Chapter - 2

A classical Encryption Techniques

Outline

- Introduction
- Symmetric Cipher Model
- Symmetric Cipher Attacks
- Substitution techniques
- Transposition techniques
- Rotor Machine
- Steganography

1. Introduction

- Human beings from ages had inherent of two needs

  (a) To communicate and share information

  (b) To communicate selectively
- These needs gave rise to art of coding message in such a way that only intended people could have access to the information.
- And unauthorized people couldn’t extract any information even if the scrambled messages fell in their hand.
- The art and science of concealing(hiding) messages to introduce secrecy in information security is recognized as ***Cryptography***
- Cryptography was coined by combining two Greek words,

  ‘krypto’ = crypto - *hide/secret*

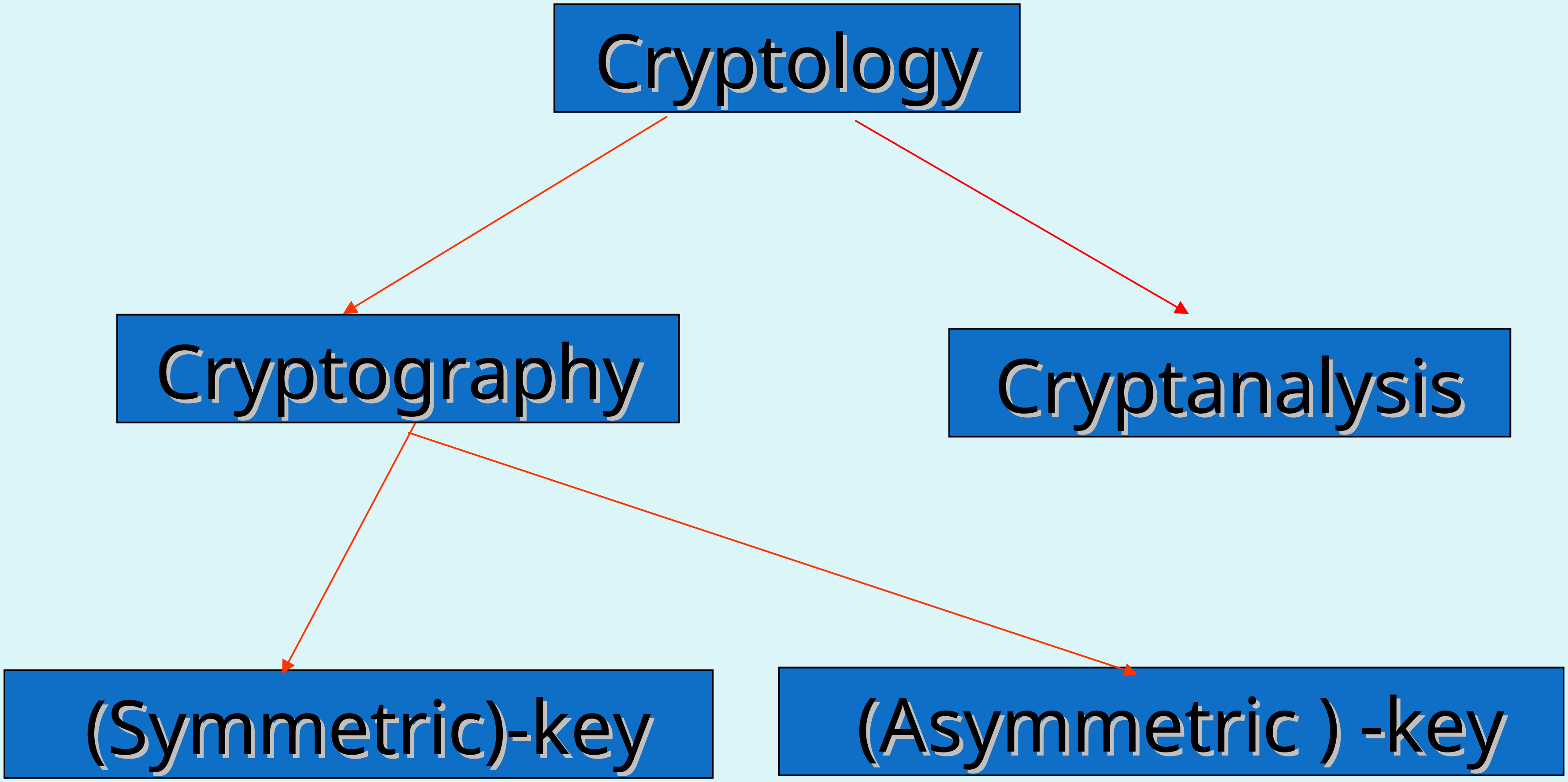
  ‘graphene’ = graphy - *writing*

Cont . . .

- ***Cryptographic System/Cipher*** - also called cryptosystem is refers to various schemes used for data encryption and decryption.
- ***Cryptology*** – The study of cryptosystem/cipher

  Field of both Cryptography and Cryptanalysis
- **Cryptography** – making cryptosystem
  - The art and science of making a cryptosystem that is capable of providing information security.
  - Deal with the actual securing of digital data
  - Refers to design of mechanisms based on mathematical algorithms

Cont . . .



Cryptology

Cryptography

Cryptanalysis

(Symmetric)-key

(Asymmetric) -key

Components of Cryptosystem

- ***Plaintext:***
  - Data to be protected during transmission
  - Original intelligible message/data that is fed into the algorithm as input.
- ***Encryption algorithms:***
  - Mathematical process that produces cipher text for any given plaintext and encryption key.
  - Input = plaintext + Secret key , Output = Cipher text
  - Perform various transformation/substitutions on the plaintext to transform plaintext to cipher text.
- ***Secret Key/Encryption key:***
  - Information used in cipher known only to sender/receiver
  - INPUT -----> Encryption algorithm

Cont . . .

- ***Cipher text:***
  - The Scrambled/coded version of message/plaintext produced as output.
  - It depends on plaintext and secret key, for given message two different keys will produce two different cipher text.
- ***Encipher (Encryption):-*** Converting plaintext to cipher text
- ***Decipher (Decryption):-*** Recovering plaintext from cipher text
- ***Decryption algorithms:***
  - Transform cipher text to plain text
  - Mathematical process, that produces a unique plaintext for a given cipher text and decryption key.
- ***Decryption key:*** value known by receiver and related to encryption key.

Cont . . .

Type of Cryptographic System/Cipher

(1) **The type of operations used for transforming plaintext to cipher text.**

- Substitution: in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and
- Transposition: in which elements in the plaintext are rearranged.

(2) **The number of keys used**

- If both receiver and sender use the same key, the system is referred to as Symmetric/single-key/secret-key. But If the receiver and sender use different keys, the system is referred to as Asymmetric, two-key/public-key encryption.

(3) **The way in which the plaintext is processed.**

- Block cipher: processes the input one block of elements at a time, producing an output block for each input block.
- Stream cipher: processes the input elements continuously, producing output one element at a time, as it goes along.

Cont . . .

Security service of Cryptography

- ***Confidentiality:-*** Keep information privacy or secrecy
    - Achieved by physical securing or by use of mathematical algorithms
- ***Data integrity:-*** Identifying any alteration of data and
    - Confirm whether data is intact or not, since it was last created, transmitted, or stored by authorized person
    - Cannot prevent alteration of data, only provides means of detection
- ***Authentication:-*** Provides the identification of the originator
    - Confirms to receiver, data received has been sent only by verified sender
    - It has two variants; *Message authentication and Entity authentication*
- ***Non repudiation***
    - Assure that the original creator of data cannot deny the creation or transmission of the said data to a recipient or third party

2. Symmetric Cipher Mode

- Also referred to as conventional encryption or single-key encryption.
- The only type of encryption in use prior to the development of modern encryption (1970’s).

Requirements for secure use of conventional encryption

(1) Strong encryption algorithm.

- The opponent should be unable to decrypt cipher text or discover the key even if he/she is in possession of a number of cipher texts together with the plaintext that produced each cipher text.

(2) Exchange of secret key securely

- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Cont . . .

Key management

(1) Using secret channel (2) Encrypt the key

(3) Third trusted party (4) Sender and Receiver

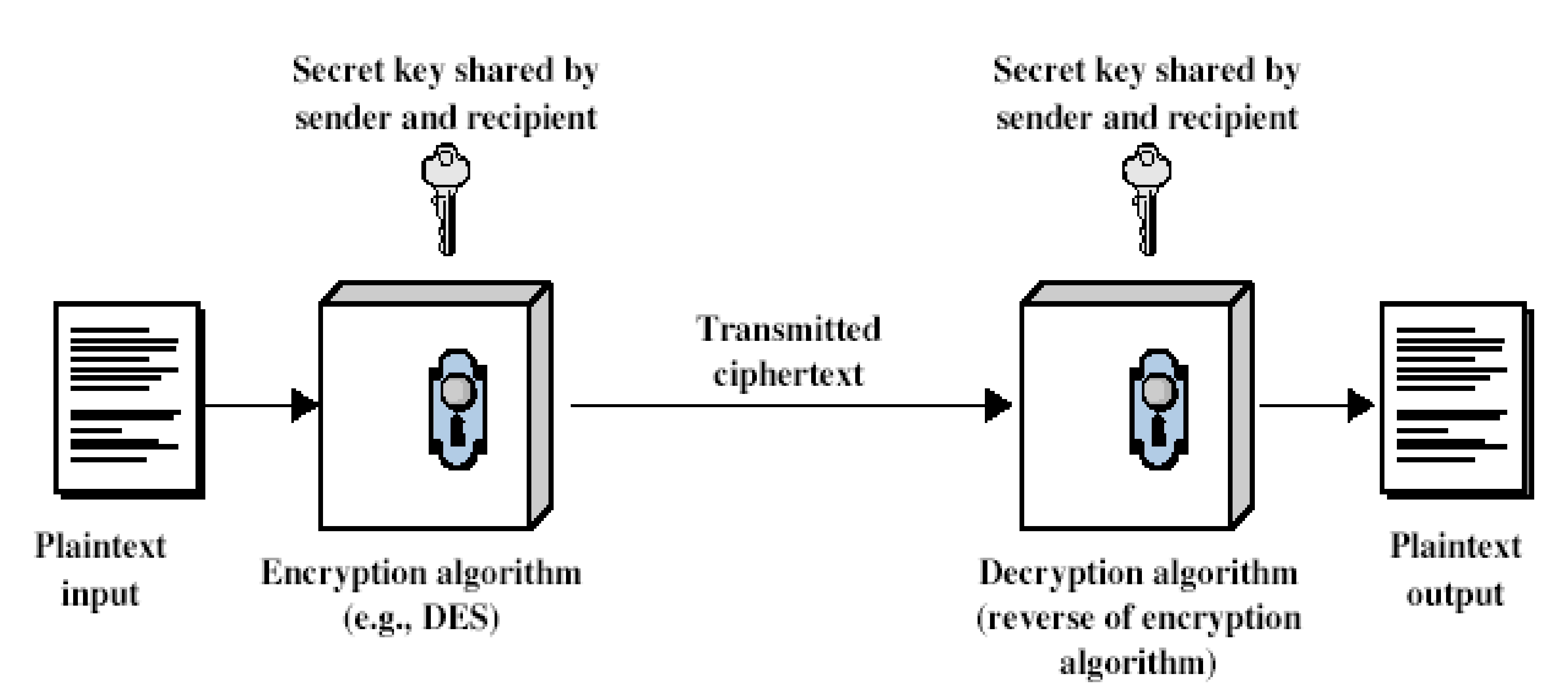

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig 2.1: Simplified Model of Symmetric Encryption

Cont . . .

Features of Symmetric encryption

- Participants needs to share a common key prior to exchange of information
- Keys are recommended to be changed on regular bases to prevent attack.
- Only secret key is kept secure and no need to keep the algorithms secret,
  - It is impractical to decrypt message on the basis of cipher text plus knowledge of encryption/decryption algorithms.
  - This allows manufacturers to developed low-cost chip implementations of data encryption algorithms.
  - Result in widespread uses
- Faster encryption-decryption process as a result of smaller length of key.
- In group of *n* people, to enable two party communication b/n any two persons , *n*(n - 1)/2* number of keys are required for the group.
- ***Problem:-*** maintaining the **secrecy of the key** and **Trust issues**

Cont . . .

Example: Assume sender produces a message in plaintext, X = [x_1, x_2, ... x_m]. The *M* elements of *X* are letters in some finite alphabet (Traditionally consisted of 26 capital letters and Nowadays consist binary alphabet [0,1]).

- For encryption, a key of the form K = [k_1, k_2, ... k_j] is generated and provided to destination by means of some secure channel or a third party.
- With the message X and the encryption key k as input, the encryption algorithm forms the cipher text and We can write this as

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

- Notation indicates that Y is produced by using encryption algorithm E as a function of plaintext, with specific function determined by the value of the key
- Intended receiver, in possession of the key, is able to invert transformation:

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

- An opponent, observing *Y* but not having access to *K or Y*, may attempt to recover *K or Y* or both *K and Y.*

Cont . . .

- It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms and the opponent is interested in:
  - Only the particular message, then the focus of the effort is to recover X by generating a pla$\hat{K}$ntext estimate
  - However, if being able to read future messages as well, an attempt is made to recover K by gener$\hat{X}$ing an estimate .

