Lec. 1

Symmetric Ciphers

Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security.

The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures, encryption is a primary method of protecting valuable electronic information.

By far the most important automated tool for network and communications security is encryption. Two forms of encryption are in common use: conventional, or symmetric, encryption and public-key, or asymmetric, encryption.

Part One provides a survey of the basic principles of symmetric encryption, looks at widely used algorithms, and discusses applications of symmetric cryptography.

Cryptology

Is the science and study of systems for secret communications. It consists of two complementary fields of study: **Cryptography,** the design of secret communications systems, and **Cryptanalysis** , the study of ways to compromise of secret communications systems.

Cryptology primarily has been applied in military and diplomatic communications systems, but other significant applications are becoming apparent.

Cryptography methods applied by authorized information sharers to design and develop encryption schemes in order to ensure confidentiality of information.

Crypt-Analysis (mathematical and statistical attempts by unauthorized persons to break cipher in order to reveal the meaning of the underlying protected data).

Cryptography

Is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptography is not the only means of providing information security, but rather one set of techniques. Cryptography classified into two type:

1- Symmetric

2- Asymmetric

as shown in Fig. (2.1).

A Symmetric cryptography ciphers may in fact be sub classified into **Block Ciphers** (in which blocks of data, known as plaintext, are transformed into cipher text which appears unintelligible to unauthorized persons) and **Stream Ciphers** (which involve streams of typically binary operations and are well suited for efficient computer implementation).

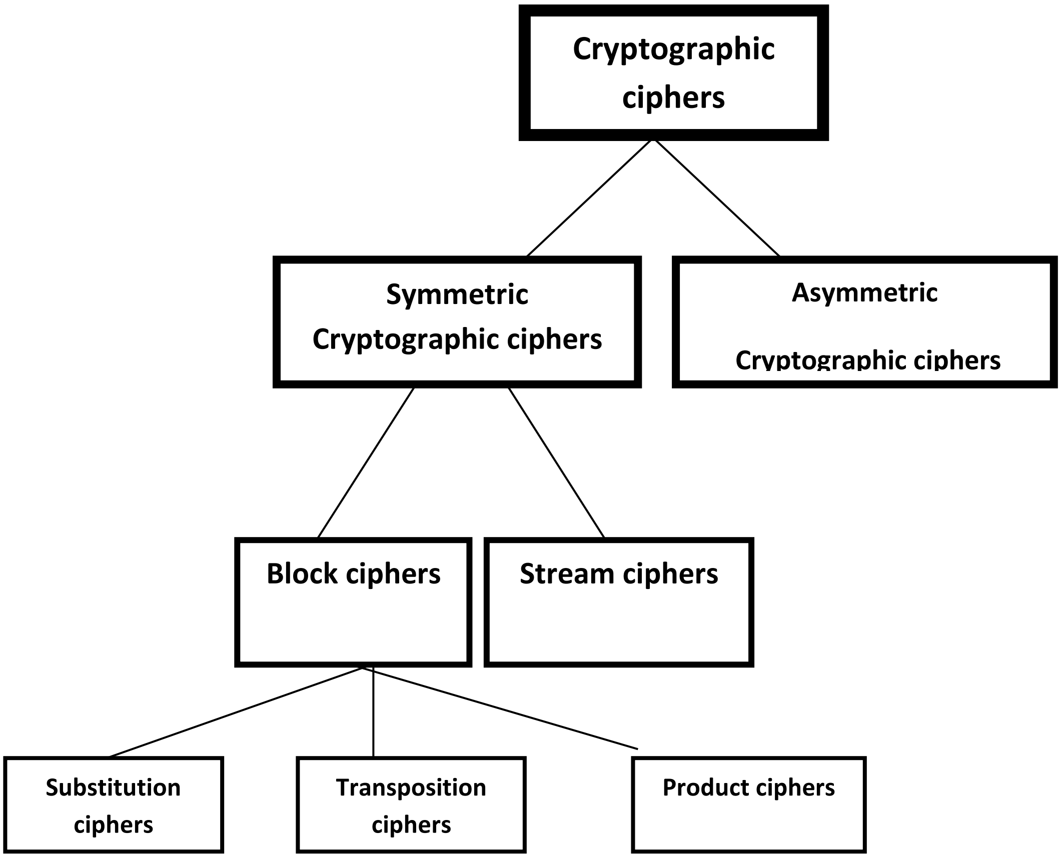


Figure 2.1 : Schematic representation of cryptographic cipher classification

The process of transforming plaintext into ciphertext is called **Encryption**; the reverse process of transforming ciphertext into plaintext is called **Decryption**. Both encryption and decryption are controlled by cryptographic key parameters as shown in Fig 3.2.

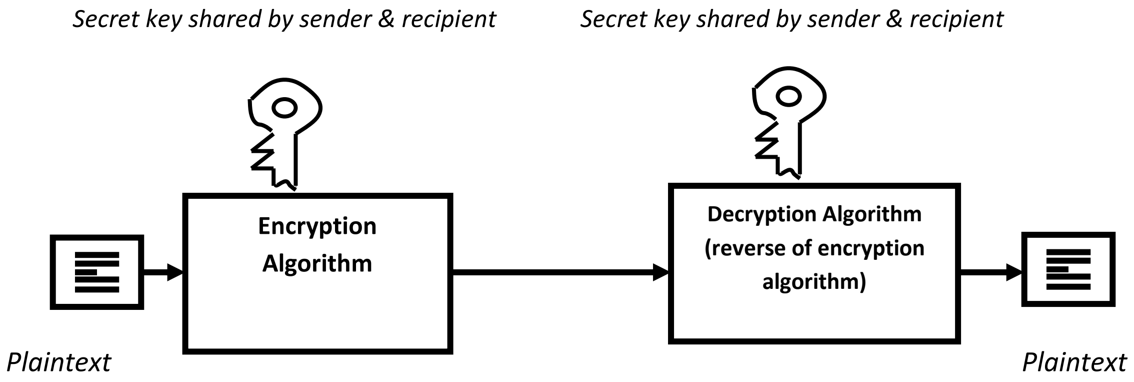
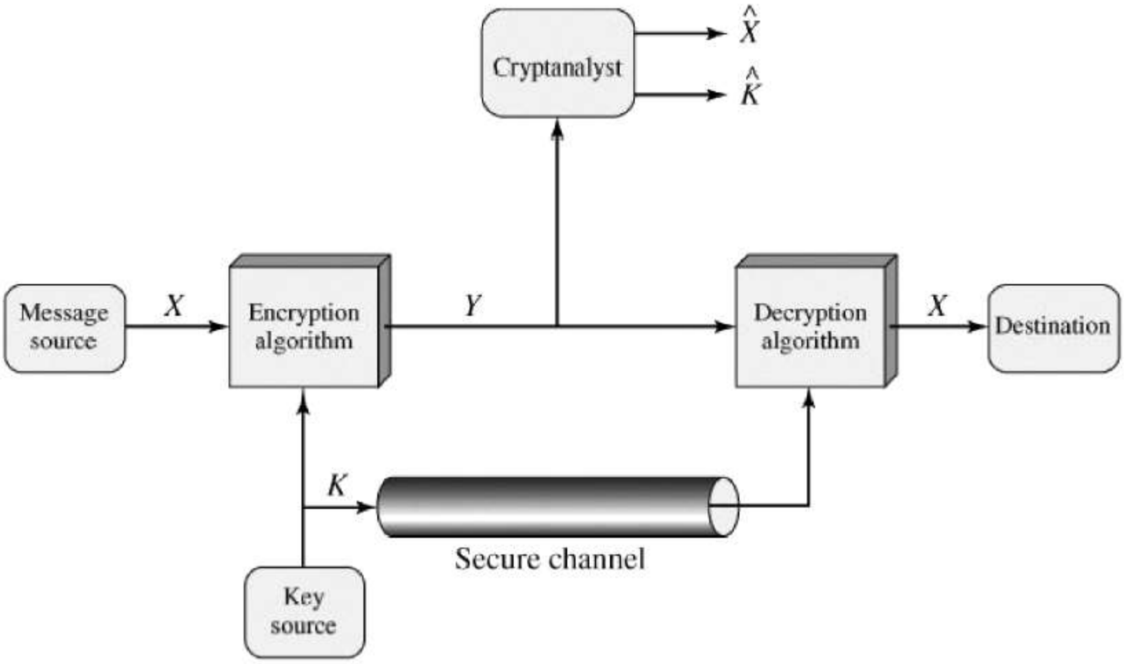

Secret key shared by sender & recipient
Secret key shared by sender & recipient
Encryption Algorithm
Decryption Algorithm (reverse of encryption algorithm)
Plaintext
Plaintext

Figure 3.2 : Simplified Model of Conventional Encryption

Model for Network Security

A model for much of what we will be discussing is captured, in very general terms, in Figure 1.5. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.



Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender Some secret information shared by the two principals and, it is hoped, unknown to the o. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Part Two discusses a form of encryption, known as public-key encryption, in which only one of the two principals needs to have the secret information.

Secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information toachieve a particular security service.

Parts One through Three of this book concentrates on the types of security mechanisms and services that fit into the model shown in Figure 1.5. However, there are other security-related situations of interest that do not neatly fit this model but that are considered in this book. A general model of these other situations is illustrated by Figure 1.6, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

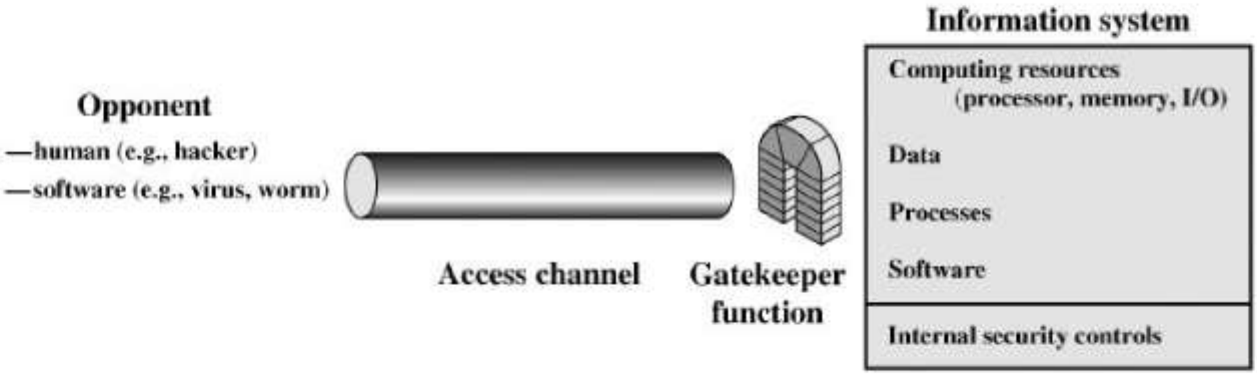


Figure 1.6. Network Access Security Model

Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

Information access threats intercept or modify data on behalf of users who should not have access to that data.

