Unit 3

Cryptography: Encryption, Decryption, Substitution and Transposition, Confusion and diffusion, Symmetric and Asymmetric encryption, Stream and Block ciphers, DES, cryptanalysis. Public-key cryptography, Diffie-Hellman key exchange, man-in-the-middle attack Digital signature, Steganography, Watermarking

Basic Concepts

Cryptography The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

Plaintext The original intelligible message

Cipher text The transformed message

Cipher An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key Some critical information used by the cipher, known only to the sender& receiver

Encipher (encode) The process of converting plaintext to cipher text using a cipher and a key

Decipher (decode) the process of converting cipher text back into plaintext using a cipher and a key

Cryptanalysis The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **code breaking**

Cryptology Both cryptography and cryptanalysis

Code An algorithm for transforming an intelligible message into an unintelligible one using a code-book

- **cipher text** - the coded message
- **Cipher** - algorithm for transforming plaintext to cipher text
- **Key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to cipher text
- **decipher (decrypt)** - recovering cipher text from plaintext
- **Cryptography** - study of encryption principles/methods

Cryptanalysis (code breaking) - the study of principles/ methods of deciphering cipher text *without* knowing key

- **Cryptology** - the field of both cryptography and cryptanalysis

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

Cryptographic Systems are categorized according to:

1. The operation used in transferring plaintext to ciphertext:

   - **Substitution:** each element in the plaintext is mapped into another element

   - **Transposition:** the elements in the plaintext are re-arranged.

2. The number of keys used:

   - **Symmetric (private- key)** : both the sender and receiver use the same key

   - **Asymmetric (public-key)** : sender and receiver use different key

3. The way the plaintext is processed :

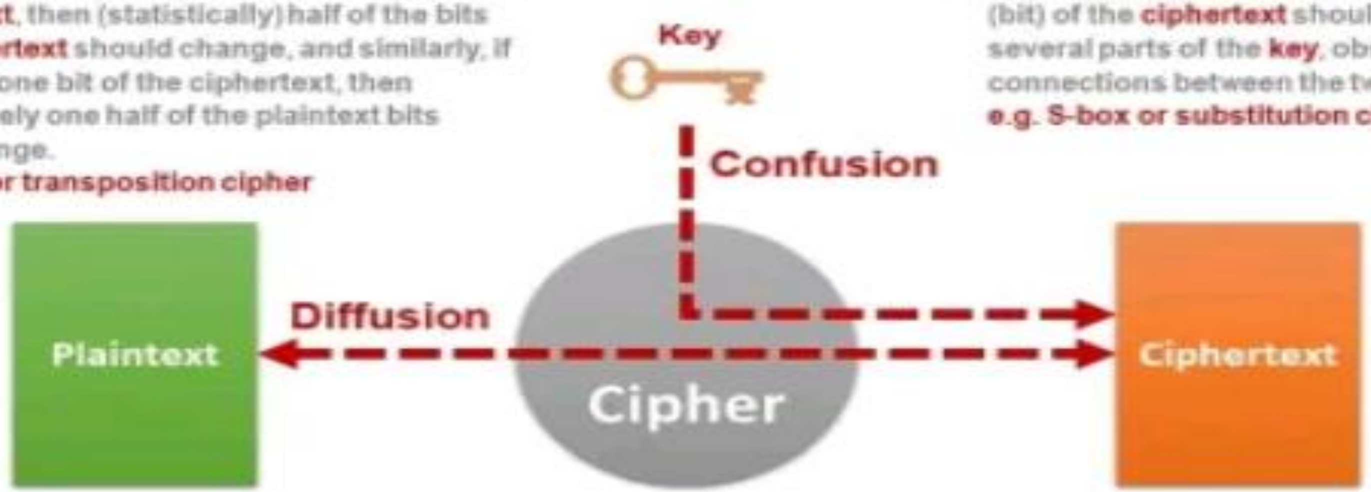
   - **Block cipher** : inputs are processed one block at a time, producing a corresponding output block.

   - **Stream cipher**: inputs are processed continuously, producing one element at a time (bit,

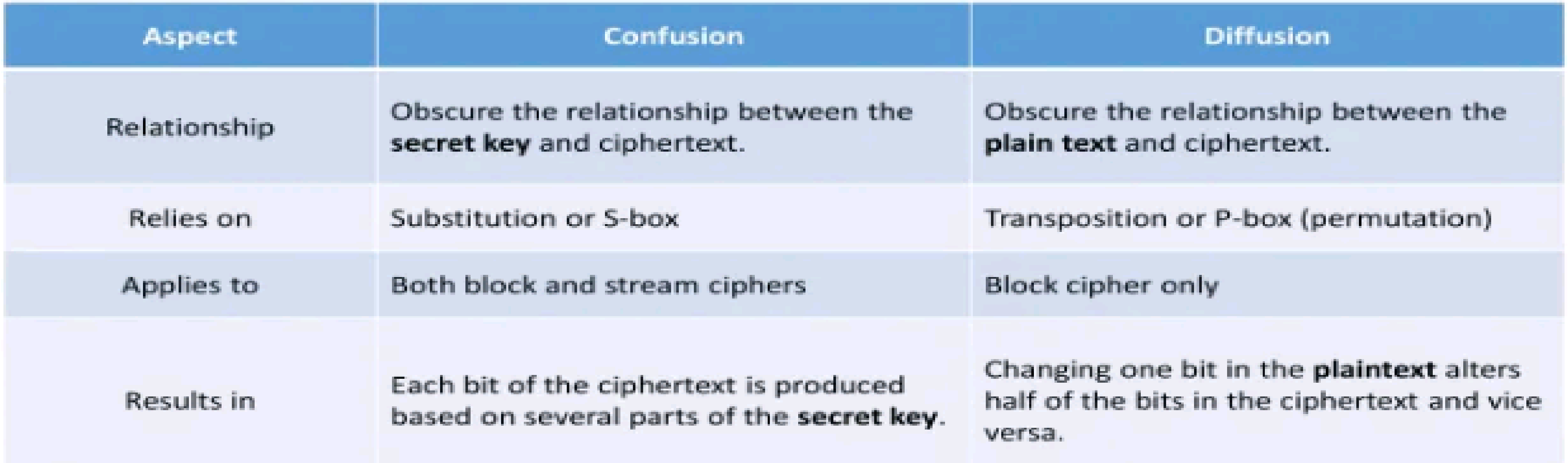
Confusion and Diffusion

Diffusion means that if we change a single bit of the **plaintext**, then (statistically) half of the bits in the **ciphertext** should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.
e.g. P-box or transposition cipher

Confusion means that each binary digit (bit) of the **ciphertext** should depend on several parts of the **key**, obscuring the connections between the two.
e.g. S-box or substitution cipher

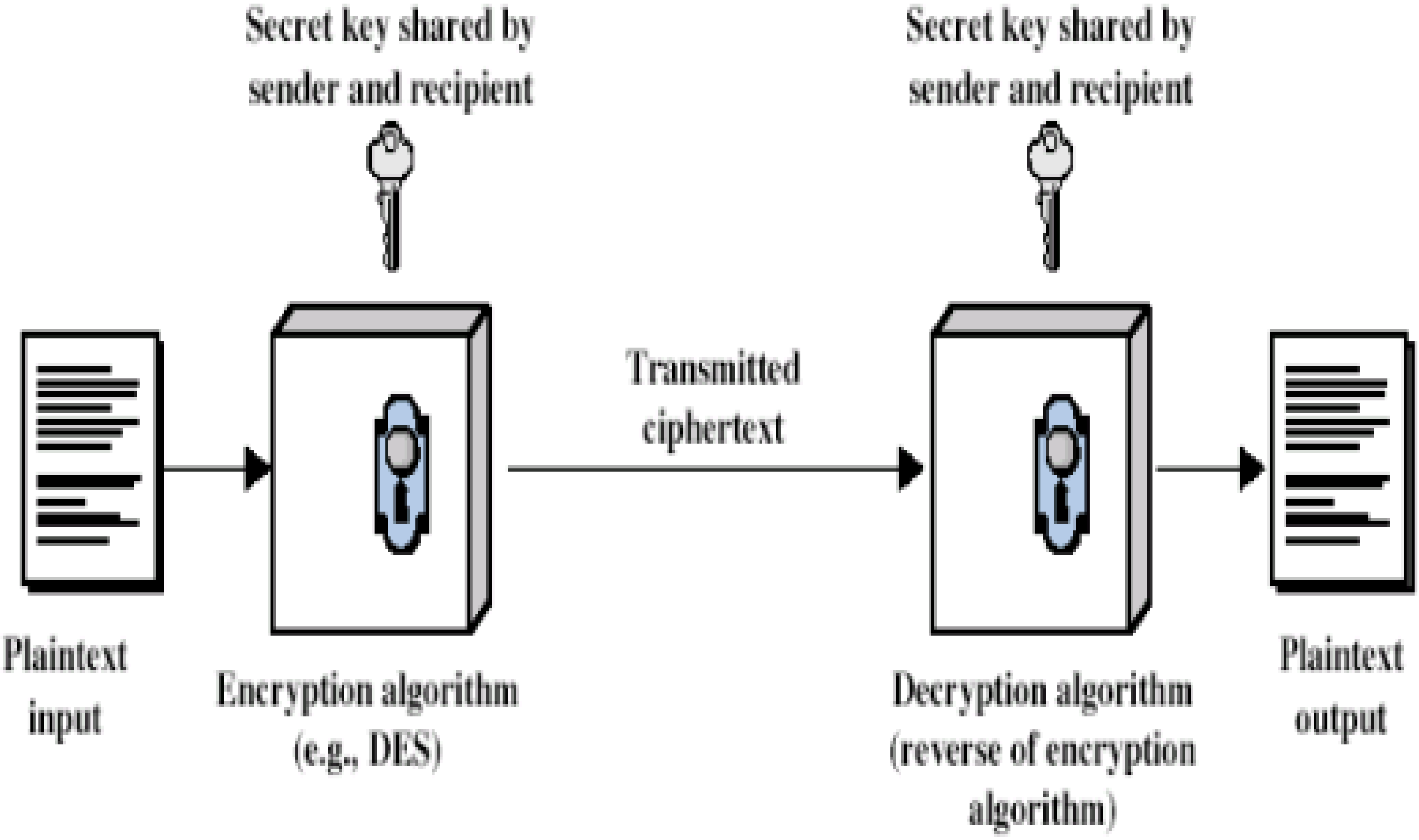


Confusion and Diffusion



Aspect	Confusion	Diffusion
Relationship	Obscure the relationship between the **secret key** and ciphertext.	Obscure the relationship between the **plain text** and ciphertext.
Relies on	Substitution or S-box	Transposition or P-box (permutation)
Applies to	Both block and stream ciphers	Block cipher only
Results in	Each bit of the ciphertext is produced based on several parts of the **secret key**.	Changing one bit in the **plaintext** alters half of the bits in the ciphertext and vice versa.

Symmetric Encryption Model


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

- two requirements for secure use of symmetric encryption:

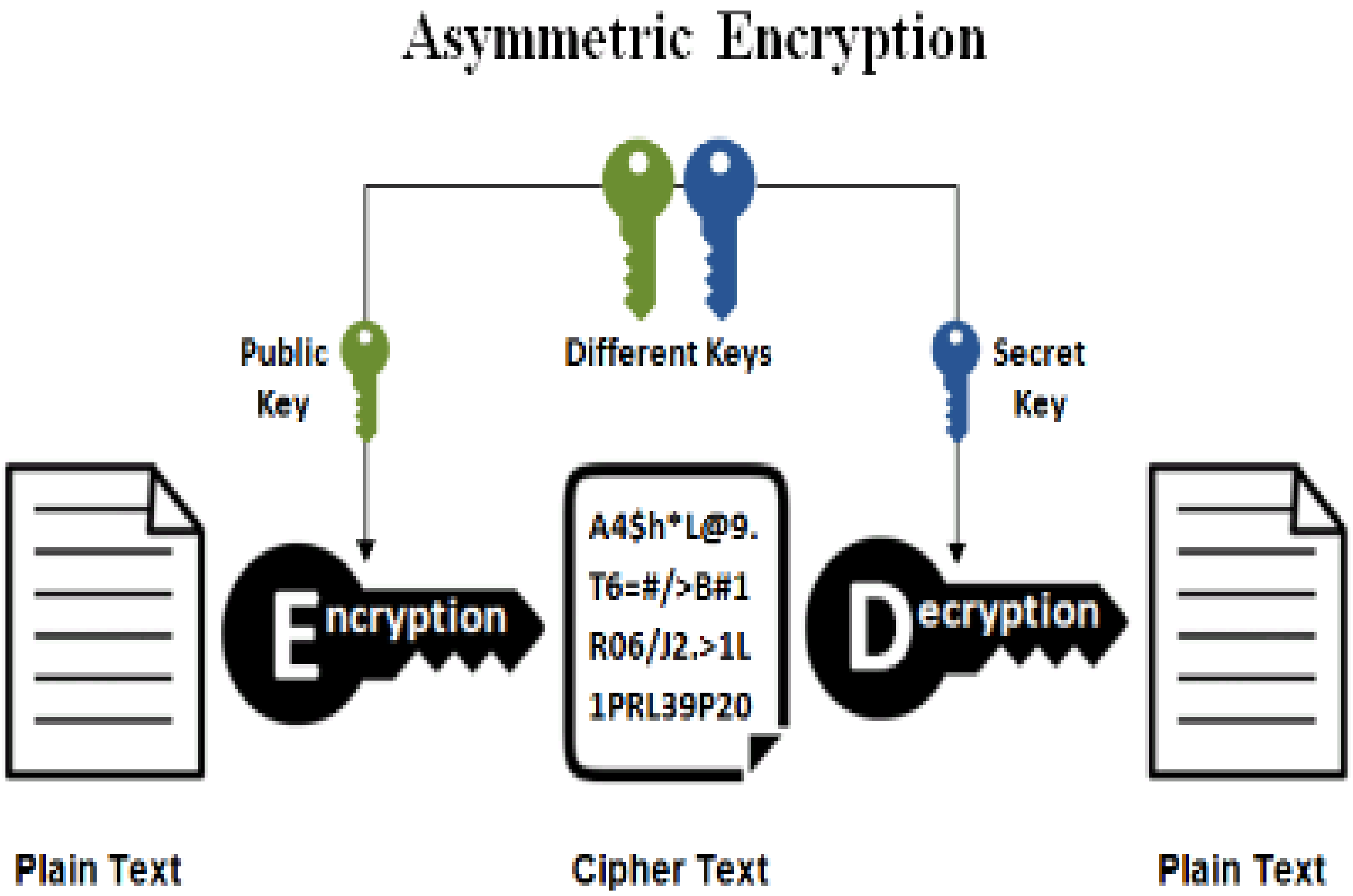
1. a strong encryption algorithm
2. a secret key known only to sender / receiver

   - $Y = E_k(X)$, where X: the plaintext, Y: the ciphertext
   - $X = D_k(Y)$

Attacks:

1. Cryptanalytic Attacks: depends on the nature of the encryption algorithm used.
   - Uses information such as plaintext/ciphertext pairs to deduce the key
2. Brute-force Attack: try all the possible keys – depends on the key length.