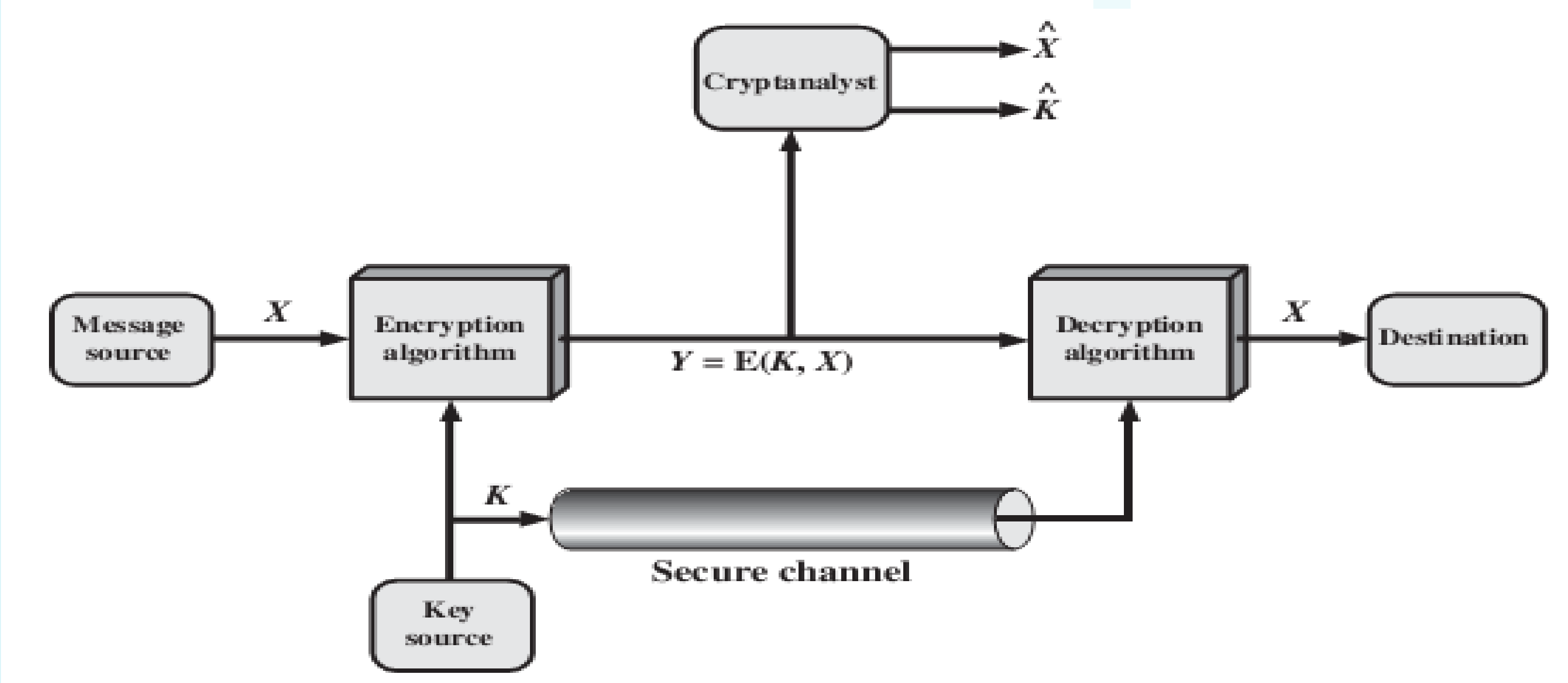
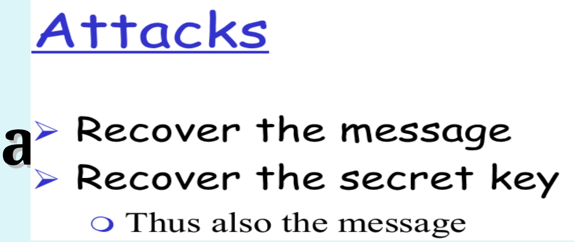


Fig 2.2: Model of Symmetric Cryptosystem

3. Symmetric Cipher Attacks

- Objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.



Attacks

- Recover the message
- Recover the secret key
  - Thus also the message

Conventional encryption Attack approa

- ***Cryptanalysis:***
  - Rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs.
  - Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
  - There are various kind of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

    - Ciphertext only
    - Chosen plaintext
    - Chosen text
    - Known plaintext
    - Chosen ciphertext

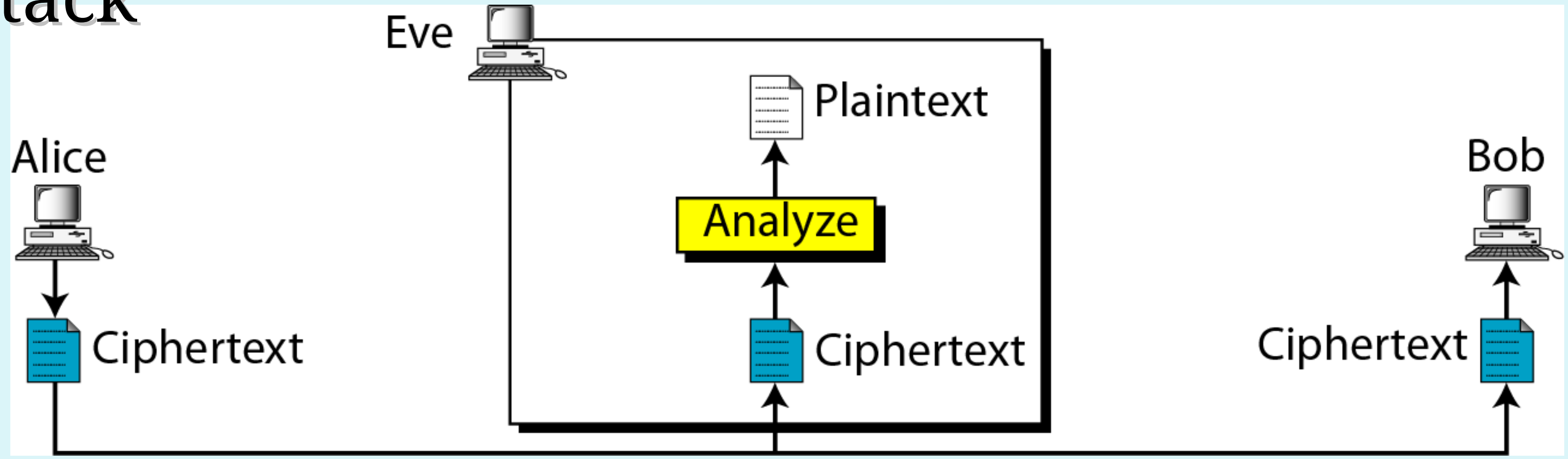
Cont . . .

- **Ciphertext only**
  - Only ciphertext and encryption algorithm (not always).
  - Opponent must have some general idea of the type of plaintext such as English or French text, an EXE file, a Java source listing etc.
  - Opponents use statistical tests or brute force attack
  - Easiest to defend against
- **Known plaintext**
  - Information known by the opponent are:
    - Plaintext and encryption algorithm
    - One or more plaintext-ciphertext pairs.
  - Analyst may be able to deduce the secret key on the basis of the way in which known plaintext is transformed.

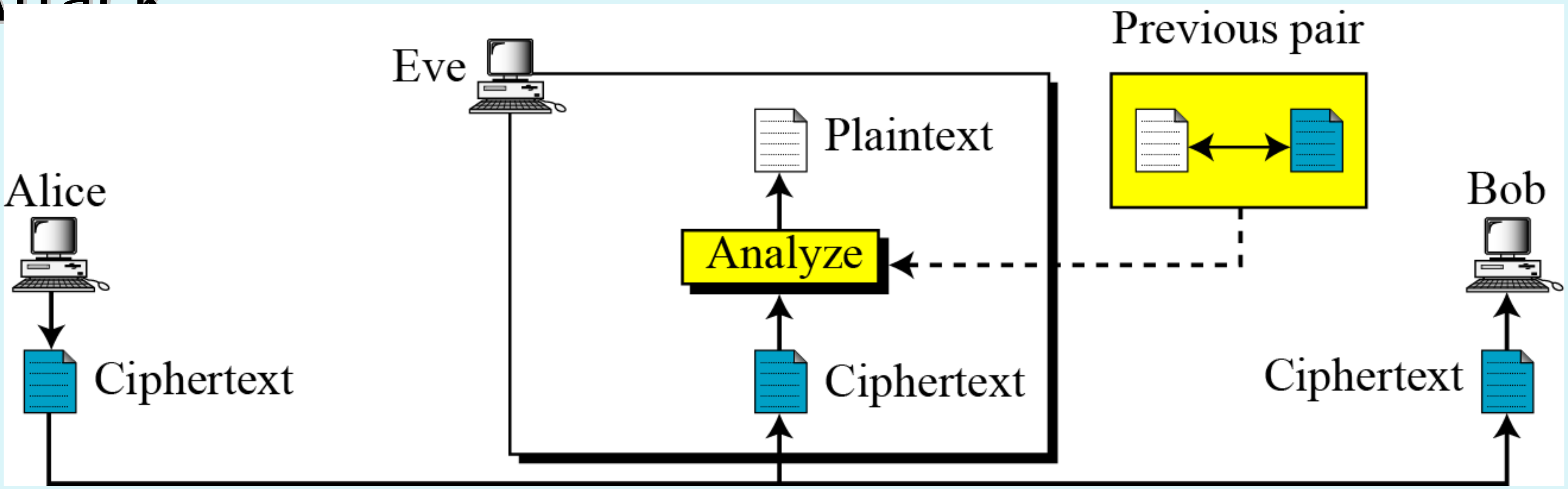
Cont . . .

- **Chosen plaintext**
  - What known by opponents are ciphertext, encryption algorithm, and plaintext message chosen by cryptanalysts, together with its corresponding ciphertext generated with the secret key.
  - E.g., if an entire accounting file is being transmitted, opponent may know the placement of certain key words in the header of the file.
- **Chosen ciphertext**
  - What known by opponents are ciphertext, encryption algorithm, and ciphertext chosen by cryptanalysts, together with its corresponding decrypted plaintext generated with the secret key.
- **Chosen text**
  - Use the combination of both chosen plaintext and chosen ciphertext
  - Less commonly employed as cryptanalytic techniques

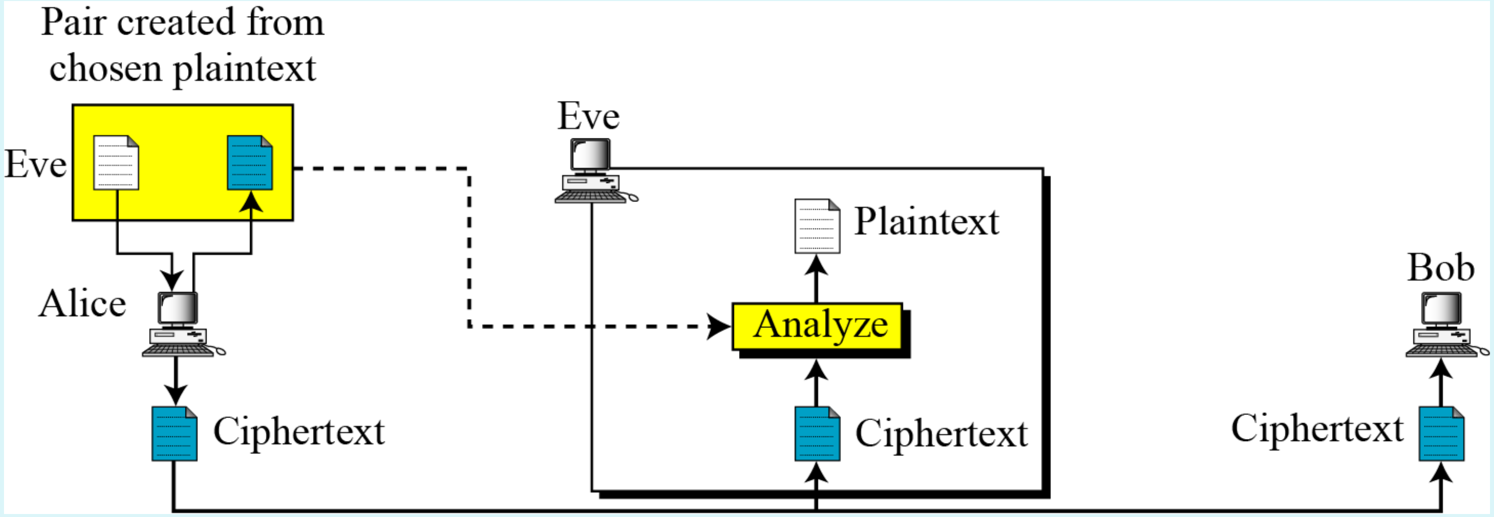
Ciphertext-Only Attack



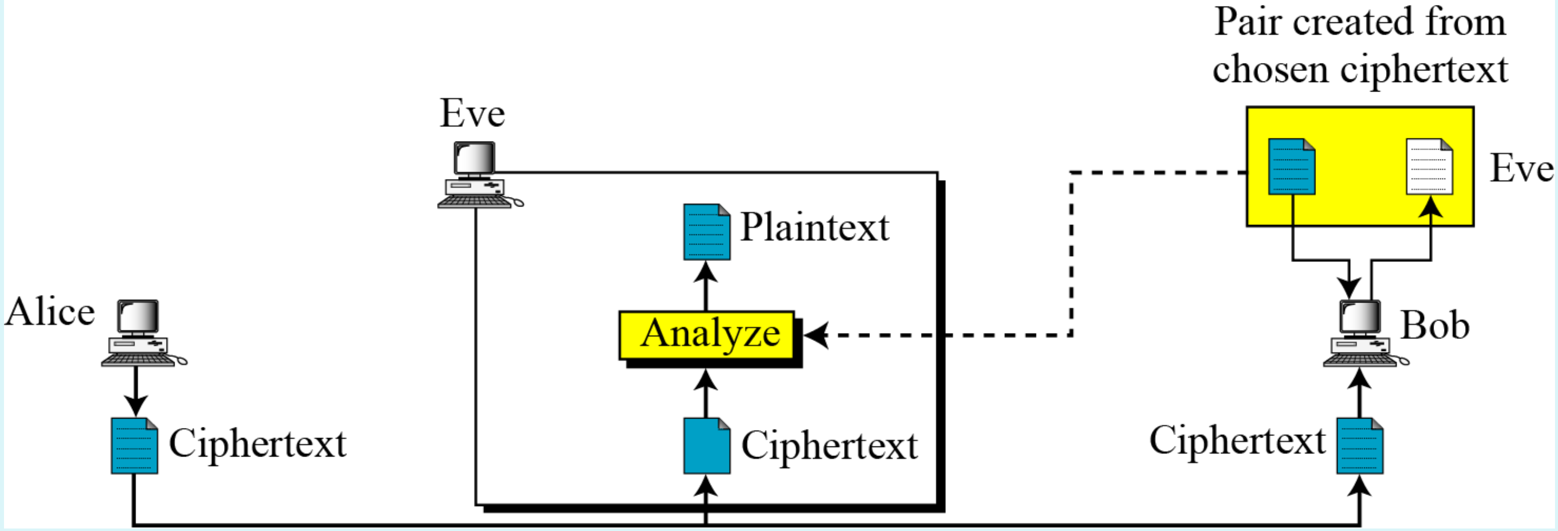
Known-Plaintext Attack



Chosen plaintext Attack



Chosen Ciphertext Attack



Cont . . .

DES – 56 bits key size
AES – 128 bits key size

- ***Brute-force attack:***
  - Involves trying every possible 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.
  - Most basic attack, proportional to key size

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
26 characters (permutatio	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^{6} years

Table 2.1 Average Time Required for Exhaustive Key Search

Secure encryption

- In general, a security definition has two components: a security guarantee and a threat model.

Security guarantee

- *Defines what the scheme is intended to prevent the attacker from doing, (or, from attacker's point of view, what constitutes a successful attack on the scheme).*
- *The encryption scheme have to be enough secure*

Threat model

- *Describes the power of the adversary, i.e., what actions the attacker is assumed able to carry out.*

Cont . ...

What should a secure encryption scheme guarantee?