Service threats exploit service flaws in computers to inhibit use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.6). The first category might

be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or

unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders. These issues are explored in Part Four.

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Stream Ciphers and Block Ciphers

A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the autokeyed Vigenère cipher and the Vernam cipher.

A **block cipher** is one in which a block of plaintext is treated as a whole and used to

produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used. Using some of the modes of operation explained in Chapter 6, a block cipher can be used to achieve the same effect as a stream cipher. Far more effort has gone into analyzing block ciphers. In general, they seem applicable to a broader range of applications than stream ciphers. The vast majority of network-based symmetric cryptographic applications make use of block ciphers. Accordingly, the concern in this chapter, and in our discussions throughout the book of symmetric encryption, will focus on block ciphers.

Note:

Plaintext → small letter	Key → capital letter	Cipher text → capital letter

Decipher

Cipher text → capital letter	Key → small letter	Plain text → small letter

Block: A sequence of consecutive characters encoded at one time

block length: The number of characters in a block

An algorithm for performing encryption (and the reverse, decryption) - a series of well-defined steps that can be followed as a procedure. Works at the level of individual letters, or small groups of letters

Ciphertext: A text in the encrypted form produced by some cryp- tosystem. The convention is for ciphertexts to contain no white space or punctuation

Cryptanalysis: The analysis and deciphering of cryptographic writings or systems.

cryptography: The process or skill of communicating in or deciphering secret writings or ciphers

cryptosystem: The package of all processes, formulae, and instructions for encoding and decoding messages using cryptography

decryption: Any procedure used in cryptography to convert cipher- text (encrypted data) into plaintext

digram: Sequence of two consecutive characters

encryption: The process of putting text into encoded form

key: A relatively small amount of information that is used by an algorithm to customize the transformation of plaintext into ciphertext (during encryption) or vice versa (during decryption)

key length: The size of the key - how many values comprise the key

monoalphabetic: Using one alphabet - refers to a cryptosystem where each alphabetic character is mapped to a unique alphabetic character

one-time pad: Another name for the Vernam cipher

plaintext: A message before encryption or after decryption, i.e., in its usual form which anyone can read, as opposed to its encrypted form

polyalphabetic: Using many alphabets - refers to a cipher where each alphabetic character can be mapped to one of many possible alphabetic characters

trigram: Sequence of three consecutive characters unigram

The field of Cryptology today represents that branch of information theory which deals with the security of information confidentiality. Methods in cryptology may be subdivided into two classes, namely that of **cryptography** (methods applied by authorized information sharers to design and develop encryption schemes in order to ensure confidentiality of information) and that of **cryptanalysis** (mathematical and statistical attempts by unauthorized persons to break cipher in order to reveal the meaning of the underlying protected data)[1].

Cryptography may in fact be sub classified into **Symmetric** and **Asymmetric** cryptography ciphers. Symmetric cryptography ciphers sub classified into block ciphers and stream cipher.

In **Symmetric** cryptography ciphers the enciphering and deciphering keys are the same, as shown in Fig. 1.1.

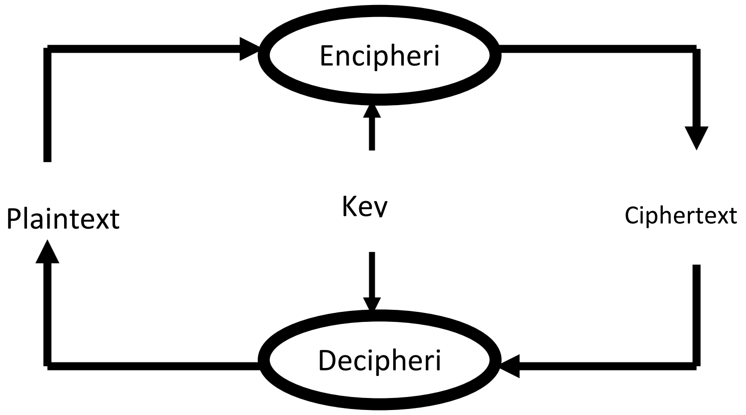


Fig. 1.1: Secret Writing

Block ciphers, in which blocks of data, known as plaintext, are transformed into cipher text which appears unintelligible to unauthorized persons.

Stream ciphers, which involve streams of typically binary operations and are well suited for efficient computer implementation.

The ***ciphertext*** is created by choosing a permutation of the 26-character alphabet and using it to replace each letter in the *plaintext* message.

Lec. 2

Type of Ciphers:

Encryption and Authentication

Nearly all modern security mechanisms are based on keeping secrets private to certain individuals. Security systems use encryption to keep secrets, and they use authentication to prove the identity of individuals. These two basic security mechanisms are the foundation upon which nearly all security mechanisms are based.

1-Secret key encryption

2-Hashes and one-way functions

3-Public key encryption

4-Password authentication

5-Challenge/response authentication

6-Sessions

7-Public key authentication

8-Digital signatures

9-Certificates

10-Biometric authentication

Data security is the sciences and study of methods of protecting data in computer and communication systems for unauthorized disclosure and modification.

Or

* **Cipher** is a secret method of writing.

1- Caser cipher

It is believed that Julius Caesar, in the period 58 BCE to 51 BCE, enciphered messages to his lawyer Marcus Tullius Cicero and other Roman senators using a monoalphabetic substitution.

In the Caesar cipher, each plaintext letter was replaced by the letter standing three places to-the-right in the alphabet. If we neglect that the original Roman or Latin alphabet did not contain a J, U, or W, then, Julius' query in the present day Roman alphabet.

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10
L	M	N	O	P	Q	R	S	T	U	V
11	12	13	14	15	16	17	18	19	20	21
W	X	Y	Z							
22	23	24	25							

Example: (Caser method) use k=3

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

Plaintext: Ali
(Encipher process)………………………….. **(P+K) mod 26**
Sol:

A=0
0+3 mod 26 = 3 = D
L=11
11+3 mod 26=14=O
I=8
8+3 mod 26=11= L

Cipher text: DOL

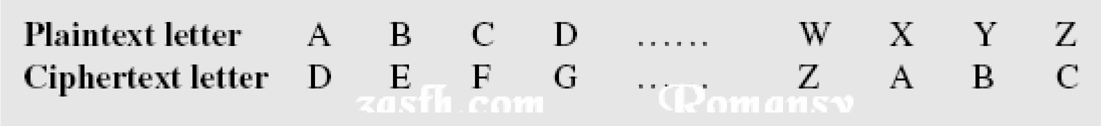
(Decipher process)……………………………. **(C-K) mod 26**
Sol:

D=3
3-3 mod 26=0=A
O=14
14-3mod26=11=L
L=11
11-3mod26=8=I

EX: 2

Plain text; anyone know where i can get decent pizza?

Cipher text: DQBRQH NQRZ ZKHUH L EDQ JHW GHFHQW SLCCD?



Plaintext letter	A	B	C	D	……	W	X	Y	Z
Ciphertext letter	D	E	F	G	……	Z	A	B	C

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

Plain : meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as
follows:

plain: 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

cipher: 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

Let us assign a numerical equivalent to 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 follows. For each plaintext letter p, substitute the ciphertext letter C:

We define a mod n to be the remainder when a is divided by n. For example, 11 mod 7 = 4.

$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$

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

$C = \mathrm{E}(k, p) = (p + k) \bmod 26$

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$p = \mathrm{D}(k, C) = (C - k) \bmod 26$

2- Substitution Ciphers

Substitution ciphers are block ciphers which replace symbols (or groups of symbols) by other symbols or groups of symbols.

Mono alphabetic substitution ciphers

The simplest cipher of those attacked is the mono alphabetic substitution cipher. This cipher is described as follows:

- Let the plaintext and the cipher text character sets be the same, say the alphabet Z
- Let the keys, K, consist of all possible permutations of the symbols in Z
- For each permutation $\pi \in$ K,

1. define the encryption function $e_\pi(x) = \pi(x)$
2. and define the decryption function $d_\pi(y) = \pi^{-1}(y)$, where $\pi^{-1}$is the inverse permutation to π.

For example, define Z to be the 26 letter English alphabet. Then, a random permutation π could be (plaintext characters are in lower case and cipher text characters in upper case)as shown in figure 1 **.**

Plaintext:

upon this basis i am going to show you how a bunch of bright young folks did find a champion a man with boys and girls of his own.

Key:

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

Figure 1: Example of a key of a single character substitution cipher.

Substitution Ciphers

1.1 Mono alphabetic
1.2 Poly alphabetic

Substitution Cipher:-

Is a symmetric cryptography ciphers, a substitution cipher is classify into two part (Mono alphabetic & Poly alphabetic).

In a substitution ciphers the value of character or character string is changed when transforming the plaintext into cipher text, but the position of the original string and its value replacement correspond exactly in the plain and cipher texts.

Plain Text Character:-

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

Cipher Text Character (key cipher)

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

Let the Plain text = "dulce et decorm est pro patria mori"

Now the cipher text is GXYUCCIGCUBLXQCFIRLBRHILEHQBLE

Note:- Remove all spaces, special characters in plain text

Example:

Keyword= CRYPTOGRAPHIC SYSTEM

P: 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

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

To encipher the plaintext= cryptography
ciphertext=YKXFNDGKCFAX

3-Polyalphabetic Ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is **polyalphabetic substitution cipher**. All these techniques 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.

The best known, and one of the simplest, such algorithm is referred to as the Vigenère cipher. In this scheme, the 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 a. Thus, a Caesar cipher with a shift of 3 is denoted by the key value *d*.

To aid in understanding the scheme and to aid in its use, a matrix known as the Vigenère tableau is constructed (Table 2.3). Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of encryption is simple: Given a key letter *x* and a plaintext letter y, the ciphertext letter is at the intersection of the row labeled *x* and the column labeled y; in this case the ciphertext is V.

3-1Poly alphabetic substitution ciphers

The poly alphabetic substitution cipher is a simple extension of the mono alphabetic one. The difference is that the message is broken into blocks of equal length, say B, and then each position in the block (1… B) is encrypted (or decrypted) using a different simple substitution cipher key. The block size (B) is often referred to as the period of the cipher.

All these techniques have the following features in common**.**

1. A set of related mono alphabetic substitution rules is used.

2. A key determines which particular rule is chosen for a given transformation[13, 21].

The best known, and one of the simplest, such algorithm is referred to as the Vigenère cipher. In this scheme, the set of related mono alphabetic substitution rules consists of the 26 Caesar ciphers, with shifts of 0 through 25 as shown in Table 1. Each cipher is denoted by a key letter, which is the cipher text letter that substitutes for the plaintext letter a. Thus, a Caesar cipher with a shift of 3 is denoted by the key value *d*. To aid in understanding the scheme and to aid in its use, a matrix known as the Vigenère tableau is constructed (Table.3. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of encryption is simple: Given a key letter *x* and a plaintext letter y, the cipher text letter is at the intersection of the row labeled *x* and the column labeled y; in this case the cipher text is V. Table 2 shows the cipher text in Vigenere method.

