CLASSICAL ENCRYPTION TECHNIQUES

BY

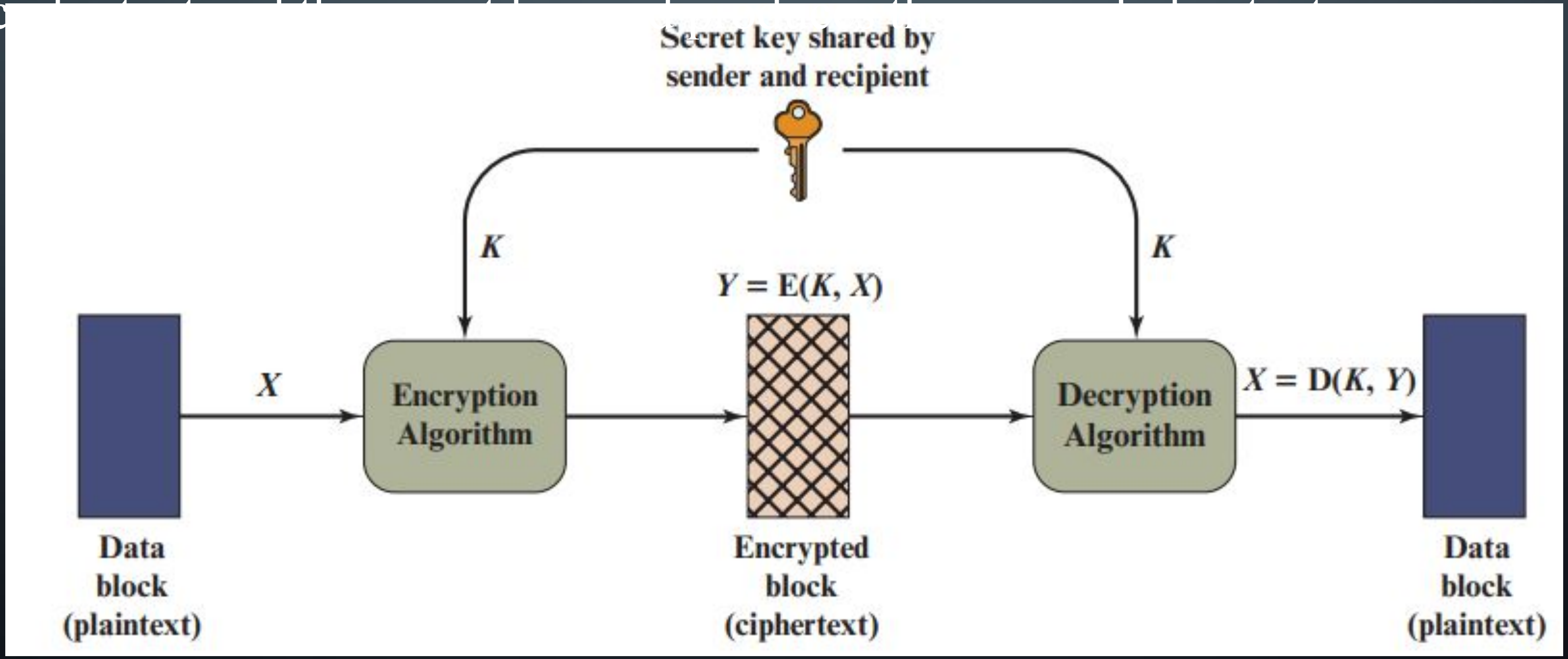
DR. ZIA UR REHMAN

SYMMETRIC ENCRYPTION

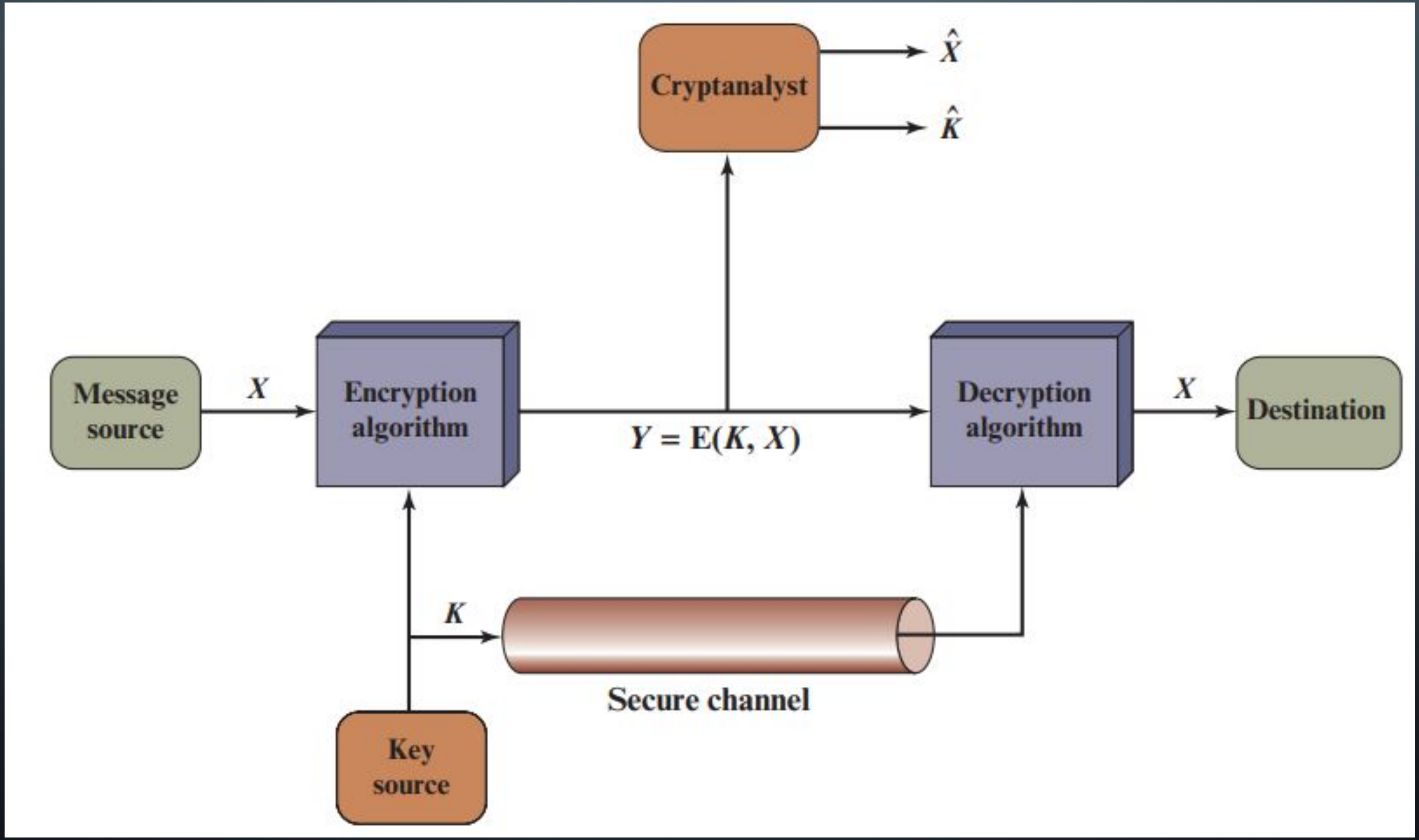
- Plaintext – Original message
- Ciphertext – Coded message
- Enciphering or Encryption - The process of converting from plaintext to ciphertext.
- deciphering or decryption - restoring the plaintext from the ciphertext.
- Cryptanalysis - Techniques used for deciphering a message without any knowledge of the enciphering. It is also called breaking the code.

SYMMETRIC CIPHER MODEL

- 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.
- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the c