- A secure encryption scheme should be grantee that it should be impossible for an attacker

1. **To recover the key** - *Not sufficient for security*
2. **To recover the entire plaintext from the ciphertext**
   - ❖ *A better definition, but is still far from satisfactory*
3. **To recover any character of the plaintext from the ciphertext.**
   - ❖ *looks like a good definition, yet is still not sufficient*

Cont. . .

- All the above three are not satisfactory.
- The “right” answer is regardless of any information an attacker already has, a ciphertext should leak no additional information about the underlying plaintext.
- This informal definition captures all the concerns outlined above.
- Note in particular that it does not try to define what information about the plaintext is “meaningful”; it simply requires that no information be leaked.
- This is important, as it means that a secure encryption scheme is suitable for all potential applications in which secrecy is required.
  - ***Unconditionally secure***
  - ***Computational secure***

Cont. . .

Unconditionally secure

- Ciphertext doesn’t contain enough information to determine uniquely the corresponding plaintext.
- No matter how much ciphertext is available and how much time or computational power (processor) an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there.
- Only a scheme known as the one-time pad is unconditionally secure

Cont . . .

- **Computational secure**
  - All users of an encryption algorithm striving/looking for an algorithm that meets one or both of the following criteria:
    - ✓ *Cost of breaking the cipher exceeds value of encrypted info.*
    - ✓ *Time required to break cipher exceeds the useful lifetime of the information.*
  - An encryption scheme is said to be computationally secure if either of the foregoing two criteria are met.

Notes:

- All forms of cryptanalysis for symmetric encryption schemes are designed to exploit the fact that traces of structure or pattern in the plaintext may *survive encryption* and be *discernible in the ciphertext*.

4. Substitution Techniques

- Technique in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher-text bit patterns.
- Form the first of the fundamental building blocks

(1) Caesar Cipher

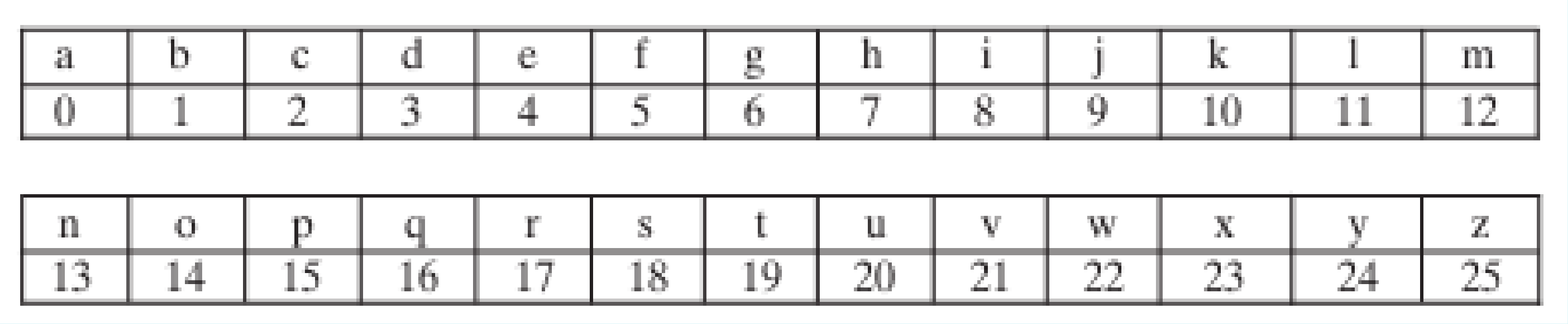
- Earliest known substitution cipher, by Julius Caesar and First attested use in military affairs, in Greeks
- Additive cipher - Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Example:

Plain-Text :	meet	me	after	the	toga	party
Cipher-Text:	PHHW	PH	DIWHU	WKH	WRJD	SDUWB

Cont . . .

Caesar Cipher

- Let us mathematically to give a number for each letter



a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Then the algorithm can be expressed as, for each plaintext *p* letter , substitute the cipher-text letter *c.*

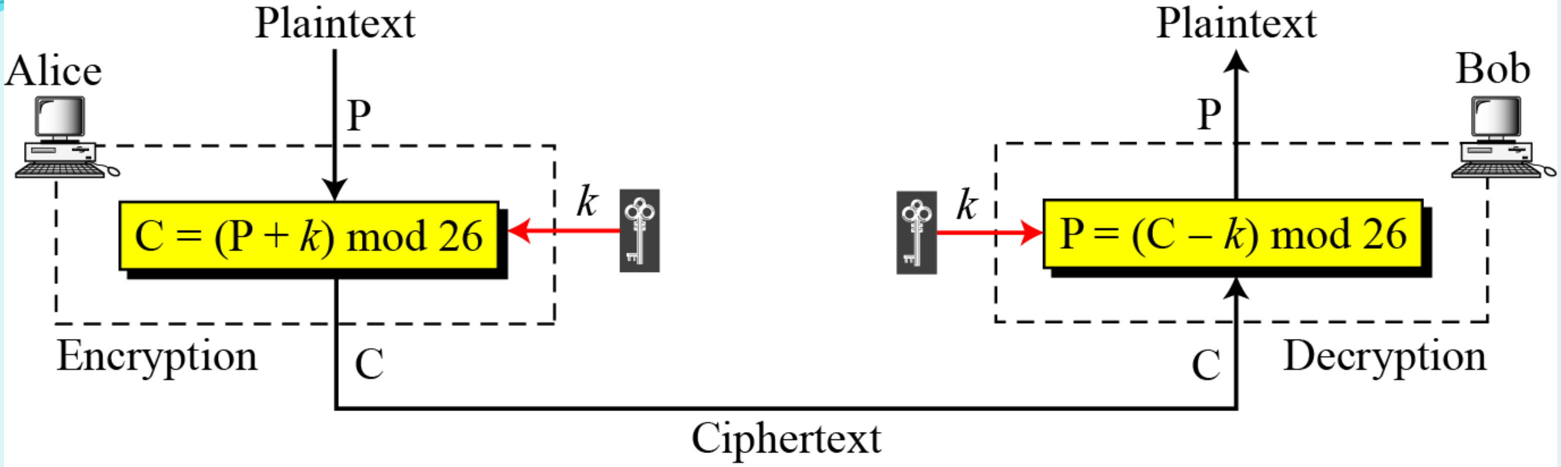
$$c = E(3, p) = (p + 3) \bmod 26$$

- A shift may be of any amount, so that the general Caesar algorithm is:

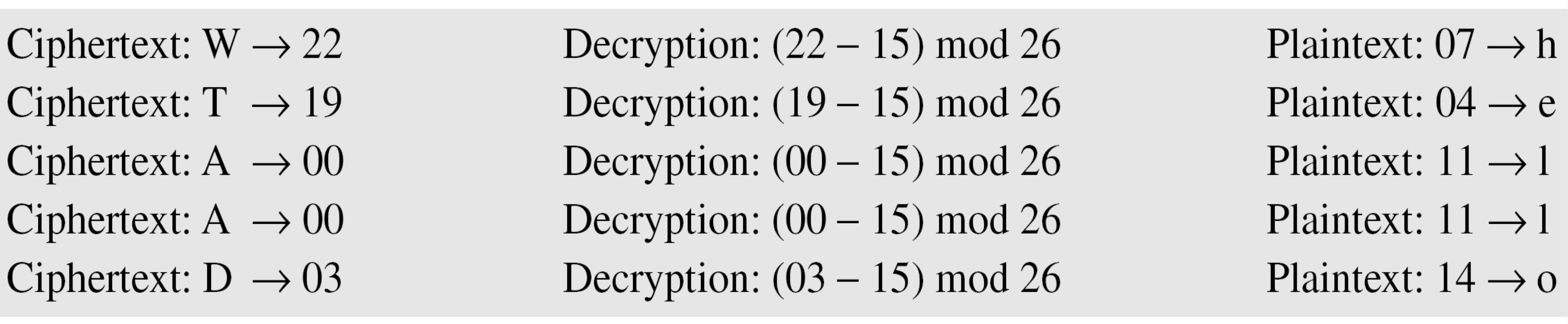
$$c = E(p) = (p + k) \bmod (26)$$

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

Cont . . .



- **Exercise:** *Use the additive cipher with key = 15 to decrypt the message “WTAAD”.*
- **Solution:-** *We apply decryption algorithm to the plaintext character by character:*



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

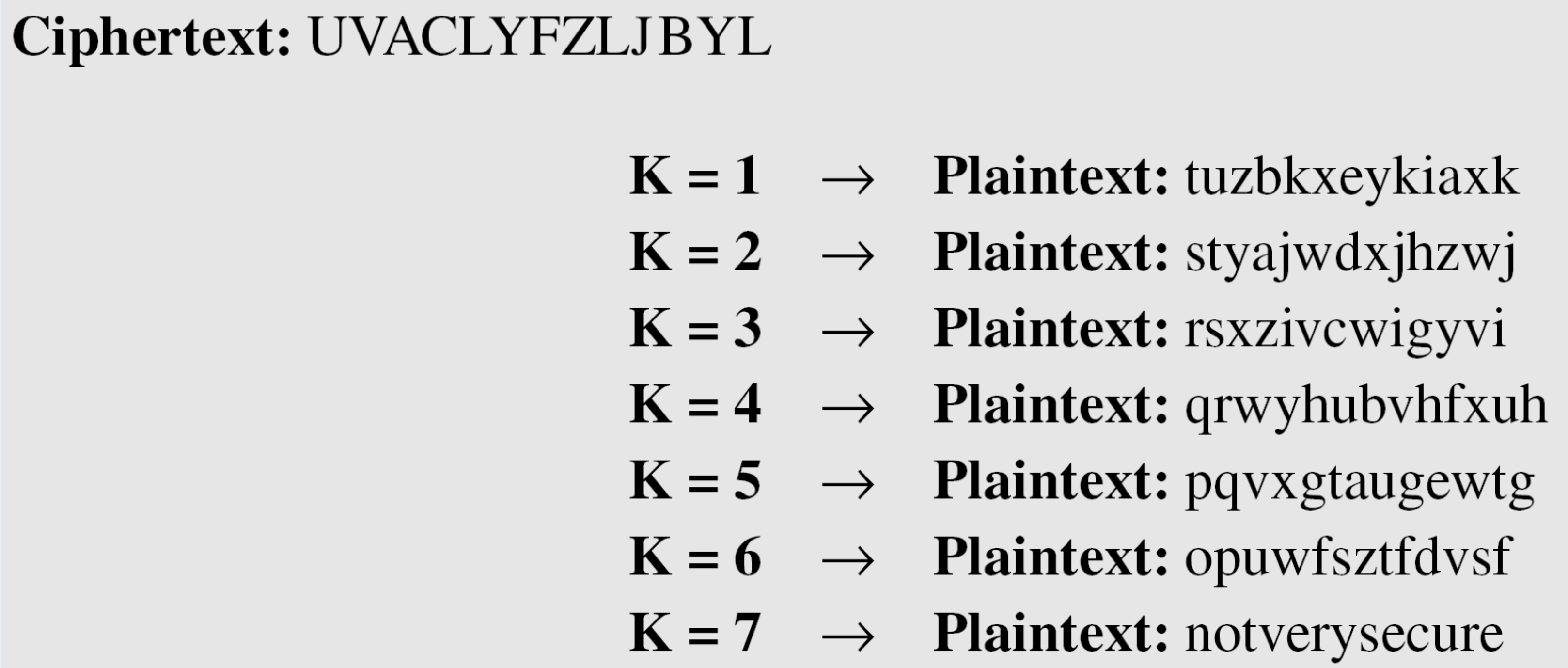
Cont . . .

Cryptanalysis of Caesar Cipher

- A brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.
- The characteristics of this problem enabled us to use a brute-force
  - The encryption & decryption algorithms are known.
  - There are only 25 keys to try, so given ciphertext, just try all shifts of letters
  - The language of plaintext is known and easily recognizable.
- **Example:**
  - Eve has intercepted the ciphertext “UVACLYFZLJBYL”.
  - See on next slide how she can use a brute-force attack to break the cipher.

Cont . . .

Example of Brute-Force Cryptanalysis of Caesar Cipher



Ciphertext: UVACLYFZLJBYL

K = 1 → **Plaintext:** tuzbkxeykiaxk

K = 2 → **Plaintext:** styajwdxjhzwj

K = 3 → **Plaintext:** rsxzivcwigyvi

K = 4 → **Plaintext:** qrwyhubvhfxuh

K = 5 → **Plaintext:** pqvxgtaugewtg

K = 6 → **Plaintext:** opuwfsztfdvsf

K = 7 → **Plaintext:** notverysecure

Exercise: break a ciphertext beloew

"GCUA VQ DTGCM"

Cont . . .

(2) Mono alphabetic Ciphers

- This is also additive cipher
- Rather than just shifting the alphabet, could shuffle (jumble) the letters arbitrarily .
- Each plaintext letter maps to a different random cipher text letter
- Arbitrary substitution dramatically increase the key space, where the translation alphabet can be any permutation of the 26 alphabetic characters.
- ***A permutation*** of a finite set of elements *S* is an ordered sequence of all the elements of *S*, with each element appearing exactly once.
- For example, if *S* = *{a,b,c}*, there are six permutations of *S*:

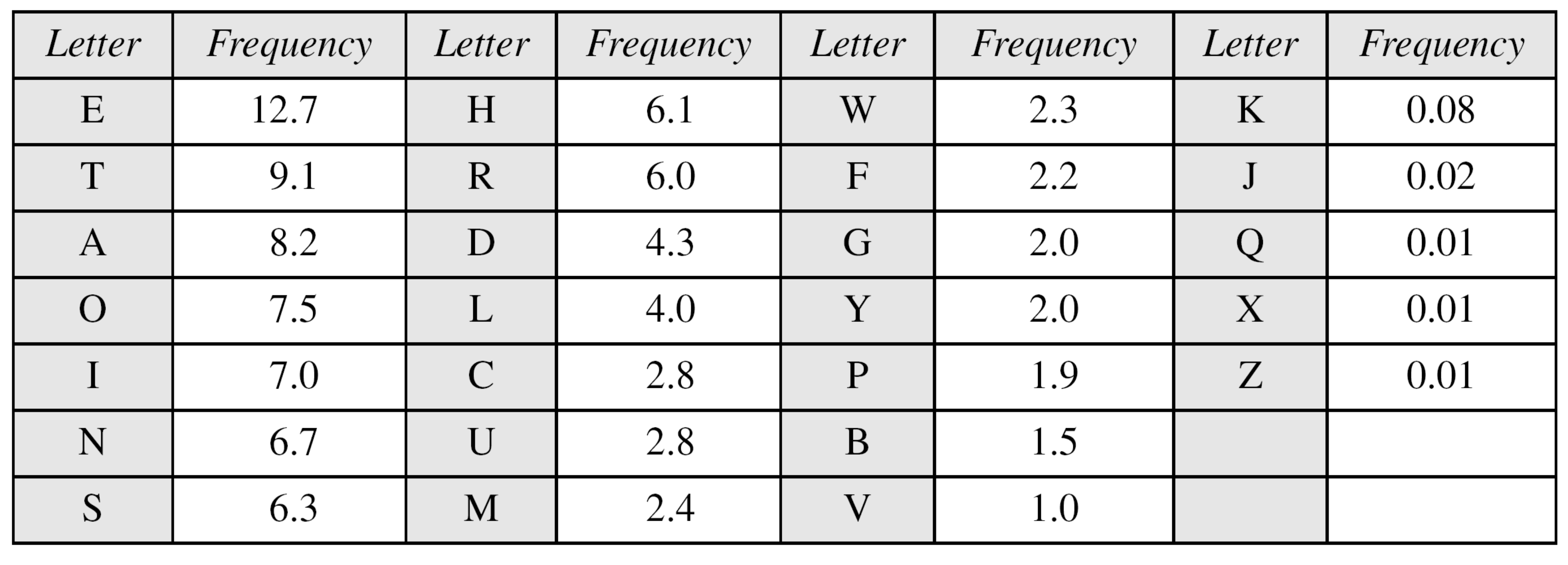
abc, bca, cab, acb, bac, cba

Cont . . .

- The “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 x 10^{26} possible keys.
- *Advantage:* Avoid brute force attack
- *Problem:* Nature of Language/characteristics
  - Human languages are **redundant**. e.g. "th lrd s m shphrd 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 and other letters like Z, J, K, Q, X are fairly rare
  - Have tables of single, double & triple letter frequencies for various languages

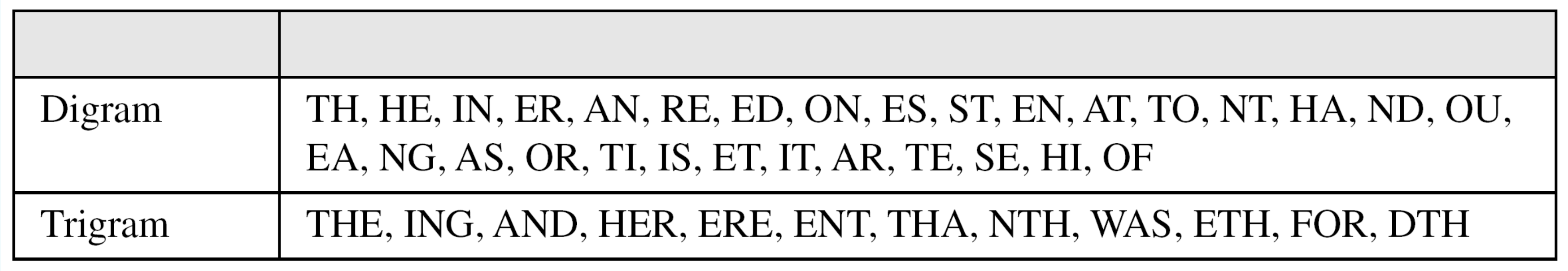
Cont . . .

Frequency of characters in English



Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Frequency of diagrams and trigrams



Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Cont . . .

- **Example 2:** *Decryption using frequency of letter*

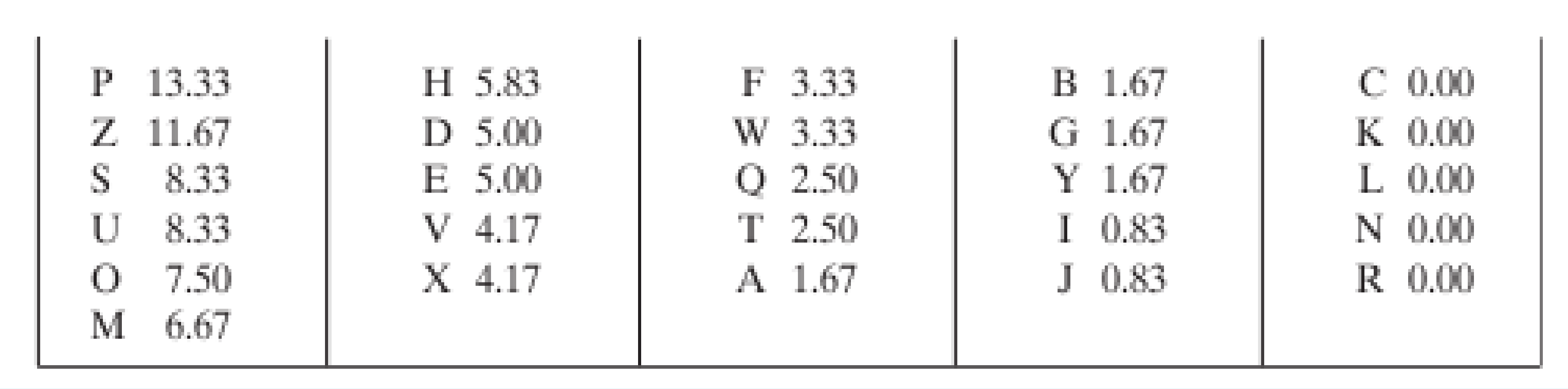
  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDB

  METSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZ

  WYMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZH

  MDJUDTMOHMQ

- Relative frequencies of the letters in the ciphertext (in %) are as follows

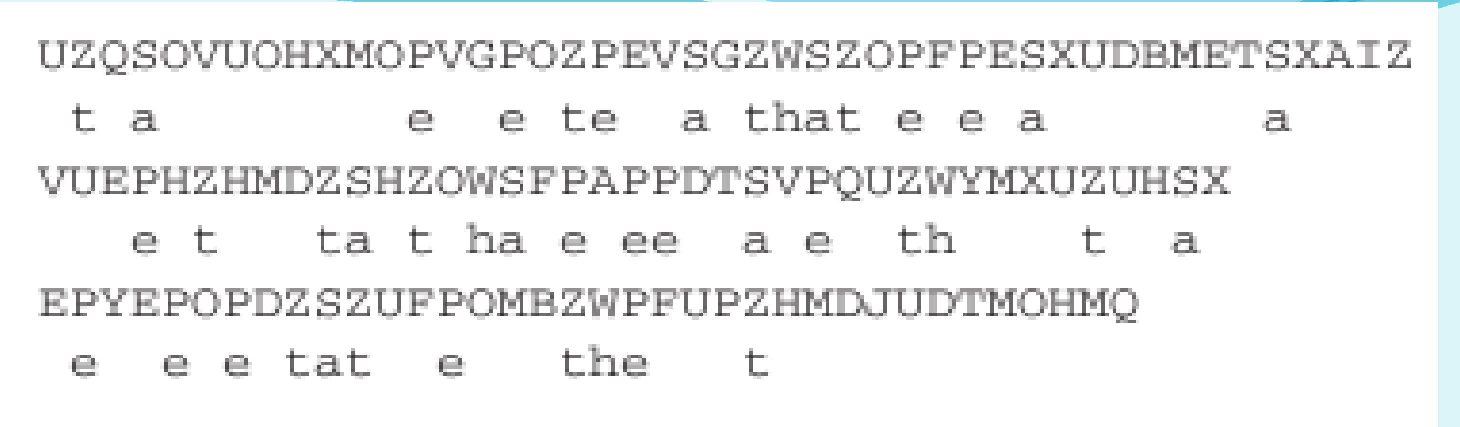


P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

Cont . . .

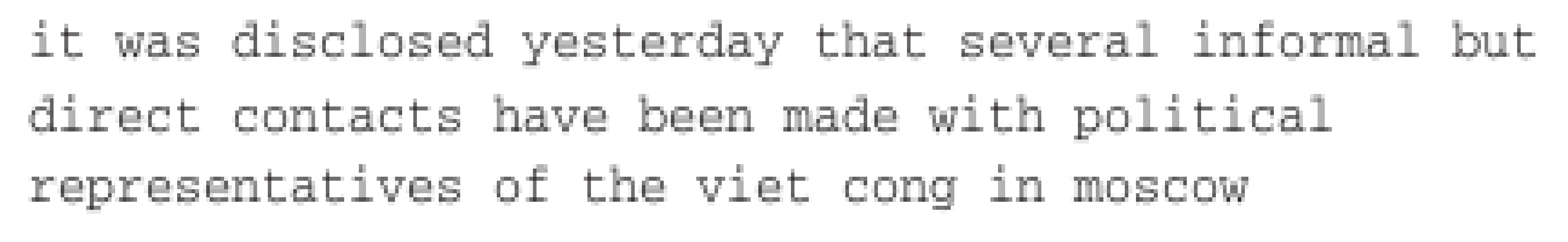
- Comparing this breakdown with English letter frequencies, it seems likely,
  - *Cipher letters P and Z are equivalents of plain letters e and t, but it is not certain.*
- The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}.
- The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.
- Make some tentative assignments and start to fill in the plaintext to see if it looks like a reasonable “skeleton” of a message.

Cont . . .



```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

- Continued analysis of frequencies plus trial and error should easily yield a solution from this point.



```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

- **Exercise:** Eve has intercepted the following ciphertext. Using a statistical attack, show how it find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Cont . . .

(3) Playfair Ciphers/ Playfair Square

- Not even the large number of keys in a monoalphabetic cipher provides security
- In case of just mapping one letter always to another, the frequency distribution is just shuffled.
- One approach to improve security is to encrypt multiple letters
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.
- A manual symmetric encryption technique and was the first literal digraph substitution cipher but regarded as insecure now a days.
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- *Based on use of 5×5 matrix of letters constructed using a keyword.*

Playfair Encryption Rules

Rule 1: Construction of 5x5 matrix with secret key

1. Chose a key consisting of a string of unique characters
2. Build 5x5 table beginning with key followed by remaining alphabet

   - *The rules for filling in 5x5 matrix are: Left to Right, Top to Bottom, first with keyword after duplicate letters have been removed, and then with the remain letters, with I/J used as a single letter.*

- *Example:*

  Using a key string “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

Cont . . .

Rule 2: Encryption of plaintext

- Encrypt two letters of the plaintext at a time by the following rules

1. Remove any punctuation and numbers in the plaintetx .
2. Identify any *consecutive double letters* in plaintext and replace the second occurrence with X', e.g. 'hammer' ----> 'hamxer' and "balloon" becomes "balxoxn".
3. If plaintext has an odd number of characters append 'x' to the end to make it even e.g. "balxoxn" --> "balxoxnx" .
4. Break the plaintext into pairs of letters e.g. 'hamxer' --> 'ha mx er' and "balxoxn" --> "ba lx ox nx" .
5. Locate the letters in the key square

Cont . . .

7. If both letters fall in the same row, replace each with letter to their immediate right respectively (wrapping back to start from end).
8. If both letters fall in the same column, replace each with the letter immediately below it (again wrapping to top from bottom).
   - *The "belowness" property is to be considered circular, in the sense that the topmost entry in a column is below the bottom-most entry.*
9. Otherwise (letters found in different rows and columns) each letter is replaced by the letter in the same row which found in the column of the other letter of the pair. The order is important (the first encrypted letter of the pair is the one that lies on the same row as the first plaintext).

Cont . . .

Example: Encrypt the plaintext “**Playfair ciphers are block ciphers**” using the keyword MO NA RC HY

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

PL AY FA IR CI PH ER SA RE BL OC KC IP HE RS

- Rule 2: “PL" encrypts as “QP"
- Rule 4: “AY" encrypts to “NB", and “FA" to “IO" or "JO“, and “IR -----> KA” and “CI -----> BE”
- Rule 3: “PH" encrypts to “VF“
- Do in the same way for the rest pair of letters

Playfair Decryption Rules

Rule 1: Construction of 5x5 matrix with secret key

1. Chose a key consisting of a string of unique characters
2. Build 5x5 table beginning with key followed by remaining alphabet

- *The rules for filling in 5x5 matrix are: Right to Left, Bottom to Top, first with keyword after duplicate letters have been removed, and then with the remain letters, with I/J used as a single letter.*

- *Example:*

Using a key string “MONARCHY”

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

Cont . . .

Rule 2: Decryption of plaintext

- Encrypt two letters of the plaintext at a time by the following rules

1. Break the ciphertext into pairs of letters e.g. 'HEGHERDRY' --> "HE GH ER DR YN" .
2. Locate the letters in the key square
3. If both letters fall in the same row, replace each with letter to their immediate right respectively (wrapping back to start from end).
4. If both letters fall in the same column, replace each with the letter immediately below it (again wrapping to top from bottom).
5. Otherwise (letters found in different rows and columns) each letter is replaced by the letter in the same row which found in the column of the other letter of the pair. The order is important

Cont . . .

Generally:

- Used in WW1 and WW2
- Security much improved over monoalphabetic
- Since have 26 x 26 = 676 digrams
- Would need a 676 entry frequency table to analyse and correspondingly more ciphertext
- Was widely used for many years

  e.g. by Austrialians, US & British military in WW1, WW2
- It **can** be broken, given a few hundred letters
- Since still has much of plaintext structure

Prons

- Harder to crack. In this method, it breaks the usual rules of letters arranging to form a word, like ‘th’, ‘ph’,’ea’ a letters that are always together, but playfair separated them to other irrelevant-look letters that are not so easy to observe.
- The simplicity and reliability of this primitive code-cracking method made it extremely popular on the battlefield.
- It doesn’t contain any complex mathematic or number theory.

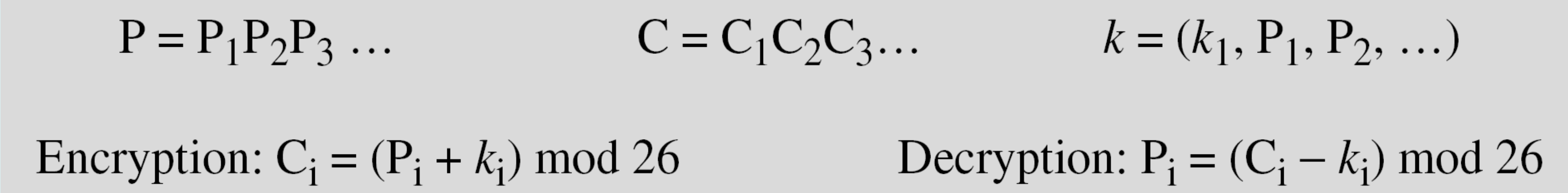
Cons

- The frequency analysis of digraphs can be undertaken
- Like most pre-modern era ciphers, the Playfair cipher can be easily cracked if there is enough text.
- Nowadays, with the proper software, you could use a computer to discover the original text without knowing the cipher key. Some skilled cryptographists and puzzle experts can even break it with nothing more than pen and paper.

Cont . . .

(4) Polyalphabetic Ciphers

- In polyalphabetic substitution, 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 unlike mono-a alphabetic which is one-to-one.*
  - *The same plaintext letter could be replaced by several ciphertext letters, depending on which alphabet is used.*



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

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

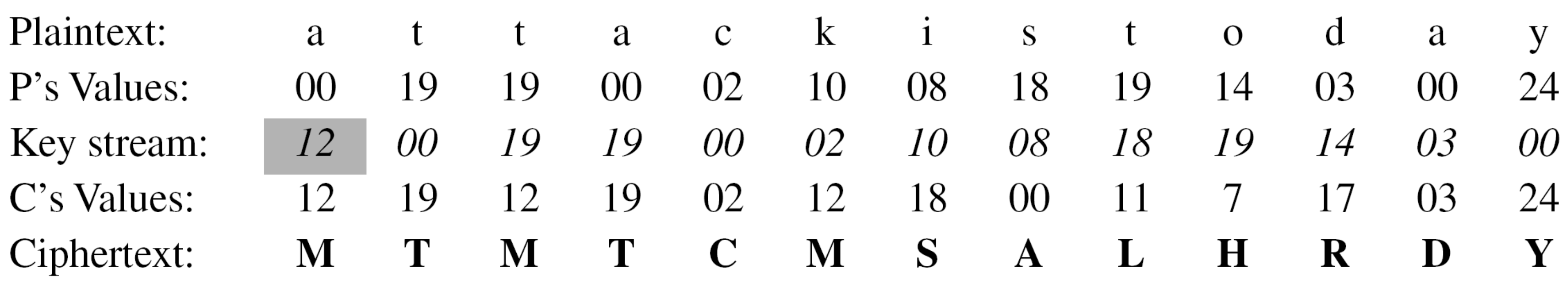
be guessed, and because the frequency distribution is more complex.

Cont . . .

- All type of polyalphabetic substitution have the following features in common:

  1. A set of related monoalphabetic substitution rules is used.
  2. A key determines which particular rule is chosen for a given transformation.

- Assume that Alice and Bob agreed to use an autokey cipher with initial key value k1 = 12. Now Alice wants to



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**

is

Cont . . .

(a) Vigenère Cipher

- Set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter.
- Thus, a Caesar cipher with a shift of 3 is denoted by the key value

Mathematical definition

- Assume a sequence of plaintext letters $P = P_0,P_1,P_2,\ldots.P_{n-1}$ and a key consisting of the sequence of letters $K = K_0,K_1,K_2,\ldots.K_{m-1}$, where $m < n$.
- The sequence of ciphertext letters $C=C_0,C_1,C_2,\ldots.C_{n-1}$ is calculated as: $C = C_0,C_1,C_2,\ldots.C_{n-1} = \mathrm{E}(K,P) = \mathrm{E}[(K_0,K_1,\ldots.K_{m-1}), (P_0,P_1,\ldots.P_{n-1})] =$ $(p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26,$
  $(p_m + k_1) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26 \ldots\ldots$

Cont . . .

Vigenère Cipher

- A general equation of the encryption process look as follow:

$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

- While decryption

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

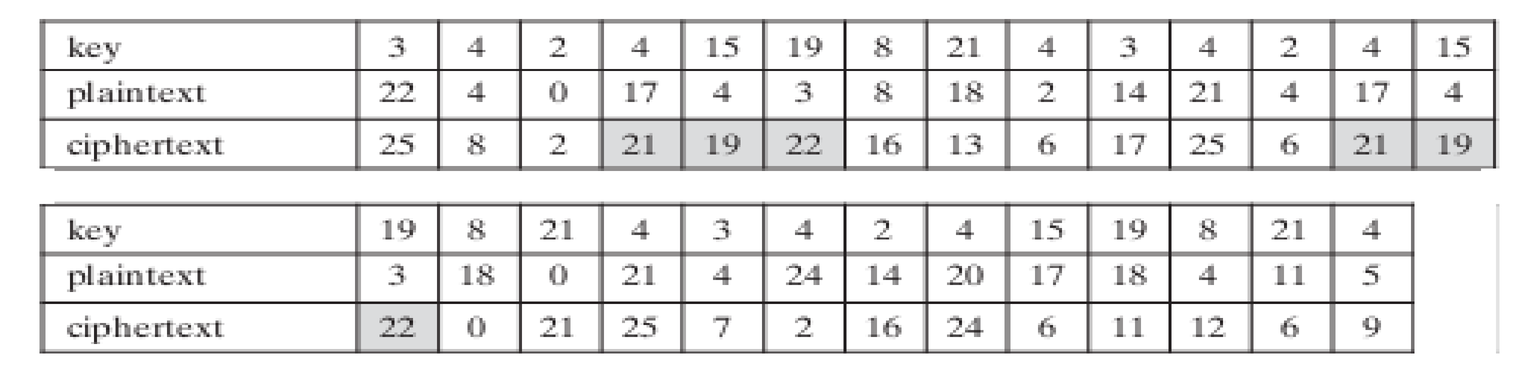
- To encrypt message, a key is needed that is as long as the message and usually the key is a repeating keyword.

Example:

plaintext:	we are discovered save yourself
key:	deceptive
ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Cont . . .

- Expressed numerically, we have the following result.



key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Security of vigenère cipher

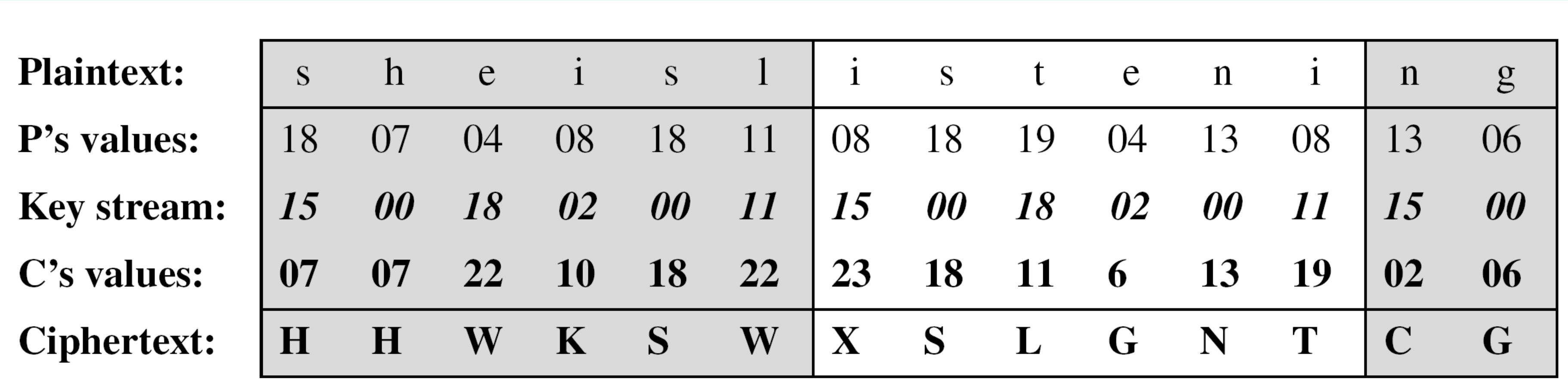
- The letter frequency information is obscured, since there are multiple ciphertext letters for each plaintext letter.
- However, not all knowledge of the plaintext structure is lost

Problem in vigenère cipher

- If two identical sequences of plaintext letters occur at a distance that is an integer multiple of the keyword length, they will generate identical ciphertext sequences.

Cont . . .

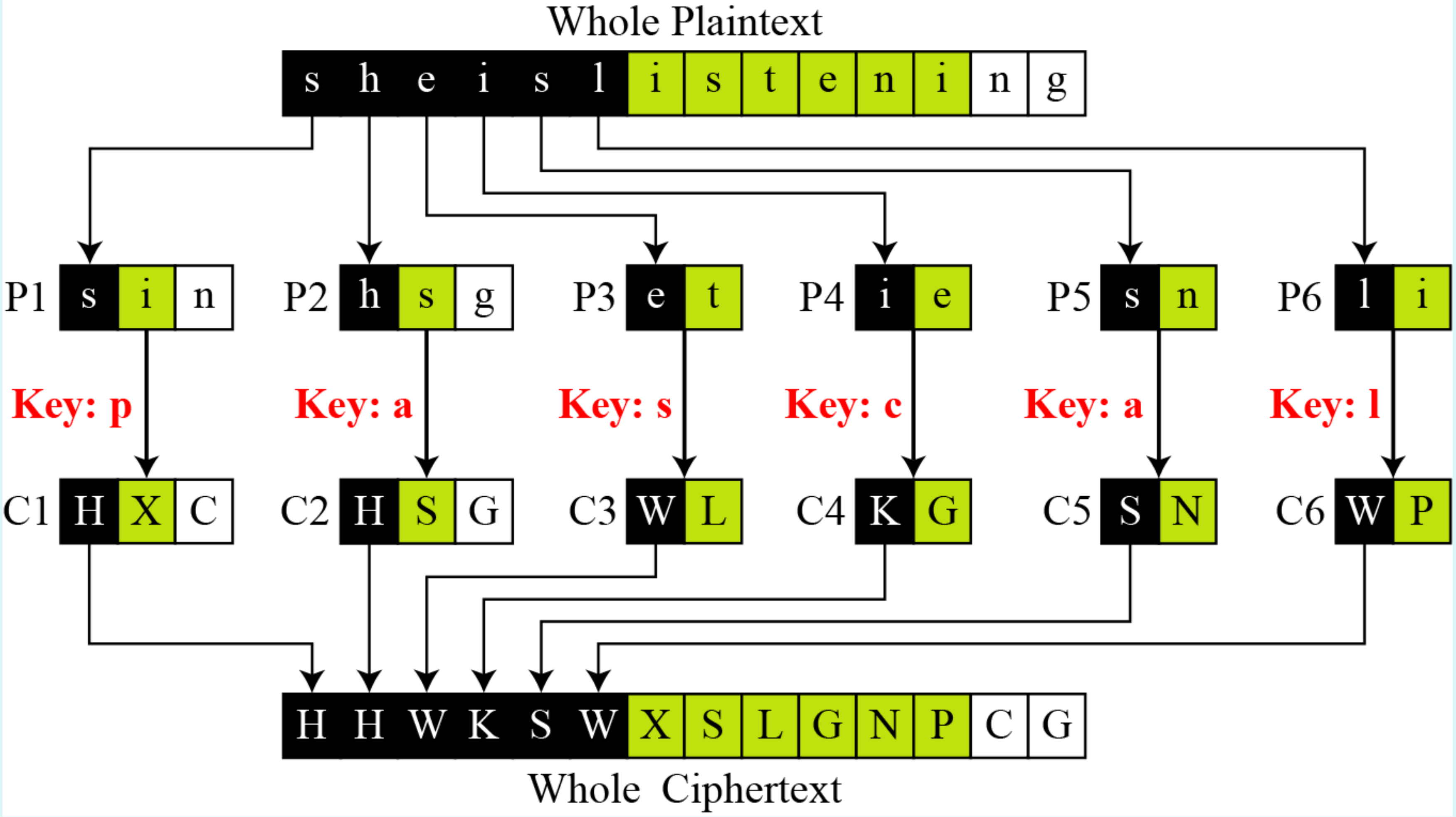
- **Example:**
    - We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.
- Let us see how we can encrypt the message “She is listening” using the 6-character keyword “PASCAL”. The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial 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**

Cont . . .

- Vigenere cipher can be seen as ***combinations of m additive*** ciphers



Cont . . .

(b) Vernam Cipher

- To overcome the draw back of **vigenère cipher**, this technique choose a keyword that is as long as the plaintext and has no statistical relationship to it.
- Works on binary data (bits) rather than letters

$$C_i = P_i \oplus K_i$$

- where

P_i = ith binary digit of plaintext

K_i = ith binary digit of key

C_i = ith binary digit of ciphertext

$\oplus$ = exclusive-or (XOR) operation

- The ciphertext is generated by performing the bitwise XOR of the plain-text and the key.

Cont . . .

(c) One-Time Pad

- Proposed an improvement to the Vernam cipher that yields the ultimate in security.
- Features
    - Key need not to be repeated
    - Key is to be used to encrypt and decrypt a single message, then discarded
    - Each new message requires a new key of the same length as the new message
    - It produces random cipher-text output that bears no statistical relationship to the plaintext.
    - Ciphertext contains no information whatsoever about the plaintext

Cont . . .

Example:

- *Ciphertext:* ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
  - *Key:* pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
  - *Plaintext:* mr mustard with the candlestick in the hall
  - *Key:* mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
  - *Plaintext:* miss scarlet with the knife in the library

Difficulties

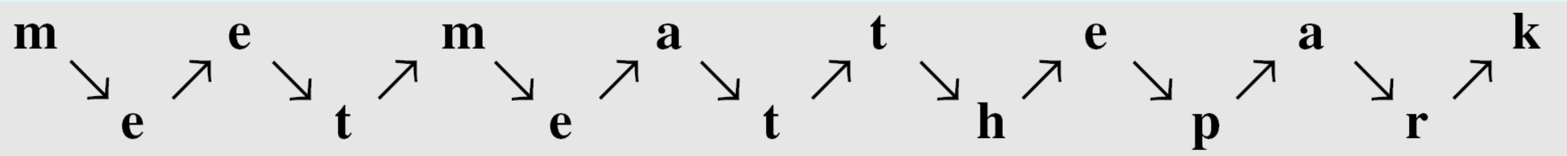
- There is the practical problem of making large quantities of random keys
- Even more daunting is the problem of key distribution and protection

5. Transposition Techniques

- A kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
- Simple transposition ciphers, which were used in the past, are keyless.

(1) Rail fence technique

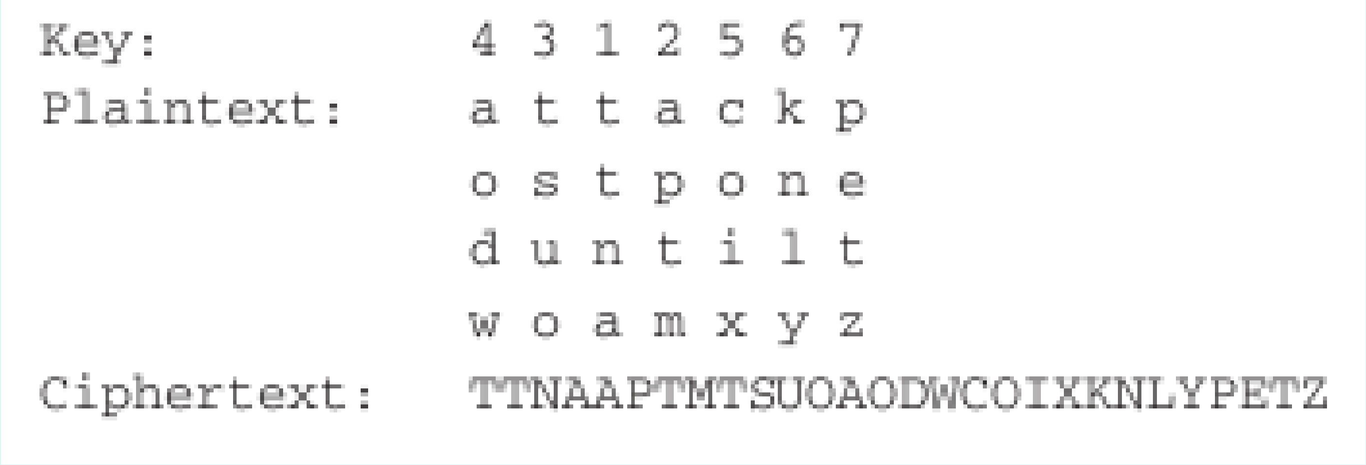
- The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- The ciphertext is created reading the pattern row by row. For example, to send the message “Meet me at the park” to Bob, Alice writes
- E.g. to encipher the message *“meet me after the toga party”* with a rail fence of depth 2, we write it as follow:
- Th



Cont . . .

(2) Rectangular technique

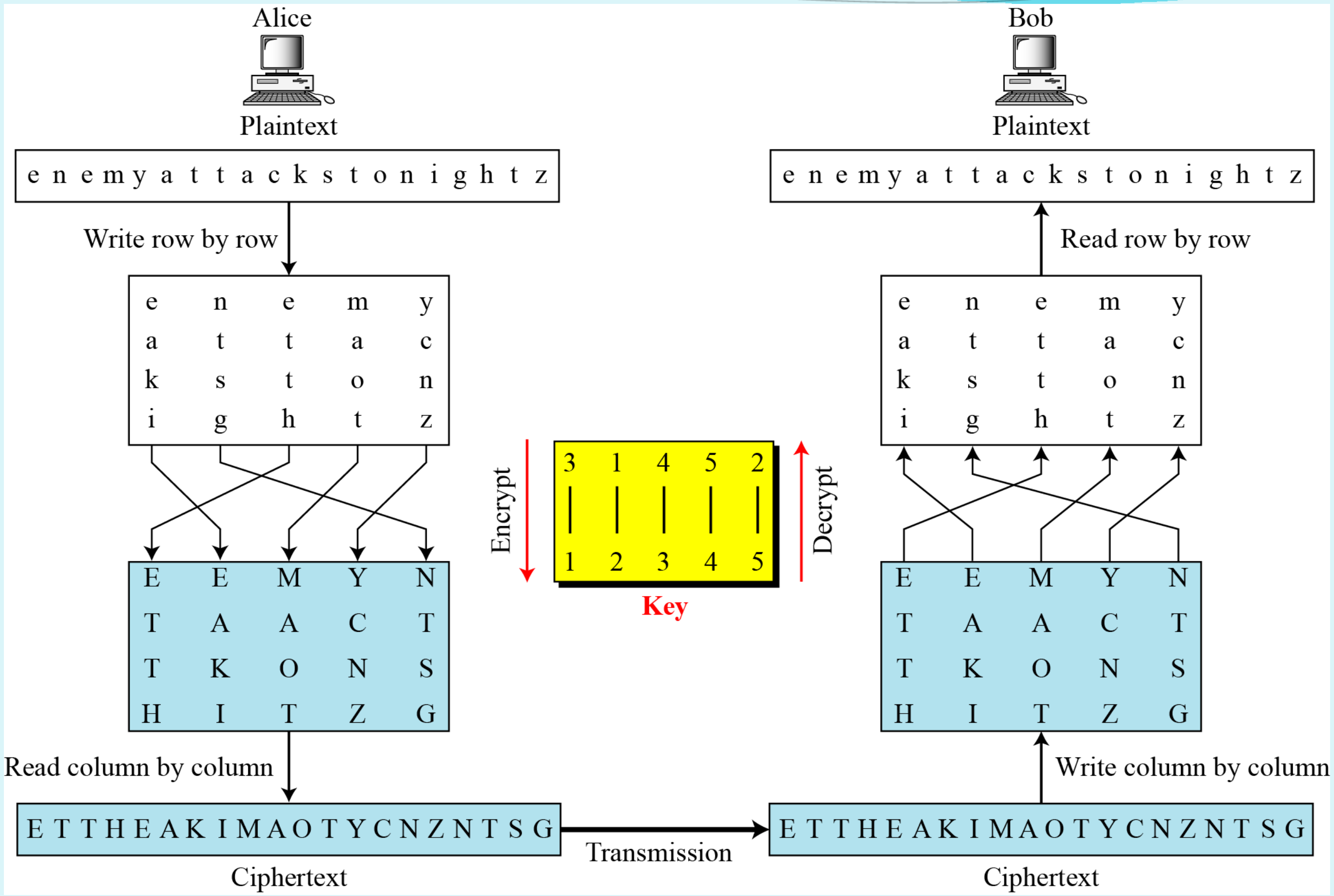
- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- The order of the columns then becomes the key to the algorithm.
- For example



```
Key:           4 3 1 2 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
```

- The key is 4312567. To encrypt, start with the column that is labeled 1, in this case column 3. Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.

Combining encryption and decryption two Approaches

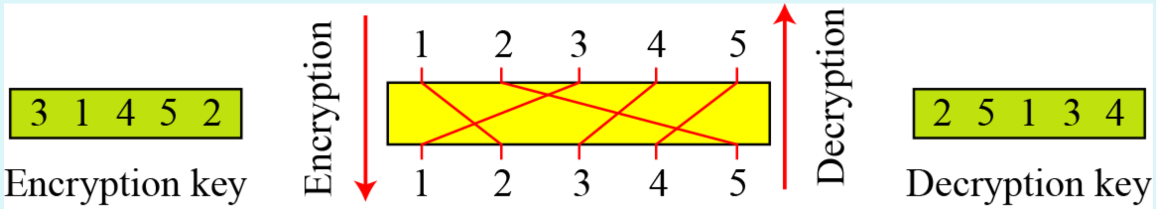


enemyattackstonightz

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

ETTHEAKIMAOTYCNZNTSG



Encryption/decryption keys in transpositional ciphers

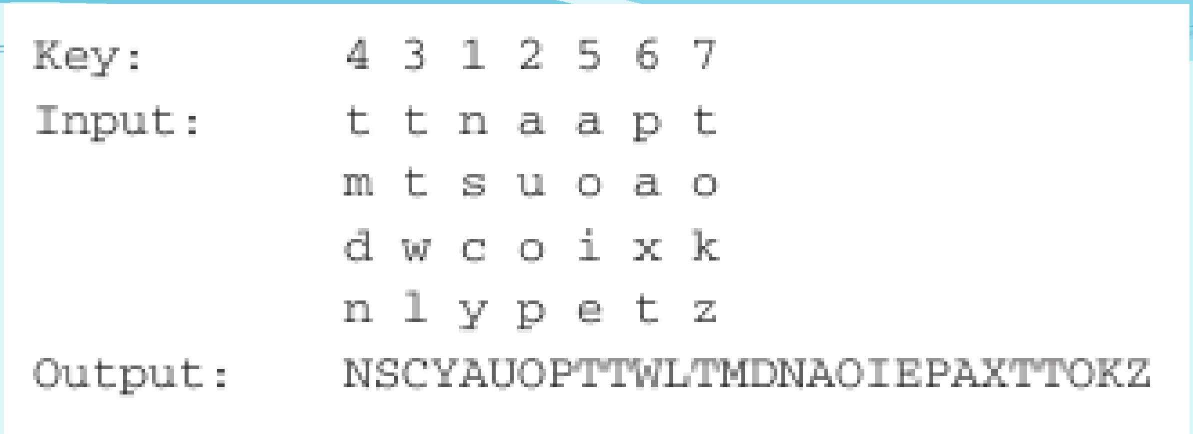
Cont . . .

(3) Digram/trigram transposition techniques

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext
- Columnar transposition just shown before, cryptanalysis is fairly *straightforward* and involves laying out the ciphertext in a matrix and playing around with column positions.
- *Digram and trigram frequency tables* can be useful
- The transposition cipher can be made significantly more secure by performing ***more than one stage of transposition***.
- The result is a more complex permutation that is not easily reconstructed

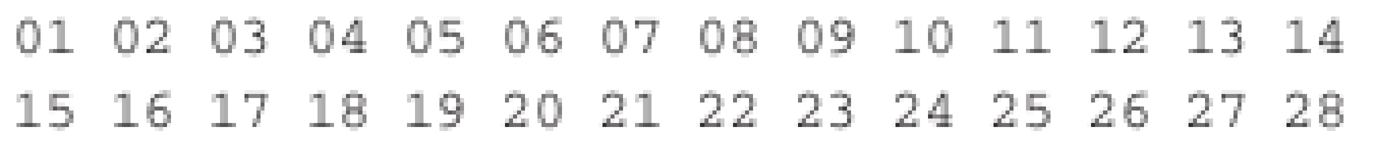
Cont . . .

- **Example:**



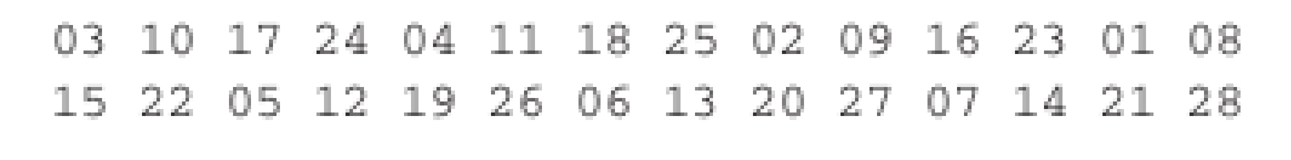
```
Key:      4 3 1 2 5 6 7
Input:    t t n a a p t
          m t s u o a o
          d w c o i x k
          n l y p e t z
Output:   NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

- With 28 letters in the message, the original sequence of letters is



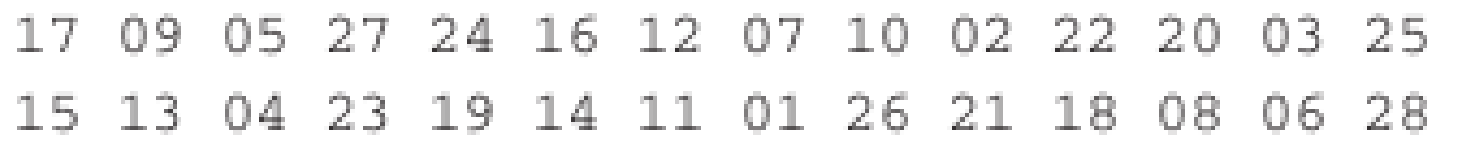
```
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28
```

- After the first transposition, we have which has a somewhat regular str



```
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28
```

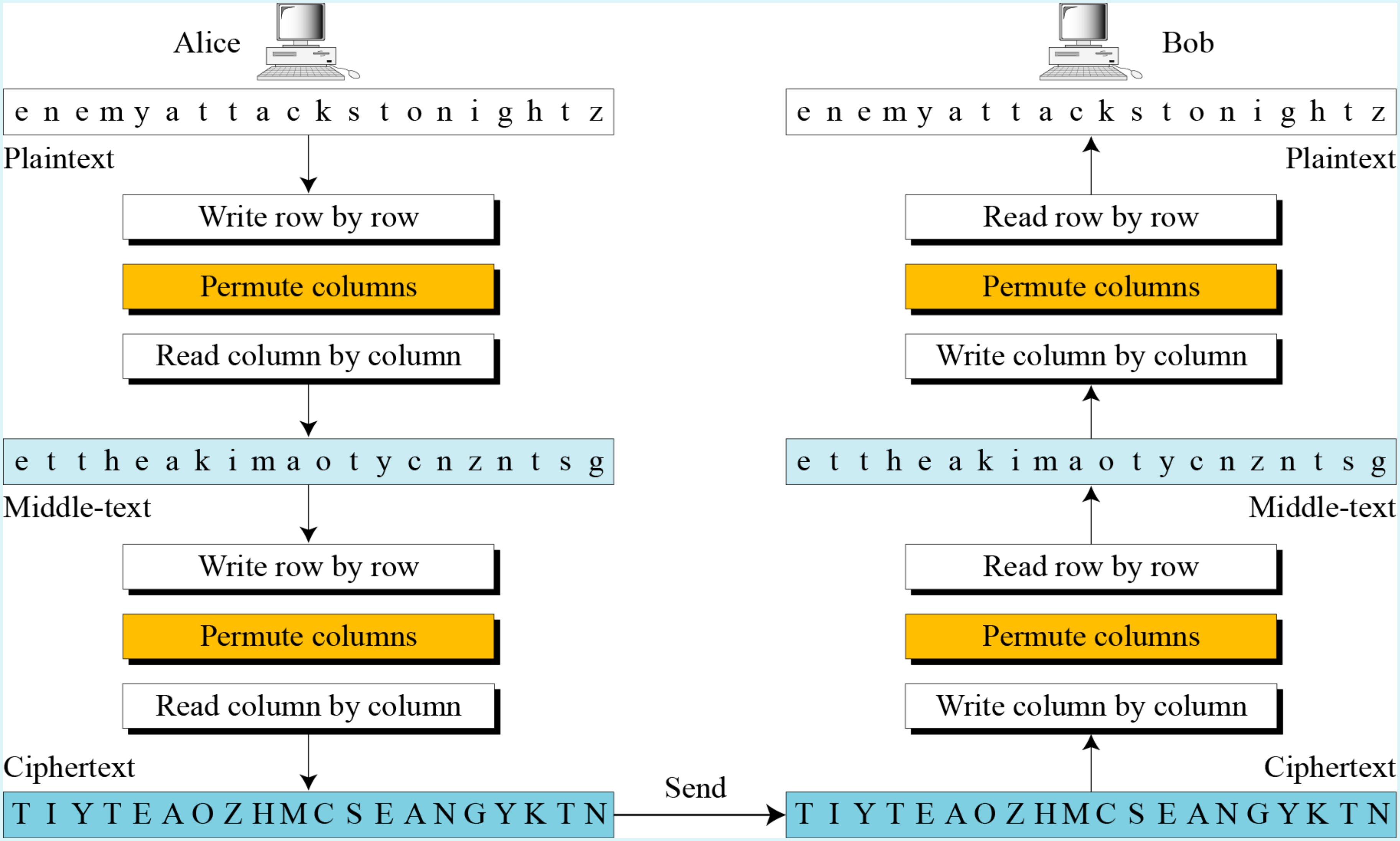
- After the second transposition we have, much less structured permutation and is much more difficult to cryp