Table (1): Mapping Letters To Integers And Back

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The encryption function seen in Equation 2.

$$E(k, m_i) = m_i + k \pmod{26} \quad ....(2)$$

Table (2): Vigenere Cipher Encryption Example

Keyword:																													
S	U	B	S	T	I	T	U	T	I	O	N	S	U	B	S	T	I	T	U	T	I	O	N	S	U	B	S	T	I
As integer																													
18	20	1	18	19	8	19	20	19	8	14	13	18	20	1	18	19	8	19	20	19	8	14	13	18	19	1	18	19	8
Plaintext:																													
t	o	b	e	o	r	n	o	t	t	o	b	e	t	h	a	t	i	s	t	h	e	q	u	e	s	t	i	o	n
As integer																													
19	14	1	4	14	17	13	14	19	19	14	1	4	19	7	0	19	8	18	19	7	4	16	20	4	18	19	8	14	13
Addition																													
11	8	2	22	7	25	6	8	12	1	2	14	23	13	8	18	12	16	11	13	0	12	4	7	23	12	20	0	7	21
Cipher text:																													
L	I	C	W	H	Z	G	I	M	B	C	O	W	N	I	S	M	Q	L	N	A	M	E	H	W	M	U	A	H	V

The Vigenere Tableau

The Vigenere Cipher, proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century, is a poly alphabetic substitution based on the following tableau(Table 3).

For example, suppose we wish to encipher the plaintext message: “TO BE OR NOT TO BE THAT IS THE QUESTION", using the keyword SUBSTITUTION. We begin by writing the keyword, repeated as many times as necessary, above the plaintext message. To derive the ciphertext using the tableau, for each letter in the plaintext, one finds the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the cipher text letter[13, 23].

Table 3: The Vigenere Tableau

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

Lec. 3

4-Hill Cipher

Introduction

The computation used in the Hill cipher is based on linear algebra techniques. As time progressed, the study of cryptography continued to mature and, more recently, began to involve higher level mathematics. With this more advanced math came more advanced ciphers based on the idea of encryption and decryption keys. Encryption keys are a special value or set of values used in an encryption algorithm to convert a plaintext into a cipher text. A decryption key is the opposite. Decryption keys are used as part of a decryption algorithm to convert the cipher text back into the original plaintext.

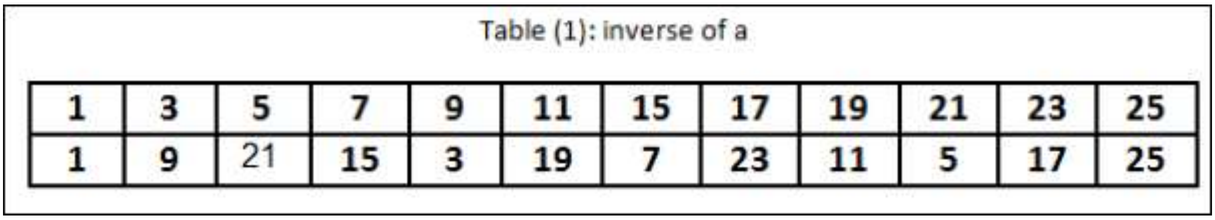


Table (1): inverse of a

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

Encryption Low

$C = (k * p) \bmod 26$

Decryption Low

$P = (k_{-1} * C) \bmod 26$

- **C** is the cipher text
- **k** is the key matrix or encryption matrix
- **k**$_{-1}$ inverse key matrix or decryption matrix
- **P** is the plaintext

Example 1

Use Hill cipher method to encrypt the plaintext ***"TOP SECRET MESSAGE"*** with

encryption matrix 3 2

5 7

Answer

•**Encryption process with the Hill Cipher:**

Encrypting text using the Hill cipher is accomplished by breaking a given plaintext into blocks of size *n* (where *n* is an integer), writing these blocks as column vectors, if you have an odd number of letters, repeat the last letter, and then multiplying these column vectors by any invertible *n* x *n* matrix.

The encryption matrix must be invertible because its inverse will be used to decrypt the cipher texts created with the Hill cipher and this encryption matrix. The inevitability of the encryption matrix allows us to say that its determinant must not be 0. The determinant of the encryption matrix must also be relatively prime to the size of the alphabet.

Compute the determinate of the matrix

This matrix has the determinant (3*7) – (2*5) = 21 – 10 = 11. Since 11 is ≠ 0, this matrix is invertible. 11 is also relatively prime to 26. These two qualities satisfy the requirements listed previously, making this encryption matrix a valid choice for use in the Hill cipher

Split the plaintext into blocks of size 2 (ignoring spaces), determine the letters' numerical values, and align these as column vectors. If the length of the plaintext is not evenly divisible by 2, add a previously decided character to the end of the string until the plaintext is evenly divisible by 2.

Divide the message (top secret message)to pairs

$$\begin{vmatrix} T \\ O \end{vmatrix} = \begin{vmatrix} 19 \\ 14 \end{vmatrix} \quad \begin{vmatrix} P \\ S \end{vmatrix} = \begin{vmatrix} 15 \\ 18 \end{vmatrix} \quad \begin{vmatrix} E \\ C \end{vmatrix} = \begin{vmatrix} 4 \\ 2 \end{vmatrix} \quad \begin{vmatrix} R \\ E \end{vmatrix} = \begin{vmatrix} 17 \\ 4 \end{vmatrix} \quad \begin{vmatrix} T \\ M \end{vmatrix} = \begin{vmatrix} 19 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} E \\ S \end{vmatrix} = \begin{vmatrix} 4 \\ 18 \end{vmatrix} \quad \begin{vmatrix} S \\ A \end{vmatrix} = \begin{vmatrix} 18 \\ 0 \end{vmatrix} \quad \begin{vmatrix} G \\ E \end{vmatrix} = \begin{vmatrix} 6 \\ 4 \end{vmatrix}$$

Multiply each of these column vectors by the encryption matrix and take mod 26 of the result. The encryption formula for hill method is

C = (k * p) mod 26

top secret message

C = (k * p) mod 26

$$\begin{vmatrix} T \\ O \end{vmatrix} = \begin{vmatrix} 19 \\ 14 \end{vmatrix}$$

$$\begin{vmatrix}3 & 2\\5 & 7\end{vmatrix}\begin{vmatrix}19\\14\end{vmatrix} = \begin{vmatrix}(3*19)+(2*14)\\(5*19)+(7*14)\end{vmatrix} = \begin{vmatrix}85\\193\end{vmatrix}(\text{mod } 26) = \begin{vmatrix}7\\11\end{vmatrix} = \begin{vmatrix}H\\L\end{vmatrix}$$

top secret message

C = (k * p) mod 26

$$\begin{vmatrix}P\\S\end{vmatrix} = \begin{vmatrix}15\\18\end{vmatrix}$$

$$\begin{vmatrix}3 & 2\\5 & 7\end{vmatrix}\begin{vmatrix}15\\18\end{vmatrix} = \begin{vmatrix}(3*15)+(2*18)\\(5*15)+(7*18)\end{vmatrix} = \begin{vmatrix}81\\201\end{vmatrix}(\text{mod } 26) = \begin{vmatrix}3\\19\end{vmatrix} = \begin{vmatrix}D\\T\end{vmatrix}$$

top secret message

C = (k * p) mod 26

$$\begin{vmatrix}E\\C\end{vmatrix} = \begin{vmatrix}4\\2\end{vmatrix}$$

$$\begin{vmatrix}3 & 2\\5 & 7\end{vmatrix}\begin{vmatrix}4\\2\end{vmatrix} = \begin{vmatrix}(3*4)+(2*2)\\(5*4)+(7*2)\end{vmatrix} = \begin{vmatrix}16\\34\end{vmatrix}(\text{mod } 26) = \begin{vmatrix}16\\8\end{vmatrix} = \begin{vmatrix}Q\\I\end{vmatrix}$$

top secret message

C = (k * p) mod 26

$$\begin{vmatrix}R\\E\end{vmatrix} = \begin{vmatrix}17\\4\end{vmatrix}$$

$$\begin{vmatrix}3 & 2\\5 & 7\end{vmatrix}\begin{vmatrix}17\\4\end{vmatrix} = \begin{vmatrix}(3*17)+(2*4)\\(5*17)+(7*4)\end{vmatrix} = \begin{vmatrix}59\\113\end{vmatrix}(\text{mod } 26) = \begin{vmatrix}7\\9\end{vmatrix} = \begin{vmatrix}H\\J\end{vmatrix}$$

top secret message

$$\begin{vmatrix} T \\ M \end{vmatrix} = \begin{vmatrix} 19 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 19 \\ 12 \end{vmatrix} = \begin{vmatrix} (3*19)+(2*12) \\ (5*19)+(7*12) \end{vmatrix} = \begin{vmatrix} 81 \\ 179 \end{vmatrix} \pmod{26} = \begin{vmatrix} 3 \\ 23 \end{vmatrix} = \begin{vmatrix} D \\ X \end{vmatrix}$$

$$\begin{vmatrix} E \\ S \end{vmatrix} = \begin{vmatrix} 4 \\ 18 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 4 \\ 18 \end{vmatrix} = \begin{vmatrix} (3*4)+(2*18) \\ (5*4)+(7*18) \end{vmatrix} = \begin{vmatrix} 48 \\ 146 \end{vmatrix} \pmod{26} = \begin{vmatrix} 22 \\ 16 \end{vmatrix} = \begin{vmatrix} W \\ Q \end{vmatrix}$$

$$\begin{vmatrix} S \\ A \end{vmatrix} = \begin{vmatrix} 18 \\ 0 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 18 \\ 0 \end{vmatrix} = \begin{vmatrix} (3*18)+(2*0) \\ (5*18)+(7*0) \end{vmatrix} = \begin{vmatrix} 54 \\ 90 \end{vmatrix} \pmod{26} = \begin{vmatrix} 2 \\ 12 \end{vmatrix} = \begin{vmatrix} C \\ M \end{vmatrix}$$

$$\begin{vmatrix} G \\ E \end{vmatrix} = \begin{vmatrix} 6 \\ 4 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 6 \\ 4 \end{vmatrix} = \begin{vmatrix} (3*6)+(2*4) \\ (5*6)+(7*4) \end{vmatrix} = \begin{vmatrix} 26 \\ 58 \end{vmatrix} \pmod{26} = \begin{vmatrix} 0 \\ 6 \end{vmatrix} = \begin{vmatrix} A \\ G \end{vmatrix}$$

Cipher text:

“HLDTQIHJDXWQCMAG”

Decryption process

•We are interested in how the party receiving a secret message encoded by the Hill cipher can decode it into the original plaintext. As previously described, the Hill cipher is based on matrix multiplication and any encryption matrix used in the Hill cipher must be invertible.The process is the same as encryption, but with the inverse matrix instead of the original encryption matrix.

