Subject Name: Cryptography and Network Security

Unit No: 01 Unit Name: Introduction to Cryptography

Faculty Name:

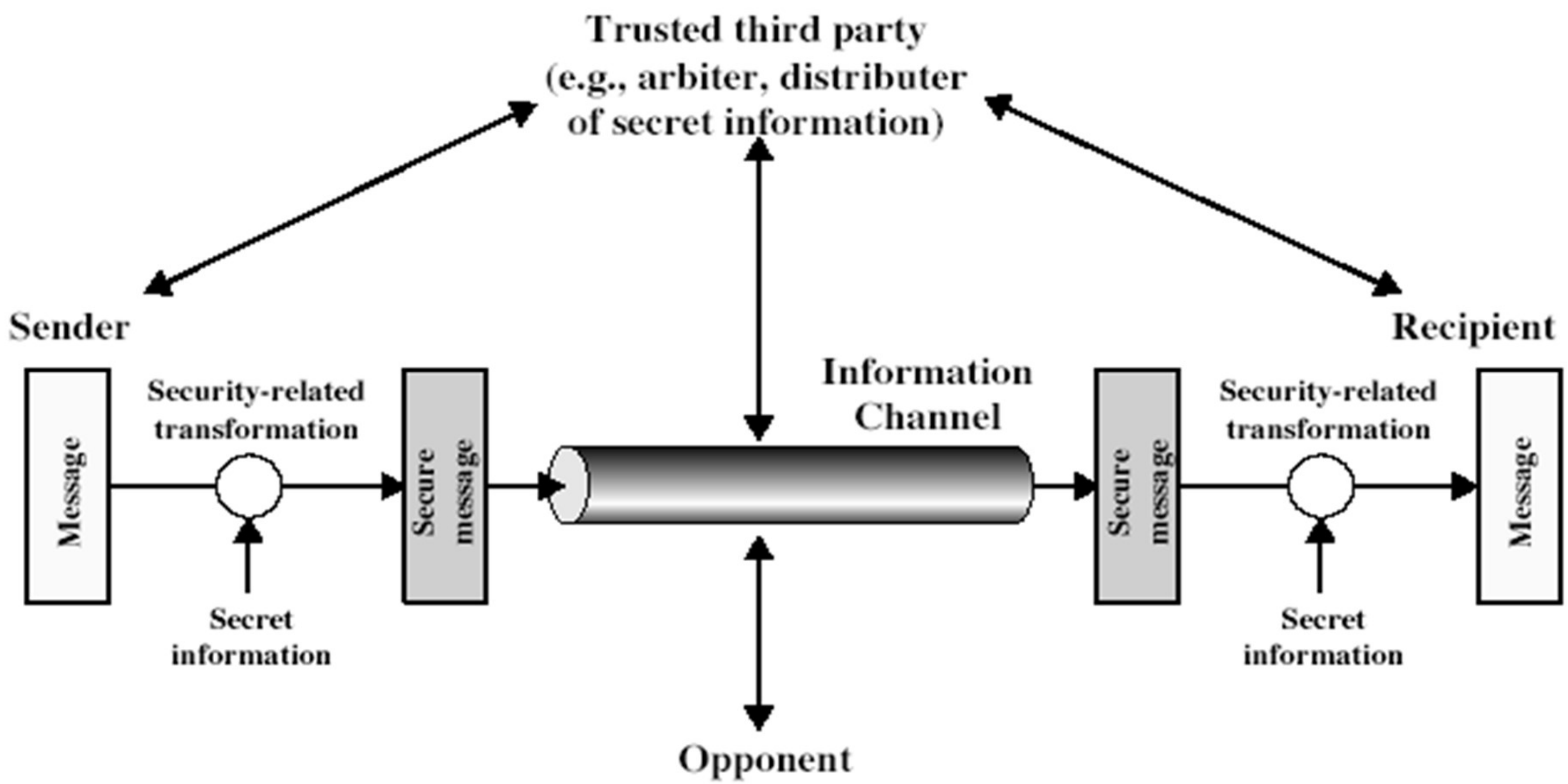
Dr. Sangita Chaudhari
Dr.Pallavi Sapkale

Index

Unit No: 1 Unit Name: Introduction & Number Theory

Lecture No: 1
Classical Encryption techniques, Symmetric cipher model

Model for Network Security



Model for Network Security

This model requires :

1. Design a suitable algorithm for the security transformation
2. Generate the secret information (keys) used by the algorithm
3. Develop methods to distribute and share the secret information
4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Classical Security Techniques

- Cryptography
- Symmetric Key Encipherment/Secret Key Cryptography/Private Key Cryptography
- Asymmetric Key Encipherment/ Shared Key Cryptography/ Public Key Cryptography
- Steganography