MODEL OF SYMMETRIC CRYPTOSYSTEM

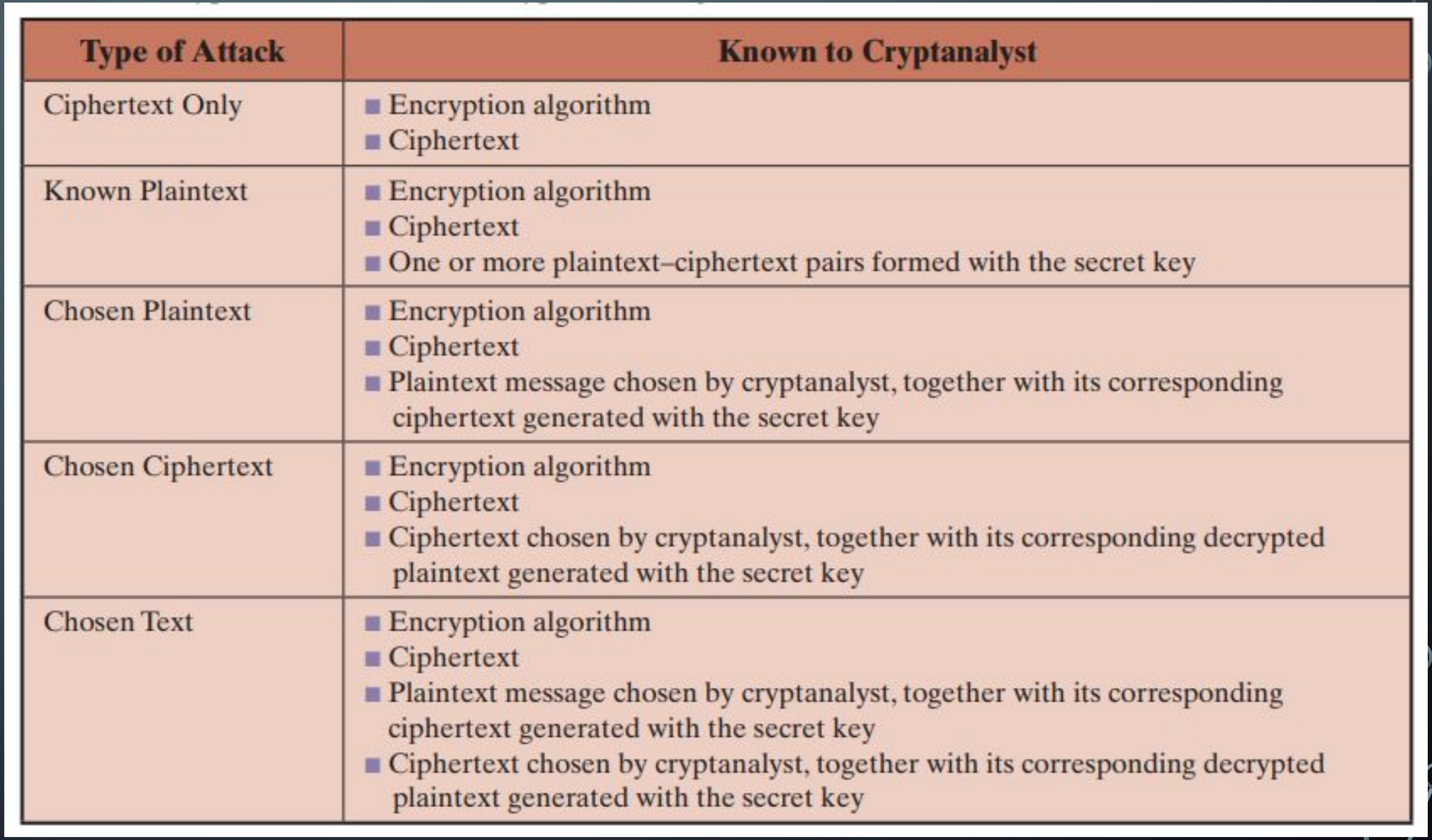


CRYPTANALYSIS AND BRUTE-FORCE ATTACK

- There are two general approaches to attacking a conventional encryption scheme.
- **Cryptanalysis**: Cryptanalytic attacks 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.
- **Brute-force attack**: The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

CRYPTANALYSIS

- The table summarizes the various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.



Type of Attack	Known to Cryptanalyst
Ciphertext Only	■ Encryption algorithm ■ Ciphertext
Known Plaintext	■ Encryption algorithm ■ Ciphertext ■ One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	■ Encryption algorithm ■ Ciphertext ■ Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	■ Encryption algorithm ■ Ciphertext ■ Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	■ Encryption algorithm ■ Ciphertext ■ Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key ■ Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

SUBSTITUTION TECHNIQUES

- The two basic building blocks of all encryption techniques are substitution and transposition.
- A substitution technique is one 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 ciphertext bit patterns. Two Substitution techniques will be discussed in the following slides:-
    - Caesar Cipher
    - Monoalphabetic Ciphers

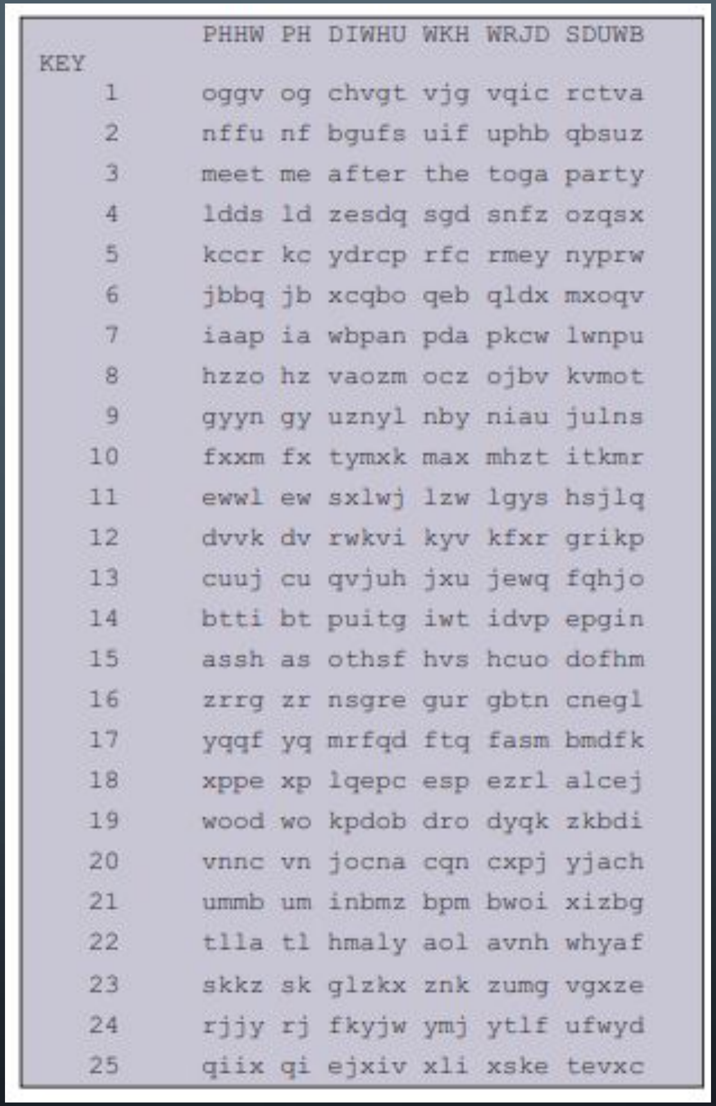
CAESAR CIPHER

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.
- plain: meet me after the party
- cipher: PHHW PH DIWHU WKH SDUWB
- the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C.
- $C = E(k, p) = (p + k) \bmod 26$
- The decryption algorithm is simply $p = D(k, C) = (C - k) \bmod 26$

CRACKING CAESER CIPHER

- Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:
    - The encryption and decryption algorithms are known.
    - There are only 25 keys to try.
    - The language of the plaintext is known and easily recognizable

BRUTE-FORCE CRYPTANALYSIS OF CAESAR CIPHER

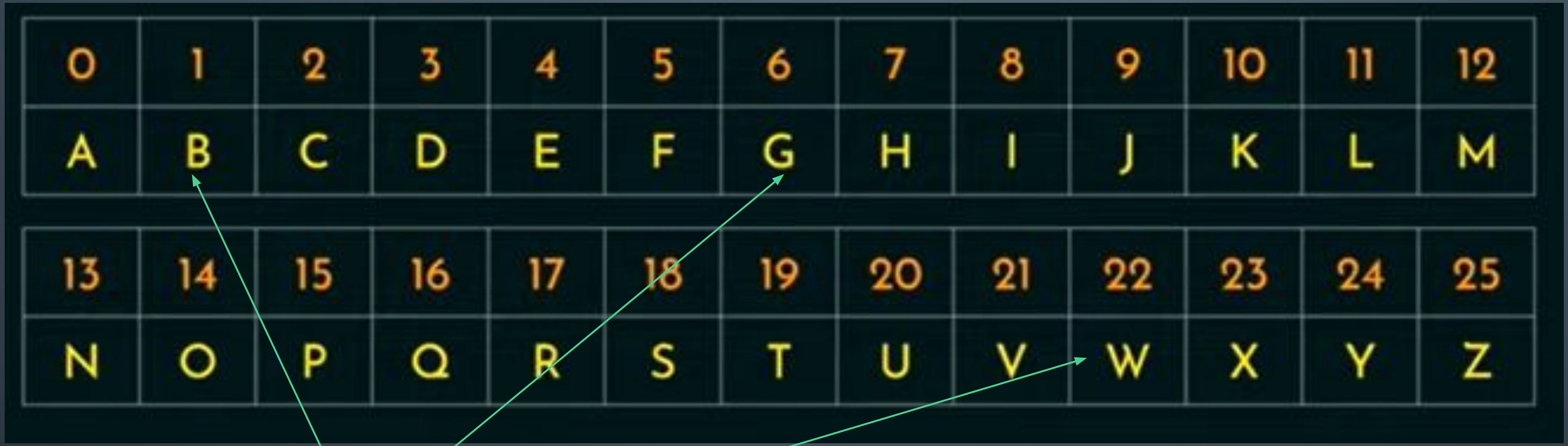


KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

MONOALPHABETIC CIPHERS

- 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.
- if S = {a, b, c}, there are six permutations of S:
  - abc, acb, bac, bca, cab, cba
- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 * 1026 possible keys.
- This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis

MONOALPHABETIC …. (CONT..)



