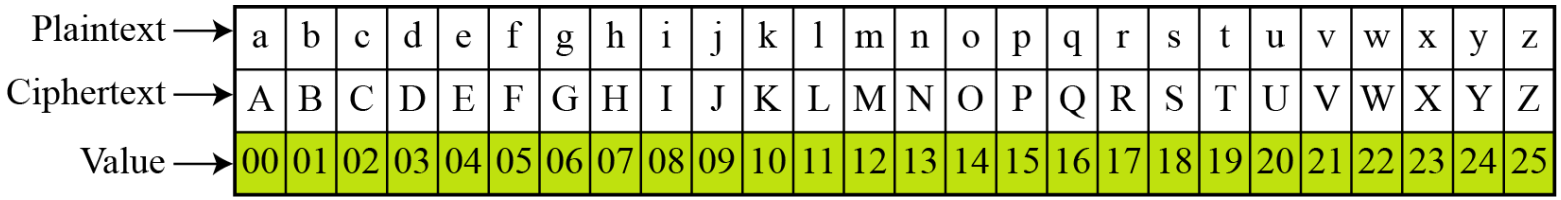
- then have Caesar cipher as:

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

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

Caesar Cipher

- PT and CT in Z_{26}



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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher

- The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.
- Eg some Z_n sets

$$Z_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$$Z_2 = \{ 0, 1 \}$$

$$Z_6 = \{ 0, 1, 2, 3, 4, 5 \}$$

$$Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

MODULAR ARITHMETIC

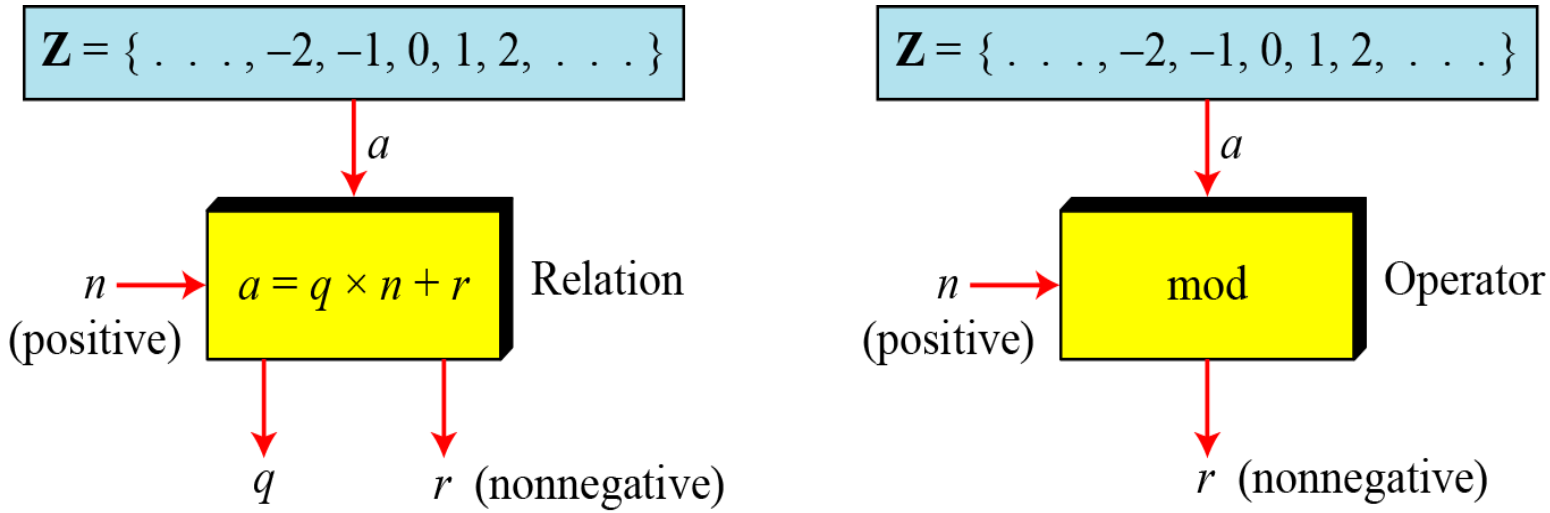
Division operation has
two inputs (a and n)
and two outputs (q and r).

$$a = q \times n + r$$

In modular arithmetic, only one of the outputs, the remainder r is of importance

Modular Operator

- The modulo operator is shown as mod. The second input (n) is called the modulus.
- The output r is called the residue.



Modular Operator

Find the result of the following operations:

a. 27 mod 5

b . 36 mod 12

c. −18 mod 14

d. −7 mod 10

Modular Operator

Find the result of the following operations:

a. 27 mod 5

Dividing 27 by 5 results in r = 2

b .36 mod 12

Dividing 36 by 12 results in r = 0.

c. −18 mod 14

Dividing −18 by 14 results in r = −4. After adding the modulus r = 10

d. −7 mod 10

Dividing −7 by 10 results in r = −7. After adding the modulus to −7, r = 3.

Set of Residues

- The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.
- Eg. Some Z_n sets

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$$\mathbf{Z}_2 = \{ 0, 1 \}$$

$$\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$$

$$\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

Congruence

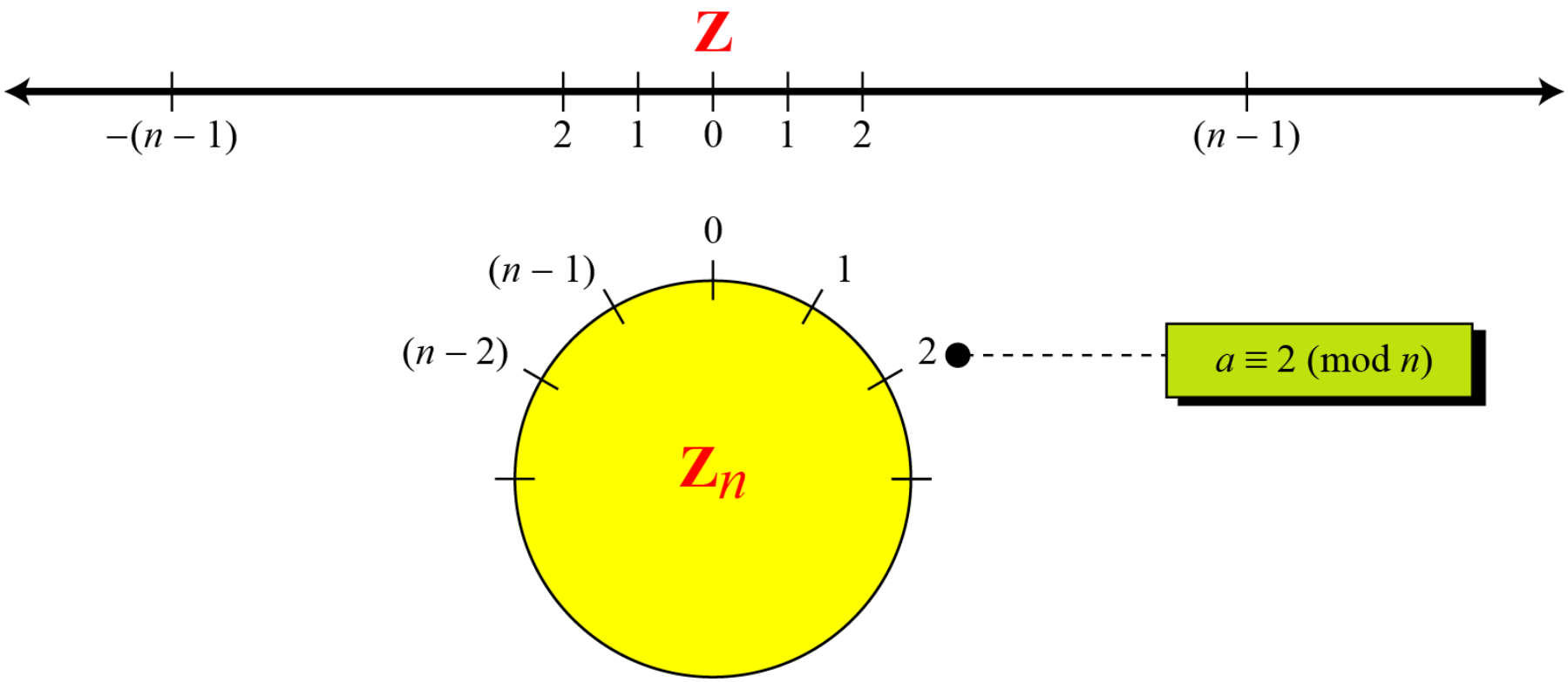
- ***In Cryptography,***
  concept of congruence is used instead of equality.