Cryptography

- ***Symmetric(Secret/Private key)***

$$C = E_k(M)$$

$$M = D_k(C)$$

- ***Asymmetric(Shared/Public key)***

$$C = E_{pu.k}(M)$$

$$M = D_{pr.k}(C)$$

Basic Terminologies

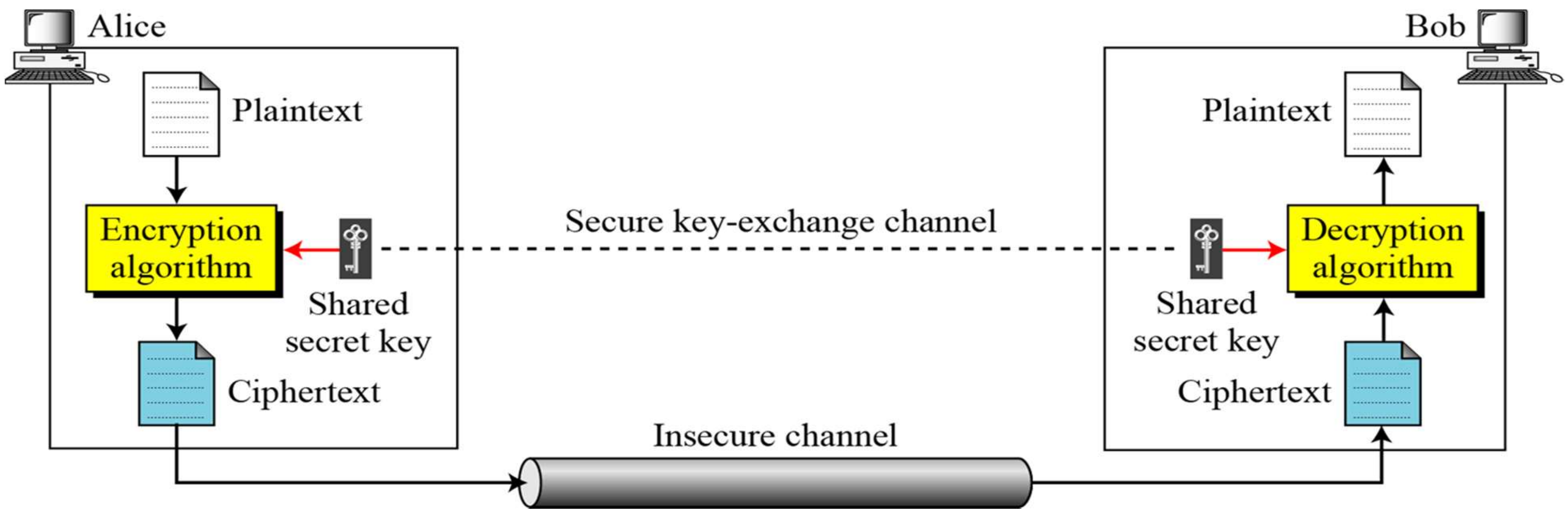
- **Plaintext** - original message
- **Ciphertext** - coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering plaintext from ciphertext
- **Cryptanalysis (code breaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **Cryptology** - field of both cryptography and cryptanalysis

Requirements of Classical Security Techniques

- Strong encryption algorithm
  - An opponent who knows one or more ciphertexts would not be able to find the plaintexts or the key
  - Ideally, even if he knows one or more pairs of plaintext-ciphertext, he would not be able to find the key
- Sender and receiver must share the key. Once the key is compromised, all communications using that key are readable
- Encryption algorithm is not a secret. It is impractical to decrypt the message on the basis of the ciphertext plus the knowledge of the encryption algorithm (**Kerckhoff's principle**)

Classical Symmetric Ciphers(Encryption Techniques)

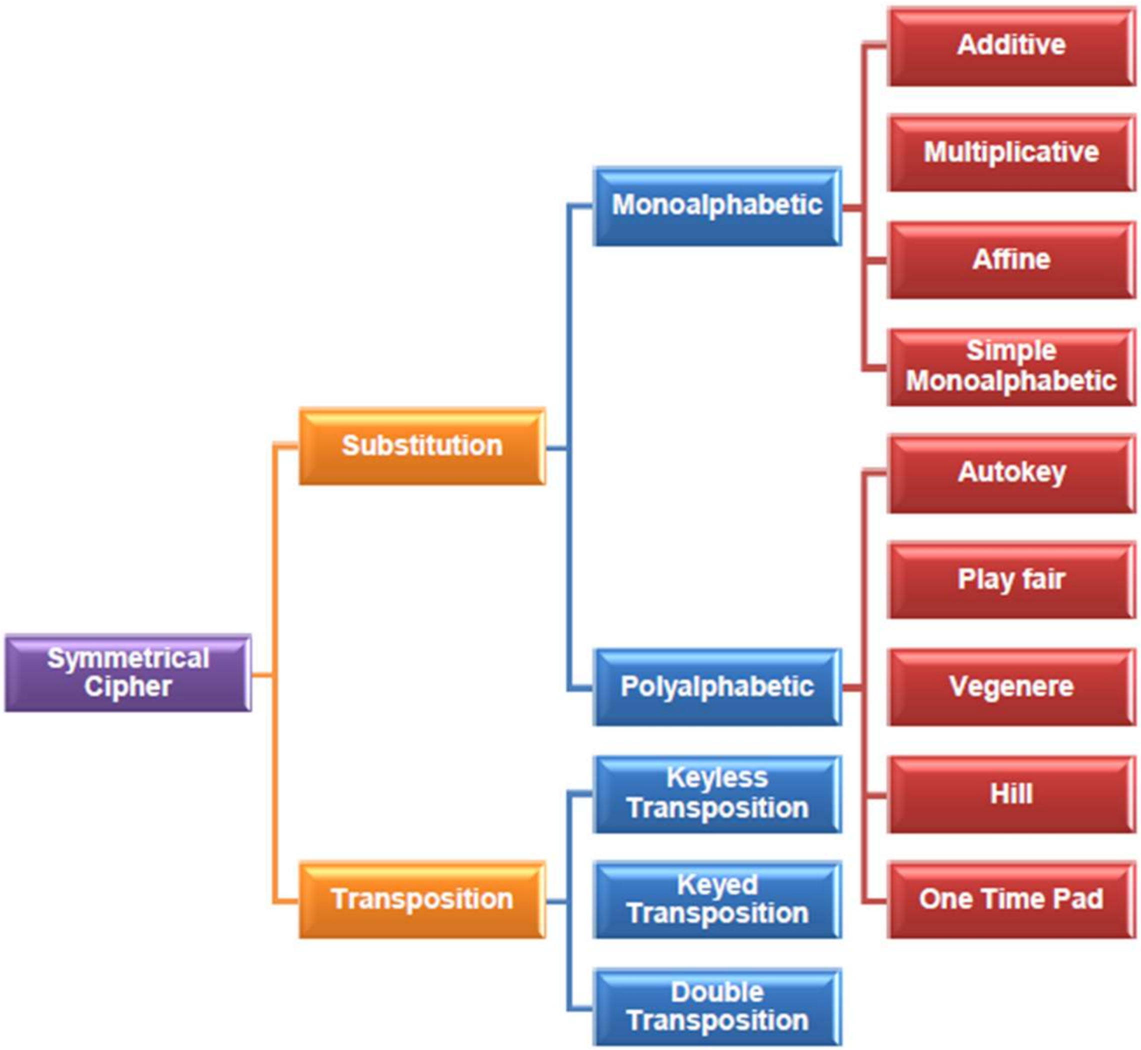
- Classical (historical) algorithms are based on substitution & permutation.



Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

Classical Symmetric Ciphers



Unit No: 1

Unit Name: Introduction & Number Theory

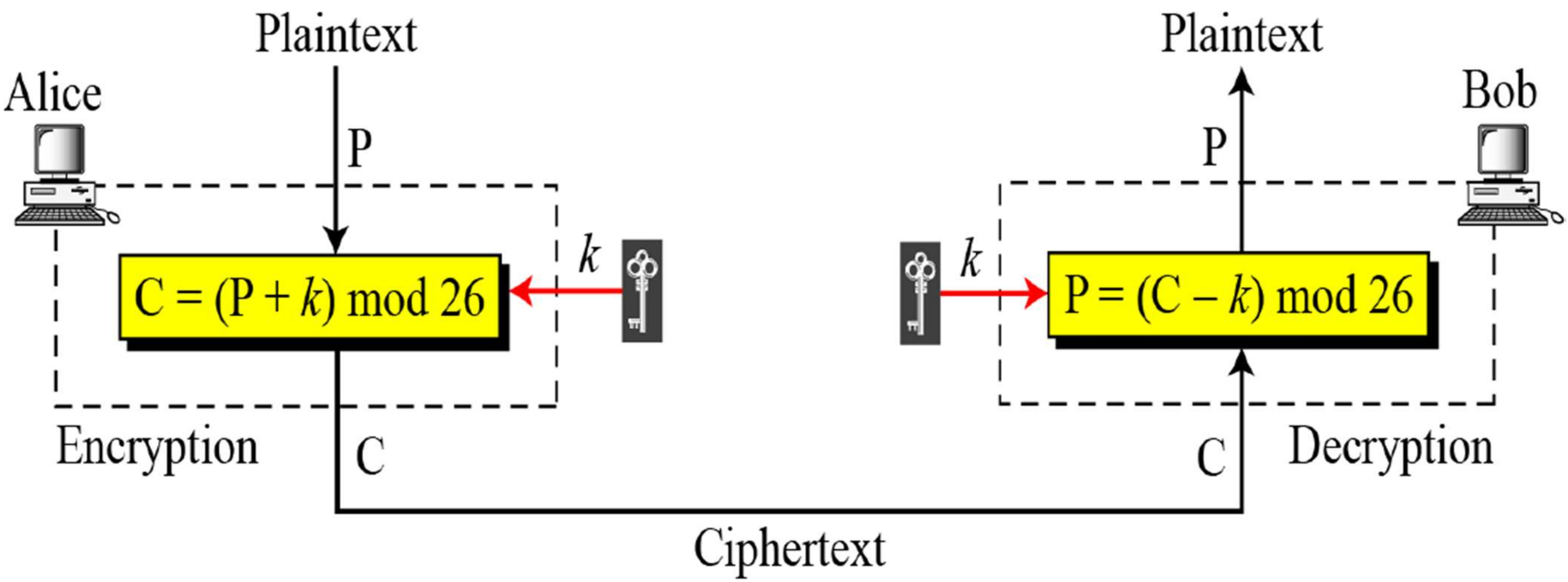
Lecture No: 2
Monoalphabetic Ciphers

Caesar Ciphers (Additive/Shift ciphers)

- The simplest monoalphabetic cipher is the additive cipher.
- This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature.

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

Caesar Ciphers (Additive/Shift ciphers)



Caesar Ciphers (Additive/Shift ciphers)

Use the additive cipher with key = 5 to encrypt the message "SECURITY".