•Decryption of the cipher text “HLDTQIHJDXWQCMAG” with the 2x2

encryption matrix previously defined would go as follows:

Example 2

Use hill cipher method to decryption the cipher text

“HLDTQIHJDXWQCMAG” with the 2x2 key

encryption [3 2

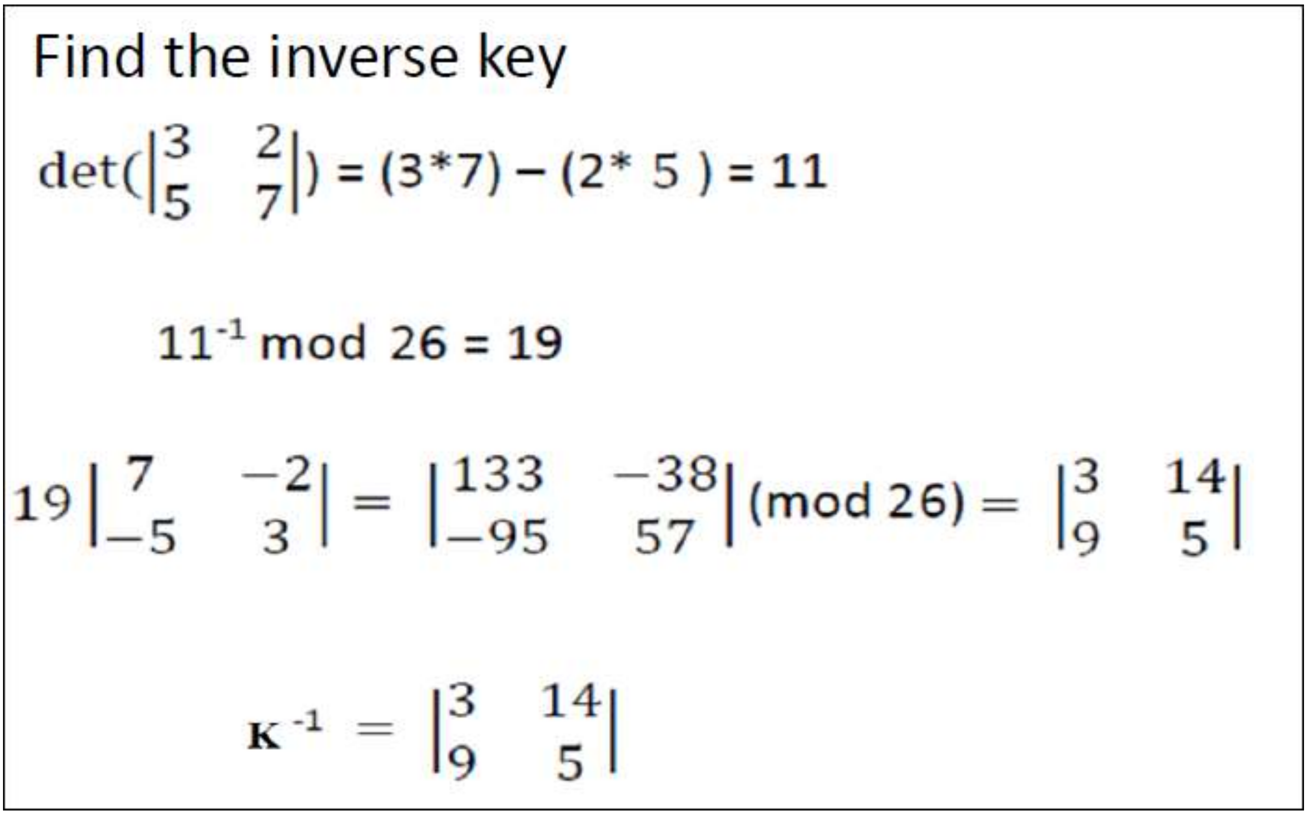
5 7]

Split the cipher text into blocks of 2, determine the letters’

numerical values, and align these as column vectors.

$\begin{vmatrix} H \\ L \end{vmatrix} = \begin{vmatrix} 7 \\ 11 \end{vmatrix}$ $\begin{vmatrix} D \\ T \end{vmatrix} = \begin{vmatrix} 3 \\ 19 \end{vmatrix}$ $\begin{vmatrix} Q \\ I \end{vmatrix} = \begin{vmatrix} 16 \\ 8 \end{vmatrix}$ $\begin{vmatrix} H \\ J \end{vmatrix} = \begin{vmatrix} 7 \\ 9 \end{vmatrix}$ $\begin{vmatrix} D \\ X \end{vmatrix} = \begin{vmatrix} 3 \\ 23 \end{vmatrix}$

$\begin{vmatrix} W \\ Q \end{vmatrix} = \begin{vmatrix} 22 \\ 16 \end{vmatrix}$ $\begin{vmatrix} C \\ M \end{vmatrix} = \begin{vmatrix} 2 \\ 12 \end{vmatrix}$ $\begin{vmatrix} A \\ G \end{vmatrix} = \begin{vmatrix} 0 \\ 6 \end{vmatrix}$



Find the inverse key

$$\det\left(\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix}\right) = (3*7) - (2*5) = 11$$

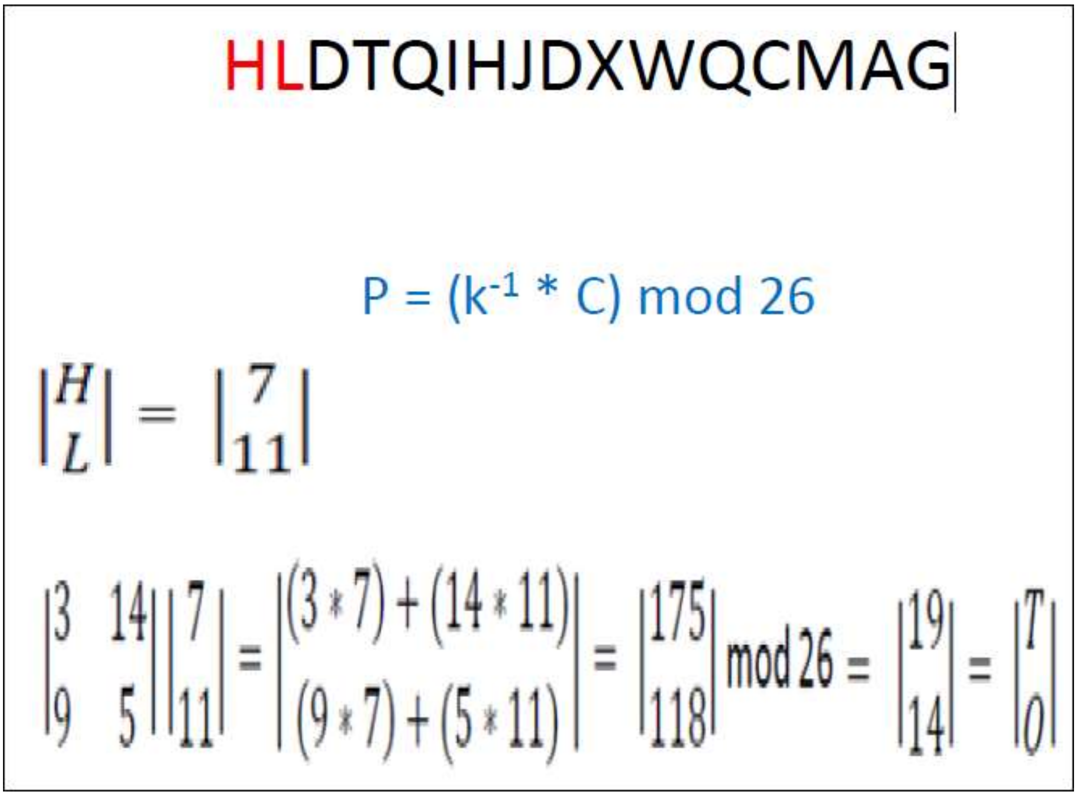
$$11^{-1} \bmod 26 = 19$$

$$19\begin{vmatrix} 7 & -2 \\ -5 & 3 \end{vmatrix} = \begin{vmatrix} 133 & -38 \\ -95 & 57 \end{vmatrix}(\text{mod } 26) = \begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix}$$

$$K^{-1} = \begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix}$$

Multiply each of these column vectors above by the decryption matrix calculated in step 1 and take mod 26 of the result. The decryption formula for hill method is

P = (k^{-1} * C) mod 26



HLDTQIHJDXWQCMAG

P = (k^{-1} * C) mod 26

$$\begin{vmatrix}H\\L\end{vmatrix} = \begin{vmatrix}7\\11\end{vmatrix}$$

$$\begin{vmatrix}3 & 14\\9 & 5\end{vmatrix}\begin{vmatrix}7\\11\end{vmatrix} = \begin{vmatrix}(3*7)+(14*11)\\(9*7)+(5*11)\end{vmatrix} = \begin{vmatrix}175\\118\end{vmatrix} \text{mod } 26 = \begin{vmatrix}19\\14\end{vmatrix} = \begin{vmatrix}T\\O\end{vmatrix}$$

$$\begin{vmatrix}D\\T\end{vmatrix} = \begin{vmatrix}3\\19\end{vmatrix}$$

$$\begin{vmatrix}3 & 14\\9 & 5\end{vmatrix}\begin{vmatrix}3\\19\end{vmatrix} = \begin{vmatrix}(3*3)+(14*19)\\(9*3)+(5*19)\end{vmatrix} = \begin{vmatrix}275\\122\end{vmatrix} \text{mod } 26 = \begin{vmatrix}15\\18\end{vmatrix} = \begin{vmatrix}P\\S\end{vmatrix}$$

$$\begin{vmatrix}Q\\I\end{vmatrix} = \begin{vmatrix}16\\8\end{vmatrix}$$

$$\begin{vmatrix}3 & 14\\9 & 5\end{vmatrix}\begin{vmatrix}16\\8\end{vmatrix} = \begin{vmatrix}(3*16)+(14*8)\\(9*16)+(5*8)\end{vmatrix} = \begin{vmatrix}160\\184\end{vmatrix} \text{mod } 26 = \begin{vmatrix}4\\2\end{vmatrix} = \begin{vmatrix}E\\C\end{vmatrix}$$

$$\begin{vmatrix}H\\J\end{vmatrix} = \begin{vmatrix}7\\9\end{vmatrix}$$

$$\begin{vmatrix}3 & 14\\9 & 5\end{vmatrix}\begin{vmatrix}7\\9\end{vmatrix} = \begin{vmatrix}(3*7)+(14*9)\\(9*7)+(5*9)\end{vmatrix} = \begin{vmatrix}147\\108\end{vmatrix} \text{mod } 26 = \begin{vmatrix}17\\4\end{vmatrix} = \begin{vmatrix}R\\E\end{vmatrix}$$

$$\begin{vmatrix} D \\ X \end{vmatrix} = \begin{vmatrix} 3 \\ 23 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 3 \\ 23 \end{vmatrix} = \begin{vmatrix} (3*3)+(14*23) \\ (9*3)+(5*23) \end{vmatrix} = \begin{vmatrix} 331 \\ 142 \end{vmatrix} \bmod 26 = \begin{vmatrix} 19 \\ 12 \end{vmatrix} = \begin{vmatrix} T \\ M \end{vmatrix}$$

$$\begin{vmatrix} W \\ Q \end{vmatrix} = \begin{vmatrix} 22 \\ 16 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 22 \\ 16 \end{vmatrix} = \begin{vmatrix} (3*22)+(14*16) \\ (9*22)+(5*16) \end{vmatrix} = \begin{vmatrix} 290 \\ 278 \end{vmatrix} \bmod 26 = \begin{vmatrix} 4 \\ 18 \end{vmatrix} = \begin{vmatrix} E \\ S \end{vmatrix}$$

$$\begin{vmatrix} C \\ M \end{vmatrix} = \begin{vmatrix} 2 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 2 \\ 12 \end{vmatrix} = \begin{vmatrix} (3*2)+(14*12) \\ (9*2)+(5*12) \end{vmatrix} = \begin{vmatrix} 174 \\ 78 \end{vmatrix} \bmod 26 = \begin{vmatrix} 18 \\ 0 \end{vmatrix} = \begin{vmatrix} S \\ A \end{vmatrix}$$