- ***To show that two integers are congruent, we use the congruence operator (≡).***
- ***Congruence optr maps a member from Z to a member of Z_n.***

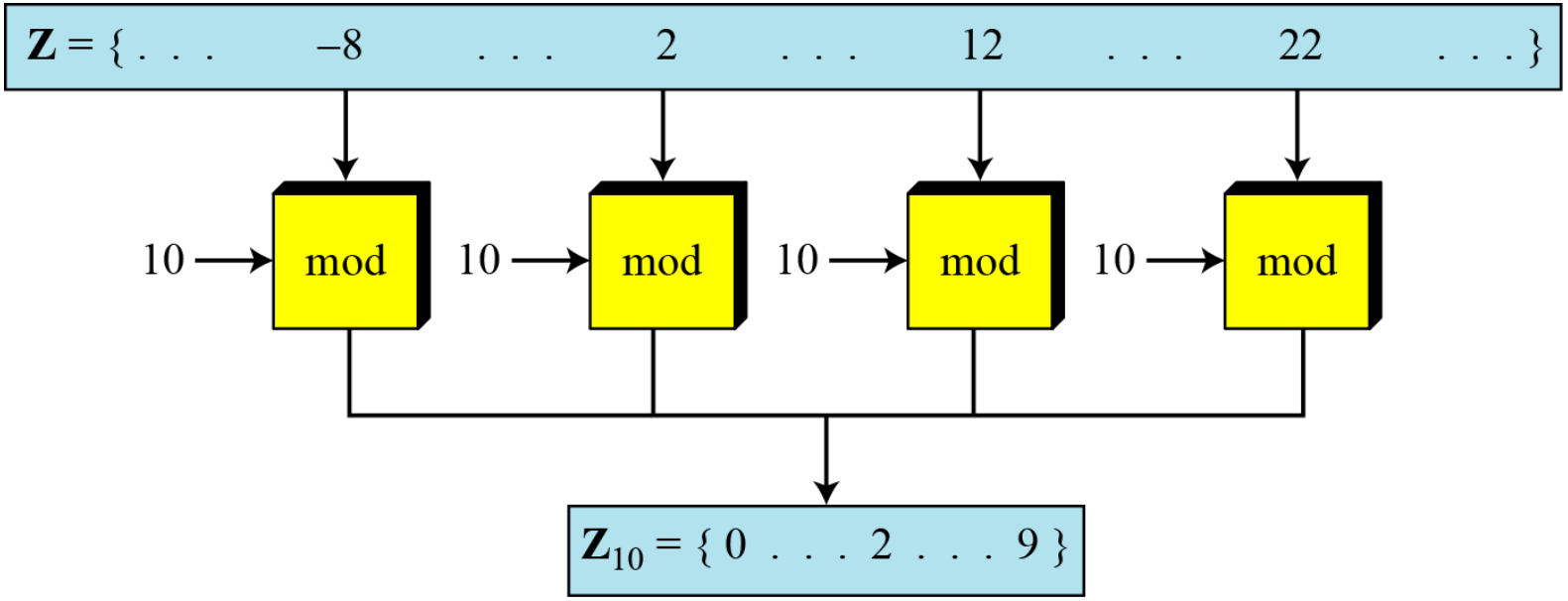
$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$

$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

Comparison of Z and Z_n using graphs



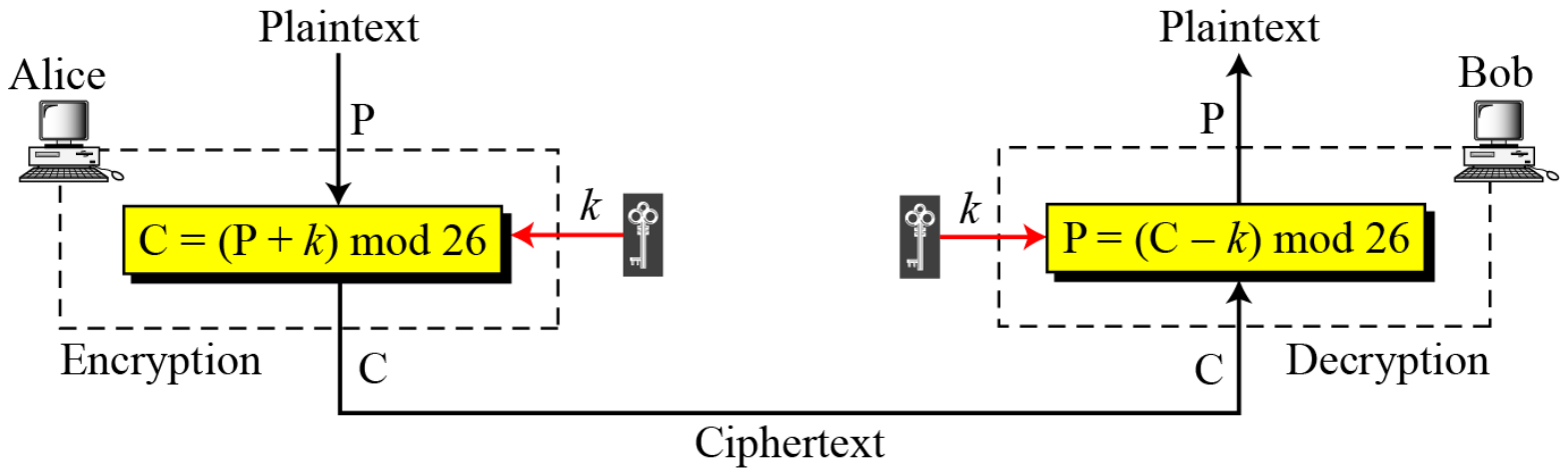
Concept of congruence - Continued



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

Additive cipher



When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

Additive cipher

Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

Additive cipher

Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Additive cipher

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

$$a + b \equiv 0 \pmod{n}$$

Additive inverse of a is calculated as b=n-a

Additive cipher

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Additive cipher

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

```
XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW
```

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences.