Public Key Encryption



CLASSICAL ENCRYPTION TECHNIQUES

Substitution Techniques

It is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

Monoalphabetic Cipher

Monoalphabetic cipher is a substitution cipher, where the cipher alphabet for each plain text alphabet is fixed, for the entire encryption.

In simple words, if the alphabet 'p' in the plain text is replaced by the cipher alphabet 'd'. Then in the entire plain text wherever alphabet 'p' is used, it will be replaced by the alphabet 'd' to form the ciphertext.

Caesar cipher

- The encryption rule is simple; replace each letter of the alphabet with the letter standing 3 places further down the alphabet.
- The alphabet is wrapped around so that Z follows A.
- Generally Plain text is in lower case and Cipher text is Upper Case.

- Example:

  Plaintext: meet me after the party

  Ciphertext: PHHW PH DIWHU WKH SDUWB

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

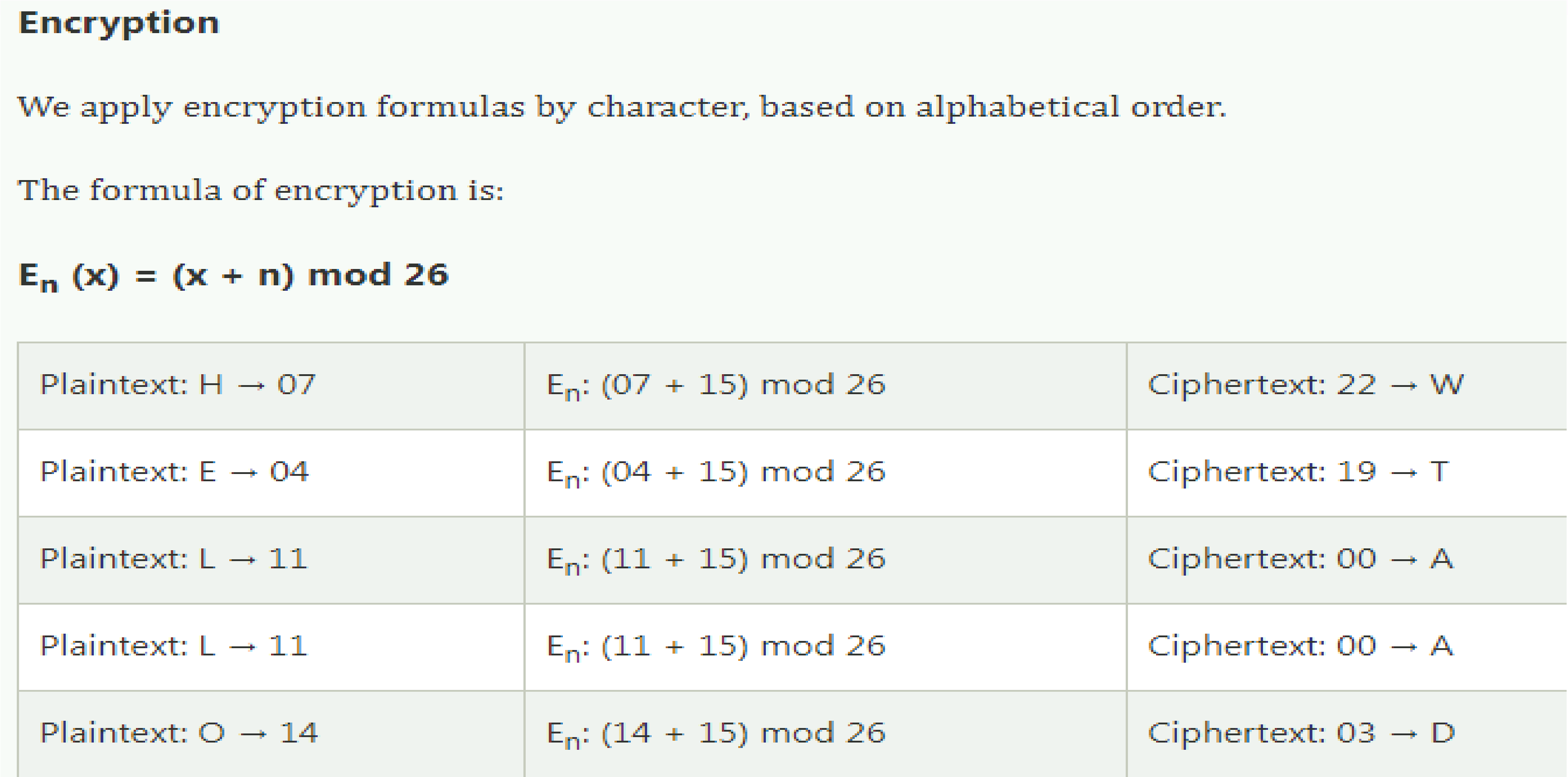
- Here, the key is 3. If different key is used, different substitution will be obtained.
- Mathematically, starting from a=0, b=1 and so on, Caesar cipher can be written as:

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

Encryption k=3 $\mathrm{E}(p) = (p + k) \bmod (26)$	**Result**	**Cipher Text** **D(C) = (C – k) mod (26)**	**Result**
M=E(M)=(12+3)mod26	15=P	D(P)=(15-3)mod26	12=m
E=E(E)=((4+3)mod26	7=H	D(H)=(7-3)mod26	4=e
E= E(E)=((4+3)mod26	7=H	D(H)=(7-3)mod26	4=e
T=E(T)=((19+3)mod26	21=V	D(V)=(21-3)mod26	19=t

- This cipher can be broken
  - If we know one plaintext-cipher text pair since the difference will be same.
  - By applying Brute Force attack as there are only 26 possible keys.

Example: 2 Use the Caesar cipher to encrypt and decrypt the message "HELLO," and the key (shift) value of this message is 15.



Encryption

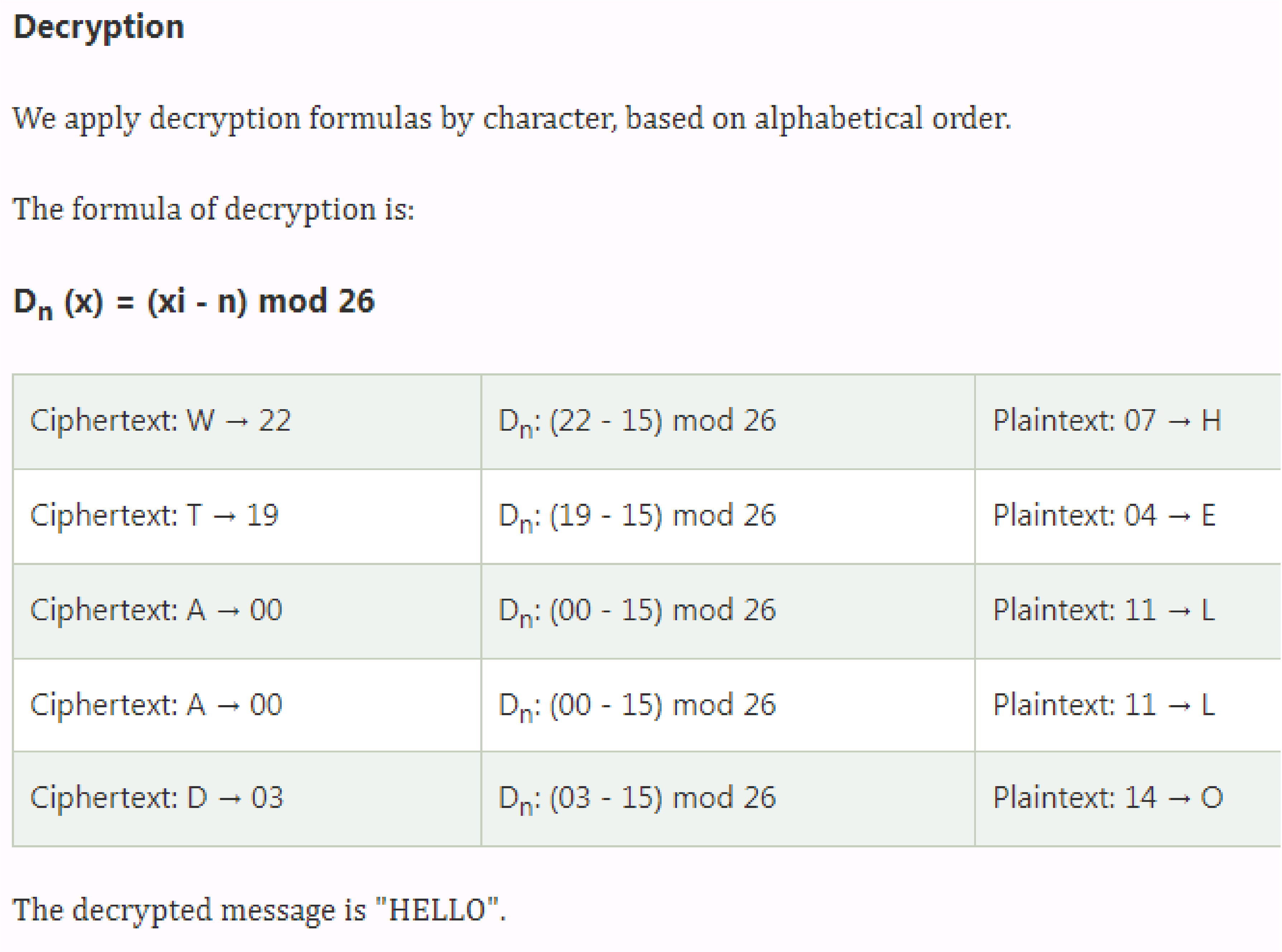
We apply encryption formulas by character, based on alphabetical order.

The formula of encryption is:

E_n (x) = (x + n) mod 26

Plaintext: H → 07	E_n: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: E → 04	E_n: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: L → 11	E_n: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: L → 11	E_n: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: O → 14	E_n: (14 + 15) mod 26	Ciphertext: 03 → D

The encrypted message of this plain text is "WTAAD".



Decryption

We apply decryption formulas by character, based on alphabetical order.

The formula of decryption is:

$D_n (x) = (xi - n) \bmod 26$

Ciphertext: W → 22	D_n: (22 - 15) mod 26	Plaintext: 07 → H
Ciphertext: T → 19	D_n: (19 - 15) mod 26	Plaintext: 04 → E
Ciphertext: A → 00	D_n: (00 - 15) mod 26	Plaintext: 11 → L
Ciphertext: A → 00	D_n: (00 - 15) mod 26	Plaintext: 11 → L
Ciphertext: D → 03	D_n: (03 - 15) mod 26	Plaintext: 14 → O

The decrypted message is "HELLO".