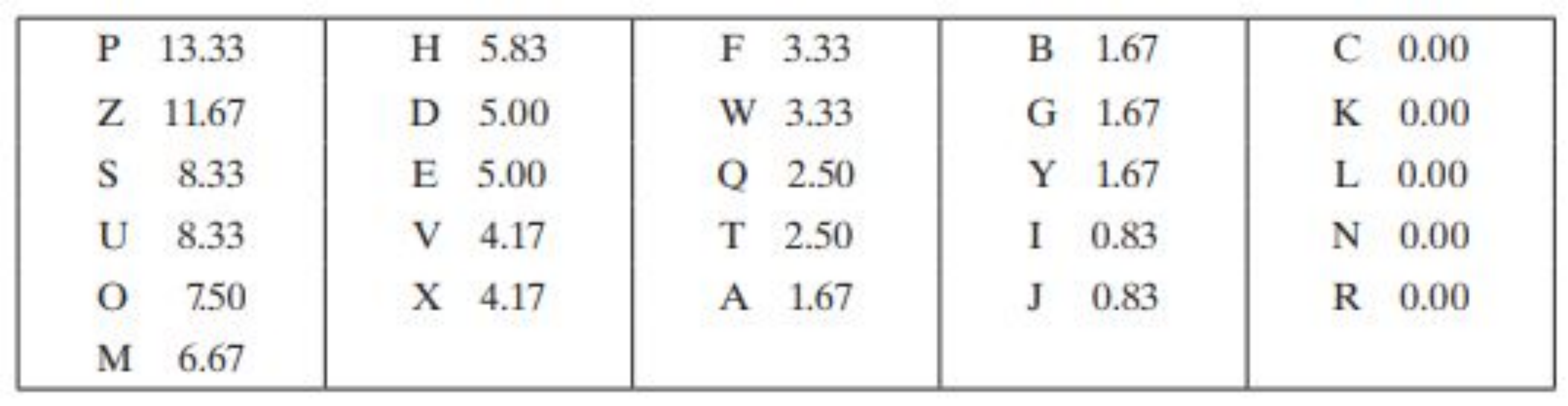
0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- Plain-text: TRY
- Cipher-text: GBW

CRYPTANALYSIS OF MONOALPHABETIC

- If the cryptanalyst knows the nature of the plaintext (e.g., noncompressed English text), then the analyst can exploit the regularities of the language.
- The ciphertext to be solved is
- UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English.

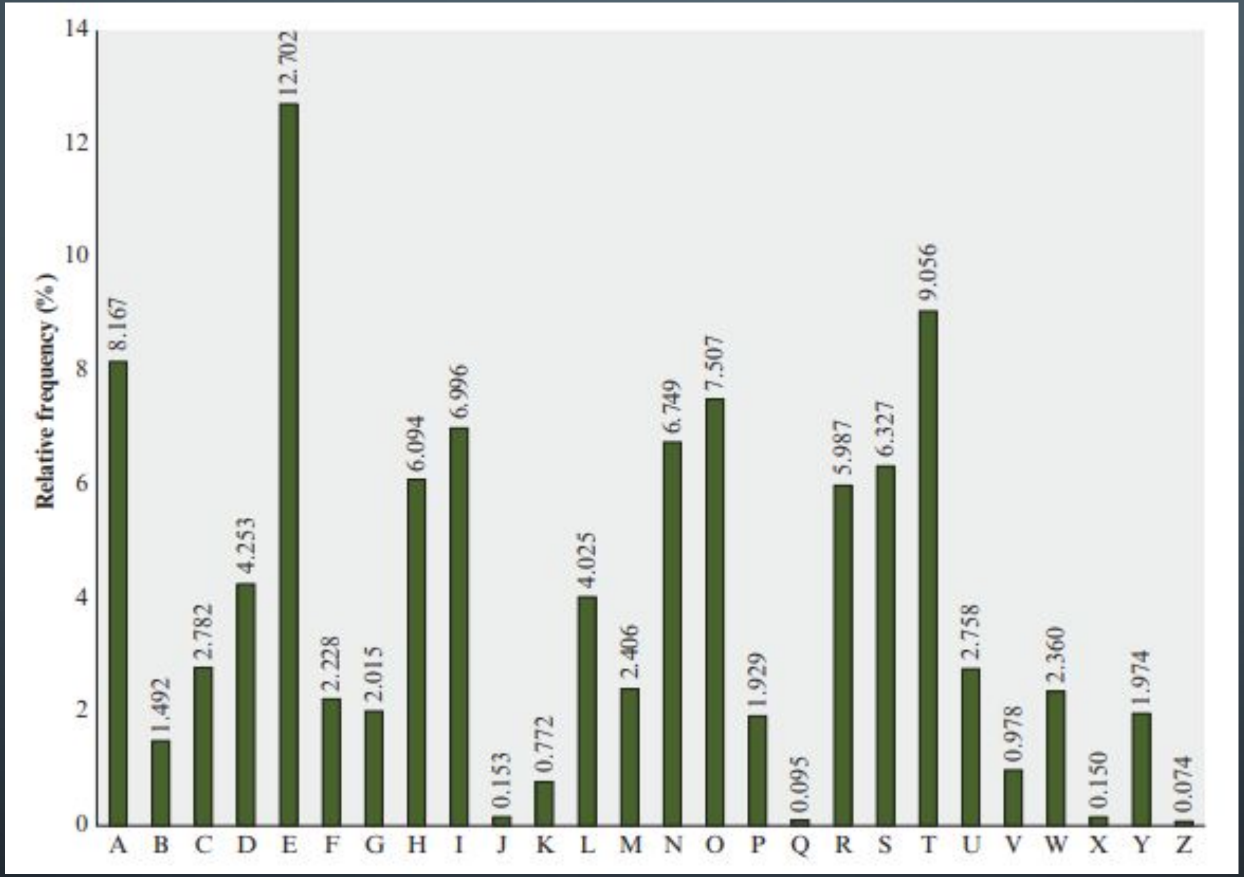
CRYPTANALYSIS…..