What is the key?

Additive cipher

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

```
XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW
```

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4.

Additive cipher

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4.

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Additive cipher

Cryptanalysis

Attacks possible

Brute Force attack

Statistical attack

Additive cipher

Cryptanalysis

Attacks possible

Brute Force attack

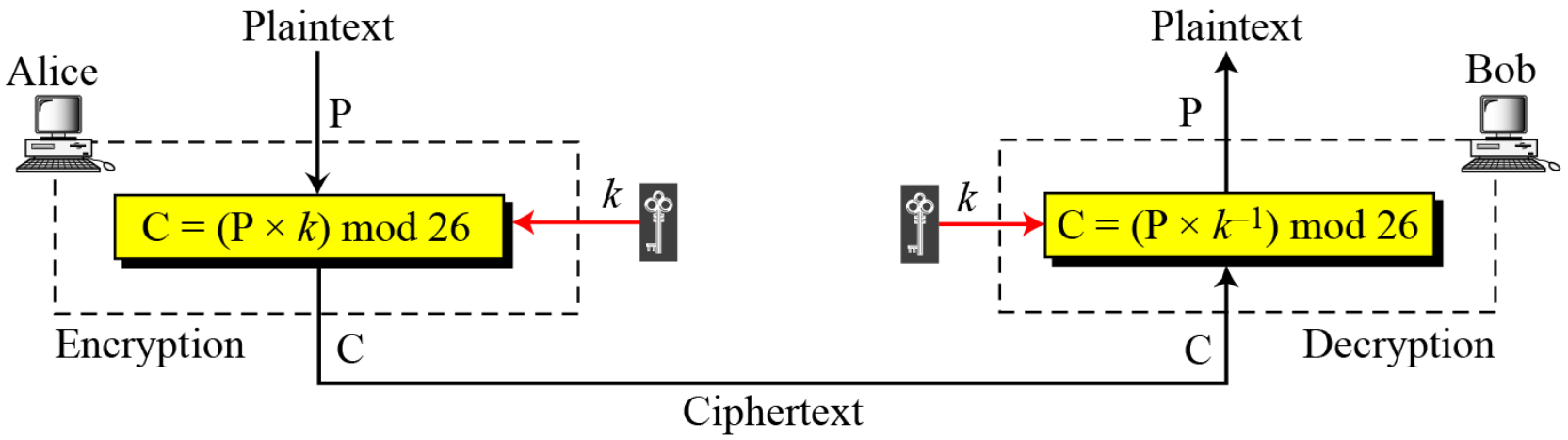
: **Exhaustive key search – key domain is small**

Statistical attack

Digrams - IN,AN,OR,AT

Trigrams - THE, AND, FOR

Multiplicative Ciphers



In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26}; the key is an integer in Z_{26}^*.

Multiplicative Cipher – Contd…

- **$a * b \equiv 1 \pmod{n}$**

- Z_n cannot be the set of possible keys because
  - **Only some members of the set have multiplicative inverse**
  - **A subset of Z_{26} with integers in Z_{26}** that have an u**nique set Z^*_{26}**

Multiplicative Ciphers

Compute Z_n^* for n = 6,7,10,26

Solution

Z_6
Z_6^*
Z_7
Z_7^*.

The key needs to be in Z_{26}^*.

This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Multiplicative Ciphers

What is the key domain for any multiplicative cipher?

Solution

The key needs to be in Z_{26}^*.

This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Multiplicative Ciphers

What is the key domain for any multiplicative cipher?

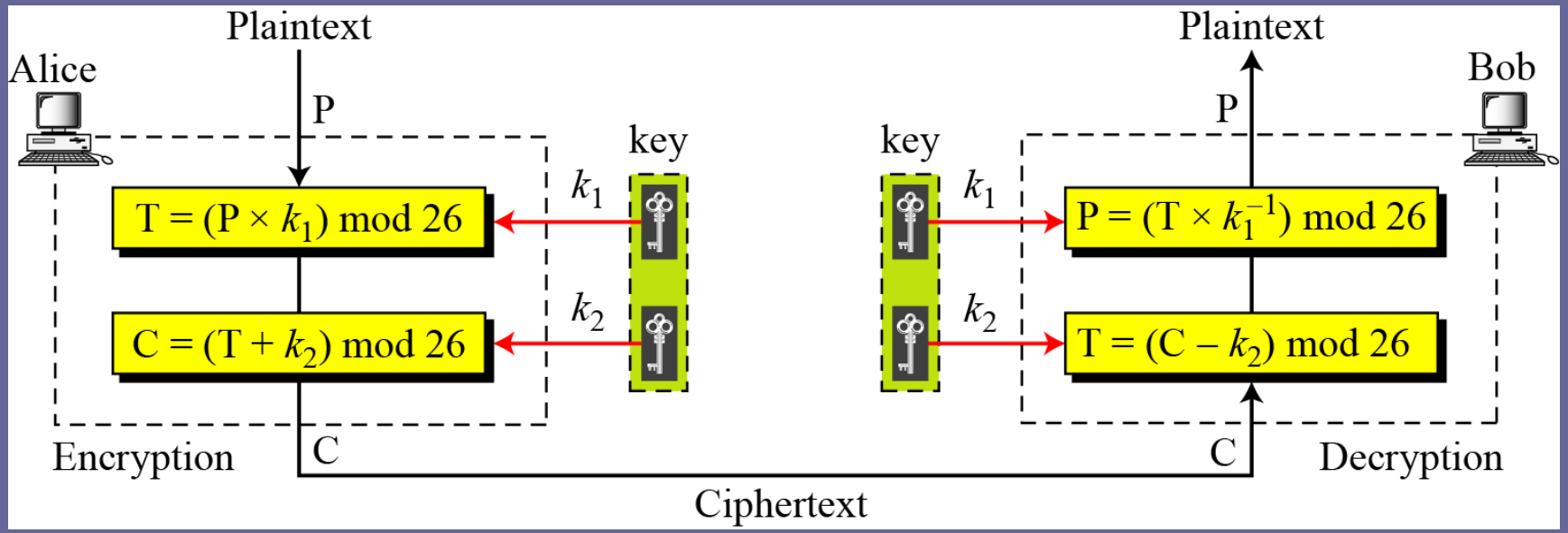
Solution

The key needs to be in Z_{26}*. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

Affine Ciphers

- Combination of Additive and Multiplicative Cipher
- 1st key is Multiplicative Cipher
- 2nd key is Additive Cipher



$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

Affine Ciphers

The affine cipher uses a pair of keys in which the first key is from Z_{26}^* and the second is from Z_{26}. The size of the key domain is $26 \times 12 = 312$.

Use an affine cipher to encrypt the message "hello" with the key pair (7, 2).