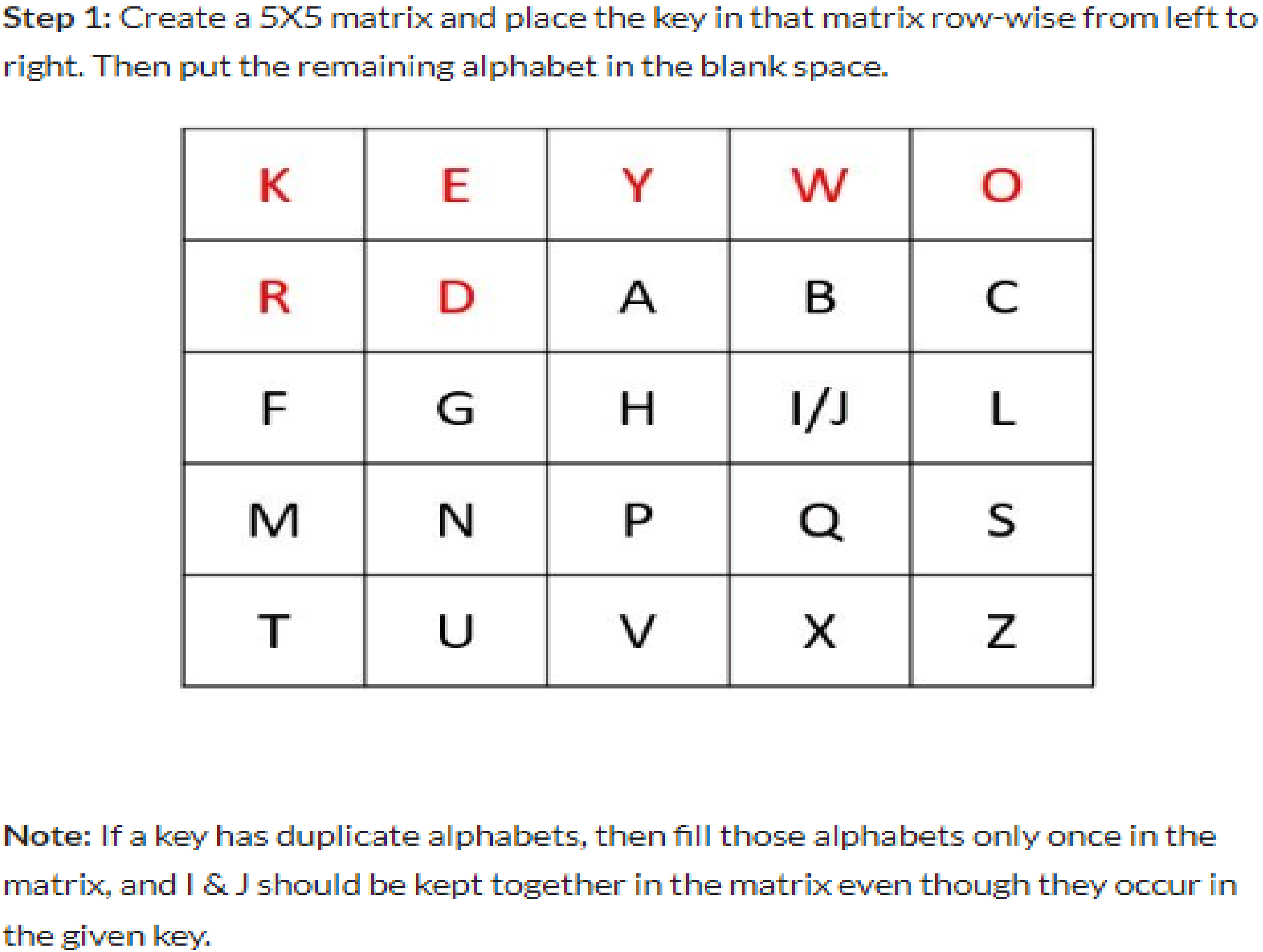
Playfair Cipher

Playfair cipher is a substitution cipher which involves a 5X5 matrix. Let us discuss the technique of this Playfair cipher with the help of an example:

Plain Text: meet me tomorrow

Key: KEYWORD

Now, we have to convert this plain text to ciphertext using the given key. We will discuss the further process in steps.



Step 1: Create a 5X5 matrix and place the key in that matrix row-wise from left to right. Then put the remaining alphabet in the blank space.

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

Note: If a key has duplicate alphabets, then fill those alphabets only once in the matrix, and I & J should be kept together in the matrix even though they occur in the given key.

Step 2: Now, you have to break the plain text into a pair of alphabets.

Plain Text: meet me tomorrow

Pair: me et me to mo rx ro wz

Note

- Pair of alphabets must not contain the same letter. In case, pair has the same letter then break it and add 'x' to the previous letter. Like in our example letter 'rr' occurs in pair so, we have broken that pair and added 'x' to the first 'r'.
- In case while making pair, the last pair has only one alphabet left then we add 'z' to that alphabet to form a pair as in our above example, we have added 'z' to 'w' because 'w' was left alone at last.
- If a pair has 'xx' then we break it and add 'z' to the first 'x', i.e. 'xz' and 'x_'.

Step 3: In this step, we will convert plain text into ciphertext. For that, take the first pair of plain text and check for cipher alphabets for the corresponding in the matrix. To find cipher alphabets follow the rules below.

Note

- If both the alphabets of the pair occur in the **same row** replace them with the alphabet to their **immediate right.** If an alphabet of the pair occurs at extreme right then replace it with the first element of that row, i.e. the last element of the row in the matrix circularly follows the first element of the same row.
- If the alphabets in the pair occur in the **same column**, then replace them with the alphabet **immediate below** them. Here also, the last element of the column circularly follows the first element of the same column.
- If the alphabets in the pair are **neither in the same column and nor in the same row,** then the alphabet is replaced by the element in its own row and the corresponding column of the other alphabet of the pair.

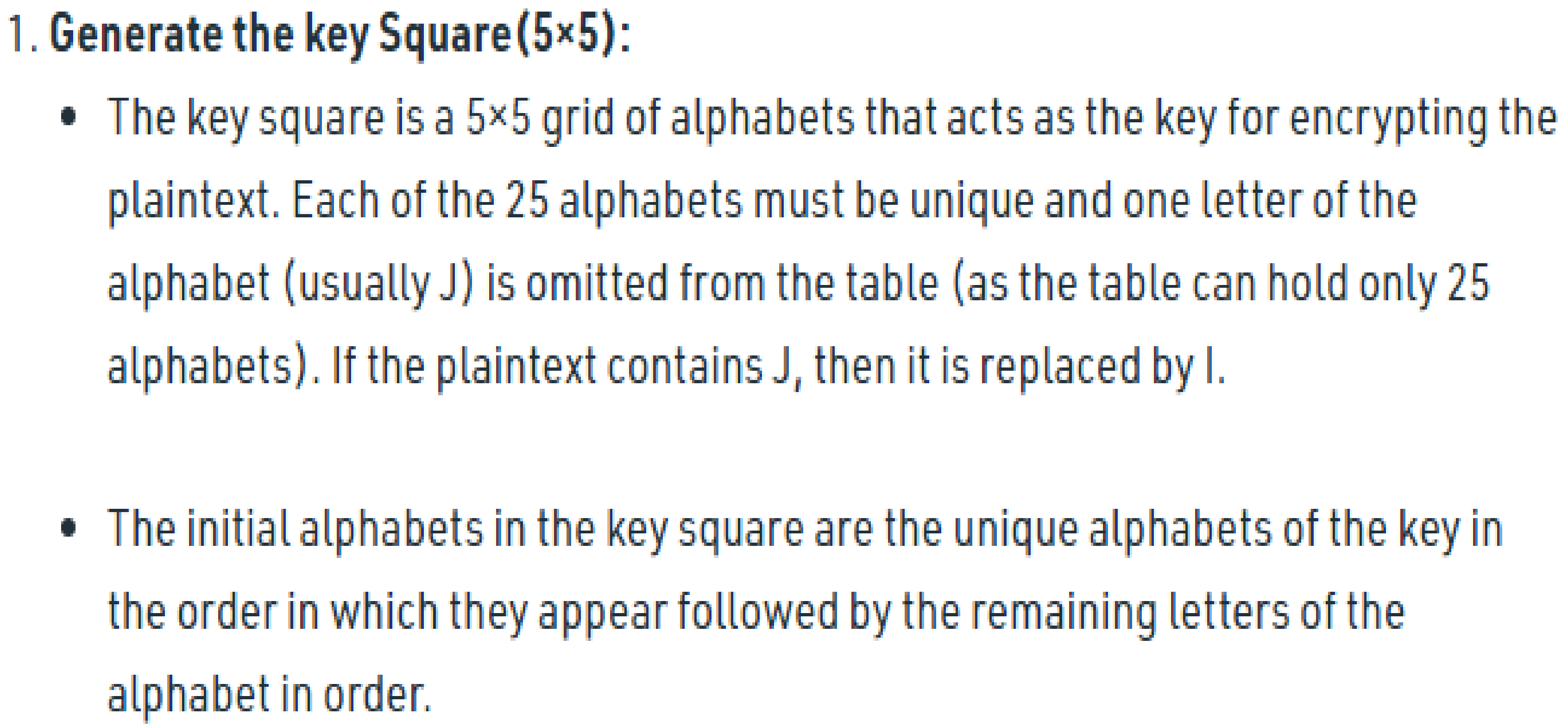
Pair: me et me to mo rx ro wz

Cipher Text: kn ku kn kz ks ta kc yo

So, this is how we can convert a plain text to ciphertext using Playfair cipher. When compared with monoalphabetic cipher Playfair cipher is much more advanced. But still, it is easy to break.

Key: monarchy

Plaintext: instruments



1. **Generate the key Square(5×5):**
   - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

   - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
   For example:

```
PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’

Here **'x'** is the bogus letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

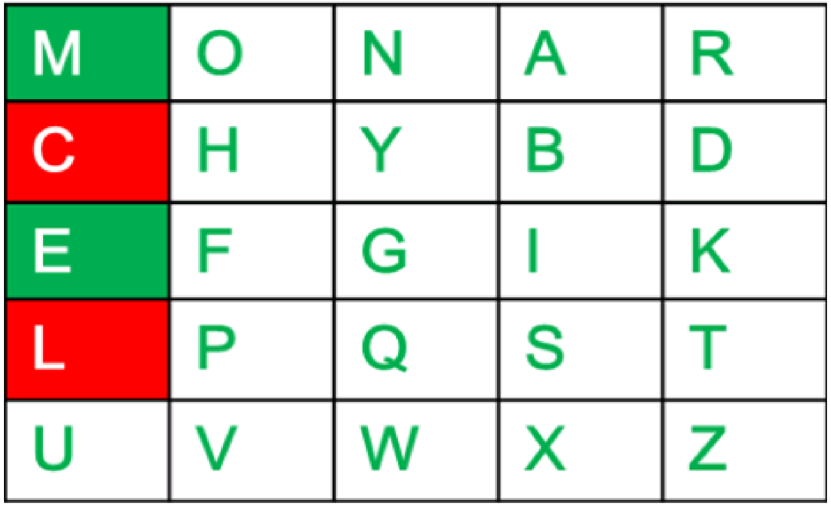
AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’

Here **‘z’** is the bogus letter.

Rules for Encryption:

- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
  For example:

```
Diagraph: "me"
Encrypted Text: cl
Encryption:
  m -> c
  e -> l
```

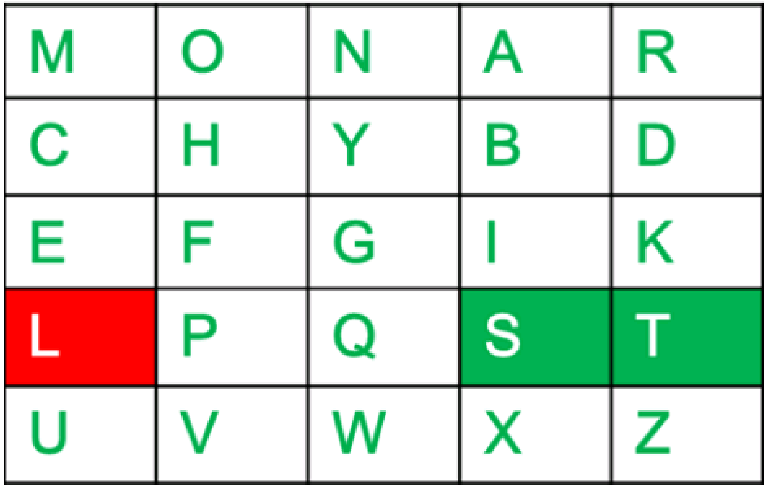


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

  For example:

```
Diagraph: "st"
Encrypted Text: tl
Encryption:
  s -> t
  t -> l
```

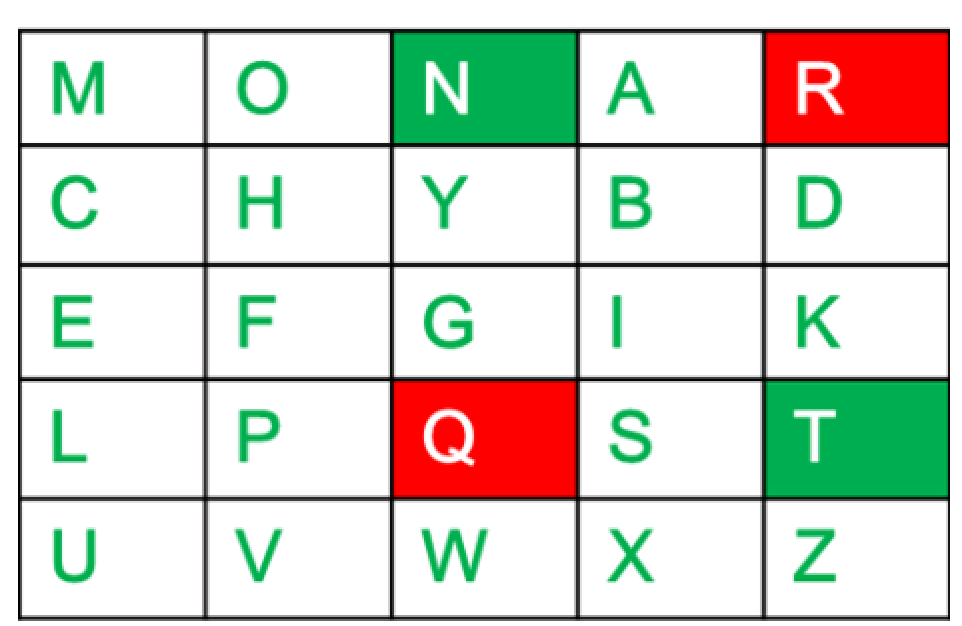


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- **If neither of the above rules is true:** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

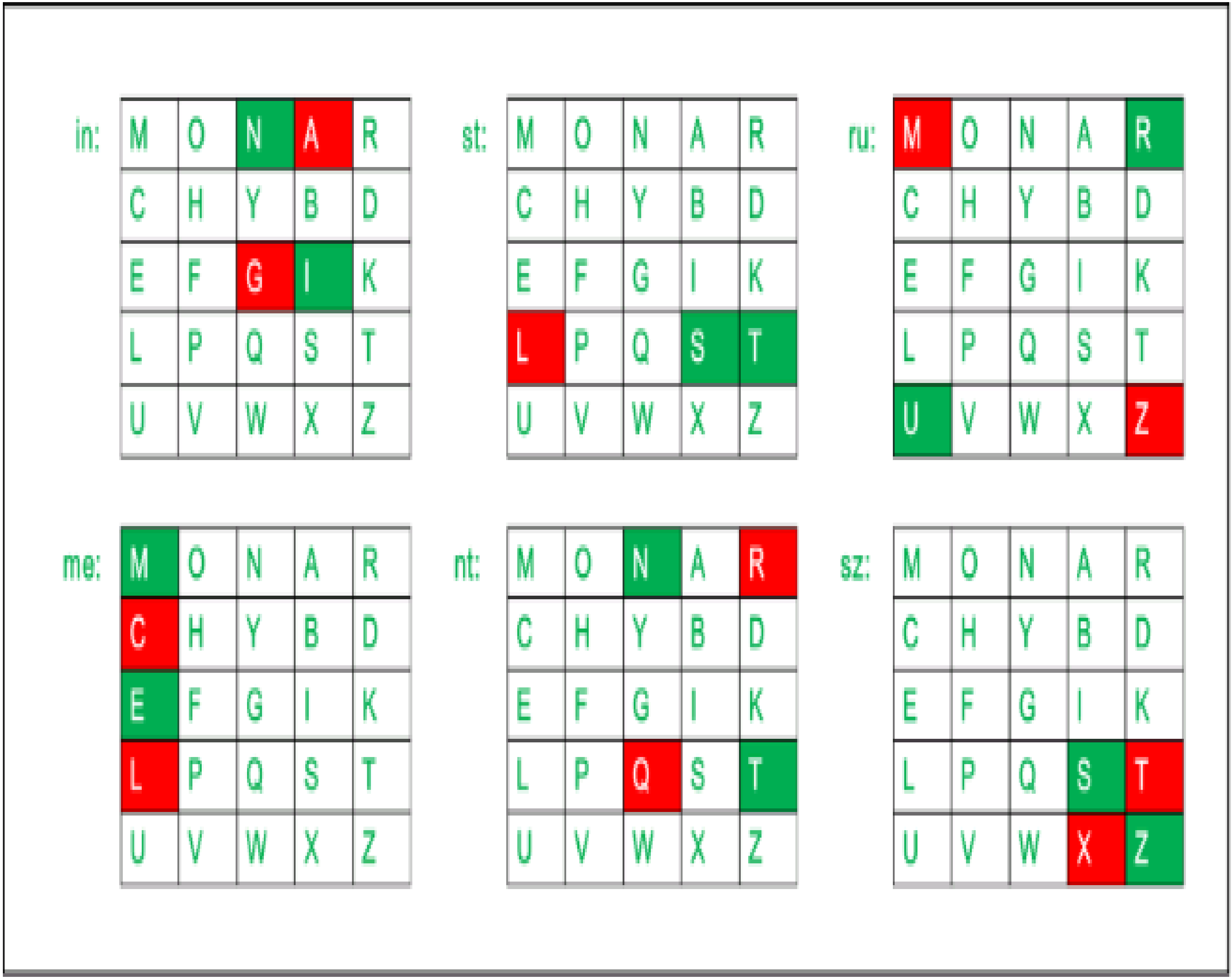
For example:

```
Diagraph: "nt"

Encrypted Text: rq

Encryption:

  n -> r

  t -> q
```



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

```
sz"
lrqtx
```



in:

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

st:

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

ru:

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

me:

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

nt:

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

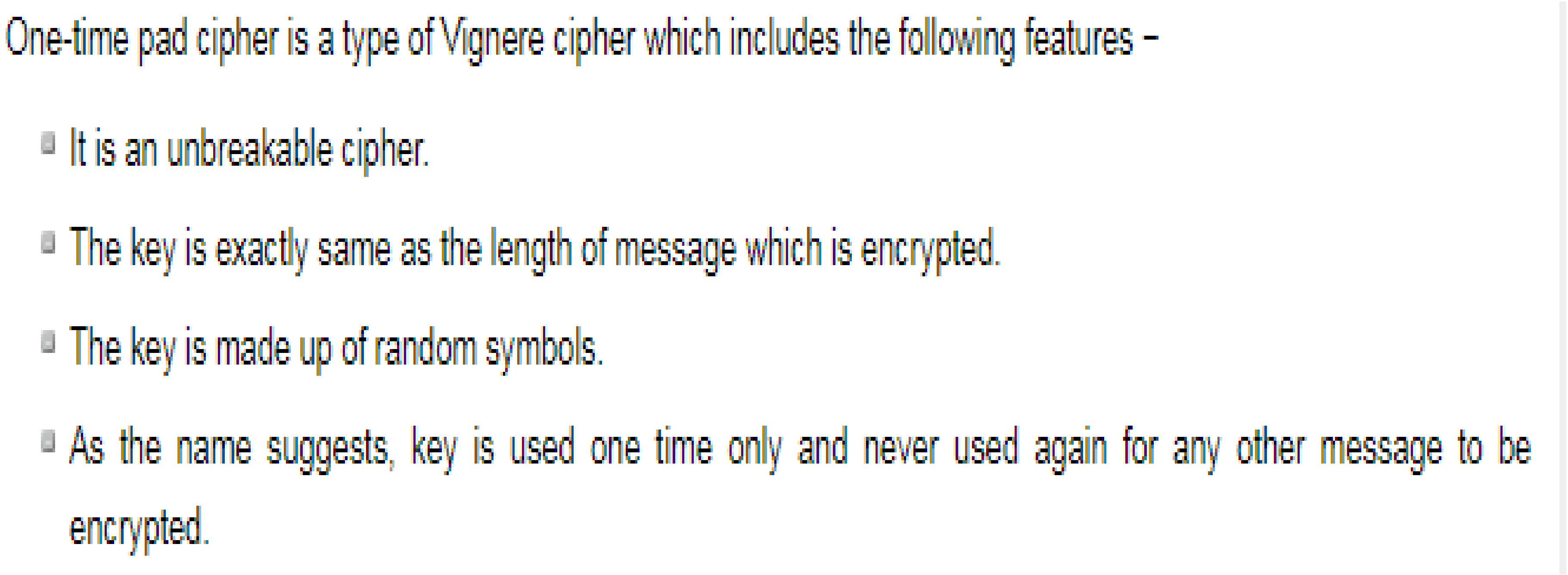
sz:

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

Polyalphabetic Cipher

Polyalphabetic cipher is far more secure than a monoalphabetic cipher. As monoalphabetic cipher maps a plain text symbol or alphabet to a ciphertext symbol and uses the same ciphertext symbol wherever that plain text occurs in the message.

But polyalphabetic cipher, each time replaces the plain text with the different ciphertext.

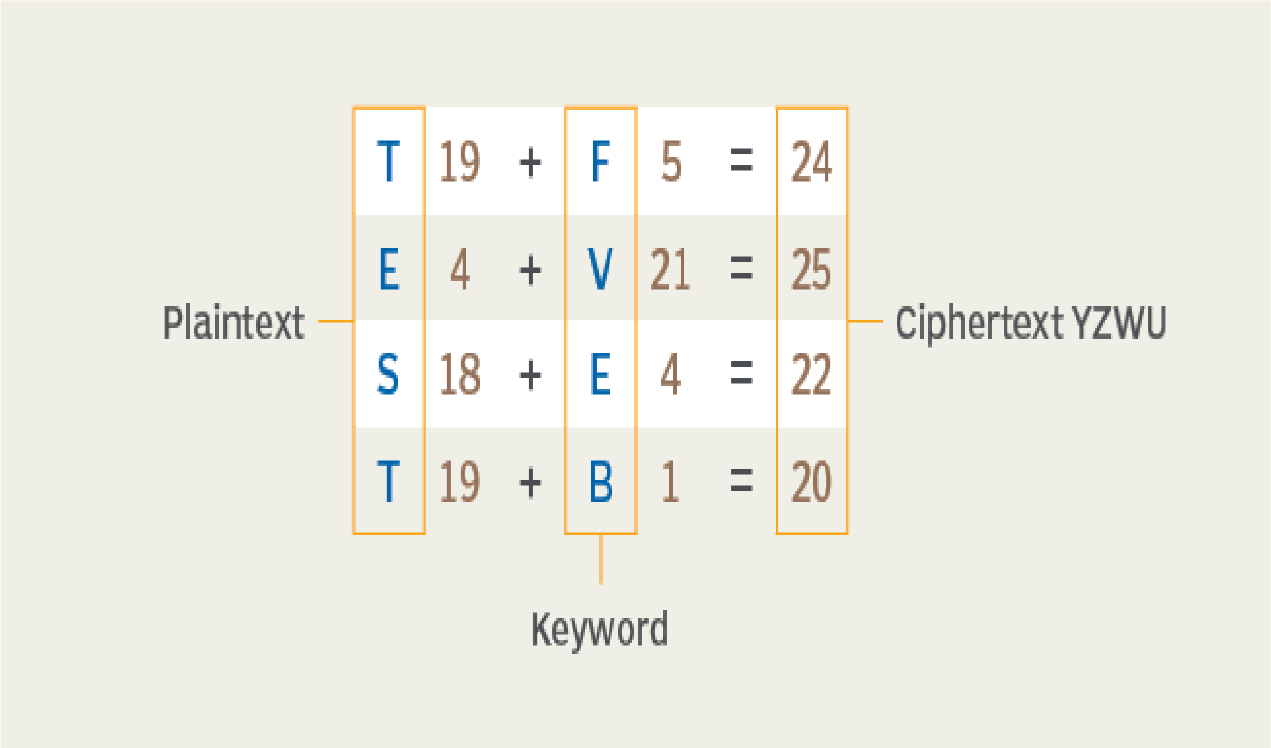


One-time pad cipher is a type of Vignere cipher which includes the following features −

- It is an unbreakable cipher.
- The key is exactly same as the length of message which is encrypted.
- The key is made up of random symbols.
- As the name suggests, key is used one time only and never used again for any other message to be encrypted.

One-time pad

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



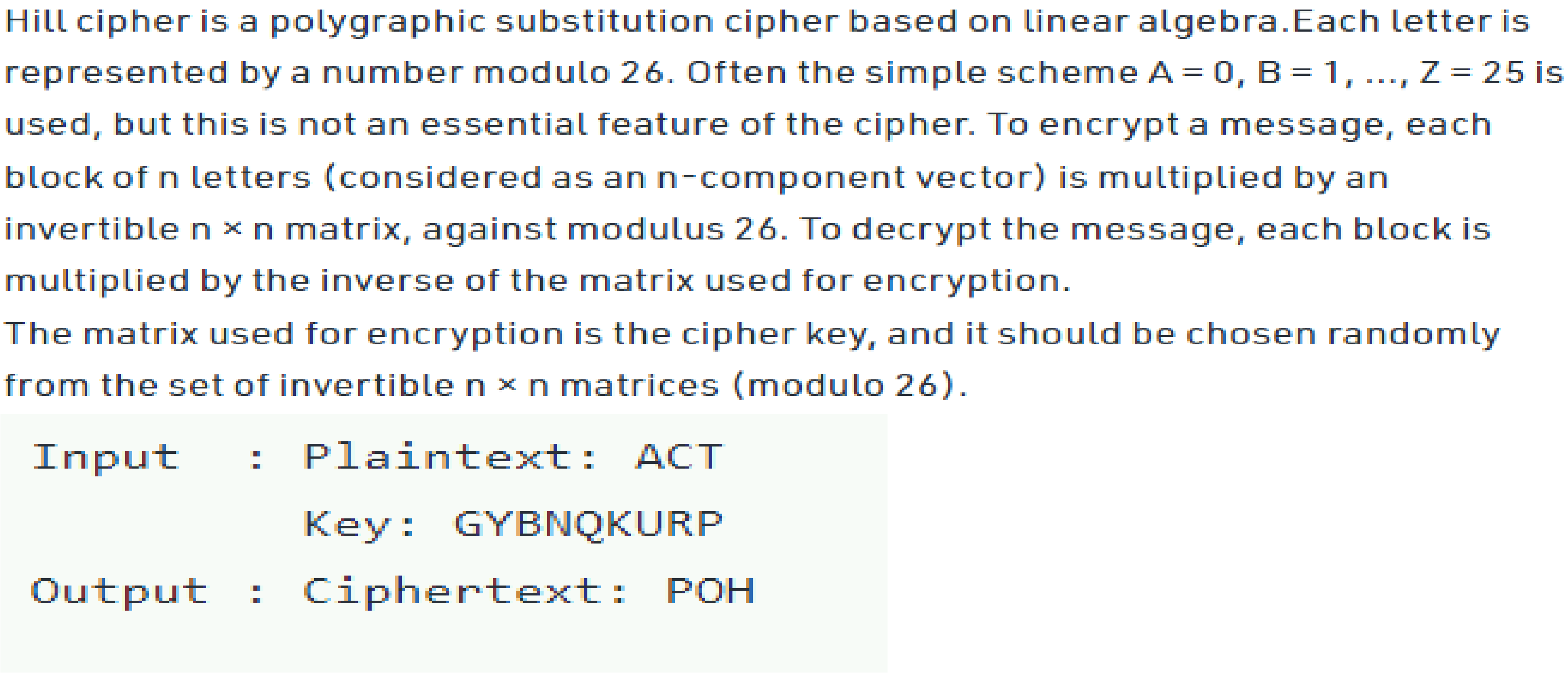
T	19	+	F	5	=	24
E	4	+	V	21	=	25
S	18	+	E	4	=	22
T	19	+	B	1	=	20

Plaintext

Ciphertext YZWU

Keyword

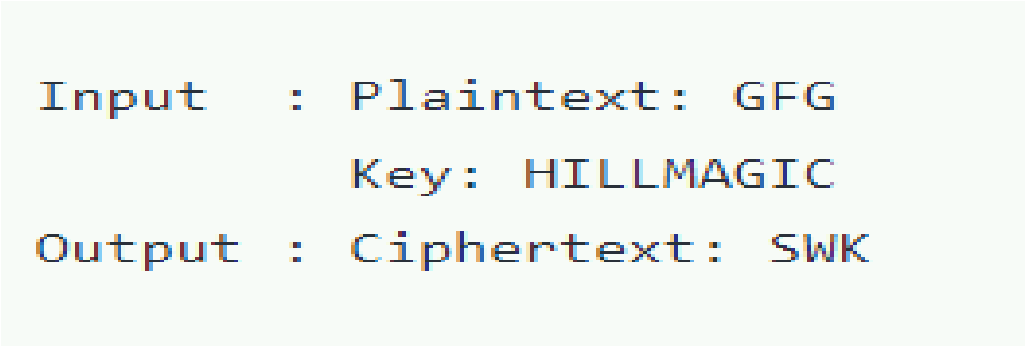
Hill cipher



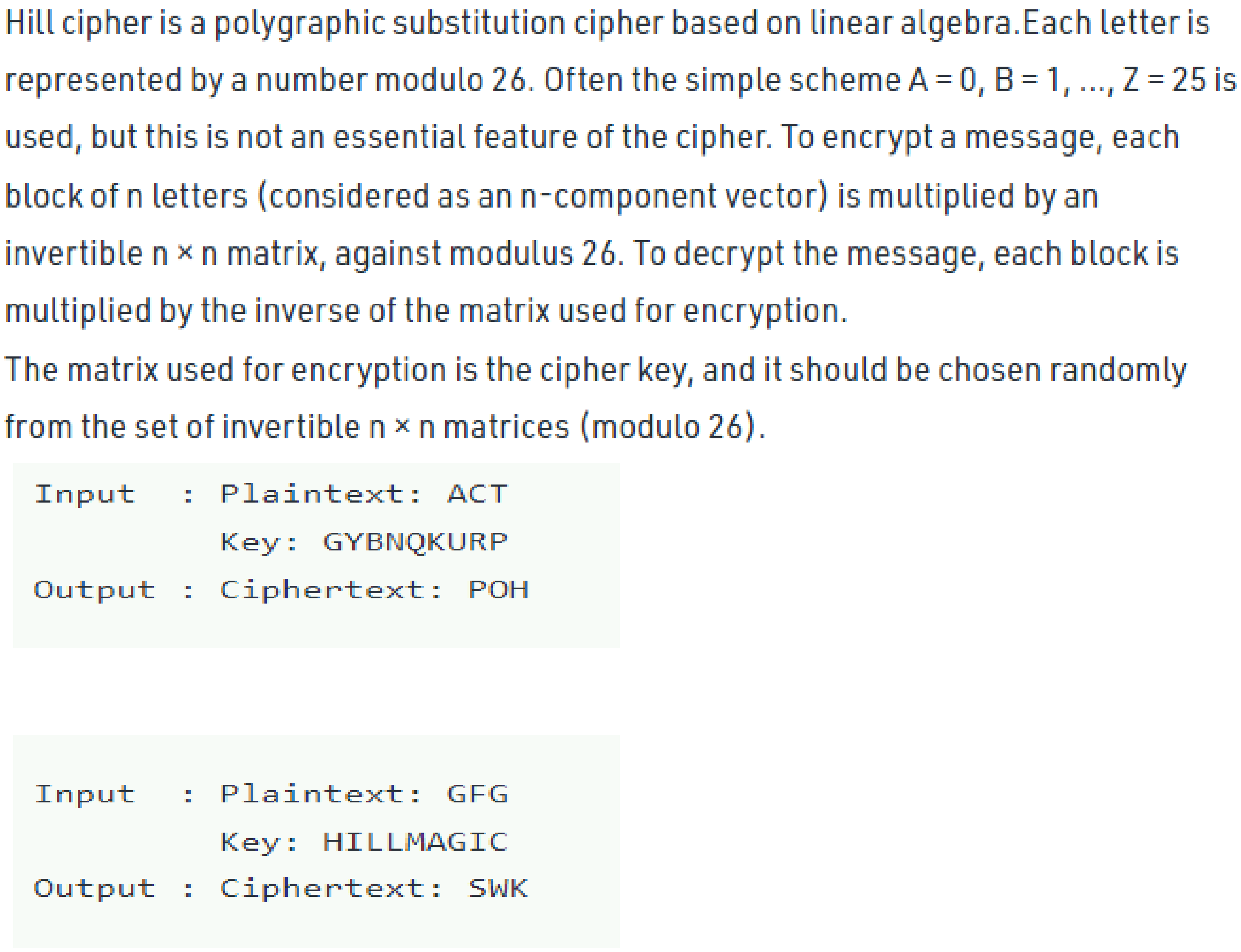
Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