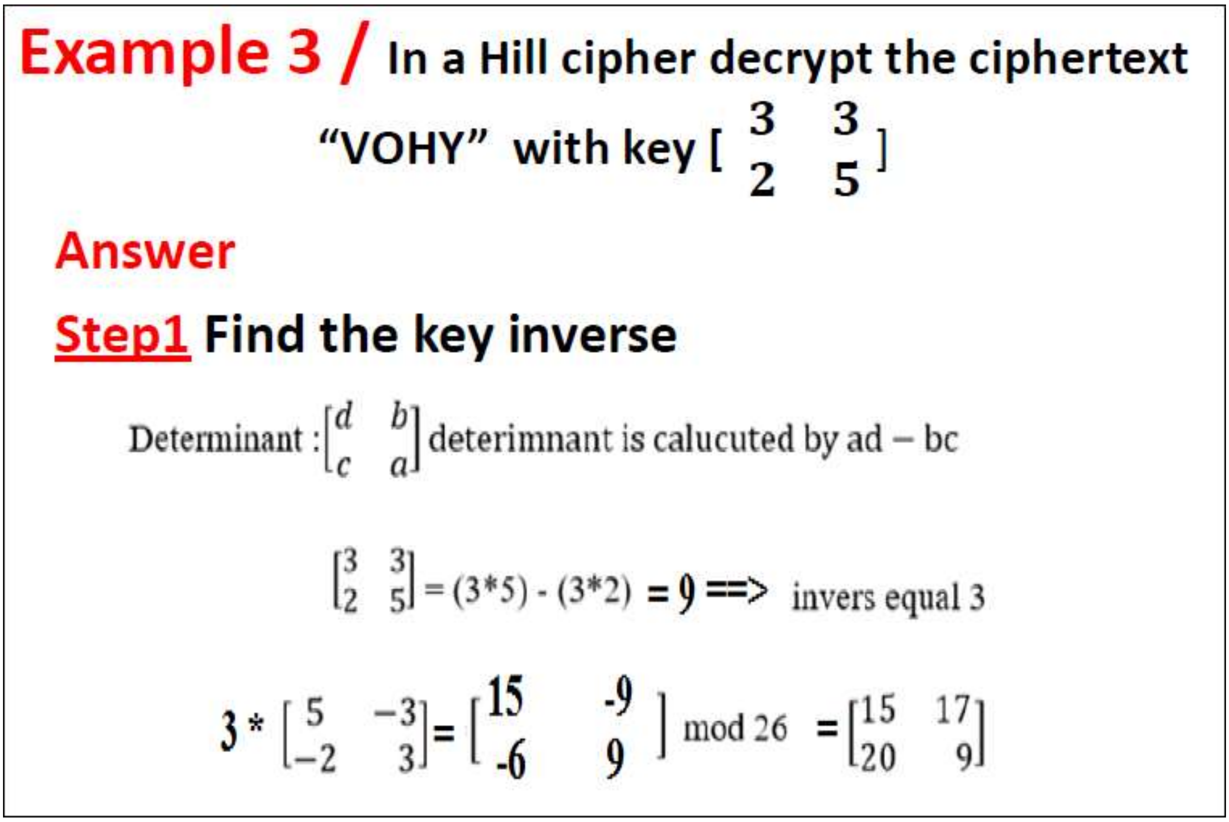
$$\begin{vmatrix} A \\ G \end{vmatrix} = \begin{vmatrix} 0 \\ 6 \end{vmatrix}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 0 \\ 6 \end{vmatrix} = \begin{vmatrix} (3*0)+(14*6) \\ (9*0)+(5*6) \end{vmatrix} = \begin{vmatrix} 84 \\ 30 \end{vmatrix} \bmod 26 = \begin{vmatrix} 6 \\ 4 \end{vmatrix} = \begin{vmatrix} G \\ E \end{vmatrix}$$

Decryption process

We are take the character above we get the Original plaintext:

“TOP SECRET MESSAGE”



Example 3 / In a Hill cipher decrypt the ciphertext "VOHY" with key $\left[\begin{matrix} 3 & 3 \\ 2 & 5 \end{matrix}\right]$

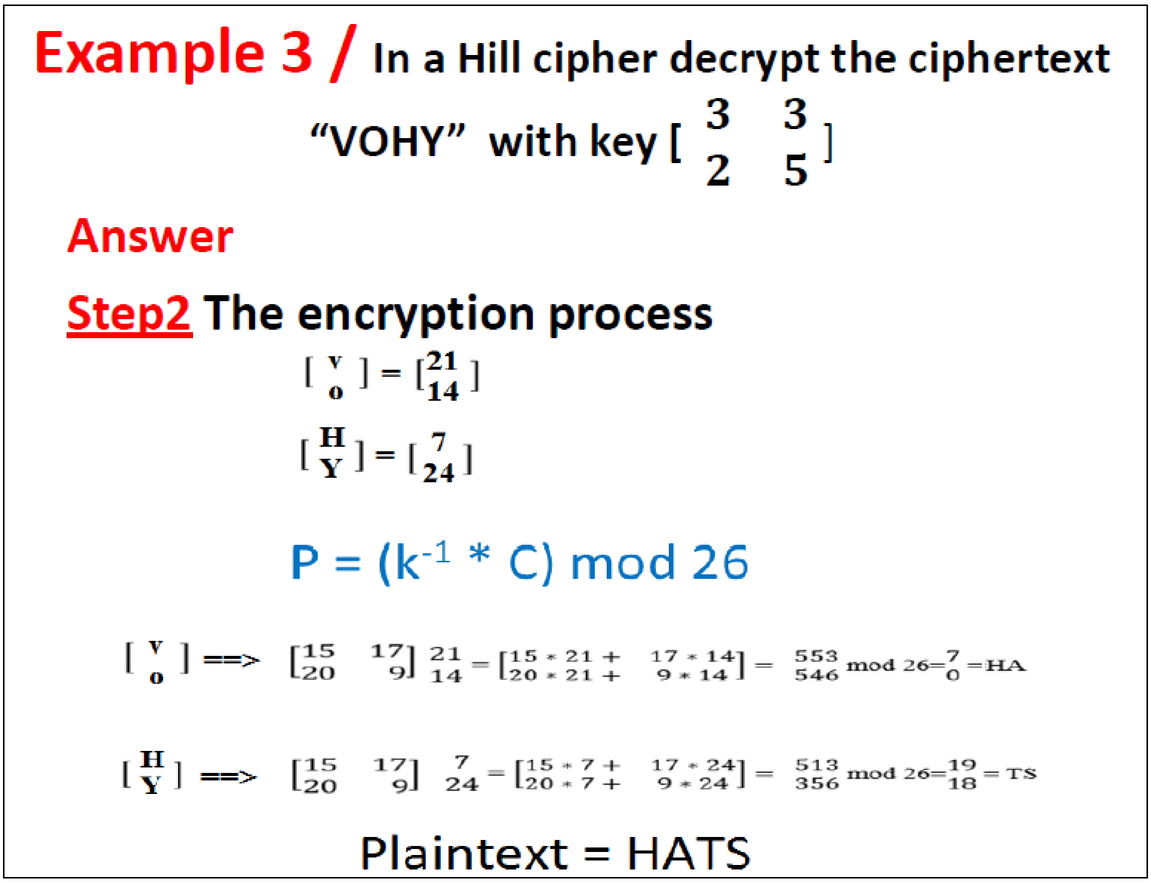
Answer

Step1 Find the key inverse

$$\text{Determinant}:\begin{bmatrix} d & b \\ c & a \end{bmatrix} \text{deterimnant is calucuted by } ad - bc$$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = (3*5) - (3*2) = 9 \Longrightarrow \text{ invers equal 3}$$

$$3 * \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$



Example 3 / In a Hill cipher decrypt the ciphertext "VOHY" with key $\left[\begin{matrix} 3 & 3 \\ 2 & 5 \end{matrix}\right]$

Answer

Step2 The encryption process

$$\left[\begin{matrix} \text{v} \\ \text{o} \end{matrix}\right] = \left[\begin{matrix} 21 \\ 14 \end{matrix}\right]$$