Affine Ciphers

The affine cipher uses a pair of keys in which the first key is from Z_{26}^* and the second is from Z_{26}. The size of the key domain is $26 \times 12 = 312$.

Use an affine cipher to encrypt the message "hello" with the key pair (7, 2).

P: h → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 → W

Affine Ciphers

Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

Solution

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 $\rightarrow$ o

Affine Ciphers

Brute force attack

CT only attack

Chosen PT attack

The additive cipher is a special case of an affine cipher in which $k_1 = 1$.

The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$.

Affine Ciphers

- Brute Force Attack
- Ciphertext only Attack
- Chosen Plaintext Attack

- Alg 1 PT et CT wc

- e - w 04 – 22 04 * k1 + k2 = 22 (mod 26)

- t -c 19 – 02 19 * k1 + k2 = 02(mod 26)

- Alg 2 PT et CT wf

- each occurrence of a character may have a different substitute.
- The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.
- Hides the letter frequency of the underlying language

To create a PC, make each CT char dependent on

- corresponding PT char
- posn of PT char in msg

- Key should be a stream of subkeys

$$K = (K_1, K_2, K_3, \ldots)$$

In which K_i is used to cipher the i^{th} char in PT to create the i^{th} char in CT

Polyalphabetic Ciphers

1st subkey is predetermined value agreed by A and B
2nd subkey is the value of 1st PT char (b/w 0 and 25)
3rd subkey is the value of 2nd PT char and so on…

Autokey Cipher

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3\ldots$ $k = (k_1, P_1, P_2, \ldots)$

Encryption: $C_i = (P_i + k_i) \bmod 26$ Decryption: $P_i = (C_i - k_i) \bmod 26$

Polyalphabetic Ciphers

- **Assume that Alice and Bob agreed to use an autokey cipher with initial key value $k_1 = 12$.**
- **Alice wants to send Bob the message**
- **"Attack is today".**
- **Enciphering is done character by character.**

Polyalphabetic Ciphers

Assume that Alice and Bob agreed to use an autokey cipher with initial key value $k_1 = 12$. Now Alice wants to send Bob the message "Attack is today". Enciphering is done character by character

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

Playfair Cipher

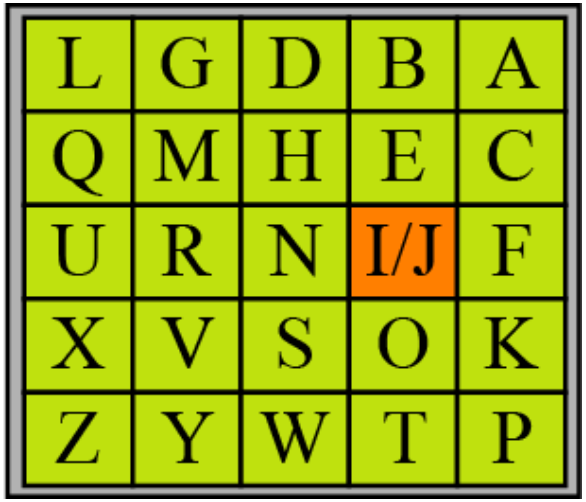
Secret key is made of 24 alphabets – 5 by 5 matrix

- letters I and J considered same
- Diff arrangements – diff secret keys
- Rules for encryption:
  - 2 letters in a pair are same, bogus letter inserted to separate them
  - No of chars is odd, one bogus letter inserted to make it even
  - if 2 letters in a pair are located in the same row of secret key, then the letter to their right is the encrypted key
  - if 2 letters in a pair are located in the same col of secret key, then the letter beneath it in the same col is the encrypted key
  - if 2 letters in a pair are not located in the same row or col of secret key, then the letter that is in its own row but in the same col as the other letter is the encrypted key

Playfair Cipher

An example of a secret key in the Playfair cipher

Secret Key =

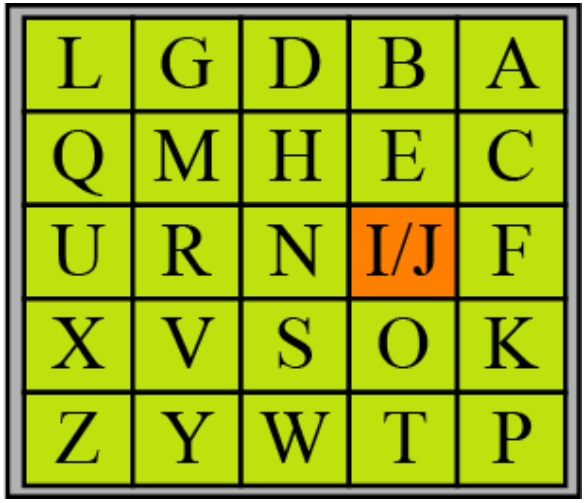


L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Playfair Cipher

An example of a secret key in the Playfair cipher

Secret Key =



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

Plain Text = hello Cipher Text = ?????

Playfair Cipher

Let us encrypt the plaintext “hello” using the key

PT is hello

- **l is repeated and so PT becomes helxlo**
- **No of chars are even**
- **he - same row , hence letter to their right is encrypted key**

so, for he , it is EC

Playfair Cipher

Let us encrypt the plaintext "hello" using the key

PT is hello

- **l is repeated and so PT becomes helxlo**
- **No of chars are even**
- **he - same row , hence letter to their right is encrypted key**

so, for he , it is EC

- **lx - same col, hence** the letter beneath it in the same col is the encrypted key, **so, for lx , it is QZ**
- **lo - not is same row or col,** letter that is in its own row but in the same col as the other letter is the encrypted key, so, for lo, it is BX

- helxlo

Playfair Cipher

Let us encrypt the plaintext "hello" using the key

PT is hello

- **l is repeated and so PT becomes helxlo**
- **No of chars are even**
- **he - same row , hence letter to their right is encrypted key**

so, for he , it is EC

- **lx - same col, hence** the letter beneath it in the same col is the encrypted key, **so, for lx , it is QZ**
- **lo - not is same row or col,** letter that is in its own row but in the same col as the other letter is the encrypted key, so, for lo, it is BX

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

Vigenere Cipher

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3 \ldots$ $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$

Example 3.16

We can encrypt the message "She is listening" using the 6-character keyword "PASCAL".