```
Input  : Plaintext: ACT
         Key: GYBNQKURP
Output : Ciphertext: POH
```



```
Input  : Plaintext: GFG
         Key: HILLMAGIC
Output : Ciphertext: SWK
```



Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

```
Input  : Plaintext: ACT
         Key: GYBNQKURP
Output : Ciphertext: POH
```

```
Input  : Plaintext: GFG
         Key: HILLMAGIC
Output : Ciphertext: SWK
```

We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:

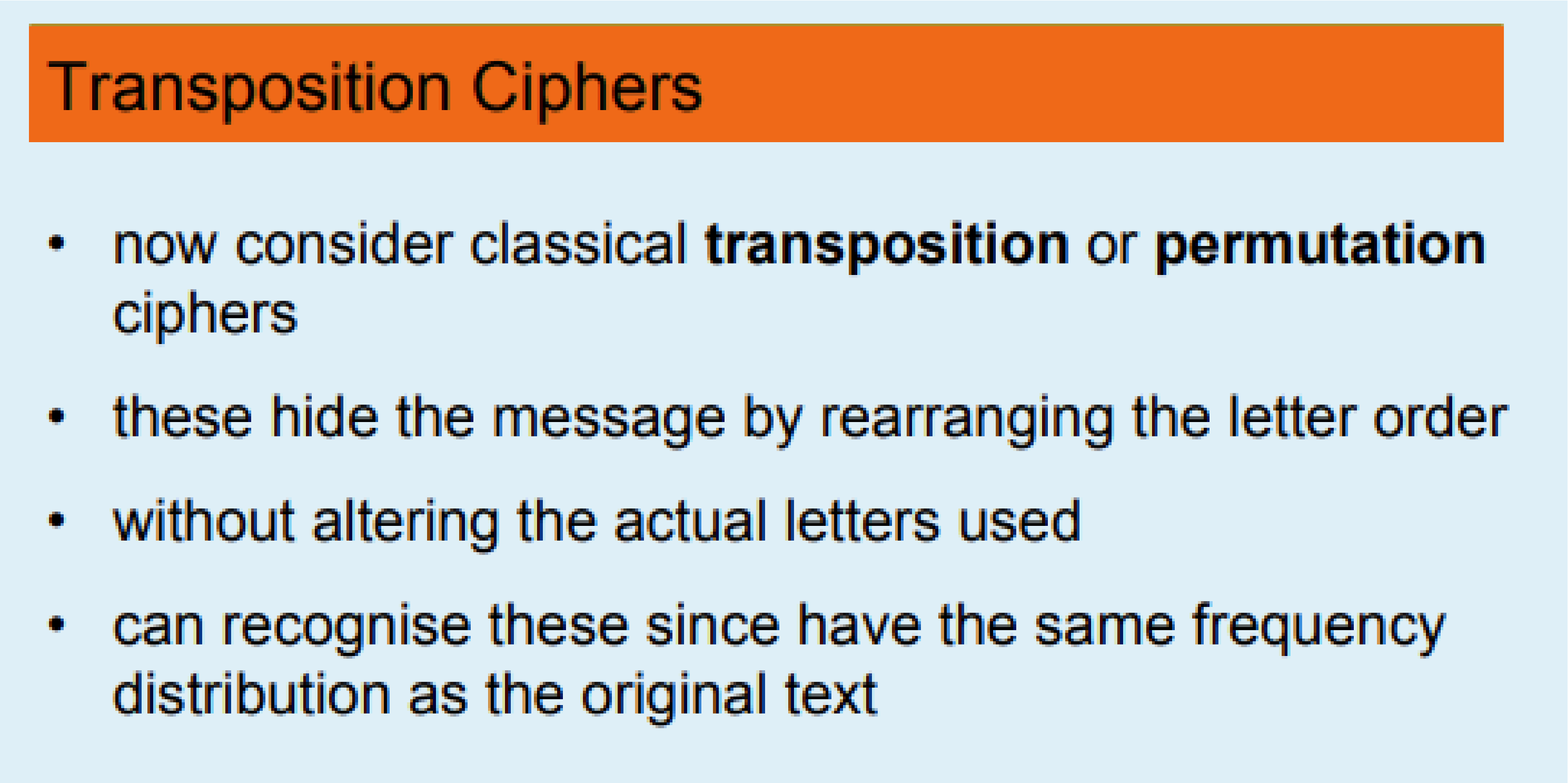
$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

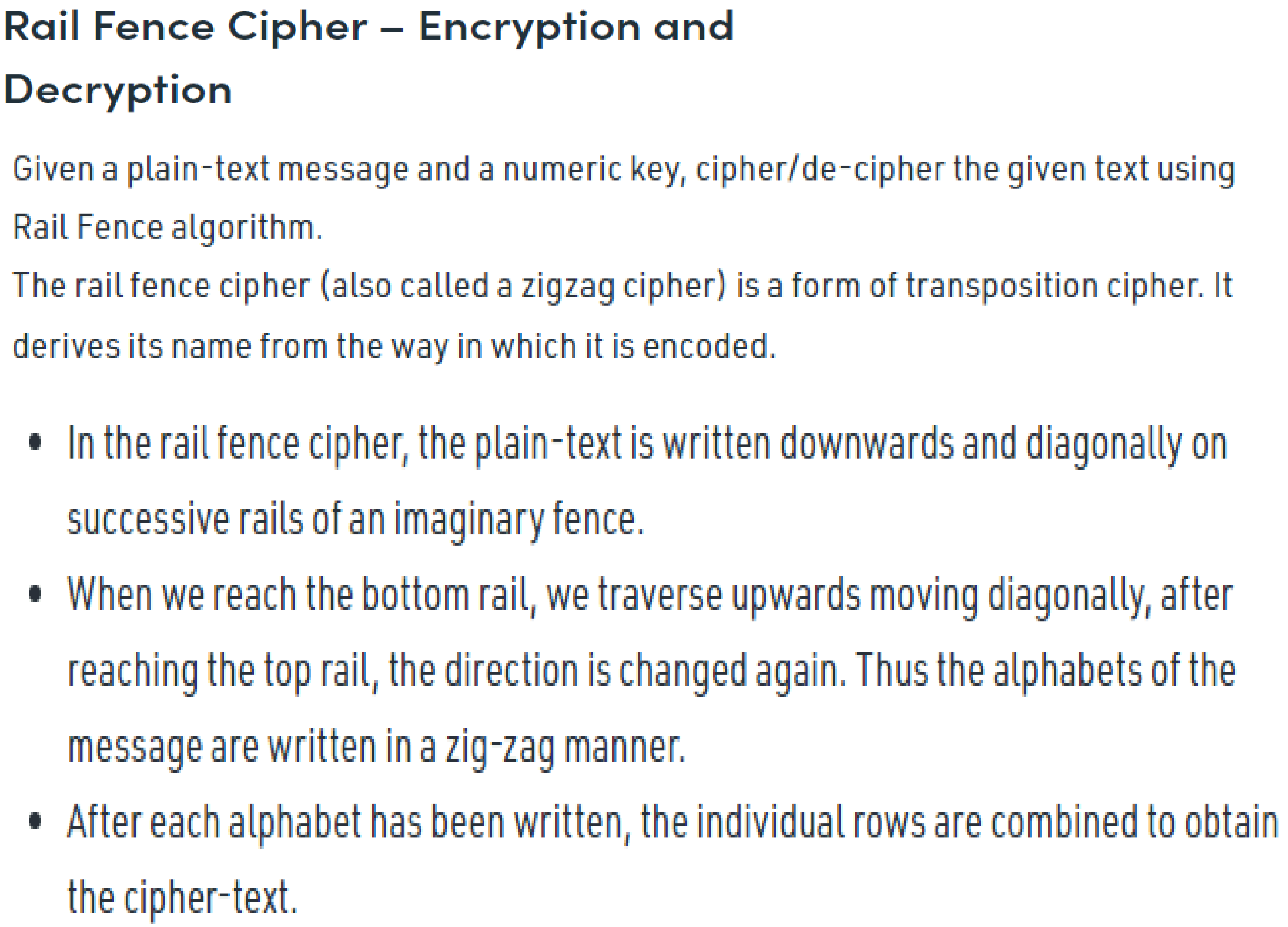
$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of ‘POH’



Transposition Ciphers

- now consider classical **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- can recognise these since have the same frequency distribution as the original text



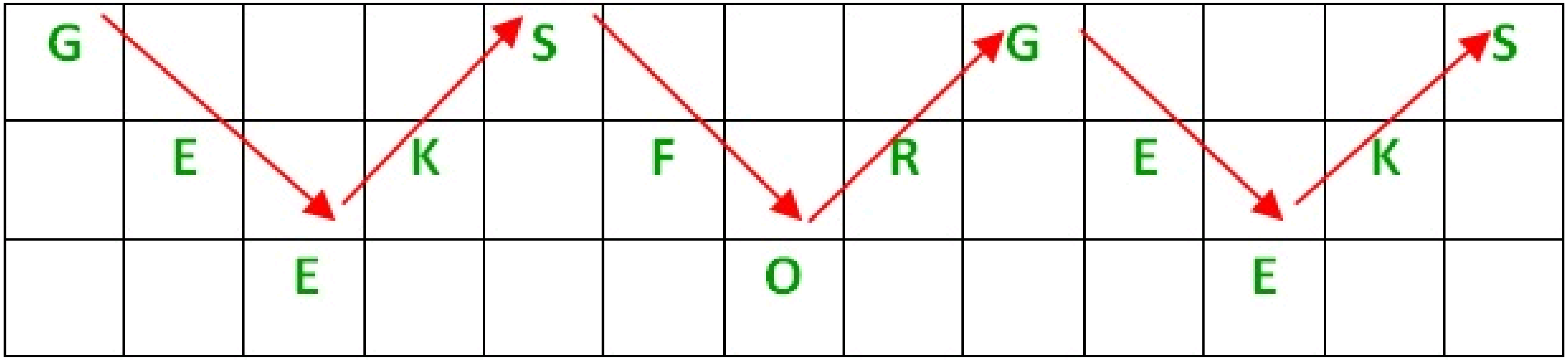
Rail Fence Cipher – Encryption and Decryption

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm.

The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

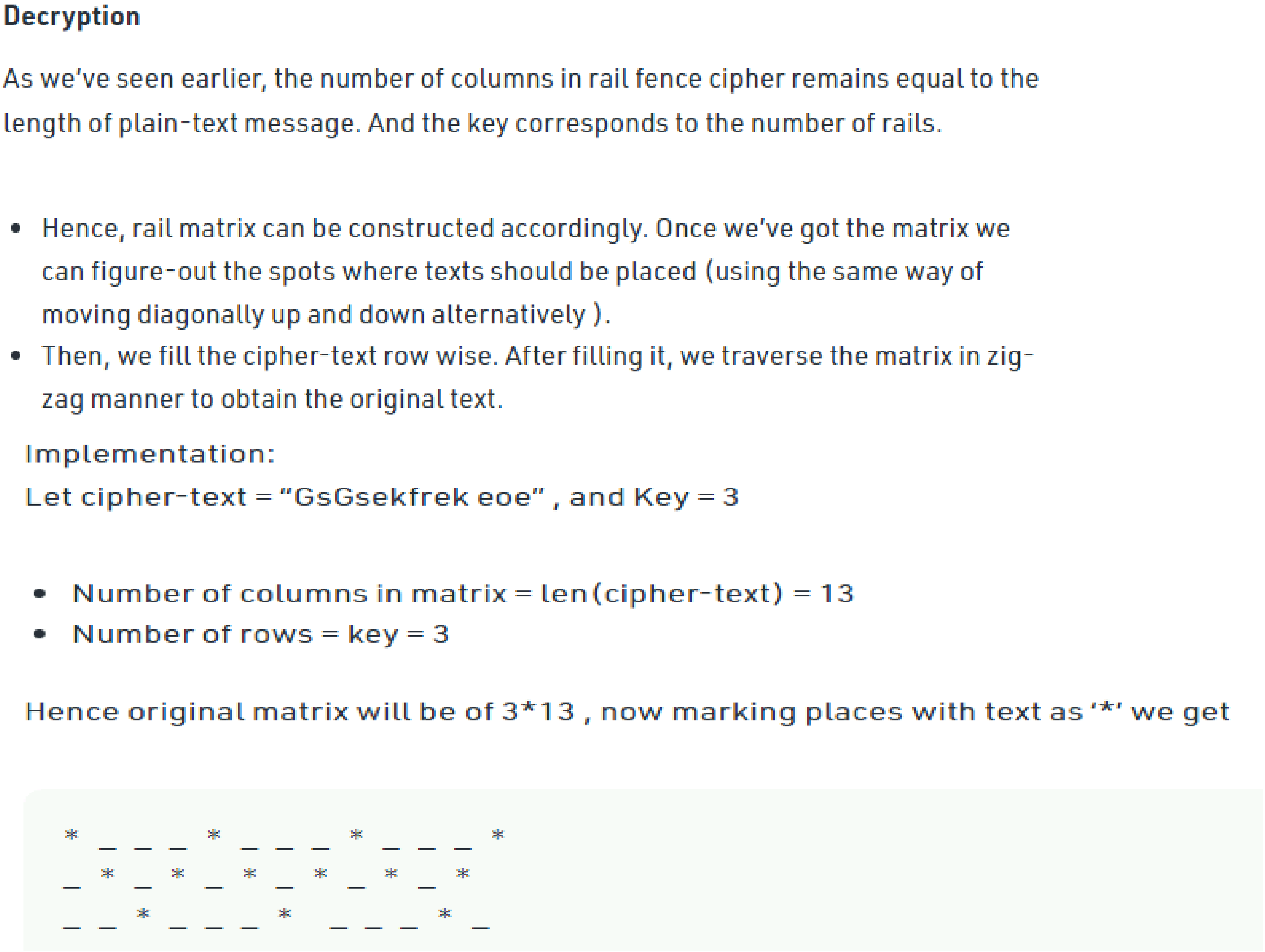
- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

For example, if the message is "GeeksforGeeks" and the number of rails = 3 then cipher is prepared as:



G				S				G				S
	E		K		F		R		E		K	
		E				O				E		

∴Its encryption will be done row wise i.e. GSGSEKFREKEOE



Decryption

As we've seen earlier, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

- Hence, rail matrix can be constructed accordingly. Once we've got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.

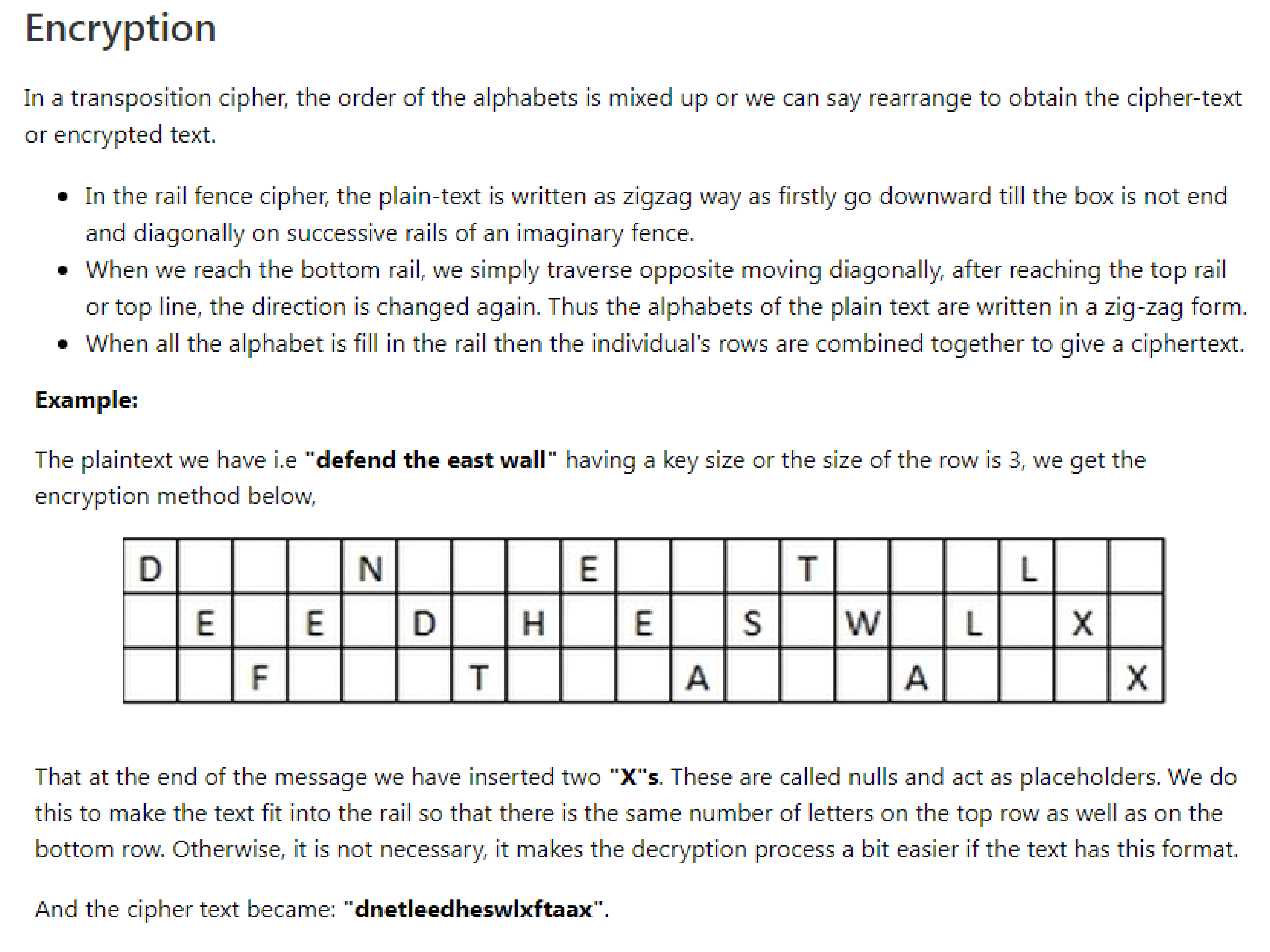
Implementation:

Let cipher-text = "GsGsekfrek eoe" , and Key = 3

- Number of columns in matrix = len(cipher-text) = 13
- Number of rows = key = 3

Hence original matrix will be of 3*13 , now marking places with text as '*' we get