```
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```

Continued

Double transposition cipher



Alice

enemyattackstonightz

Plaintext

Write row by row

Permute columns

Read column by column

ettheakimaotycnzntsg

Middle-text

Write row by row

Permute columns

Read column by column

Ciphertext

TIYTEAOZHMCSEANGYKTN

Send

Bob

enemyattackstonightz

Plaintext

Read row by row

Permute columns

Write column by column

ettheakimaotycnzntsg

Middle-text

Read row by row

Permute columns

Write column by column

Ciphertext

TIYTEAOZHMCSEANGYKTN

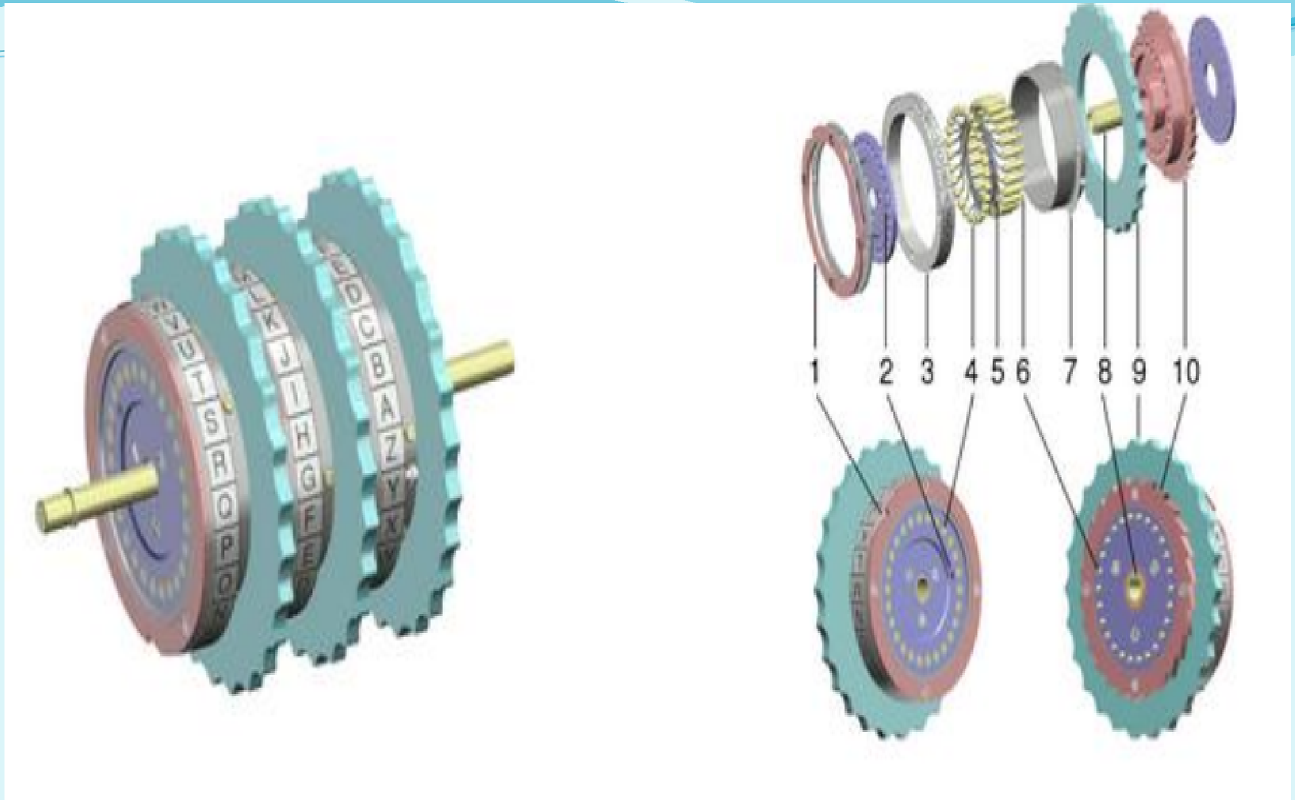
6. Rotor Machine Techniques

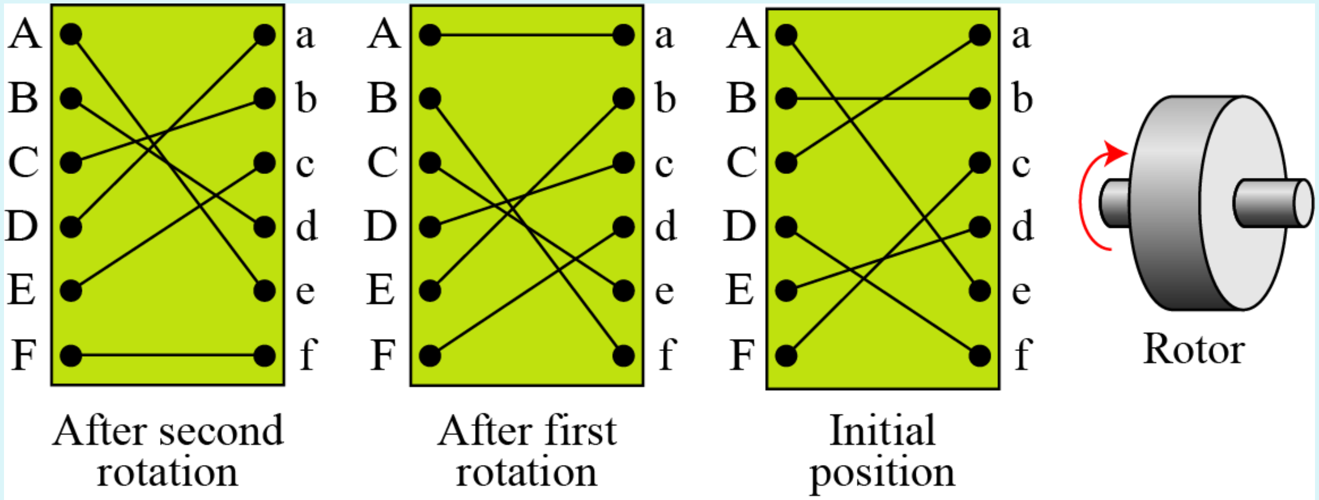
- A simple substitution cipher
- The machine consists of a set of independently rotating cylinders through which electrical pulses can flow.
- Each cylinder has 26 input pins and 26 output pins
- Internal wiring connects each input pin to a unique output pin.
- For simplicity, only three of the internal connections in each cylinder are shown.

Single cylinder Machine

- Input key depressed ----- > the cylinder rotates one position ----- > the internal connections are shifted accordingly. Thus, different monoalphabetic substitution cipher is defined.
- After 26 letters of plaintext, the cylinder would be back to the initial position. Thus, we have a poly-alphabetic substitution a period of 26.

Cont . . .


1
2
3
4
5
6
7
8
9
10


A
B
C
D
E
F
a
b
c
d
e
f
After second rotation
After first rotation
Initial position
Rotor

Cont . . .

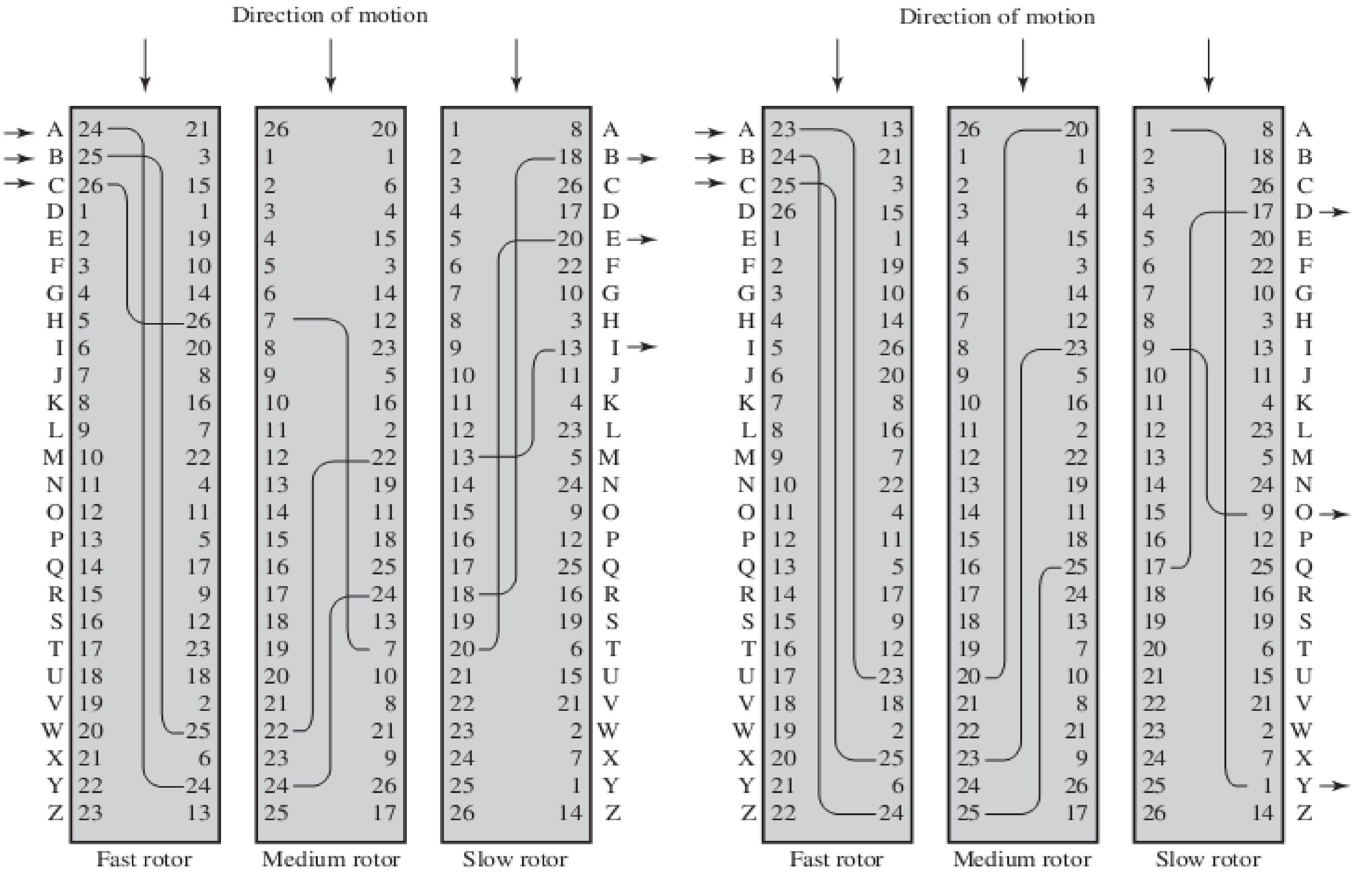
Multiple cylinder Machine

- Output pins of one cylinder are connected to input pins of the next.

Example: Three-cylinder machine

- The cylinders, closest to the operator input rotates one pin position with each keystroke.
- For every complete rotation of the inner cylinder, the middle cylinder rotates one pin position.
- Finally, for every complete rotation of the middle cylinder, the outer cylinder rotates one pin position.
- The result is that there are 26 X 26 X 26 different substitution alphabets used before the system repeats.
- Left half of figure shows position of input from operator to the first pin (plaintext letter a) is routed through the three cylinders to appear at the output of the second pin (ciphertext letter B).

Cont . . .



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

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

7. Steganography Techniques

- Unlike cryptography methods which render the message unintelligible (meaningless) to outsiders, this method conceal/hide the existence of the message.
- An alternative to encryption
- A simple form of steganography, but time-consumer to construct, is one in which an arrangement of words/letters within an apparently innocuous text spells out the real message.
  - E.g., the sequence of first letters of each word of the overall message spells out the hidden message.

Character marking:

- Selected letters of printed/typewritten text are overwritten in pencil.
- The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Cont . . .

Invisible ink:

- A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper

Pin punctures:

- Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon:

- Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Example:

- Kodak Photo CD

Cont . . .

Drawback:

- Requires a lot of overhead to hide a relatively few bits of information

Advantages:

- Can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered.
- Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide.

TREAM CIPHERS OR BLOCK CIPHERS?????

- The literature divides the symmetric ciphers into two broad categories: stream ciphers and block ciphers.
- Although the definitions are normally applied to modern ciphers, this categorization also applies to traditional ciphers.

Example of Stream Ciphers

- Ceaser cipher (i.e. additive ciphers)
- The monoalphabetic substitution ciphers
- Vigenere ciphers

Example of Block Ciphers

- Playfair ciphers
- Hill ciphers

ONO-ALPAHBETIC VS. POLY-ALPHABETIC

- We can establish a criterion to divide stream ciphers based on their key streams.
- We can say that a stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.
- ***Additive ceaser*** ciphers and ***Monoalphabetic substitution*** ciphers are monoalphabetic because k_i does not depend on the position of the corresponding character in the plaintext stream; where Vigenere ciphers are polyalphabetic ciphers because k_i definitely depends on the position of the plaintext character.
- From the definition of the block cipher, it is clear that every block cipher is a polyalphabetic cipher because each character in a ciphertext block depends on all characters in the plaintext block.

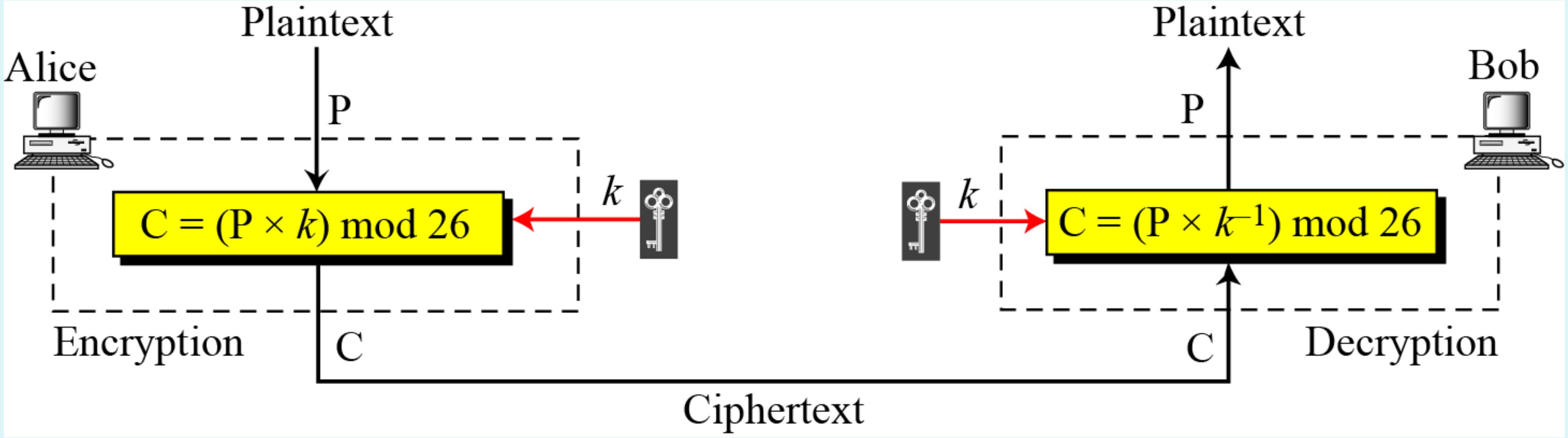
THE END

???