Vigenere Cipher

Let us see how we can encrypt the message "She is listening" using the 6-character keyword "PASCAL". The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

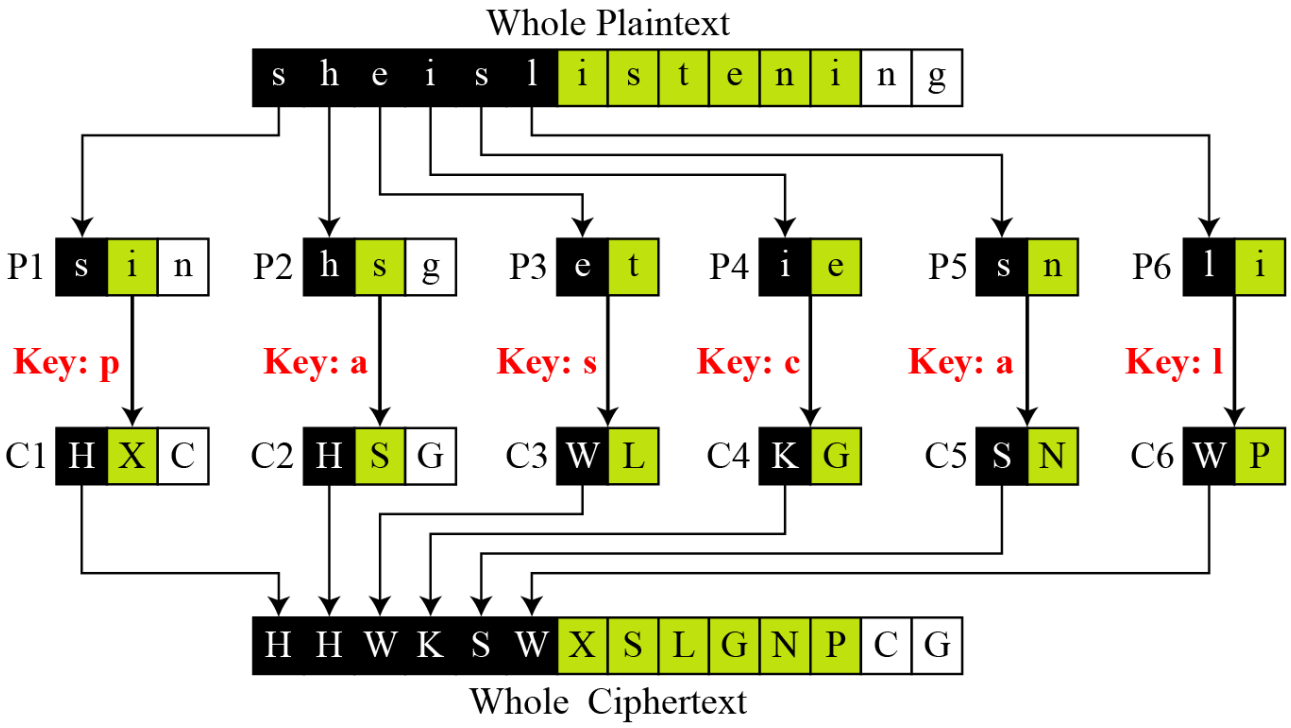
Vigenere Cipher

Let us see how we can encrypt the message "She is listening" using the 6-character keyword "PASCAL". The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Vigenere Cipher

A Vigenere cipher is a combination of m additive ciphers



the additive cipher is a special case of Vigenere cipher in which m = 1.

One-Time Pad

One of the goals of cryptography is perfect secrecy.

A study by Shannon has shown that perfect secrecy can be achieved

if each plaintext symbol is encrypted with a key randomly chosen from a key domain.

This idea is used in a cipher called One-Time Pad, invented by Vernam.

TRANSPOSITION CIPHERS

A transposition cipher

- No substitution
- Changes/ reorders / transposes the location of the symbols.

Keyless Transposition Ciphers

PT --- >Meet me at the park

A Keyless cipher is the rail fence cipher.

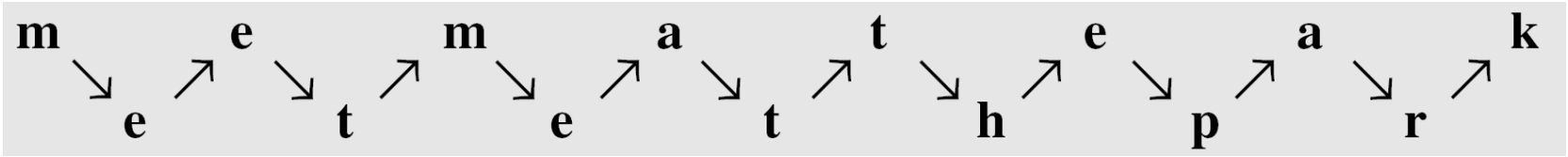
- **PT written into a table col by col - 2 ROWS**
  CT created by reading row by row
- **PT written into a table row by row – 2 COLS**
  CT created by reading col by col

Keyless Transposition Ciphers

PT --- >Meet me at the park

A Keyless cipher is the rail fence cipher.

- **PT written into a table col by col - 2 rows**
  CT created by reading row by row
- **PT written into a table row by row – 2 cols**
  CT created by reading col by col



This creates the CT as "MEMATEAKETETHPR".

Keyless Transposition Ciphers

PT --- >Meet me at the park

A Keyless cipher is the rail fence cipher.

- **PT written into a table col by col - 2 rows**
  CT created by reading row by row
- **PT written into a table row by row – 2 cols**
  CT created by reading col by col

Keyless Transposition Ciphers

Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

Keyless Transposition Ciphers

Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

This creates the CT "MMTAEEHREAEKTTP".

Transposition Ciphers

- Encryption key is (3,2,6,1,5,4)

  What is the Decryption key?

-

Transposition Ciphers

- Encryption key is (3,2,6,1,5,4)

  What is the Decryption key?

- (4,2,1,6,5,3)

- Represent (3,2,6,1,5,4) and its decryption key in matrix form

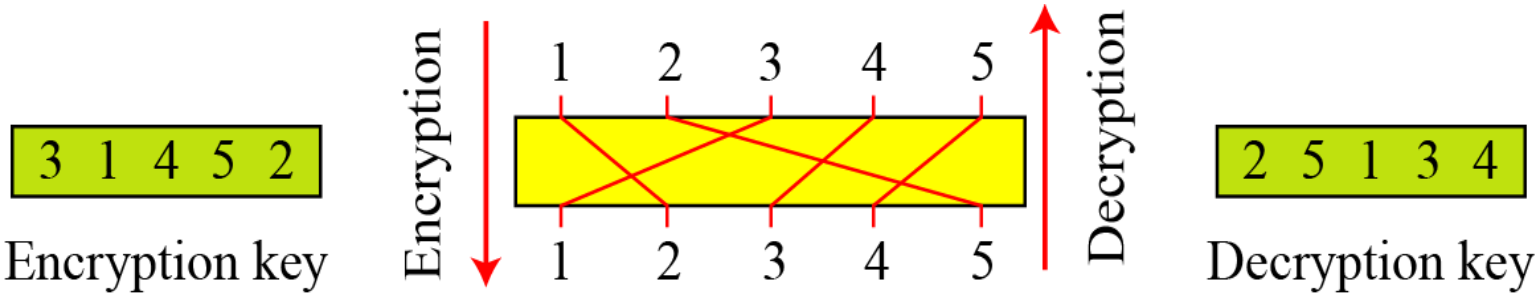
Transposition Ciphers

- Encryption key is (3,2,6,1,5,4)

  What is the Decryption key?