```
*  _  _  _  *  _  _  _  *  _  _  _  *
_  *  _  *  _  *  _  *  _  *  _  *
_  _  *  _  _  _  *   _  _  _  *  _
```



Encryption

In a transposition cipher, the order of the alphabets is mixed up or we can say rearrange to obtain the cipher-text or encrypted text.

- In the rail fence cipher, the plain-text is written as zigzag way as firstly go downward till the box is not end and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we simply traverse opposite moving diagonally, after reaching the top rail or top line, the direction is changed again. Thus the alphabets of the plain text are written in a zig-zag form.
- When all the alphabet is fill in the rail then the individual's rows are combined together to give a ciphertext.

Example:

The plaintext we have i.e **"defend the east wall"** having a key size or the size of the row is 3, we get the encryption method below,

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

That at the end of the message we have inserted two **"X"s**. These are called nulls and act as placeholders. We do this to make the text fit into the rail so that there is the same number of letters on the top row as well as on the bottom row. Otherwise, it is not necessary, it makes the decryption process a bit easier if the text has this format.

And the cipher text became: **"dnetleedheswlxftaax"**.

Decryption

As we have studied earlier, the number of columns in rail fence cipher remains equal to the length of plain-text which we took. And the key remains the same as in encryption to the number of rails.

- Hence, the Rail Fence matrix can be constructed likely. Once we have got the matrix we can find-out the places where plain texts should be placed using the same way as we doe in the encryption method of moving diagonally up and down alternatively to form text.
- Then, we fill the cipher-text accordingly to row-wise. After filling the text, we traverse the matrix in the zig-zag form to get the original text or the plain text.

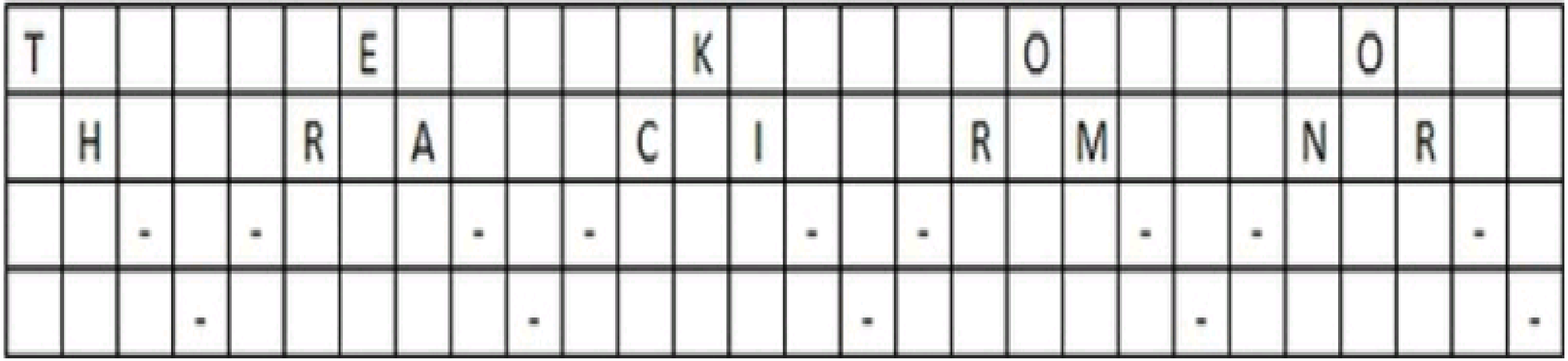
Example:

If we get the ciphertext **"TEKOOHRACIRMNREATANFTETYTGHH"**, it will be encrypted with a key size of 4.

We start by placing the **"T"** in the first square. You then dash the diagonal down places until you get back to the top line, and place the **"E"** here. Continuing to fill the rows you get the pattern below,

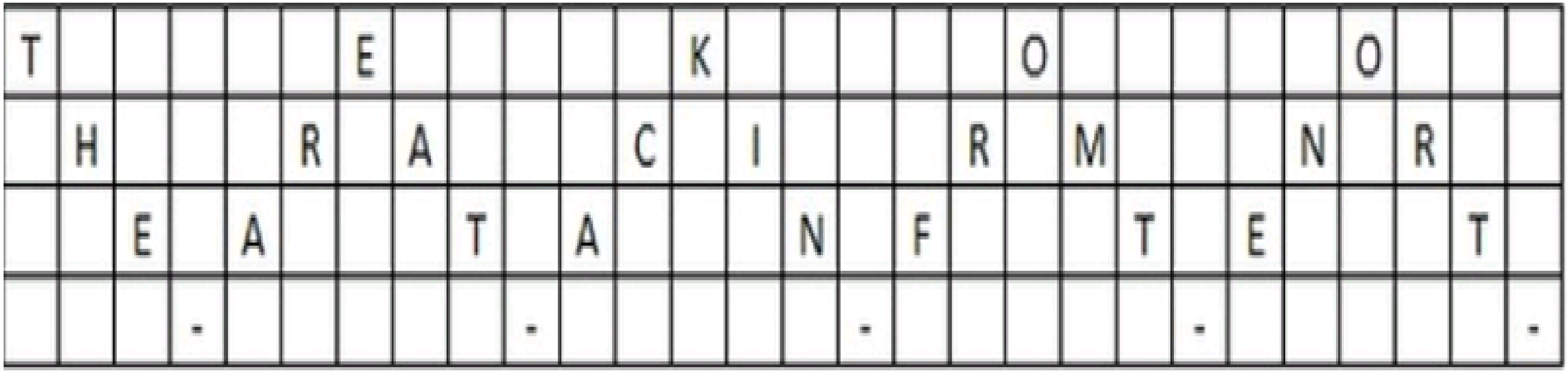
T						E						K						O						O			
	-				-		-				-		-				-		-				-		-		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-

As we have a key size of 4 and the length of the message is 28 so we make like this and continues this till all the text does not fit into it.



T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		.		.				.		.				.		.				.		.				.	
			.						.						.						.						.

Second stage in decryption process,



T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		E		A				T		A				N		F				T		E				T	
			.						.						.						.						.

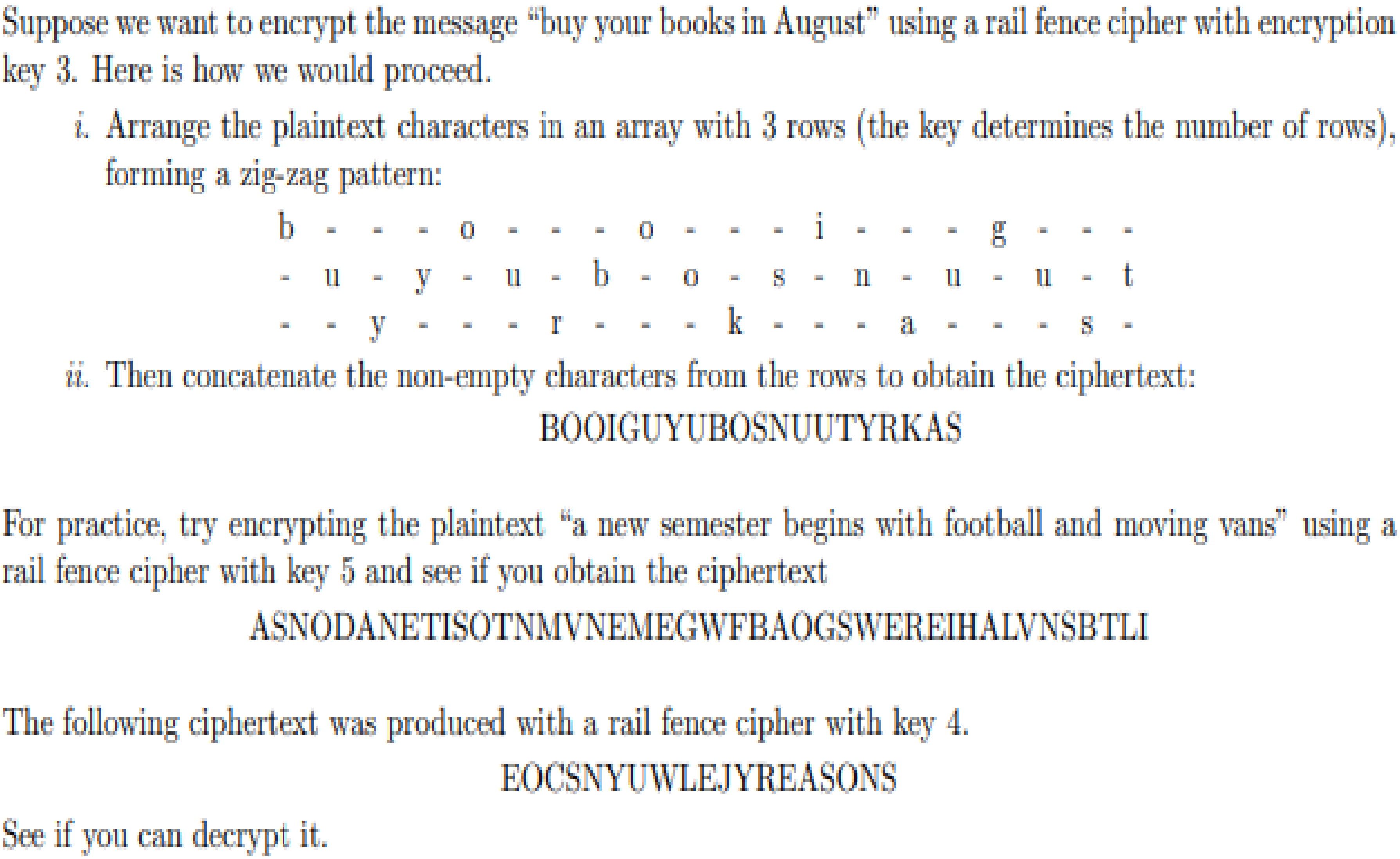
Third stage in decryption process,

T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		E		A				T		A				N		F				T		E				T	
			Y						T						G						H						H

Forth and the final stage in decrption process,

Now, we read them as diagonally from top to bottom then bottom to top and we get the plain text or the original text i.e. "**THEY ARE ATTACKING FROM THE NORTH**".

Example



Suppose we want to encrypt the message "buy your books in August" using a rail fence cipher with encryption key 3. Here is how we would proceed.

i. Arrange the plaintext characters in an array with 3 rows (the key determines the number of rows), forming a zig-zag pattern:

```
b - - - o - - - o - - - i - - - g - - -
- u - y - u - b - o - s - n - u - u - t
- - y - - - r - - - k - - - a - - - s -
```

ii. Then concatenate the non-empty characters from the rows to obtain the ciphertext:

BOOIGUYUBOSNUUTYRKAS

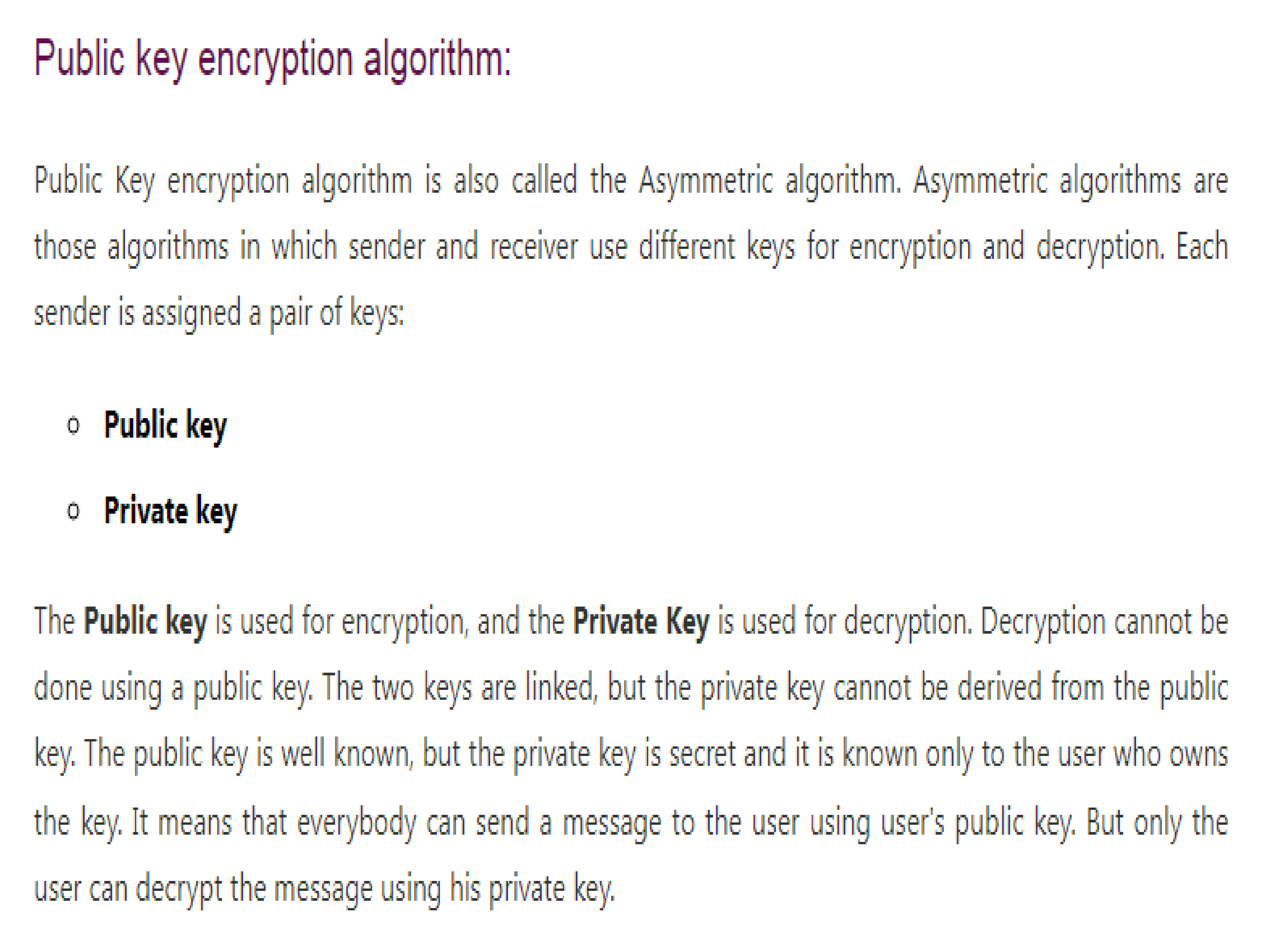
For practice, try encrypting the plaintext "a new semester begins with football and moving vans" using a rail fence cipher with key 5 and see if you obtain the ciphertext

ASNODANETISOTNMVNEMEGWFBAOGSWEREIHALVNSBTLI

The following ciphertext was produced with a rail fence cipher with key 4.

EOCSNYUWLEJYREASONS

See if you can decrypt it.



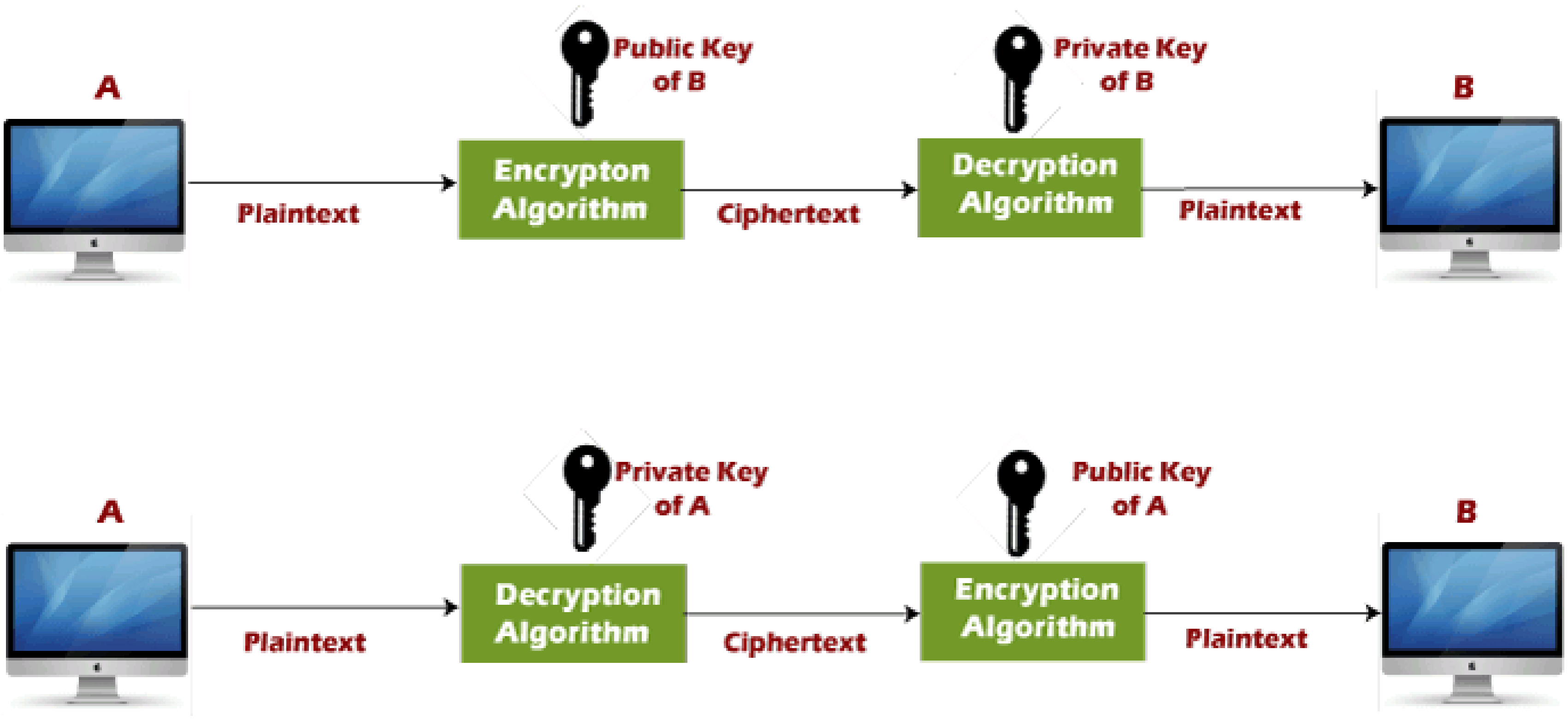
Public key encryption algorithm:

Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- **Public key**
- **Private key**

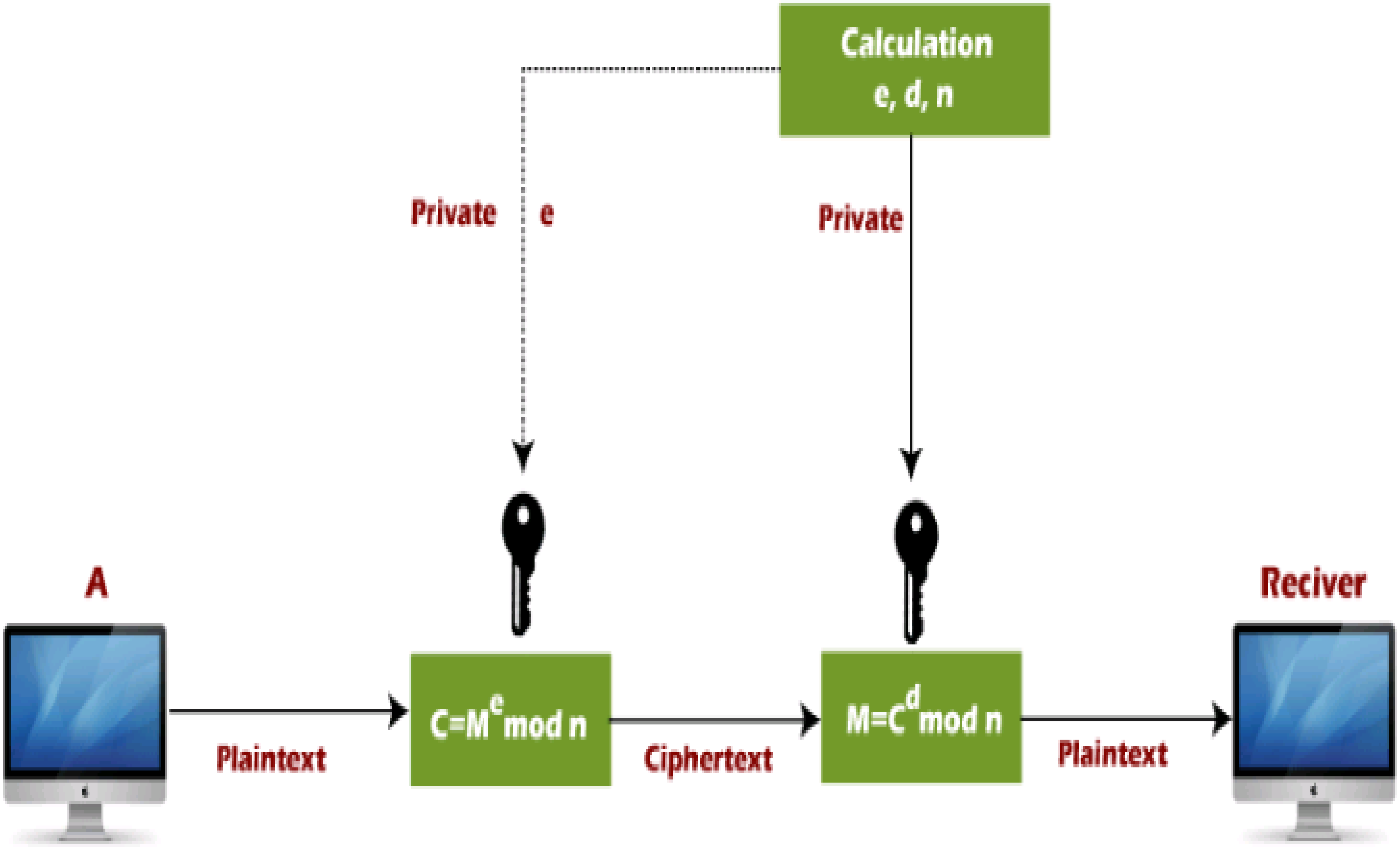
The **Public key** is used for encryption, and the **Private Key** is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

The Public key algorithm operates in the following manner:

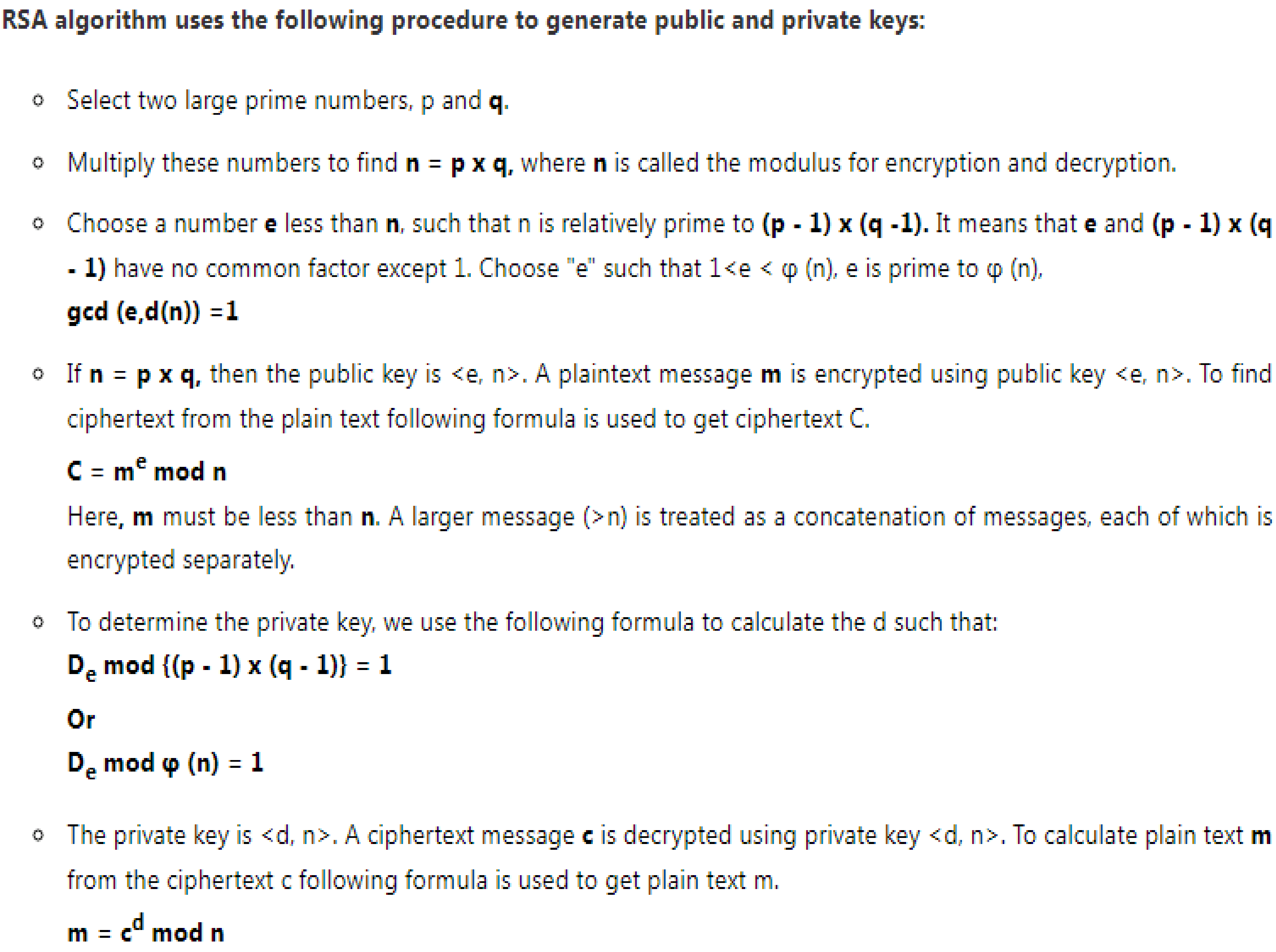


Encryption/decryption using public/private keys

- The data to be sent is encrypted by sender **A** using the public key of the intended receiver
- B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received ciphertext using its private key, which is known only to him.


Calculation
e, d, n
Private
e
Private
A
Reciver
Plaintext
$C=M^e$mod n
Ciphertext
$M=C^d$mod n
Plaintext

RSA



RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n),

  gcd (e,d(n)) =1
- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

  C = m^e mod n

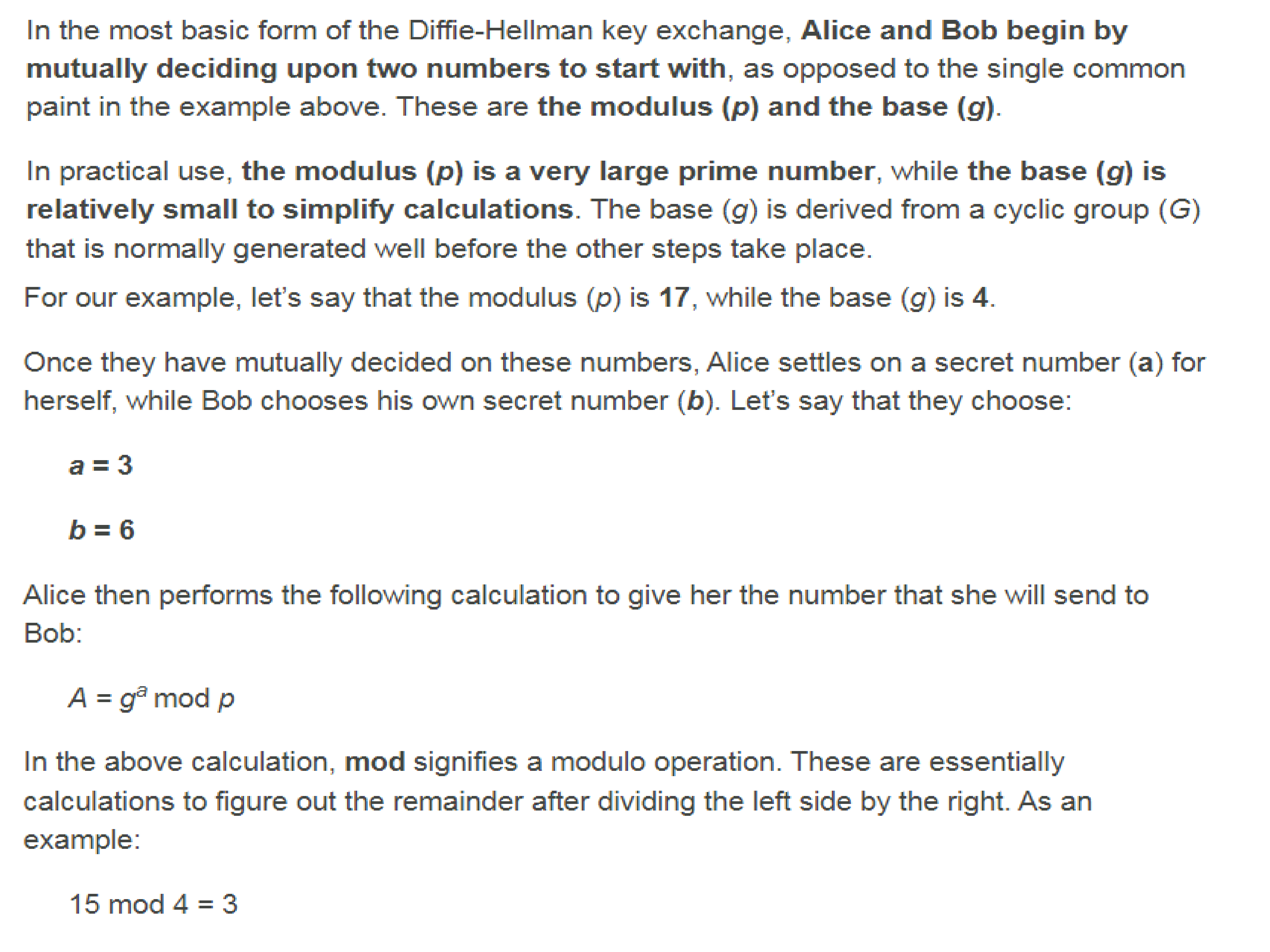
  Here, **m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:

  D_e mod {(p - 1) x (q - 1)} = 1

  Or

  D_e mod φ (n) = 1
- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.

  m = c^d mod n