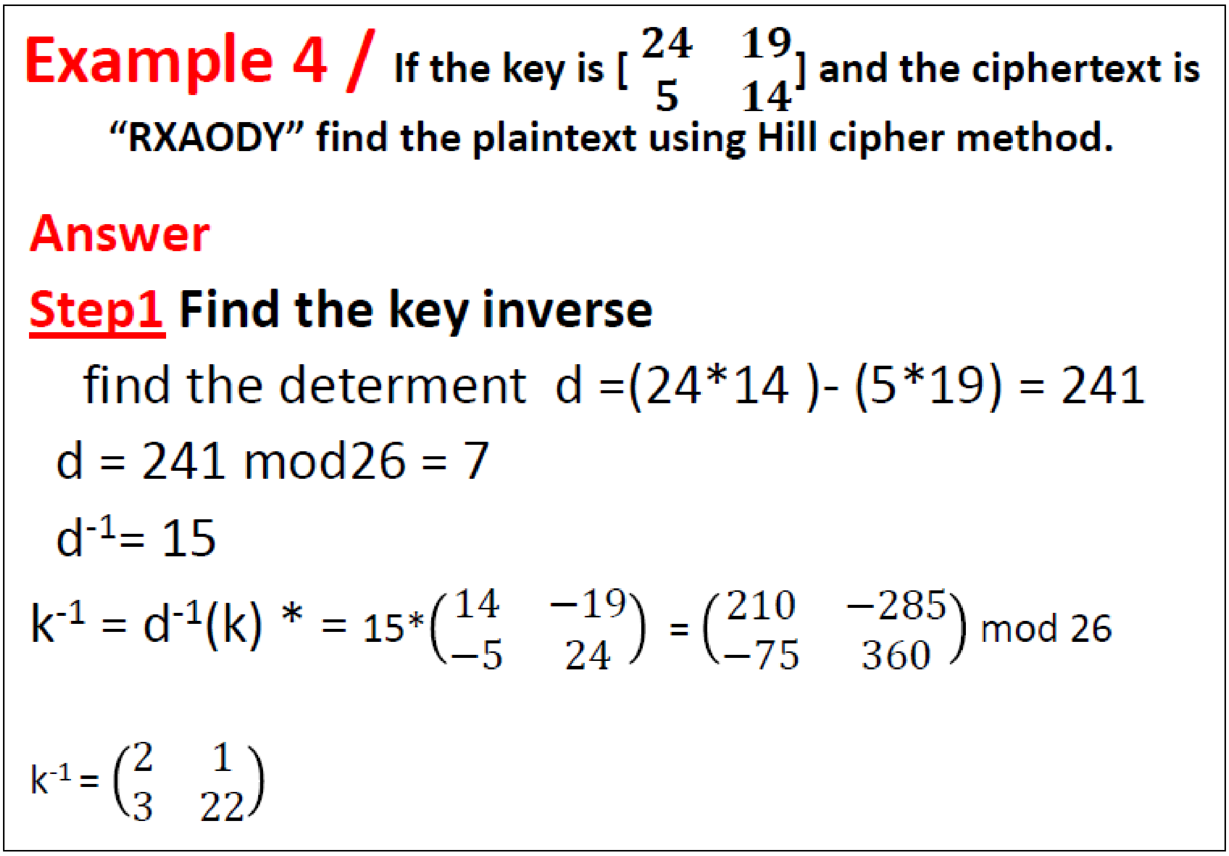
$$\left[\begin{matrix} \text{H} \\ \text{Y} \end{matrix}\right] = \left[\begin{matrix} 7 \\ 24 \end{matrix}\right]$$

$$P = (k^{-1} * C) \bmod 26$$

$$\left[\begin{matrix} \text{v} \\ \text{o} \end{matrix}\right] \Longrightarrow \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{matrix} 21 \\ 14 \end{matrix} = \begin{bmatrix} 15 * 21 + & 17 * 14 \\ 20 * 21 + & 9 * 14 \end{bmatrix} = \begin{matrix} 553 \\ 546 \end{matrix} \bmod 26 = \begin{matrix} 7 \\ 0 \end{matrix} = \text{HA}$$

$$\left[\begin{matrix} \text{H} \\ \text{Y} \end{matrix}\right] \Longrightarrow \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{matrix} 7 \\ 24 \end{matrix} = \begin{bmatrix} 15 * 7 + & 17 * 24 \\ 20 * 7 + & 9 * 24 \end{bmatrix} = \begin{matrix} 513 \\ 356 \end{matrix} \bmod 26 = \begin{matrix} 19 \\ 18 \end{matrix} = \text{TS}$$

Plaintext = HATS



Example 4 / If the key is $\begin{bmatrix}24 & 19\\ 5 & 14\end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

Answer

Step1 **Find the key inverse**

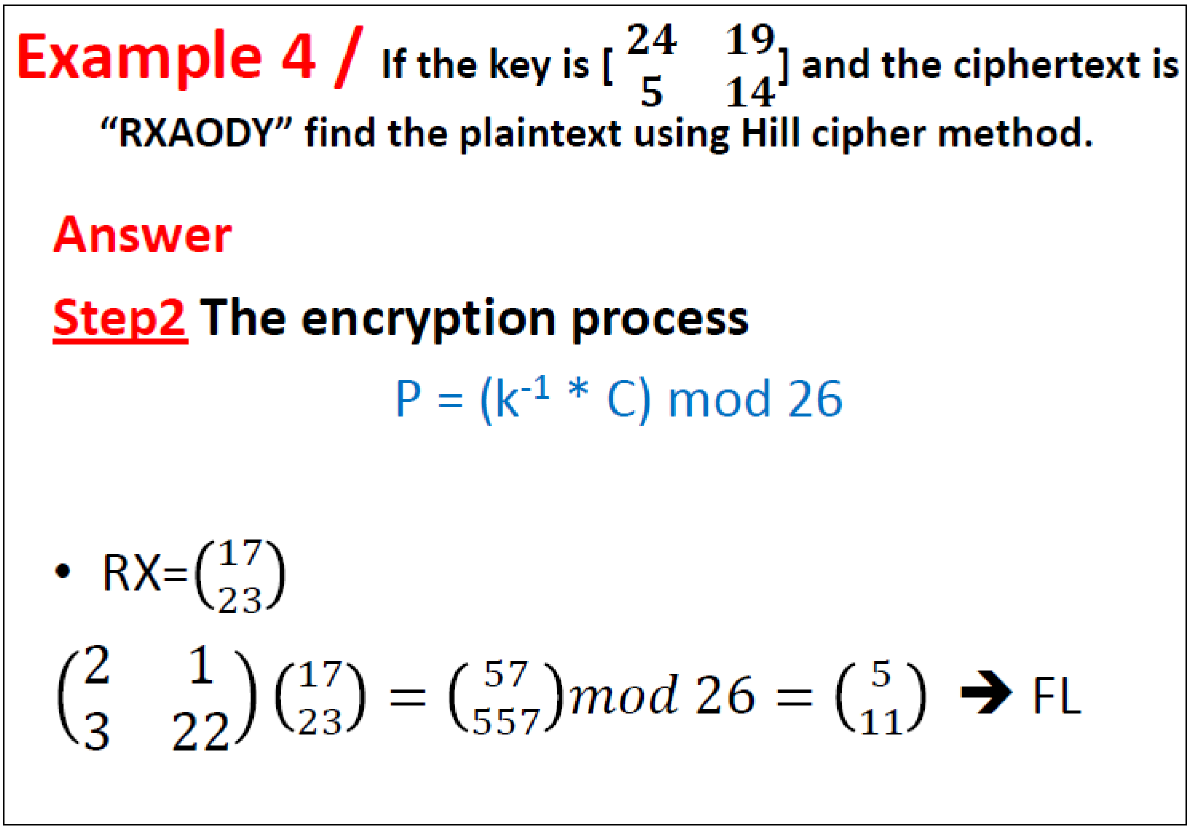
find the determent d =(24*14)- (5*19) = 241

d = 241 mod26 = 7

d^{-1}= 15

$k^{-1} = d^{-1}(k)^{*} = 15*\begin{pmatrix}14 & -19\\ -5 & 24\end{pmatrix} = \begin{pmatrix}210 & -285\\ -75 & 360\end{pmatrix} \bmod 26$

$k^{-1} = \begin{pmatrix}2 & 1\\ 3 & 22\end{pmatrix}$



Example 4 / If the key is $\begin{bmatrix}24 & 19\\ 5 & 14\end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

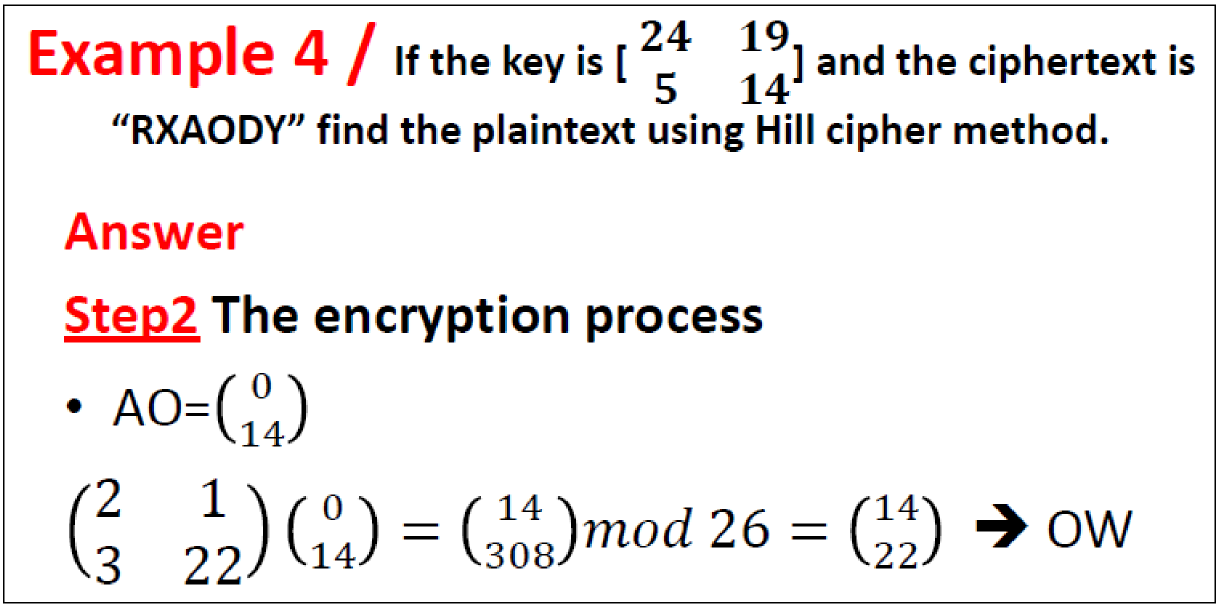
Answer

Step2 **The encryption process**

$P = (k^{-1} * C) \bmod 26$

- $RX=\binom{17}{23}$

$\begin{pmatrix}2 & 1\\ 3 & 22\end{pmatrix}\binom{17}{23} = \binom{57}{557} mod\ 26 = \binom{5}{11}$ → FL