- (4,2,1,6,5,3)

- Represent (3,2,6,1,5,4) and its decryption key in matrix form



Cryptanalysis of Transposition Ciphers

- Statistical attack
- Brute Force attack 26^m ;
- m =5: L = 20
- No of columns = 1/ 20/ 2/4/5/10
- Pattern attack

STREAM AND BLOCK CIPHERS

Symmetric ciphers ---- two broad categories

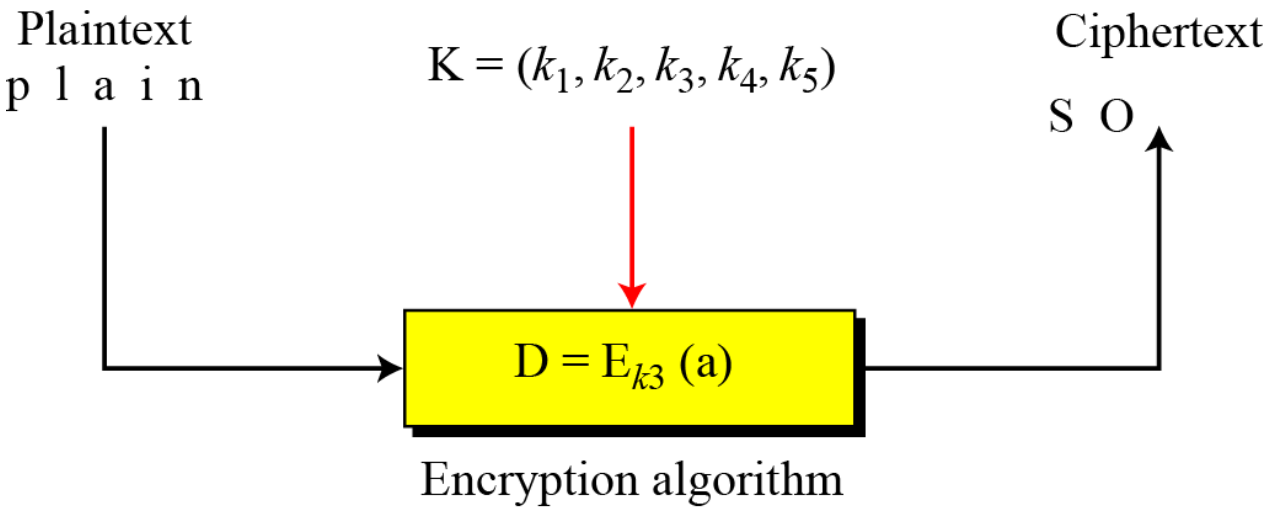
- stream ciphers
- block ciphers.

Stream Ciphers

Let the plaintext stream be P,
the ciphertext stream be C,
and the key stream K.

$P = P_1P_2P_3, \ldots$ $C = C_1C_2C_3, \ldots$ $K = (k_1, k_2, k_3, \ldots)$

$C_1 = E_{k1}(P_1)$ $C_2 = E_{k2}(P_2)$ $C_3 = E_{k3}(P_3) \ldots$



Stream Ciphers

Additive ciphers

- **stream ciphers --- key stream is the repeated value of the key.**
  K = (k, k, …, k).

In this cipher,

- **each CT char depends only on the corresponding PT char**
- **as the key stream is generated independently.**

The monoalphabetic substitution ciphers

- **stream ciphers.**
- **each value of the key stream is the mapping of the current PT char to the corresponding CT char in the mapping table.**

Stream Ciphers

Vigenere ciphers

- **stream ciphers.**
- **the key stream is a repetition of m values, where *m* is the size of the keyword.**

$$K = (k_1, k_2, \ldots k_m, k_1, k_2, \ldots k_m, \ldots)$$

A stream cipher is a monoalphabetic cipher

- **if the value of k_i does not depend on the posn of the PT char**
- **otherwise, the cipher is polyalphabetic.**

Stream Ciphers

- Additive ciphers are definitely monoalphabetic
  because k_i in the key stream is fixed; it does not depend on the position of the character in the plaintext.

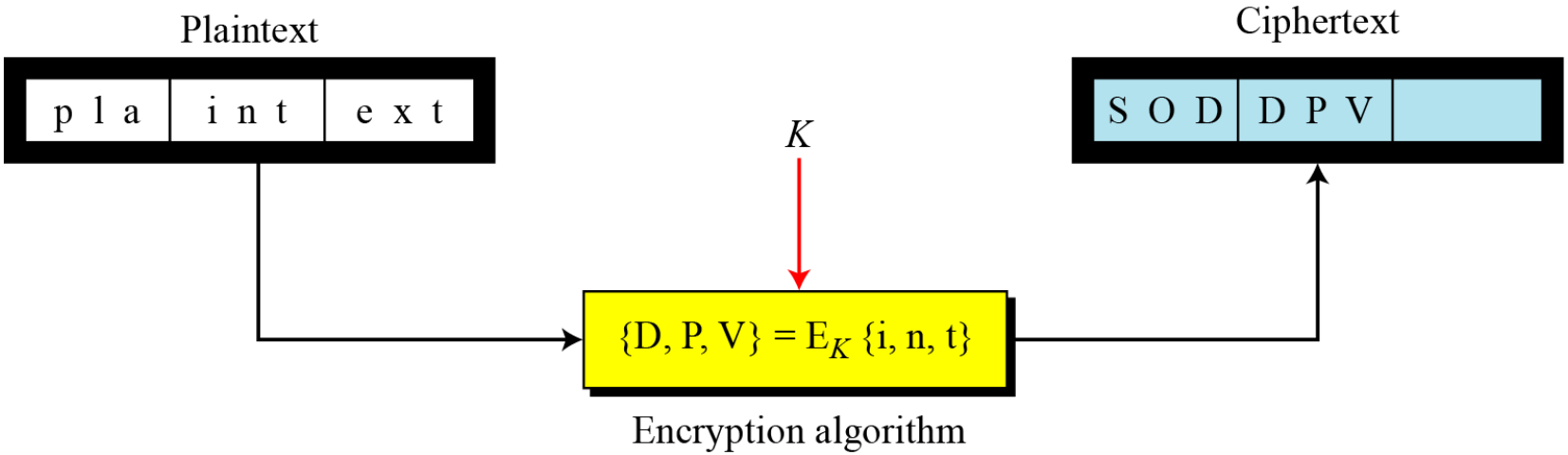
- Monoalphabetic substitution ciphers are monoalphabetic because k_i does not depend on the position of the corresponding character in the plaintext stream; it depends only on the value of the plaintext character.

- Vigenere ciphers are polyalphabetic ciphers
- because k_i definitely depends on the position of the plaintext character. However, the dependency is cyclic. The key is the same for two characters *m* positions apart.

Block Ciphers

In a block cipher,

- **a group of PT symbols of size *m* (*m* > 1) are encrypted together creating a group of CT of the same size.**
- **A single key is used to encrypt the whole block even if the key is made of multiple values.**



Block Ciphers

Playfair ciphers

- **block ciphers.**
- **size of the block is $m = 2$.**
- **Two characters are encrypted together.**

Hill ciphers

- **block ciphers.**
- **A block of plaintext, of size 2 or more is encrypted together using a single key (a matrix).**
- **In these ciphers, the value of each character in the CT depends on all the values of the characters in the PT.**
- **Although the key is made of $m \times m$ values, it is considered as a single key.**

Block Ciphers

Every block cipher

- is a polyalphabetic cipher
- as each character in a CT block depends on all characters in the PT block.