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								

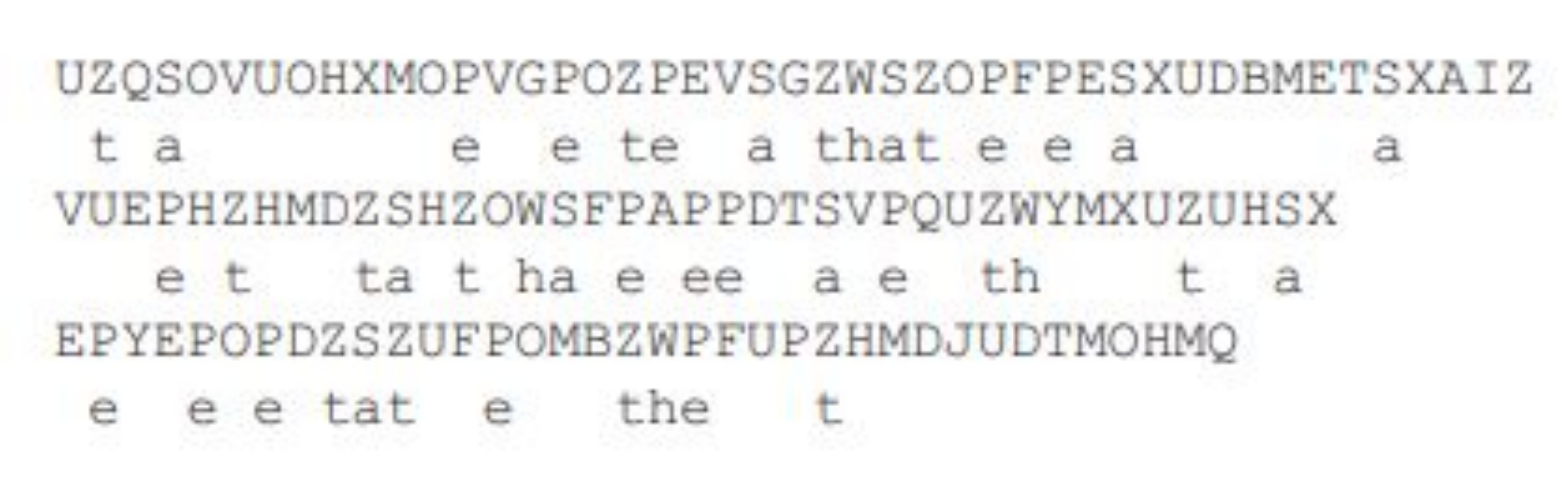
- Table showing relative frequencies of letters in ciphertext

CRYPTANALYSIS….



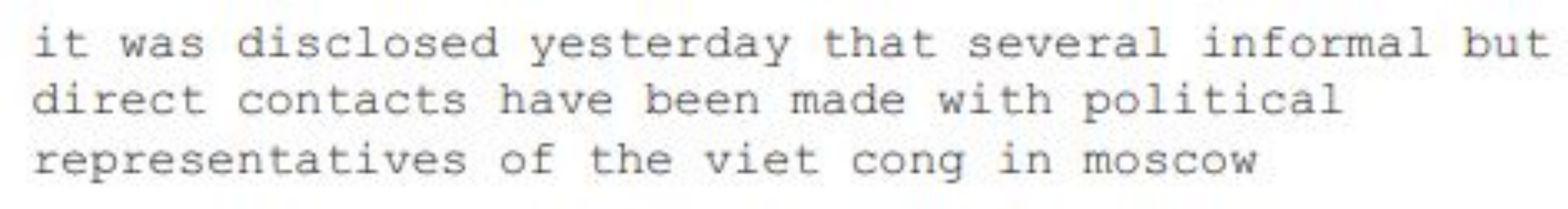
- Relative Frequency of Letters in English Text

CRYPTANALYSIS….



```
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
```

CRYPTANALYSIS….