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: S -> 18	Encryption: (18+5)mod 26	Ciphertext: 23 -> X
Plaintext: E -> 4	Encryption: (4+5)mod 26	Ciphertext: 9 -> J
Plaintext: C -> 2	Encryption: (2+5)mod 26	Ciphertext: 7 -> H
Plaintext: U -> 20	Encryption: (20+5)mod 26	Ciphertext: 25 -> Z
Plaintext: R -> 17	Encryption: (17+5)mod 26	Ciphertext: 22 -> W
Plaintext: I -> 8	Encryption: (8+5)mod 26	Ciphertext: 13 -> N
	Encryption: (19+5)mod 26	Ciphertext: 24 -> Y
24	Encryption: (24+5)mod 26	Ciphertext: 3 -> D

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

Caesar Ciphers (Additive/Shift ciphers)

Use the additive cipher with key = 5 to decrypt the message "XJHZWNYD".

Solution

We apply the decryption algorithm to the plaintext character by character:

Ciphertext: X -> 23
Ciphertext: J -> 9
Ciphertext: H -> 7
Ciphertext: Z -> 25
Ciphertext: W -> 22
Ciphertext: N -> 13
Ciphertext: Y -> 24
Ciphertext: D -> 3

Decryption: (23 - 5)mod 26
Decryption : (9 - 5)mod 26
Decryption : (7 - 5)mod 26
Decryption : (25 - 5)mod 26
Decryption : (22 - 5)mod 26
Decryption : (13 -5)mod 26
Decryption : (24 - 5)mod 26
Decryption : (3- 5) mod 26

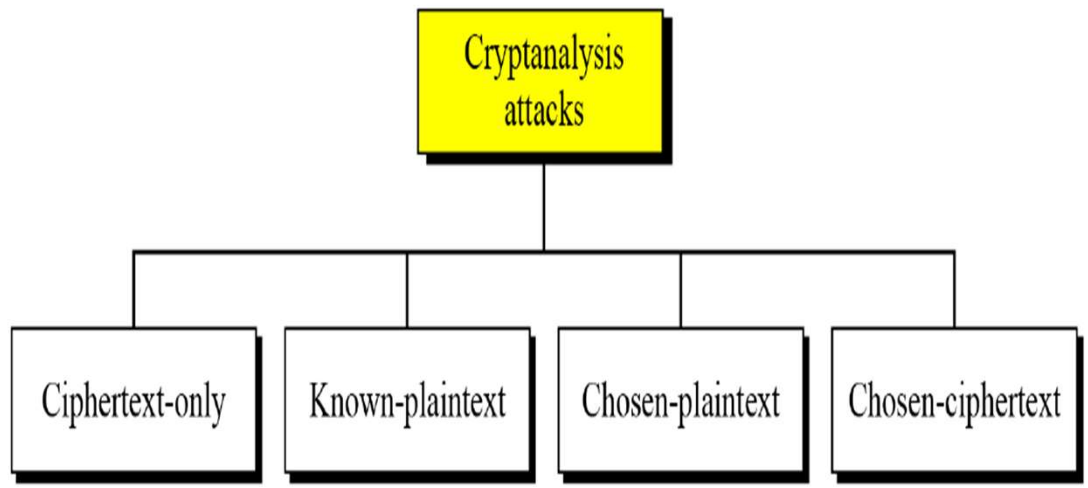
Plaintext: 18 -> S
Plaintext: 4 -> E
Plaintext: 2 -> C
Plaintext: 20 -> U
Plaintext: 17 -> R
Plaintext: 8 -> I
Y

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

Cryptanalysis

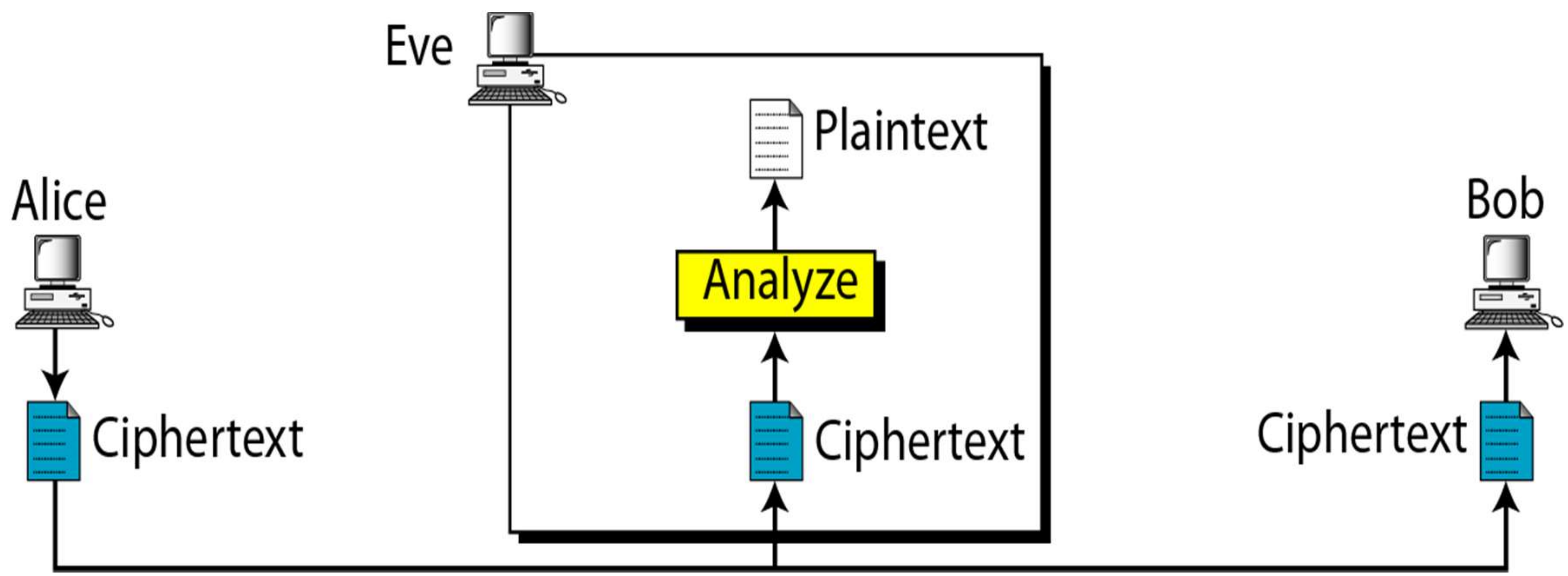
"Cryptanalysis is the science and art of breaking secret codes created by Cryptography"