In the most basic form of the Diffie-Hellman key exchange, **Alice and Bob begin by mutually deciding upon two numbers to start with**, as opposed to the single common paint in the example above. These are **the modulus (*p*) and the base (*g*)**.

In practical use, **the modulus (*p*) is a very large prime number**, while **the base (*g*) is relatively small to simplify calculations**. The base (*g*) is derived from a cyclic group (*G*) that is normally generated well before the other steps take place.

For our example, let's say that the modulus (*p*) is **17**, while the base (*g*) is **4**.

Once they have mutually decided on these numbers, Alice settles on a secret number (**a**) for herself, while Bob chooses his own secret number (***b***). Let's say that they choose:

$\boldsymbol{a = 3}$

$\boldsymbol{b = 6}$

Alice then performs the following calculation to give her the number that she will send to Bob:

$A = g^a \bmod p$

In the above calculation, **mod** signifies a modulo operation. These are essentially calculations to figure out the remainder after dividing the left side by the right. As an example:

$15 \bmod 4 = 3$

So let's put our numbers into the formula:

$$A = 4^3 \bmod 17$$

$$A = 64 \bmod 17$$

$$A = 13$$

When we do the same for Bob, we get:

$$B = 4^6 \bmod 17$$

$$B = 4096 \bmod 17$$

$$B = 16$$

Alice then sends her result (A) to Bob, while Bob sends his figure (B) to Alice. Alice then calculates the shared secret (s) using the number she received from Bob (B) and her secret number (a), using the following formula:

$s = B^a \bmod p$

$s = 16^3 \bmod 17$

$s = 4{,}096 \bmod 17$

$s = 16$

Bob then performs what is essentially the same calculation, but with the number that Alice sent him (A), as well as his own secret number (b):

$s = A^b \bmod p$

$s = 13^6 \bmod 17$

$s = 4{,}826{,}809 \bmod 17$

$s = 16$