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

CONS & COUNTERMEASURE OF MONOALPHABETIC CIPHER

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- A countermeasure is to provide multiple substitutes, known as homophones, for a single letter

POLYALPHABETIC CIPHERS

- A way to improve monoalphabetic cipher is the use of polyalphabetic cipher.
- All these techniques have the following features in common:
- A set of related monoalphabetic substitution rules is used.
- A key determines which particular rule is chosen for a given transformation.
- There are two types of polyalphabetic ciphers
  - Vigenere Cipher
  - One-Time pad cipher

VIGENERE CIPHER

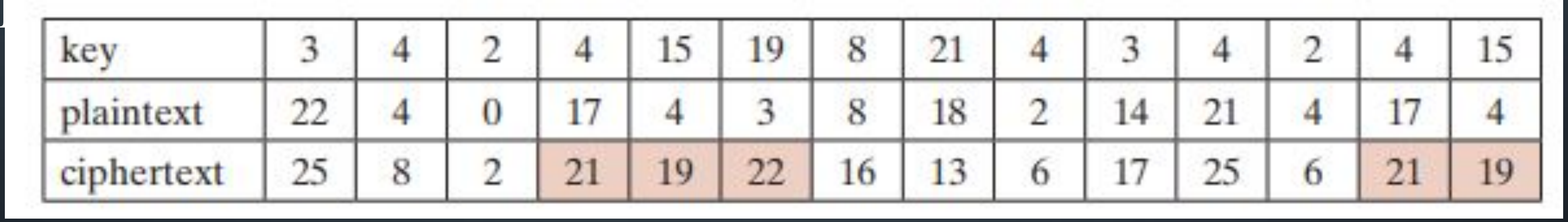
- In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter. It is expressed as:
- Plaintext letters $P = p_0, p_1, p_2, \ldots\ldots\ldots, p_{n-1}$
- Key $K = k_0, k_1, k_2, \ldots\ldots\ldots, k_{m-1}$
- Cipher letters $C = C_0, C_1, C_2, \ldots\ldots\ldots, C_{n-1}$

VIGENERE CIPHER

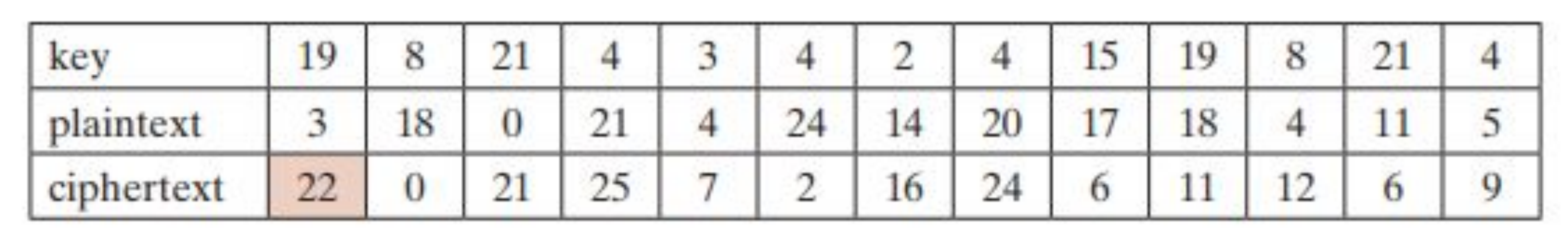
- $C = C_0, C_1, C_2, \ldots\ldots\ldots, C_{n-1} = E(K,P) = E[(k_0, k_1, k_2, \ldots\ldots\ldots, k_{m-1}), (p_0, p_1, p_2, \ldots\ldots\ldots, p_{n-1})]$
- $= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots,(p_{m-1} + k_{m-1}) \bmod 26, (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26,$ c, $(p_{2m-1} + k_{m-1}) \bmod 26,$
- $C_i = (p_i + k_{i \bmod m}) \mathrm{mod} 26$, Encrypt equation
- $p_i = (C_i - k_{i \bmod m}) \mathrm{mod} 26$, Decrypt equation.
- To encrypt key must be as long as the message.

VIGENERE CIPHER

- if the keyword is deceptive, the message “we are discovered save yourself” is encrypted as:
- key: deceptivedeceptivedeceptive
- plaintext: wearediscoveredsaveyourself
- ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ



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



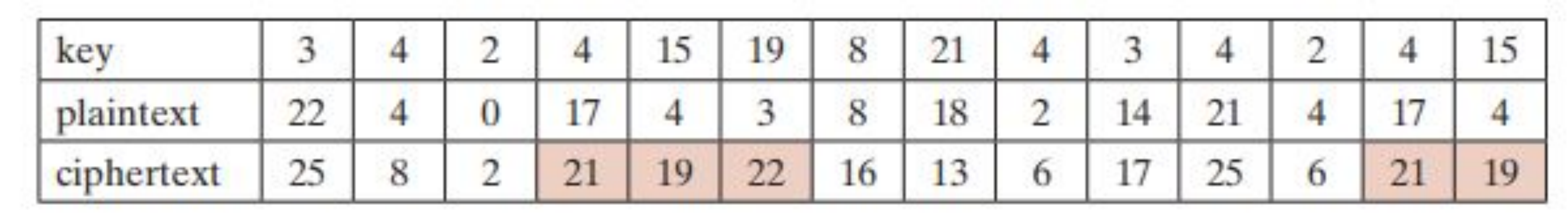
key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

VIGENERE CIPHER - CRYPTANALYSIS

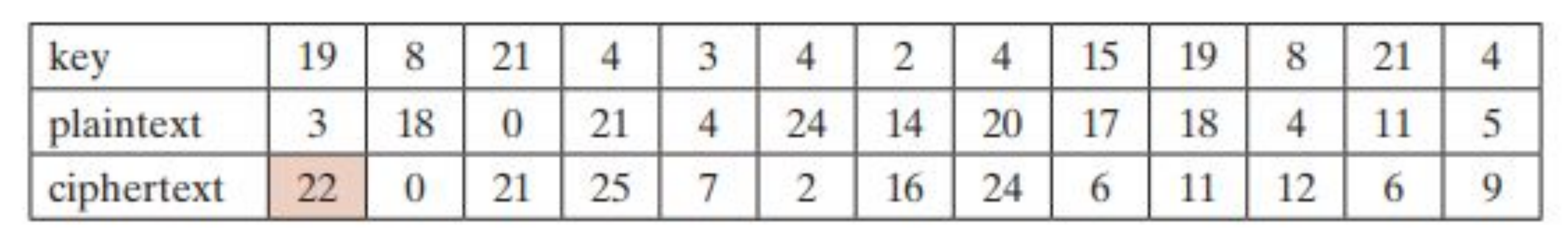
- Determining the length of the keyword.
- Key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied.

VIGENERE CIPHER - CRYPTANALYSIS

- How to determining the length of the keyword?
- 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.



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



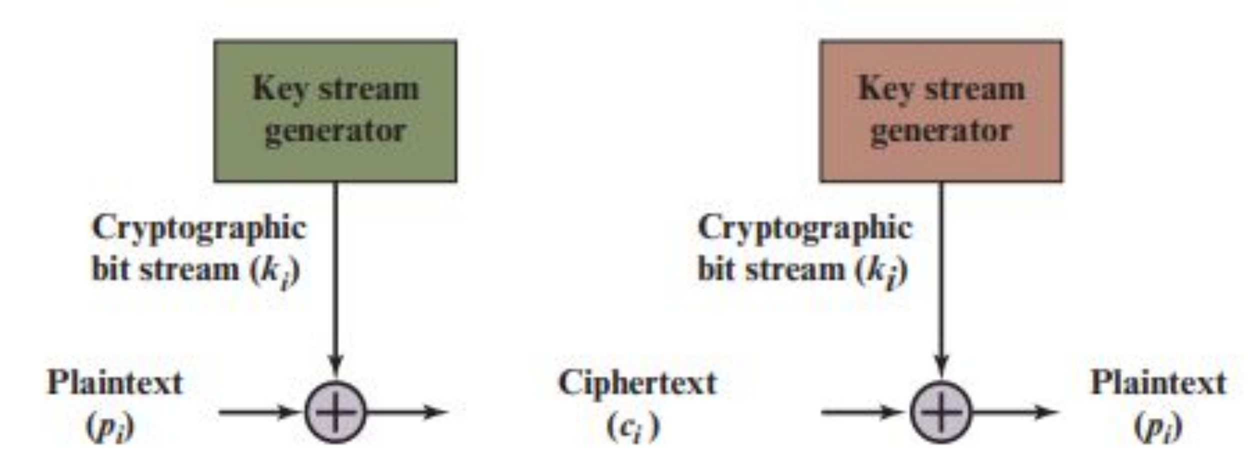
key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

VIGENERE CIPHER - AUTOKEY

- The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself.
- Vigenère proposed what is referred to as an autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key.
- key: deceptivewearediscoveredsav
- plaintext: wearediscoveredsaveyourself
- ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

VERNAM CIPHER

- The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it.
- $c_i = p_i \oplus k_i$
- where
  $p_i = i$ th binary digit of plaintext
  $k_i = i$ th binary digit of key
  $c_i = i$ th binary digit of ciphertext
  $\oplus =$ exclusive-or (XOR) operation
- for decryption
- $p_i = c_i \oplus k_i$


Key stream generator
Cryptographic bit stream (k_i)
Plaintext (p_i)
Key stream generator
Cryptographic bit stream (k_i)
Ciphertext (c_i)
Plaintext (p_i)