- Objective - to recover key not just message
- Approaches:
  - ➢ Cryptanalytic attack
  - ➢ Brute-force attack
  - ➢ Statistical attack
  - ➢ Pattern attack



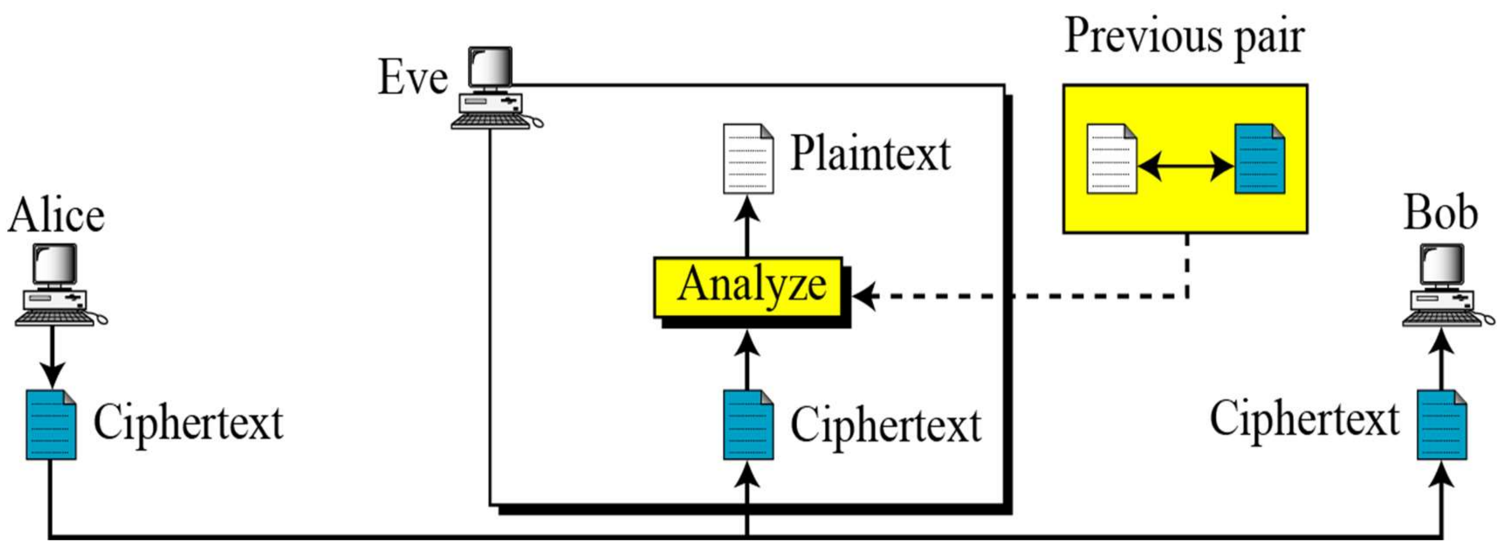
Cryptanalytic Attacks

Ciphertext only - only ciphertext is known to attacker



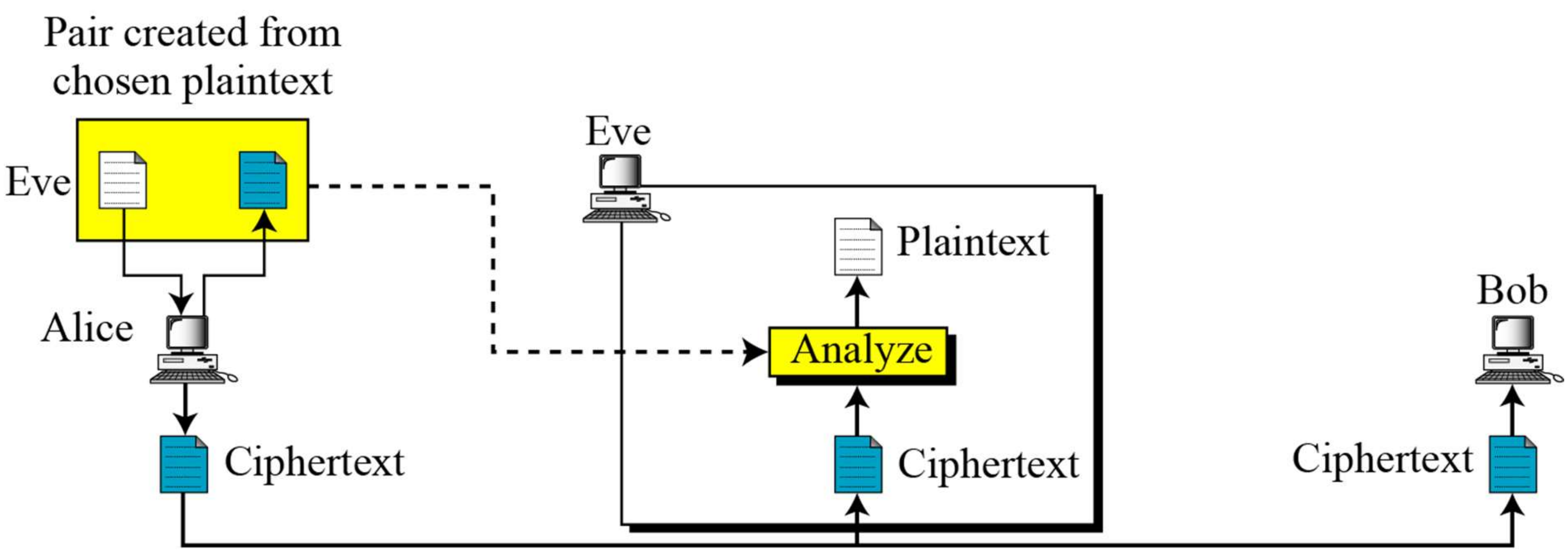
Cryptanalytic Attacks

Known Plaintext - pairs of ciphertext and corresponding to plaintext is known to attacker



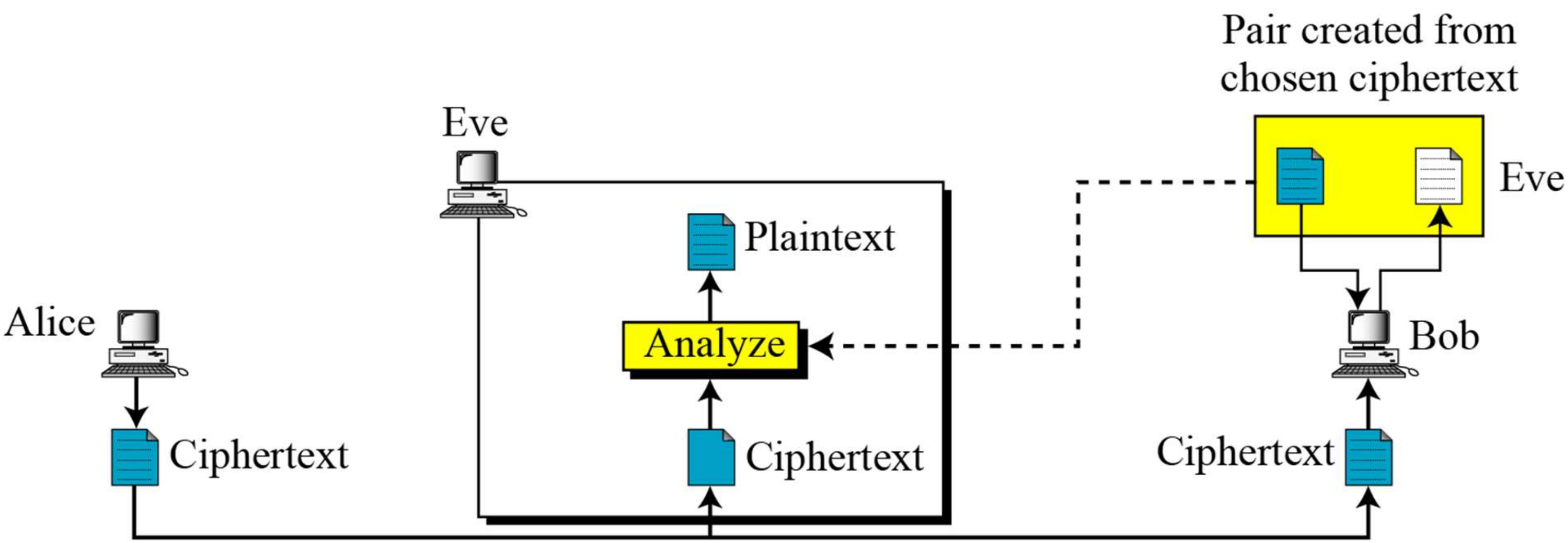
Cryptanalytic Attacks

Chosen Plaintext - attacker selects a plaintext



Cryptanalytic Attacks

Chosen Ciphertext - attacker selects a ciphertext



Cryptanalysis of Caesar Cipher

- only have 25 possible ciphers
  - A maps to B,C,...Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- Ciphertext: SGHR HR BRR BKZRR

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

Statistical Attacks

- Compute frequency of each letter in ciphertext (KHOOR ZRUOG):
- G = 0.1, H = 0.1, K = 0.1, O = 0.3, R = 0.2, U = 0.1, Z = 0.1
- Let Φ (i) be a correlation function of the frequency of each letter in ciphertext with the corresponding letter in English,

$$\phi(i) = \sum_{0 \le c \le 25} f(c)p(c-i)$$

- i is the key

- f (c) is the frequency of character c in ciphertext

- p(x) is the frequency of character x in English

D Y PATIL DEEMED TO BE UNIVERSITY
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Statistical Attack

- For ciphertext (KHOOR ZRUOG): G H K O R U Z

  $\phi(i) = 0.1p(6 - i) + 0.1p(7 - i) + 0.1p(10 - i) + 0.3p(14 - i) + 0.2p(17 - i) + 0.1p(20 - i) + 0.1p(25 - i)$