Combination

In practice,

- **blocks of plaintext are encrypted individually**
- **but they use a stream of keys to encrypt the whole message, block by block.**

In other words, the cipher

- **is a block cipher when looking at the individual blocks,**
- **but it is a stream cipher when looking at the whole message considering each block as a single unit.**

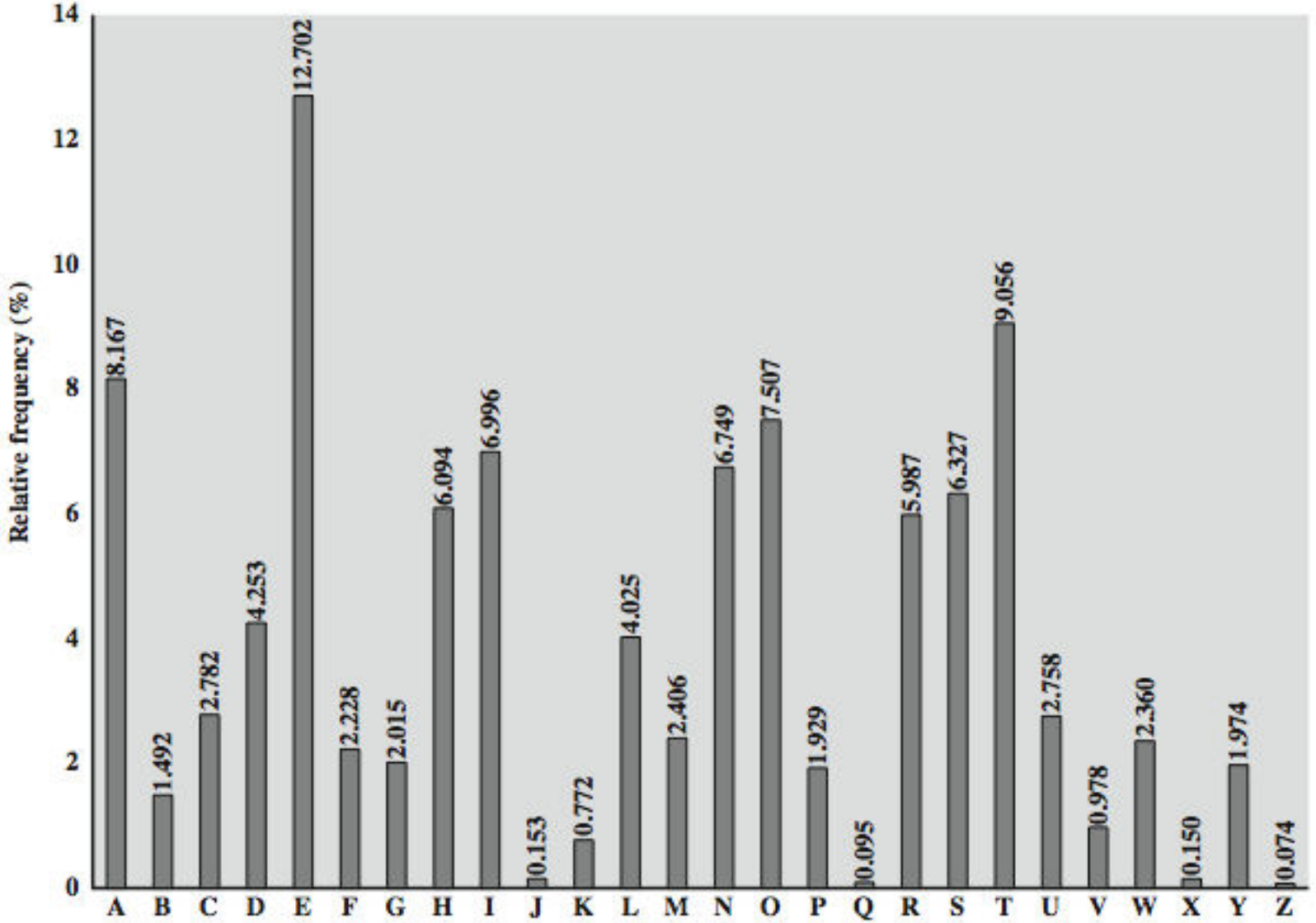
Monoalphabetic Cipher Security

- now have a total of $26! = 4 \times 10^{26}$ keys
- with so many keys, might think is secure
- but would be !!!WRONG!!!
- problem is language characteristics

Language Redundancy and Cryptanalysis

- human languages are redundant
- eg "th lrd s m shphrd shll nt wnt"
- letters are not equally commonly used
- in English E is by far the most common letter
  - followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



Use in Cryptanalysis

- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if caesar cipher look for common peaks/troughs
  - peaks at: A-E-I triple, NO pair, RST triple
  - troughs at: JK, X-Z
- for monoalphabetic must identify each letter
  - tables of common double/triple letters help

Example Cryptanalysis

- given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:

  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 keys in a monoalphabetic cipher provides security
- one approach to improving security was to encrypt multiple letters
- the Playfair Cipher is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- 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

Encrypting and Decrypting

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

Security of Playfair Cipher

- security much improved over monoalphabetic
- since have 26 x 26 = 676 digrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- and correspondingly more ciphertext
- was widely used for many years
  - eg. by US & British military in WW1
- it can be broken, given a few hundred letters
- since still has much of plaintext structure

Polyalphabetic Ciphers

- polyalphabetic substitution ciphers
- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached

Vigenère Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1\ k_2\ \ldots\ k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

Example of Vigenère Cipher

- write the plaintext out
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

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

Aids

- simple aids can assist with en/decryption
- a Saint-Cyr Slide is a simple manual aid
  - a slide with repeated alphabet
  - line up plaintext 'A' with key letter, eg 'C'
  - then read off any mapping for key letter
- can bend round into a cipher disk
- or expand into a Vigenère Tableau

Security of Vigenère Ciphers

- have multiple ciphertext letters for each plaintext letter
- hence letter frequencies are obscured
- but not totally lost
- start with letter frequencies
  - see if look monoalphabetic or not
- if not, then need to determine number of alphabets, since then can attach each

Kasiski Method

- method developed by Babbage / Kasiski
- repetitions in ciphertext give clues to period
- so find same plaintext an exact period apart
- which results in the same ciphertext
- of course, could also be random fluke
- eg repeated "VTW" in previous example
- suggests size of 3 or 9
- then attack each monoalphabetic cipher individually using same techniques as before

Autokey Cipher

- ideally want a key as long as the message
- Vigenère proposed the autokey cipher
- with keyword is prefixed to message as key
- knowing keyword can recover the first few letters
- use these in turn on the rest of the message
- but still have frequency characteristics to attack
- eg. given key *deceptive*

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

Vernam Cipher

- ultimate defense is to use a key as long as the plaintext
- with no statistical relationship to it
- invented by AT&T engineer Gilbert Vernam in 1918
- originally proposed using a very long but eventually repeating key

One-Time Pad

- if a truly random key as long as the message is used, the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for any plaintext & any ciphertext there exists a key mapping one to other
- can only use the key once though
- problems in generation & safe distribution of key

Transposition Ciphers

- now consider classical transposition or permutation ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- can recognise 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 off cipher row by row
- eg. write message 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
```

- giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

Row Transposition Ciphers

- is 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 rows

```
Key: 4312567
Column Out 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
```

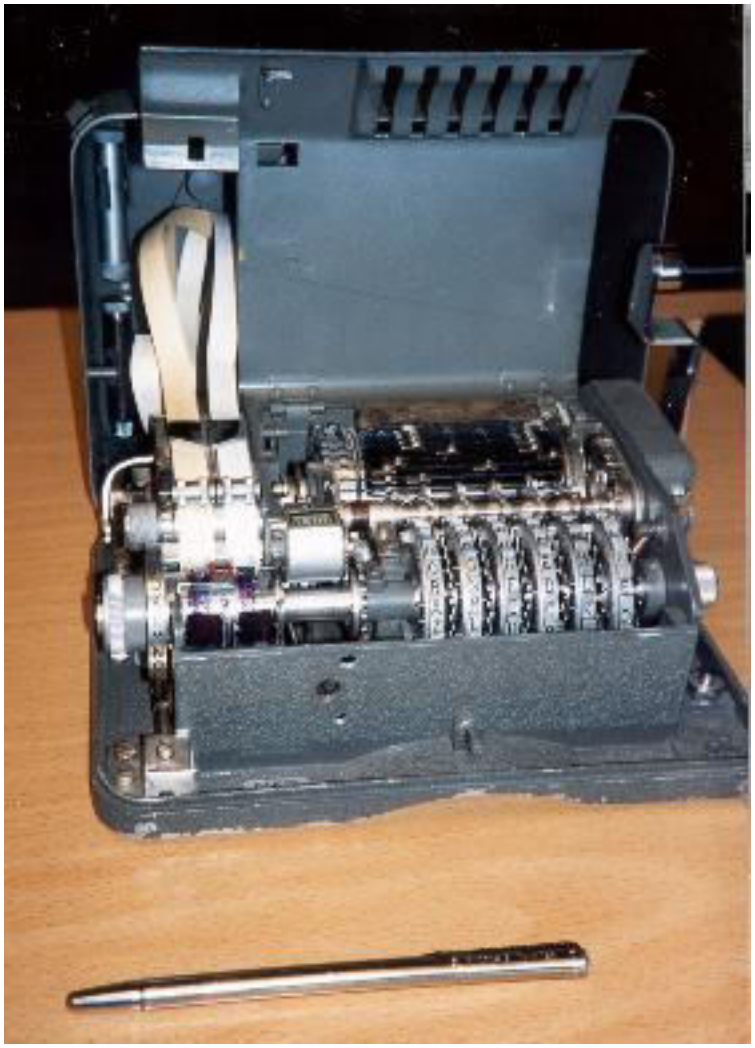
Product Ciphers

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

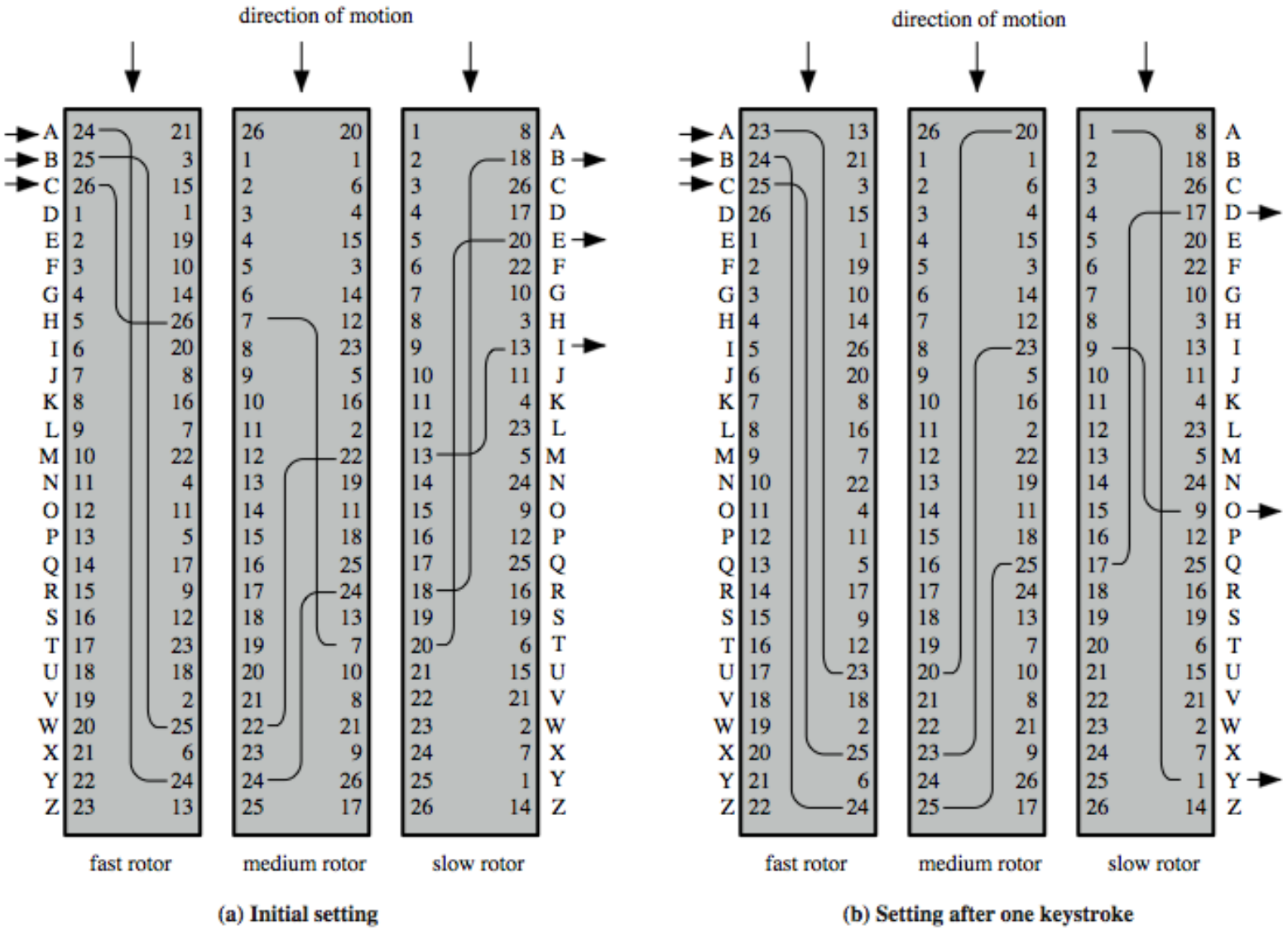
Rotor Machines

- before modern ciphers, rotor machines were most common complex ciphers in use
- widely used in WW2
  - 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

Hagelin Rotor Machine



Rotor Machine Principles



Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- has drawbacks
  - high overhead to hide relatively few info bits
- advantage is can obscure encryption use

Summary

- have considered:
  - classical cipher techniques and terminology
  - monoalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - Playfair cipher
  - polyalphabetic ciphers
  - transposition ciphers
  - product ciphers and rotor machines
  - stenography

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a brute force search
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"