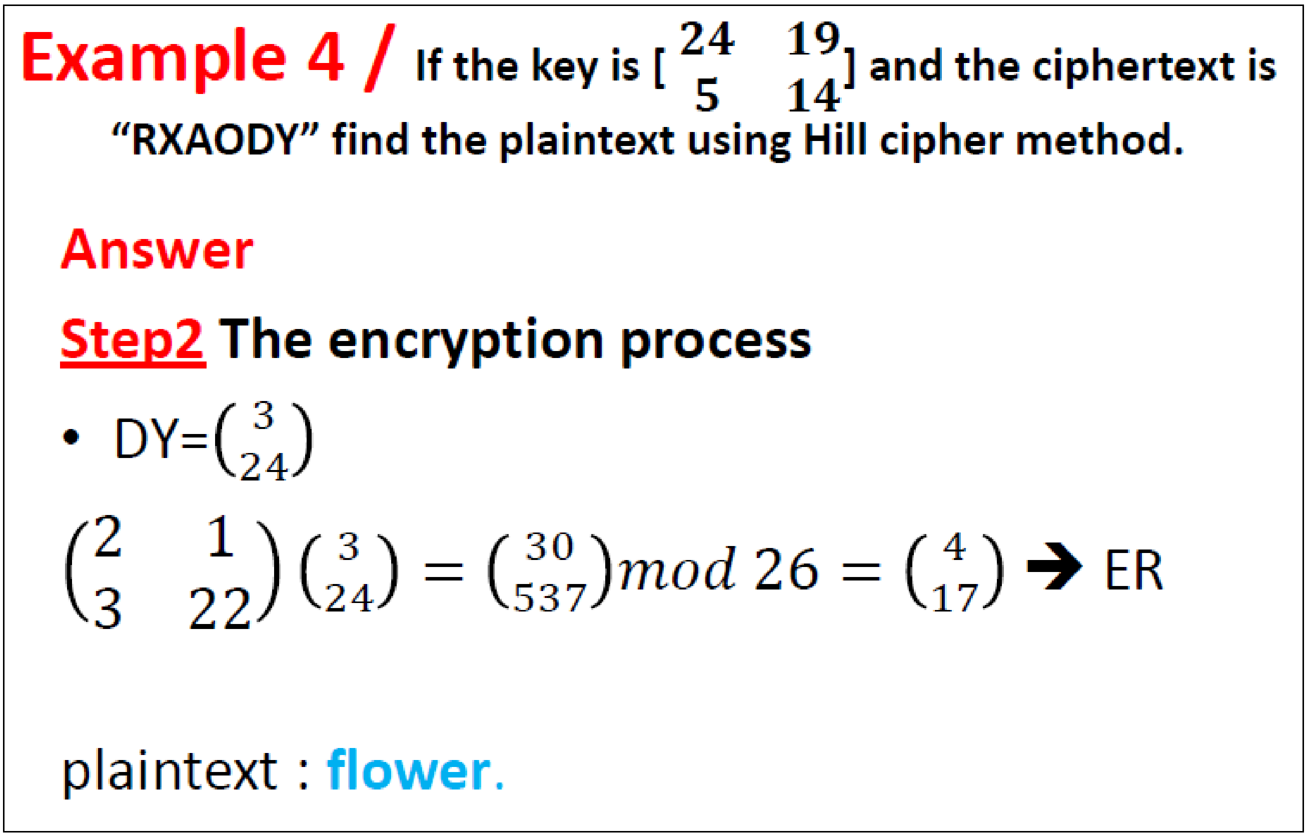
Example 4 / If the key is $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

Answer

Step2 **The encryption process**

- AO=$\begin{pmatrix} 0 \\ 14 \end{pmatrix}$

$$\begin{pmatrix} 2 & 1 \\ 3 & 22 \end{pmatrix} \begin{pmatrix} 0 \\ 14 \end{pmatrix} = \begin{pmatrix} 14 \\ 308 \end{pmatrix} mod\ 26 = \begin{pmatrix} 14 \\ 22 \end{pmatrix}$$ ➔ OW



Example 4 / If the key is $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$ and the ciphertext is "RXAODY" find the plaintext using Hill cipher method.

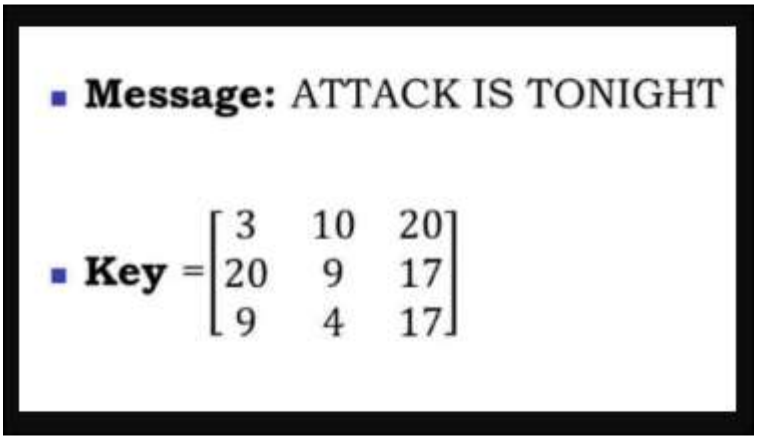
Answer

Step2 **The encryption process**

- DY=$\begin{pmatrix} 3 \\ 24 \end{pmatrix}$

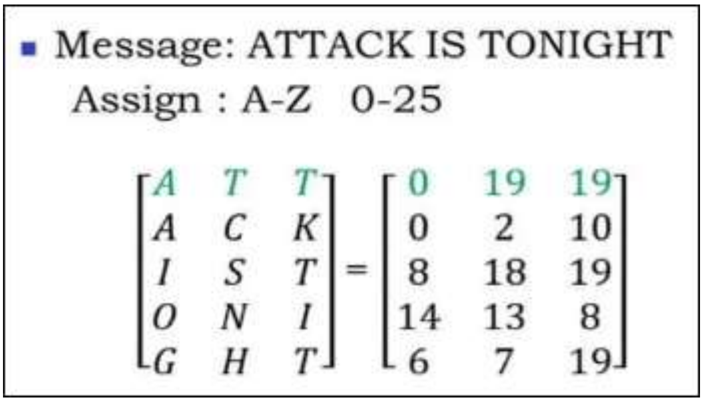
$$\begin{pmatrix} 2 & 1 \\ 3 & 22 \end{pmatrix} \begin{pmatrix} 3 \\ 24 \end{pmatrix} = \begin{pmatrix} 30 \\ 537 \end{pmatrix} mod\ 26 = \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$ ➔ ER

plaintext : flower.



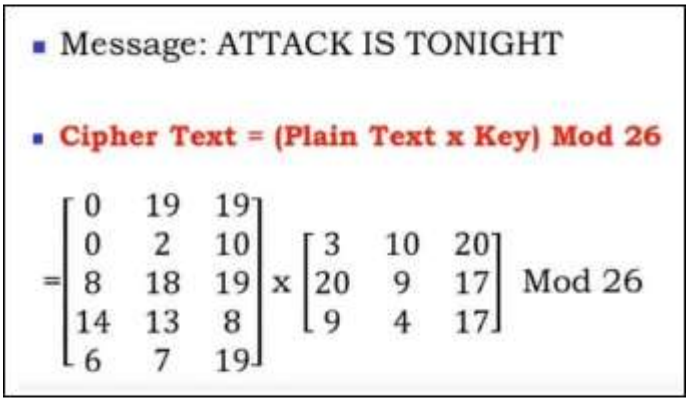
- **Message:** ATTACK IS TONIGHT
- **Key** = $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

The **first step** is to convert the given keyword to a 3x3 matrix form. Next, convert the keyword matrix into a key matrix by replacing the letters with corresponding numeric values.



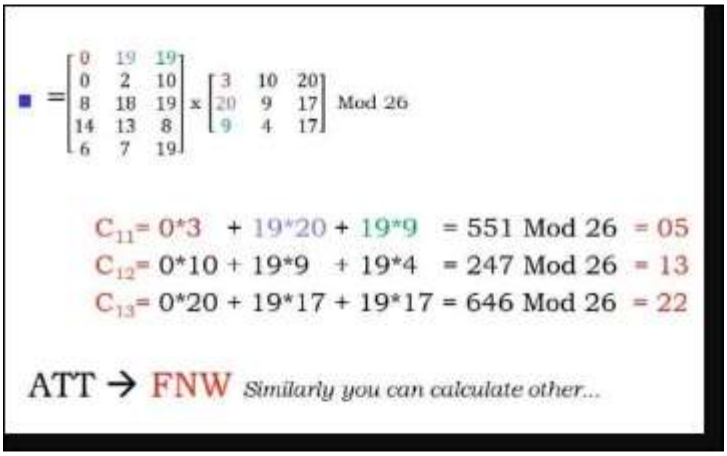
- Message: ATTACK IS TONIGHT
  Assign : A-Z 0-25

$$\begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix} = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$



- Message: ATTACK IS TONIGHT
- **Cipher Text = (Plain Text x Key) Mod 26**

$$= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \text{x} \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \text{Mod } 26$$

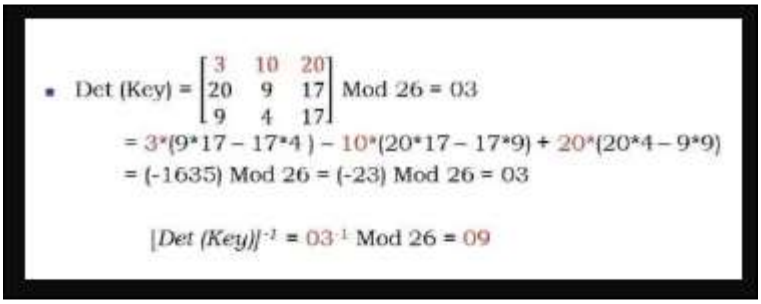


- $= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \times \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \text{ Mod } 26$

C_{11}= 0*3 + 19*20 + 19*9 = 551 Mod 26 = 05
C_{12}= 0*10 + 19*9 + 19*4 = 247 Mod 26 = 13
C_{13}= 0*20 + 19*17 + 19*17 = 646 Mod 26 = 22

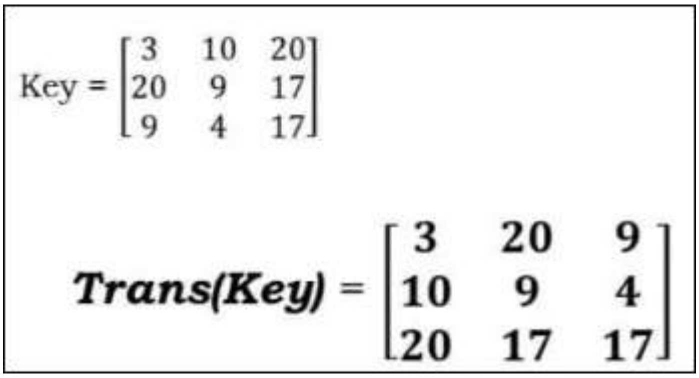
ATT → FNW *Similarly you can calculate other...*

Decryption



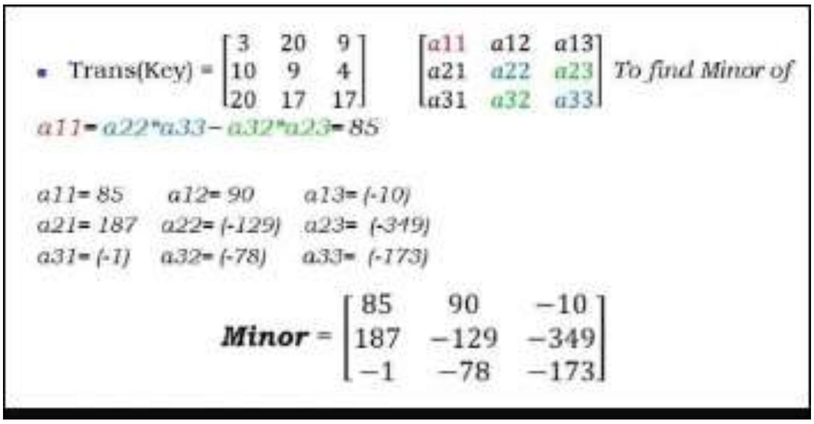
- Det (Key) = $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$ Mod 26 = 03
  = 3*(9*17 – 17*4) – 10*(20*17 – 17*9) + 20*(20*4 – 9*9)
  = (-1635) Mod 26 = (-23) Mod 26 = 03

  $[Det\ (Key)]^{-1}$ = 03^{-1} Mod 26 = 09



Key = $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

Trans(Key) = $\begin{bmatrix} \mathbf{3} & \mathbf{20} & \mathbf{9} \\ \mathbf{10} & \mathbf{9} & \mathbf{4} \\ \mathbf{20} & \mathbf{17} & \mathbf{17} \end{bmatrix}$

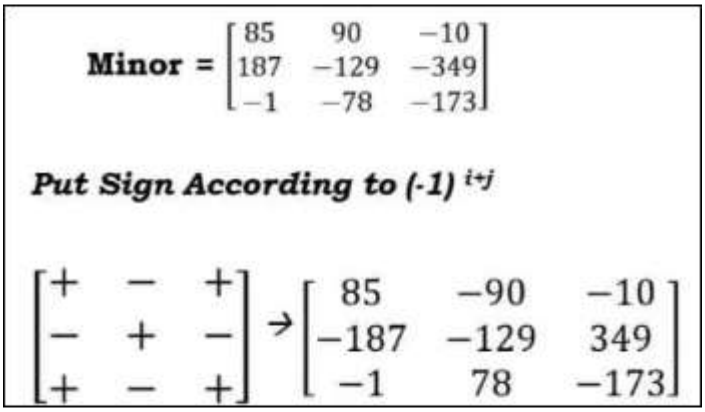


- Trans(Key) = $\begin{bmatrix} 3 & 20 & 9 \\ 10 & 9 & 4 \\ 20 & 17 & 17 \end{bmatrix}$ $\begin{bmatrix} a11 & a12 & a13 \\ a21 & a22 & a23 \\ a31 & a32 & a33 \end{bmatrix}$ *To find Minor of*

*a11= a22*a33− a32*a23= 85*

a11= 85 *a12= 90* *a13= (-10)*
a21= 187 *a22= (-129)* *a23= (-349)*
a31= (-1) *a32= (-78)* *a33= (-173)*

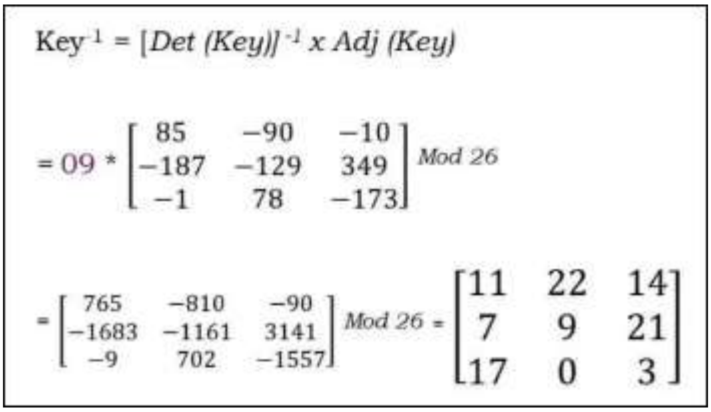
$$\textbf{\textit{Minor}} = \begin{bmatrix} 85 & 90 & -10 \\ 187 & -129 & -349 \\ -1 & -78 & -173 \end{bmatrix}$$



$$\textbf{Minor} = \begin{bmatrix} 85 & 90 & -10 \\ 187 & -129 & -349 \\ -1 & -78 & -173 \end{bmatrix}$$

Put Sign According to (-1) $^{i+j}$

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} \rightarrow \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix}$$



Key $^{-1}$ = *[Det (Key)]* $^{-1}$ *x Adj (Key)*

$$= 09 * \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix} \textit{Mod 26}$$

$$= \begin{bmatrix} 765 & -810 & -90 \\ -1683 & -1161 & 3141 \\ -9 & 702 & -1557 \end{bmatrix} \textit{Mod 26} = \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}$$

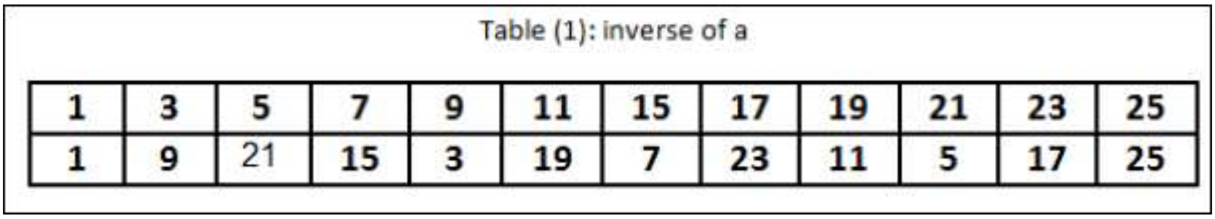


Table (1): inverse of a

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

https://www.cliffsnotes.com/study-notes/7281430

This cipher is somewhat more difficult to understand than the others in this chapter, but it illustrates an important point about cryptanalysis that will be useful later on. This subsection can be skipped on a first reading.

Another interesting multi letter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929. The encryption algorithm takes *m* successive plaintext letters and substitutes for them *m* ciphertext letters. The substitution is determined by *m* linear equations in which each character is assigned a numerical value (a = 0, b = 1 ... z = 25). For *m* = 3, the system can be described as follows:

$$c1 = (k11P1 + k12P2 + k13P3) \bmod 26$$
$$c2 = (k21P1 + k22P2 + k23P3) \bmod 26$$
$$c3 = (k31P1 + k32P2 + k33P3) \bmod 26$$

This can be expressed in term of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{KP} \bmod 26$$

where **C** and **P** are column vectors of length 3, representing the plaintext and ciphertext, and **K** is a 3 x 3 matrix, representing the

encryption key. Operations are performed mod 26.

For example, consider the plaintext "paymoremoney" and use the encryption key

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

The first three letters of the plaintext are represented by the vector

$\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$. Then $\mathbf{K}\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$ = LNS. Continuing in this fashion,

the ciphertext for the entire plaintext is LNSHDLEWMTRW.

Decryption requires using the inverse of the matrix **K**. The inverse **K**1 of a matrix **K** is defined by the equation **KK**^{1}= **K**^{1}**K** = **I**, where **I** is the matrix that is all zeros except for ones along the main diagonal from upper left to lower right. The inverse of a matrix does not always exist, but when it does, it satisfies the preceding equation. In this case, the inverse is:

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

This is demonstrated as follows:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

It is easily seen that if the matrix **K**1 is applied to the ciphertext, then the plaintext is recovered. To explain how the inverse of a matrix is determined, we make an exceedingly brief excursion into linear algebra.

For any square matrix (*m* x *m*) the **determinant** equals the sum of all the products that can be formed by taking exactly one element from each row and exactly one element from each column, with certain of the product terms preceded by a minus sign. For a 2 x 2 matrix

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

the determinant is *k*11*k*22 *k*12*k*21. For a 3 x 3 matrix, the value of the determinant is *k* 11*k*22*k*33 + *k*21*k*32*k*13 + *k*31*k*12*k*23 *k*31*k*22*k*13

*k*21*k*12*k*33 *k*11*k*32*k*23. If a square matrix **A** has a nonzero determinant, then the inverse of the matrix is computed as **A** [1]*ij* =(1)$^{i+j}$ (D*ij*)/ded(**A**), where (D*ij*) is the sub-determinant formed by deleting the *i*th row and the *j*th column of **A** and det(**A**) is the determinant of

A. For our purposes, all arithmetic is done mod 26.

In general terms, the Hill system can be expressed as follows:

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{KP} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{P}) = \mathbf{K}^{1}\mathbf{C} \bmod 26 = \mathbf{K}^{1}\mathbf{KP} = \mathbf{P}$$

As with Playfair, the strength of the Hill cipher is that it completely hides single-letter frequencies. Indeed, with Hill, the use of a larger matrix hides more frequency information. Thus a 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information.

Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack. For an *m* x *m* Hill cipher, suppose we have *m* plaintext-ciphertext pairs, each of length *m*. We label the pairs

As with Playfair, the strength of the Hill cipher is that it completely hides single-letter frequencies. Indeed, with Hill, the use of a larger matrix hides more frequency information. Thus a 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information.

Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack. For an *m* x *m* Hill cipher, suppose we have *m* plaintext-ciphertext pairs, each of length *m*. We label the pairs

$$\mathbf{P}_j = \begin{pmatrix} p_{1j} \\ p_{2j} \\ \vdots \\ p_{mj} \end{pmatrix} \text{ and } \mathbf{C}_j = \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{mj} \end{pmatrix} \text{ such that } \mathbf{C}_j = \mathbf{KP}_j \text{ for } 1 \le j \le m \text{ and for some}$$

unknown key matrix **K**. Now define two *m* x *m* matrices **X** = (*Pij*) and **Y** = (*Cij*). Then we can form the matrix equation **Y** = **KX**. If **X** has an inverse, then we can determine

K = YX

If **X** is not invertible, then a new version of **X** can be formed with additional plaintext-ciphertext pairs until an invertible **X** is obtained.

We use an example. Suppose that the plaintext "friday" is encrypted using a 2 x 2 Hill cipher to yield the

ciphertext PQCFKU. Thus, we know that

$$\mathbf{K}\begin{pmatrix}5\\17\end{pmatrix} \bmod 26 = \begin{pmatrix}15\\16\end{pmatrix};\ \mathbf{K}\begin{pmatrix}8\\3\end{pmatrix} \bmod 26 = \begin{pmatrix}2\\5\end{pmatrix}; \quad \text{and} \quad \mathbf{K}\begin{pmatrix}0\\24\end{pmatrix} \bmod 26 = \begin{pmatrix}10\\20\end{pmatrix}$$

Using the first two plaintext-ciphertext pairs, we have

$$\begin{pmatrix}15 & 2\\16 & 5\end{pmatrix} = \mathbf{K}\begin{pmatrix}5 & 8\\17 & 3\end{pmatrix} \bmod 26$$

The inverse of **X** can be computed:

$$\begin{pmatrix}5 & 8\\17 & 3\end{pmatrix}^{-1} = \begin{pmatrix}9 & 2\\1 & 15\end{pmatrix}$$

So

$$\mathbf{K} = \begin{pmatrix}15 & 2\\16 & 5\end{pmatrix}\begin{pmatrix}9 & 2\\1 & 15\end{pmatrix} = \begin{pmatrix}137 & 60\\149 & 107\end{pmatrix} \bmod 26 = \begin{pmatrix}7 & 8\\19 & 3\end{pmatrix}$$

This result is verified by testing the remaining plaintext-ciphertext pair.