Correlation: φ(i) for 0 ≤ i ≤ 25

i	φ(i)	i	φ(i)	i	φ(i)	i	φ(i)
0	0.0482	7	0.0442	13	0.0520	19	0.0315
1	0.0364	8	0.0202	14	0.0535	20	0.0302
2	0.0410	9	0.0267	15	0.0226	21	0.0517
3	0.0575	10	0.0635	16	0.0322	22	0.0380
4	0.0252	11	0.0262	17	0.0392	23	0.0370
5	0.0190	12	0.0325	18	0.0299	24	0.0316
6	0.0660					25	0.0430

Most probable keys, based on :

$\varphi(6) = 0.0660$ plaintext: EBIIL TLOLA

$\varphi(10) = 0.0635$ plaintext AXEEH PHKEW

$\varphi(3) = 0.0575$ plaintext HELLO WORLD

$\varphi(14) = 0.0535$ plaintext WTAAD LDGAS

The only English phrase is for i = 3 (key = 3 or 'D')

Pattern Attack

- Human languages are **redundant**
- Letters are not equally commonly used
- In english **e** is by far the most common letter and then t, r, n, i, o, a, s
- It have tables of single, double & triple letter frequencies

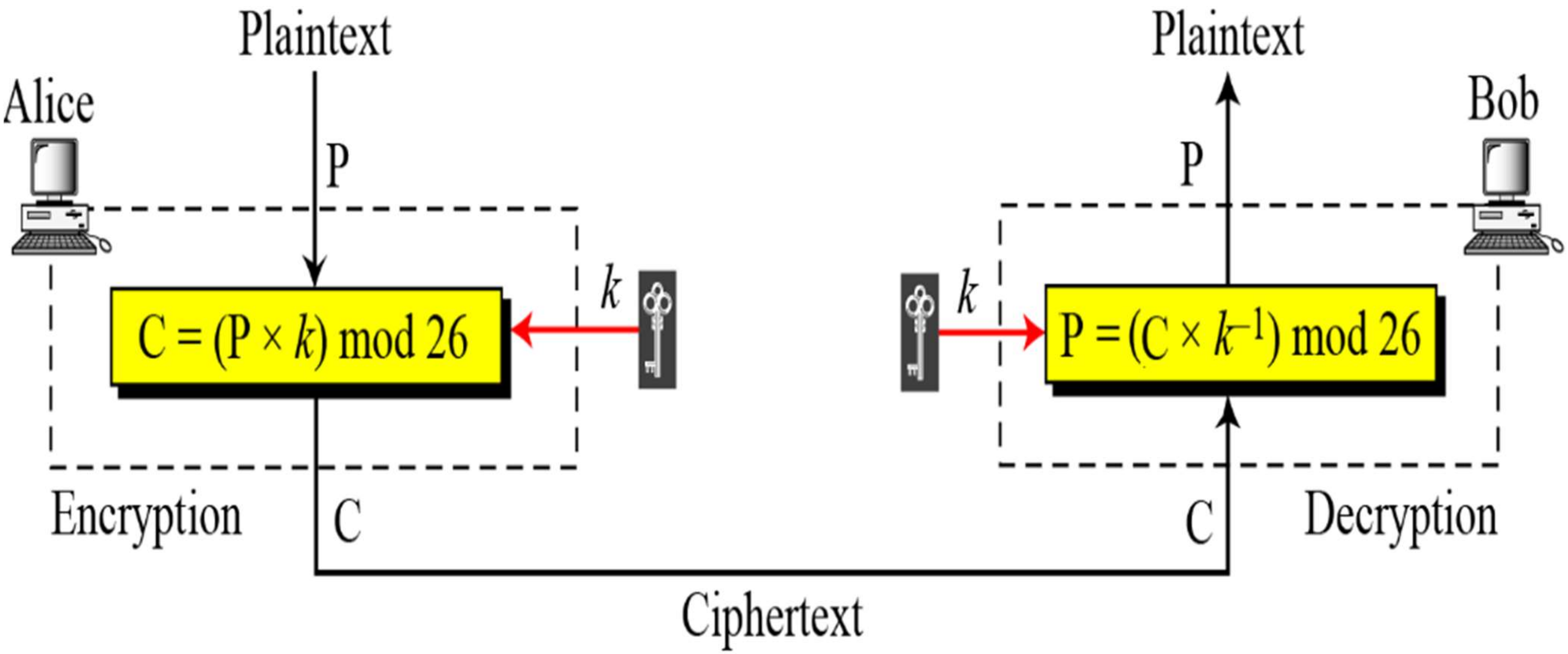
Pattern Attack

- Given ciphertext:
  - **UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETS XAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZH SXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ**
- count relative letter frequencies
- Guess: P & Z are e and t
- guess ZW is TH and hence ZWP is THE
- proceeding with trial and error finally get:
  - **it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow**