Reading Assignment

1. The Hill Algorithms/Techniques

Multiplicative Ciphers



Note

In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26}; the key is an integer in Z26*.

Continued

Example 3.7

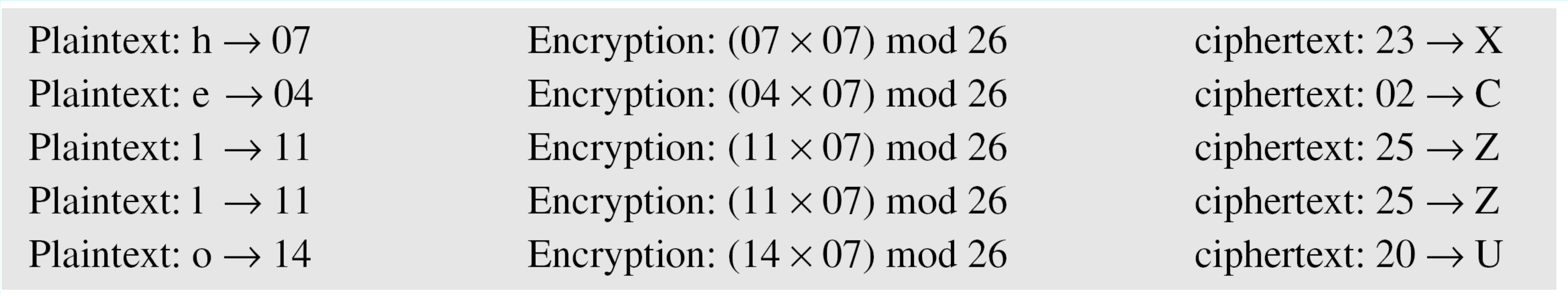
What is the key domain for any multiplicative cipher?

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.

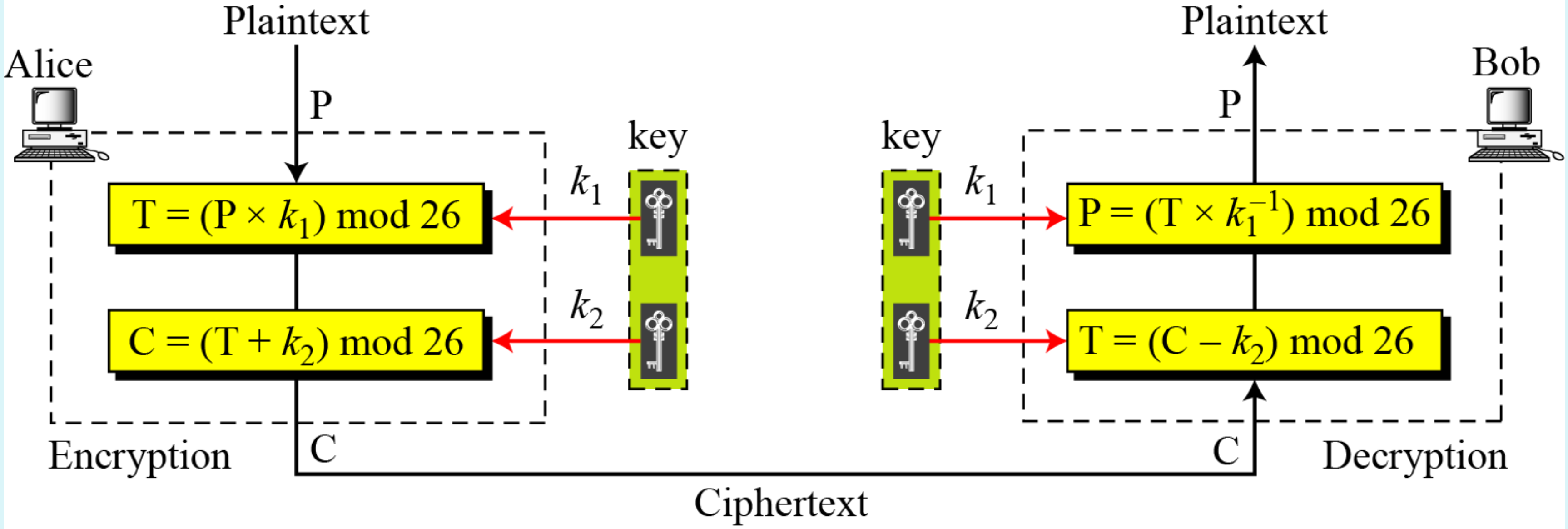
Example 3.8

We use a multiplicative cipher to encrypt the message "hello" with a key of 7. The ciphertext is "XCZZU".



Plaintext: h → 07	Encryption: (07×07) mod 26	ciphertext: 23 → X
Plaintext: e → 04	Encryption: (04×07) mod 26	ciphertext: 02 → C
Plaintext: l → 11	Encryption: (11×07) mod 26	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: (11×07) mod 26	ciphertext: 25 → Z
Plaintext: o → 14	Encryption: (14×07) mod 26	ciphertext: 20 → U

Affine Ciphers



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

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

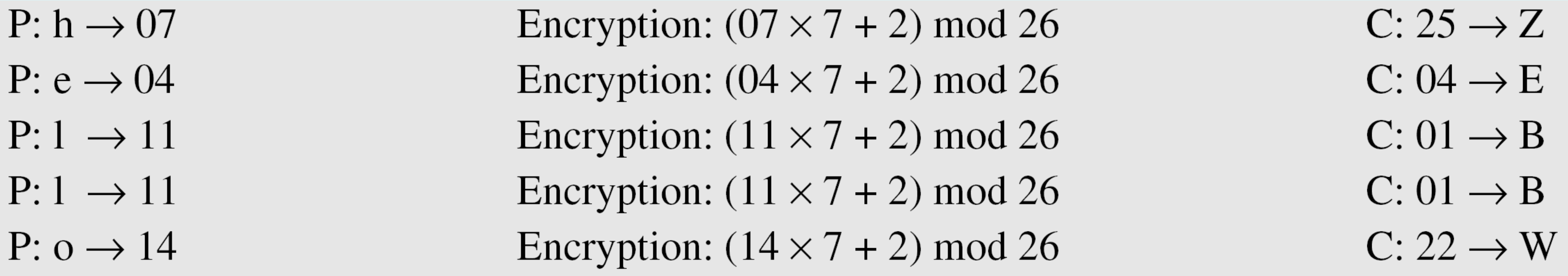
Continued

Example 3.09

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 × 12 = 312.

Example 3.10

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



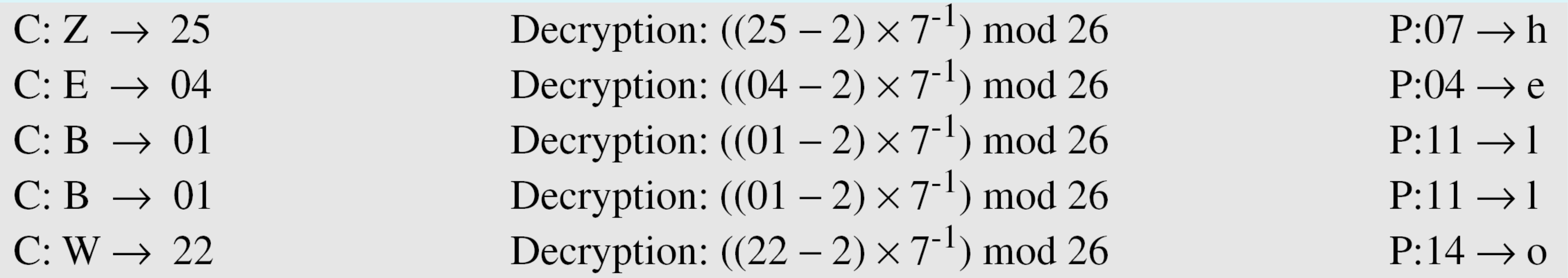
P: h → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22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

Continued

Example 3.11

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

Solution



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

Example 3.12

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 $k_2 = 0$.

Hill Cipher

Key in the Hill cipher

$$K = \begin{bmatrix} k_{11} & k_{12} & \ldots & k_{1m} \\ k_{21} & k_{22} & \ldots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{\mathrm{m}1} & k_{\mathrm{m}2} & \ldots & k_{mm} \end{bmatrix}$$

$$\begin{aligned} &\mathrm{C}_1 = \mathrm{P}_1\, k_{11} + \mathrm{P}_2\, k_{21} + \cdots + \mathrm{P}_m\, k_{m1} \\ &\mathrm{C}_2 = \mathrm{P}_1\, k_{12} + \mathrm{P}_2\, k_{22} + \cdots + \mathrm{P}_m\, k_{m2} \\ &\ldots \\ &\mathrm{C}_\mathrm{m} = \mathrm{P}_1\, k_{1m} + \mathrm{P}_2\, k_{2m} + \cdots + \mathrm{P}_m\, k_{mm} \end{aligned}$$

Note

The key matrix in the Hill cipher needs to have a multiplicative inverse.

Continued

Example 3.20

For example, the plaintext “code is ready” can make a 3 × 4 matrix when adding extra bogus character “z” to the last block and removing the spaces. The ciphertext is “OHKNIHGKLISS”.

$$\overset{\text{C}}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} = \overset{\text{P}}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} \overset{\text{K}}{\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}}$$

a. Encryption

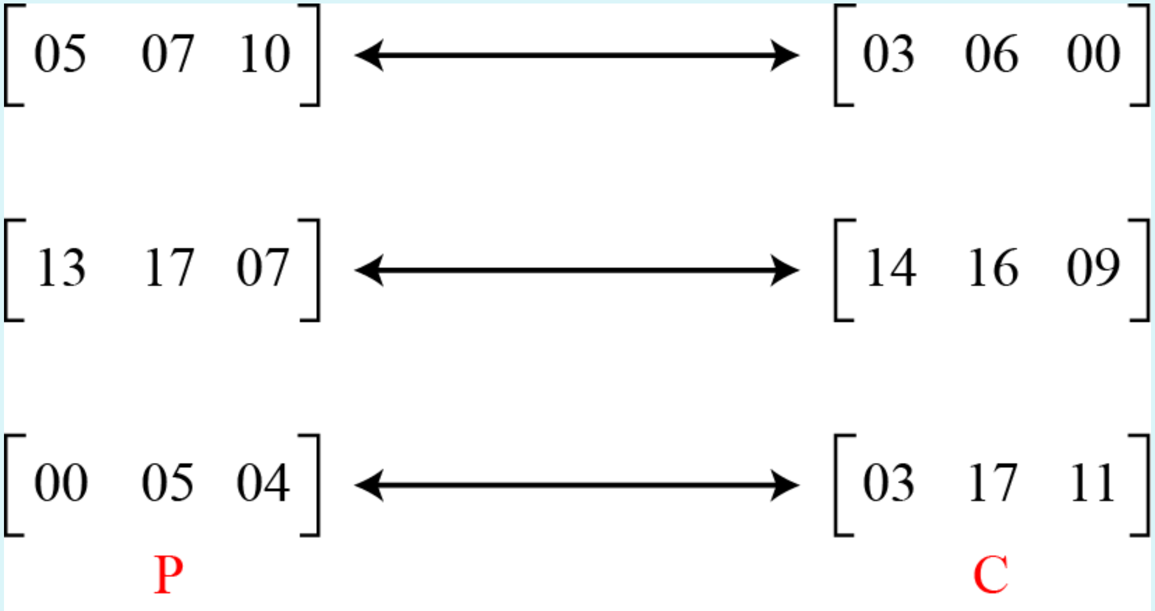
$$\overset{\text{P}}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} = \overset{\text{C}}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} \overset{\text{K}^{-1}}{\begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}}$$

b. Decryption

Continued

Example 3.21

Assume that Eve knows that m = 3. She has intercepted three plaintext/ciphertext pair blocks (not necessarily from the same message) as shown in Figure 3.17.



$$\begin{bmatrix}05 & 07 & 10\end{bmatrix} \longleftrightarrow \begin{bmatrix}03 & 06 & 00\end{bmatrix}$$

$$\begin{bmatrix}13 & 17 & 07\end{bmatrix} \longleftrightarrow \begin{bmatrix}14 & 16 & 09\end{bmatrix}$$

$$\begin{bmatrix}00 & 05 & 04\end{bmatrix} \longleftrightarrow \begin{bmatrix}03 & 17 & 11\end{bmatrix}$$

Continued

Example 3.21 (Continued)

She makes matrices P and C from these pairs. Because P is invertible, she inverts the P matrix and multiplies it by C to get the K matrix as shown in Figure 3.18.

$$\underset{\mathrm{K}}{\begin{bmatrix} 02 & 03 & 07 \\ 05 & 07 & 09 \\ 01 & 02 & 11 \end{bmatrix}} = \underset{\mathrm{P}^{-1}}{\begin{bmatrix} 21 & 14 & 01 \\ 00 & 08 & 25 \\ 13 & 03 & 08 \end{bmatrix}} \underset{\mathrm{C}}{\begin{bmatrix} 03 & 06 & 00 \\ 14 & 16 & 09 \\ 03 & 17 & 11 \end{bmatrix}}$$

Now she has the key and can break any ciphertext encrypted with that key.

Transposition using Matrix

- We can use matrices to show the encryption/decryption process for a transposition cipher.
- The below table shows the encryption process. Multiplying the 4 × 5 plaintext matrix by the 5 × 5 encryption key gives the 4 × 5 ciphertext matrix.

$$\underset{\text{Plaintext}}{\begin{bmatrix}04&13&04&12&24\\00&19&19&00&02\\10&18&19&14&13\\08&06&07&19&25\end{bmatrix}} \times \underset{\text{Encryption key}}{\begin{array}{ccccc}\boxed{3}&\boxed{1}&\boxed{4}&\boxed{5}&\boxed{2}\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ \hline 0&1&0&0&0\\0&0&0&0&1\\1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{array}} = \underset{\text{Ciphertext}}{\begin{bmatrix}04&04&12&24&13\\19&00&00&02&19\\19&10&14&13&18\\07&08&19&25&06\end{bmatrix}}$$

Representation of the key as a matrix in the transposition cipher

What makes a "Good" cipher?

- In 1949 **Shannon proposed** the below characteristics of a good cipher:
  1. The amount of required secrecy should determine the amount of encrypting/decrypting work.
  2. The choice of keys and the enciphering algorithm should be free from complexity.
  3. The implementation of the process should be as simple as possible.
  4. Errors in ciphering should not propagate, corrupting other message parts.
  5. The size of the ciphertext should be no larger than its corresponding plaintext.

- **Today’s priorities:**
  1. The encryption/decryption algorithm must be proven to be mathematically sound.’
  2. The algorithm must have been analyzed by experts for its vulnerability
  3. The algorithm must have stood the “test of time”.
  4. Time to encode/decode must still be acceptable