Caesar Cipher- Shortcomings

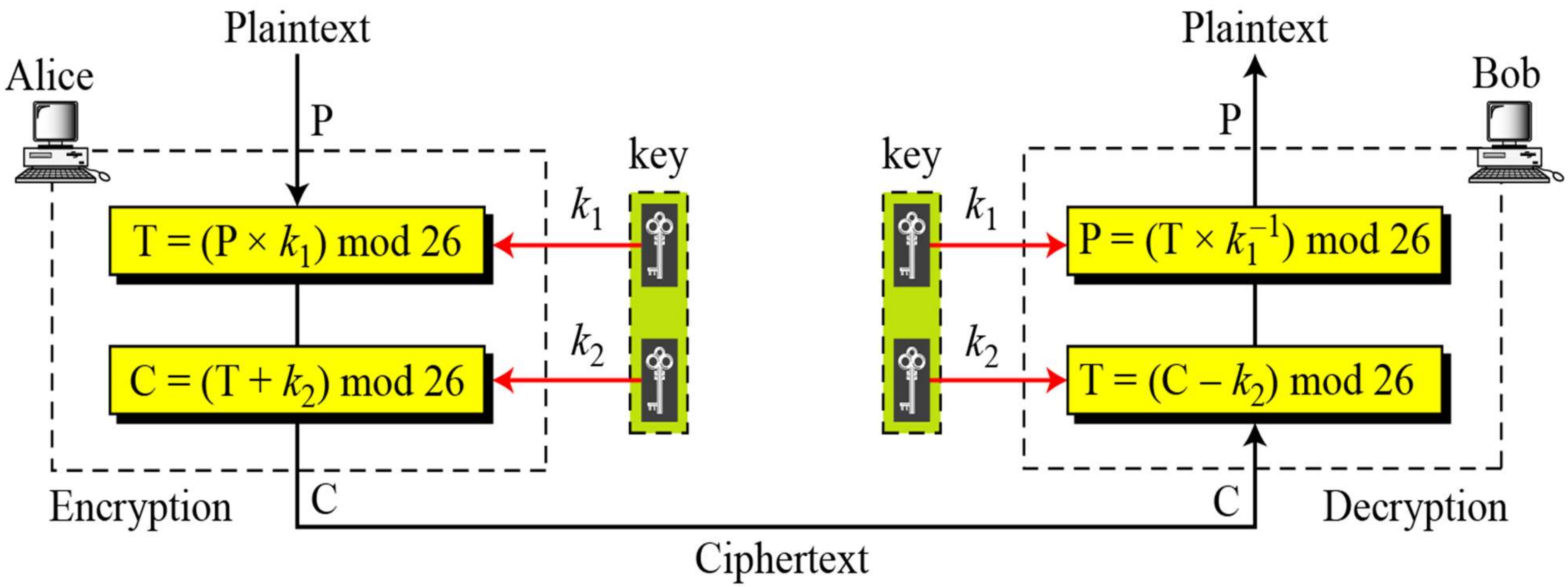
- Key is too short
- Key can be found by exhaustive search
- Statistical frequencies not concealed well
- They look too much like regular English letters

Multiplicative Cipher



D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Affine Cipher



Affine Cipher

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

Encryption:

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

Affine Cipher

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

Decryption:

Multiplicative Inverse of 7=15

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

Simple Monoalphabetic Cipher

Instead of shifting the letters with a fixed amount, any permutation of the alphabet is done.

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

Plaintext: cryptography

Ciphertext: VYZXUHBYDMJZ

Number of keys ?

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Simple Monoalphabetic Cipher

- Keys are 26! = 4×10^{26}
- Decryption without a key would need to try all the 26! Possibilities.
- With so many keys, it might be secure
- The problem is that
  - language characteristics can be used to speed up the process of decryption

Unit No: 1

Unit Name: Introduction & Number Theory

Lecture No: 3
Polyalphabetic substitution techniques: Vigenère cipher

Polyalphabetic Substitution Cipher

- Each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

- Makes cryptanalysis harder with more alphabets (substitutions) to guess and flattens frequency distribution

- A key determines which substitution is used in each step

Autokey Cipher

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

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

Plaintext = attack is today

$K_1 = 12$

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

Ciphertext = mtmtcm sa lhrdy

Vigenère Cipher

- Proposed by Giovan Batista Belaso (1553) and reinvented by Blaisede Vigenère (1586)
- Multiple caesar ciphers
- key is multiple letters long K = k1 k2 ... kd
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

Vigenère Cipher

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

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

Example: Encrypt the message "She is listening" using the 6-character keyword "PASCAL".

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

Vigenère Cipher

keyword : deceptive

key: de cep tivedecept ived eceptive

plaintext: we are discovered save yourself

ciphertext: ZI CVT WQNGRZGVTW AVZH CQYGLMGJ

KEY

PLAINTEXT

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

Vigenère Cipher

- Its strength lays in the fact that each plaintext letter has multiple ciphertext letters

  - Letter frequencies are obscured (but not totally lost)

- The Vigenère Cipher can be broken using the following steps:

  1. Find the period (key length); call it n

  2. Break ciphertext into n parts

     - Each part is enciphered using the same key letter (Caesar cipher)

  3. Solve each part as a Caesar cipher!

One Time Pad

- Idea: use a (truly) random key as long as the plaintext
- It is unbreakable since the ciphertext bears no statistical relationship to the plaintext
- Moreover, for any plaintext & any ciphertext there exists a key mapping one to the other
- Thus, a ciphertext can be decrypted to any plaintext of the same length
- The cryptanalyst is in an impossible situation

One Time Pad

- The security is entirely given by the randomness of the key
  - If the key is truly random, then the ciphertext is random
  - A key can only be used once if the cryptanalyst is to be kept in the "dark"
- Problems with this "perfect" cryptosystem
  - Making large quantities of truly random characters is a significant task
  - Key distribution is enormously difficult: for any message to be sent, a key of equal length must be

Thank You

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI