NETWORK SECURITY AND CRYPTOGRAPHY

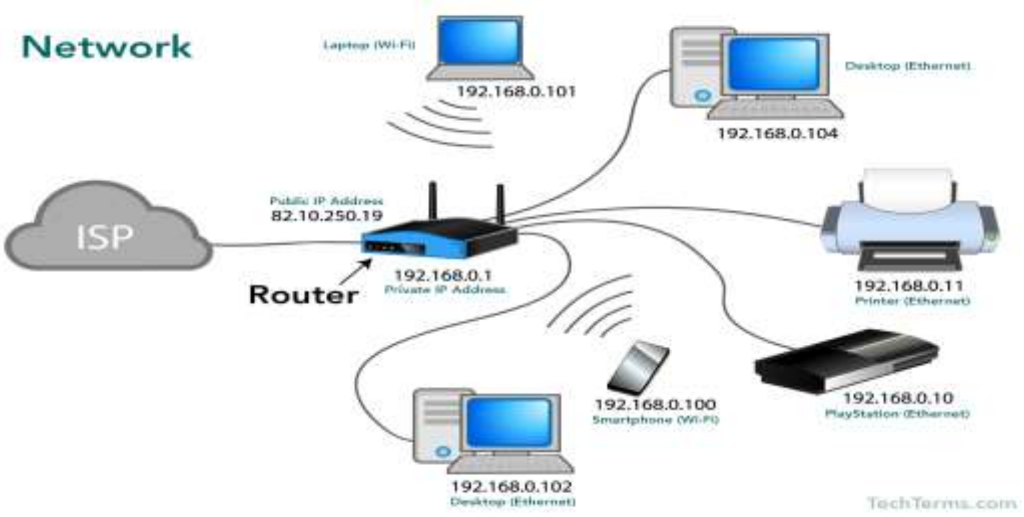
Presented By

K. APPASAMY,MCA;M.Phil

Assistant Professor,
Department of BCA & M.Sc[NT & IT]
ST. JOHN'S COLLEGE,
PALAYAMKOTTAI

NETWORK DEFINITION

A **computer network** is a set of **computers** connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered a **computer network**.

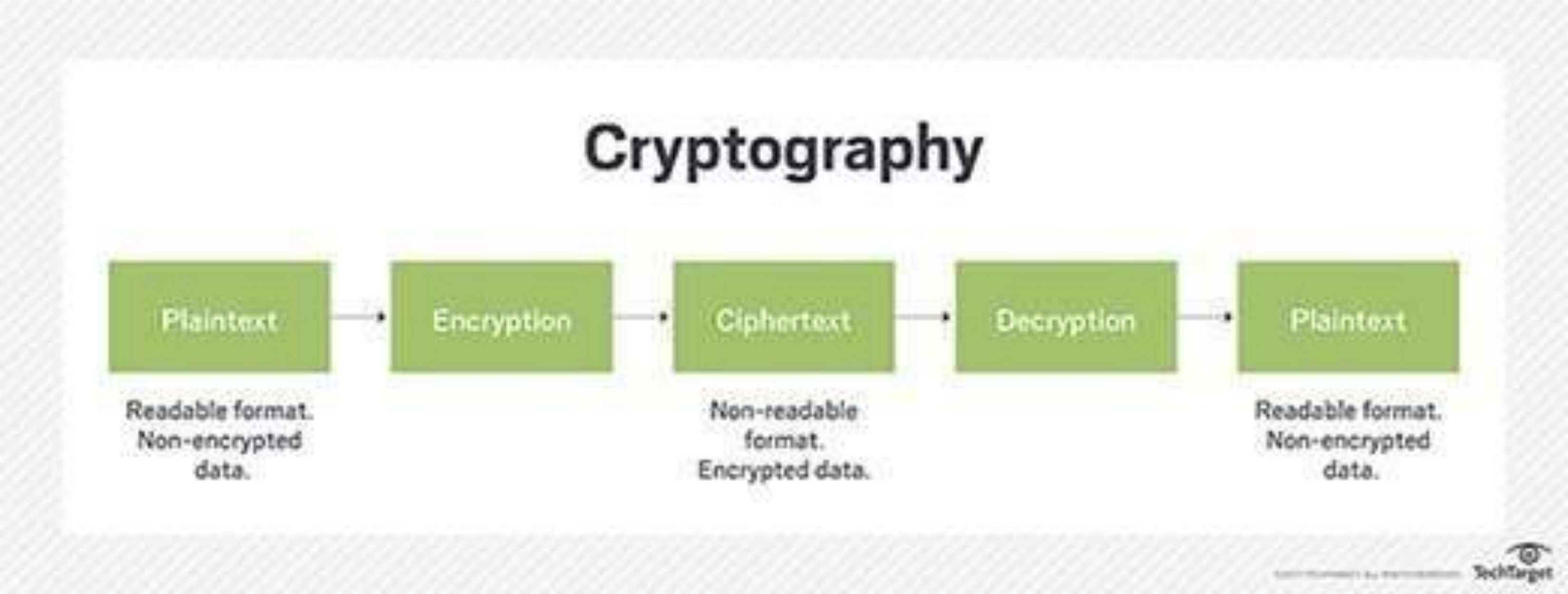


SECURITY

Computer security, also known as cyber security or IT **security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

CRYPTOGRAPHY

Cryptography. **Cryptography** is the science of protecting information by transforming it into a secure format. This process, called encryption, has been used for centuries to prevent handwritten messages from being read by unintended recipients. Today, **cryptography** is used to protect digital data


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
TechTarget

MENAING AND HISTORY OF CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

HISTORY :

The word "cryptography" is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

TYPES OF CRYPTOGRAPHY

Single-key or symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it. Types of symmetric-key cryptography include the Advanced Encryption Standard (AES), a specification established in November 2001 by the National Institute of Standards and Technology as a Federal Information Processing Standard (FIPS 1977), to protect sensitive information.

In June 2003, AES was approved by the U.S. government for classified information. It is a royalty-free specification implemented in software and hardware worldwide. AES is the successor to the Data Encryption Standard (DES) and DES3. It uses longer key lengths (128-bit, 192-bit, 256-bit) to prevent brute force and other attacks.

Public-key or asymmetric-key encryption algorithms use a pair of keys, a public key associated with the creator/sender for encrypting messages and a private key that only the originator knows (unless it is exposed or they decide to share it) for decrypting that information. The types of public-key cryptography include RSA used widely on the internet; Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin; Digital Signature Algorithm (DSA) adopted as a Federal Information Processing Standard for digital signatures by NIST in FIPS 186-4; and Diffie-Hellman key exchange.

To maintain data integrity in cryptography, hash functions, which return a deterministic output from an input value, are used to map data to a fixed data size. Types of cryptographic hash functions include SHA-1 (Secure Hash Algorithm 1), SHA-2 and SHA-3.

SOME BASIC TERMINOLOGY

- **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 ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

CONVENTIONAL ENCRYPTION PRINCIPLES

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm

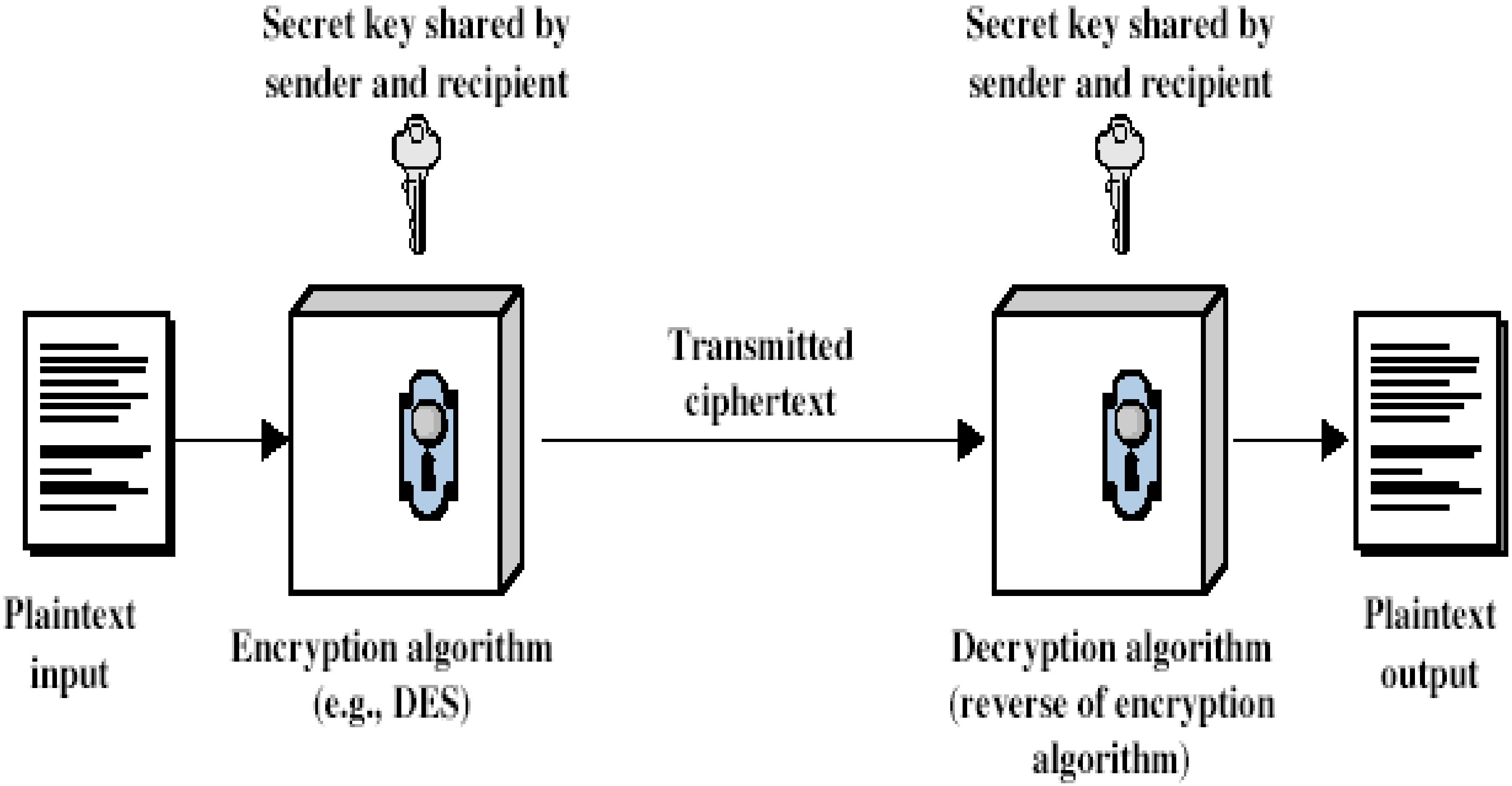
CHARACTERISTICS OF CRYPTOGRAPHIC TECHNIQUES

- Classified along three independent dimensions:
  - The type of operations used for transforming plaintext to ciphertext
  - The number of keys used
    - symmetric (single key)
    - asymmetric (two-keys, or public-key encryption)
  - The way in which the plaintext is processed

SYMMETRIC ENCRYPTION

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970’s
- and by far most widely used

SYMMETRIC CIPHER 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

REQUIREMENTS

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = E_K(X)$ [= E(K, X)] Here Y- Cipher Text, X-Plain Text

  $X = D_K(Y)$ [= D(K, Y)]

  E- Encryption Function

  D-Decryption Function

BRUTE FORCE SEARCH

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognize plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/µs	Time required at 10^6 decryptions/µs
32	$2^{32} = 4.3 \times 10^{9}$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^{6} years

CLASSICAL SUBSTITUTION CIPHERS

- where letters of plaintext are replaced by other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

CAESAR CIPHER

- earliest known substitution cipher
- Developed by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter after
- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

CAESAR CIPHER

- can define transformation as:

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
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

- mathematically give each letter a number

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

- then have Caesar cipher Algorithm as:

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

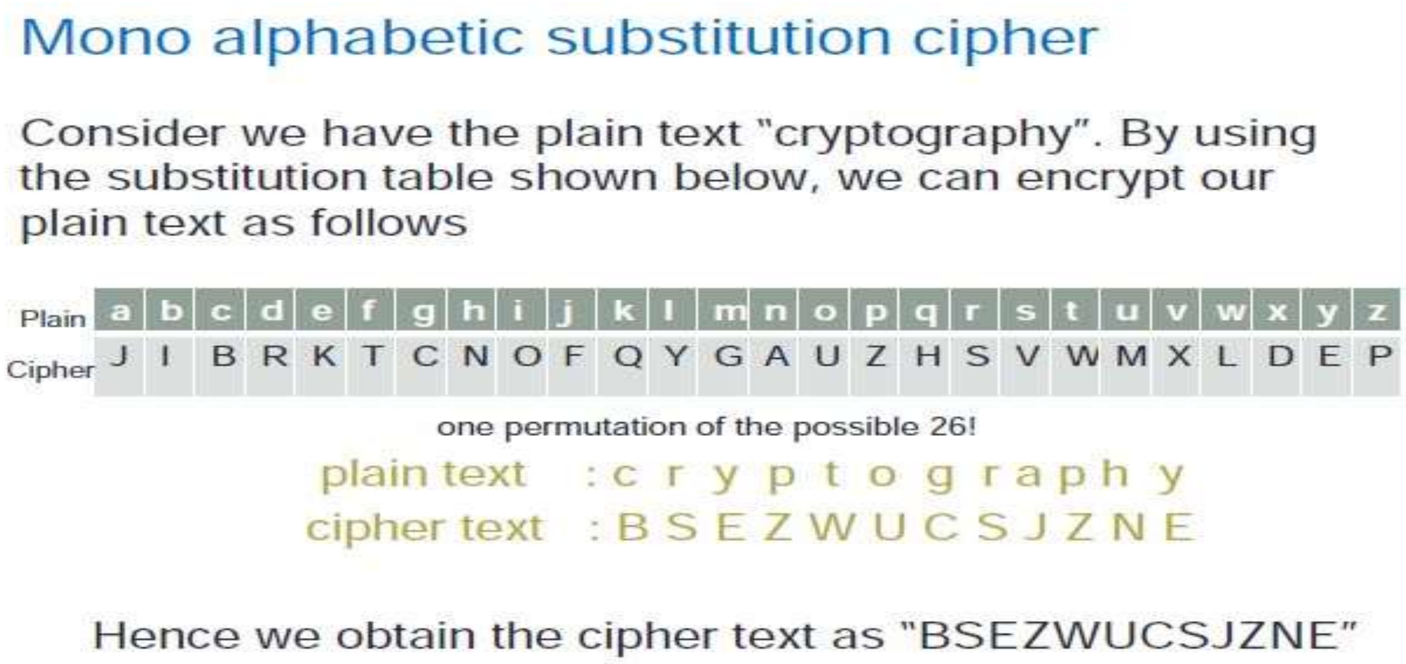
$$p = \mathrm{D}(\mathrm{c}) = (\mathrm{c} - k) \bmod (26)$$

MONOALPHABETIC CIPHER

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```



Mono alphabetic substitution cipher

Consider we have the plain text "cryptography". By using the substitution table shown below, we can encrypt our plain text 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	J	I	B	R	K	T	C	N	O	F	Q	Y	G	A	U	Z	H	S	V	W	M	X	L	D	E	P

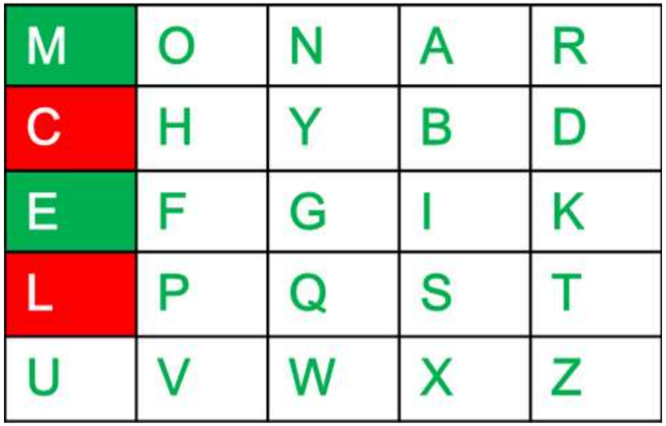
one permutation of the possible 26!

plain text : c r y p t o g r a p h y
cipher text : B S E Z W U C S J Z N E

Hence we obtain the cipher text as "BSEZWUCSJZNE"

PLAYFAIR CIPHER

- not even the large number of keys in a monoalphabetic cipher provides security
- one approach to improving security was to encrypt multiple letters
- the **Playfair Cipher** is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair



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

PLAYFAIR KEY MATRIX

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (minus duplicates)
- fill rest of matrix with other letters
- eg. using the keyword MONARCHY

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

ENCRYPTING AND DECRYPTING

- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X’ (low probability of appearance in language)
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Wireless   Wi re le sx sz   XG MK UL XA XT

POLYALPHABETIC CIPHERS

- **polyalphabetic substitution ciphers**
- A set of related monoalphabetic substitution rules is used
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution

Key:	deceptive	3 4 2 4 15 19 8 21 4
plaintext:	wireless	22 8 17 4 11 4 18 18
ciphertext:	zmtiaxao	25 12 19 8 26 23 26 39

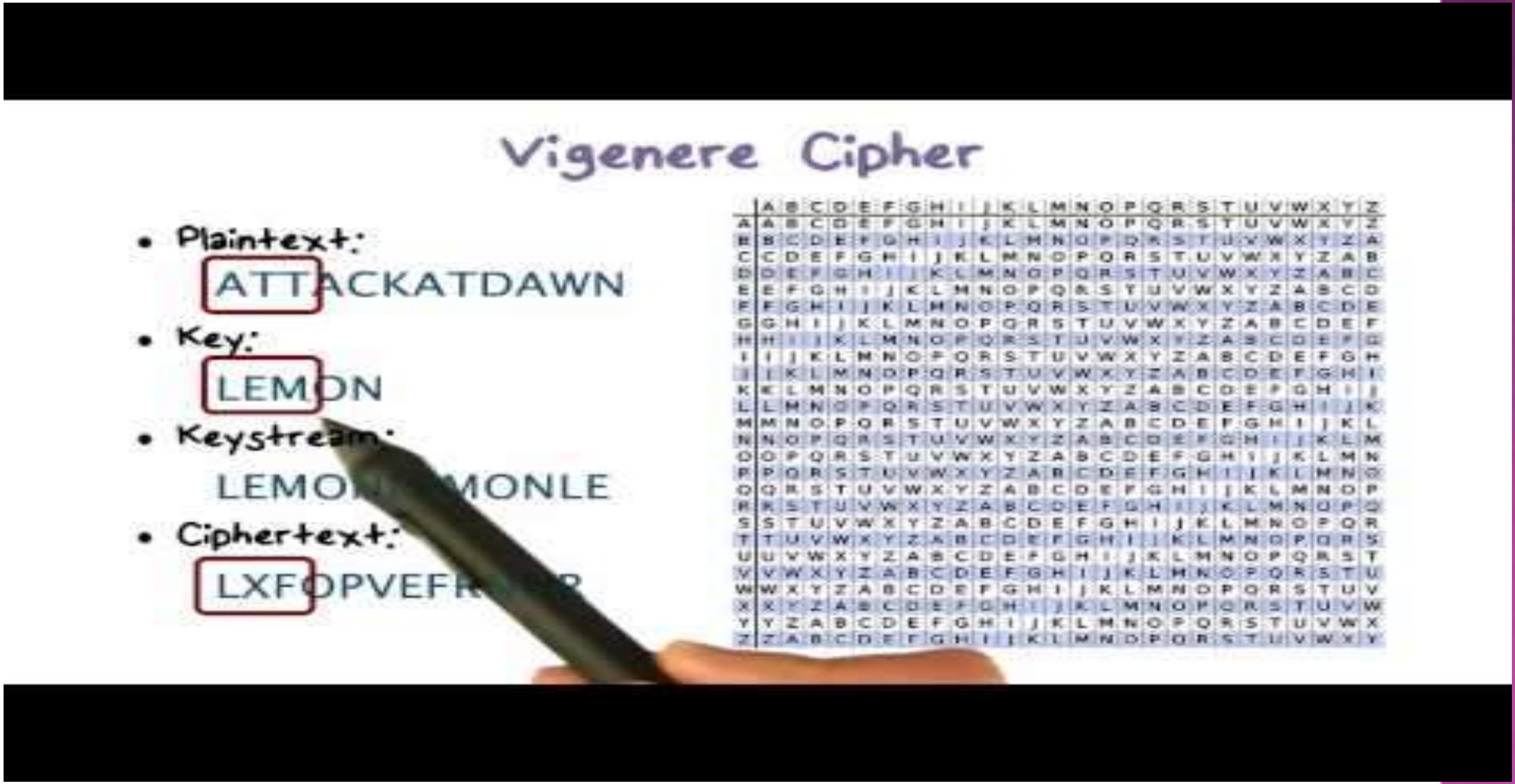
VIGENÈRE CIPHER

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1\ k_2\ \ldots\ k_d$
- 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

EXAMPLE OF VIGENÈRE CIPHER

- write the plaintext out
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

```
key:       deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```



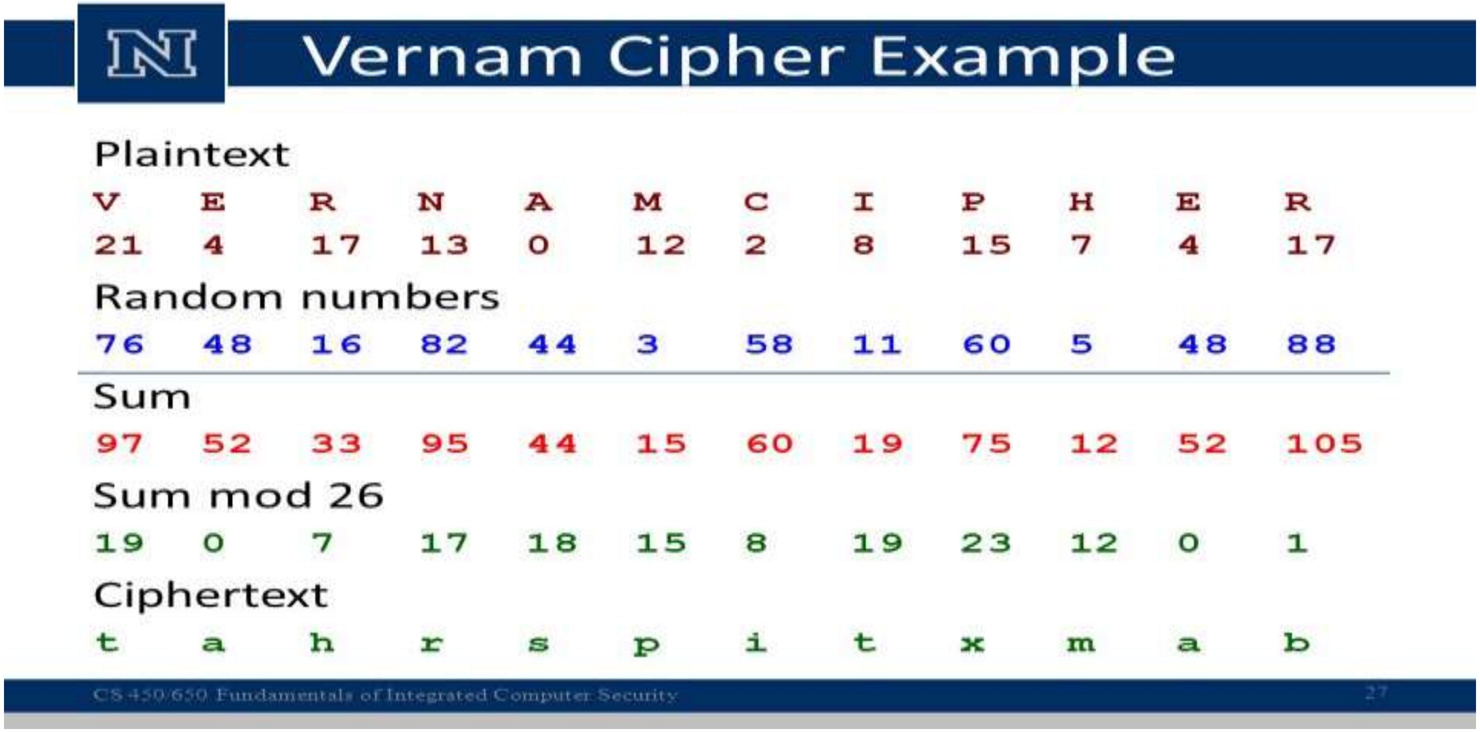
Vigenere Cipher

- Plaintext:
  ATTACKATDAWN
- Key:
  LEMON
- Keystream:
  LEMO MONLE
- Ciphertext:
  LXFOPVEFR R

	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

VERNAM CIPHER AND ONE-TIME PAD

- Keyword is as long as the plaintext and has no statistical relationship to it.
- Vernam system works on binary data with ith bit of text exclusive ored with ith bit of key to produce ith bit of cipher
- In one one-time pad key is used only once
- This scheme is unbreakable



Vernam Cipher Example

Plaintext											
V	E	R	N	A	M	C	I	P	H	E	R
21	4	17	13	0	12	2	8	15	7	4	17
Random numbers											
76	48	16	82	44	3	58	11	60	5	48	88
Sum											
97	52	33	95	44	15	60	19	75	12	52	105
Sum mod 26											
19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext											
t	a	h	r	s	p	i	t	x	m	a	b

CS 450/650 Fundamentals of Integrated Computer Security 27

TRANSPOSITION CIPHER

- Mapping is performed by some sort of permutation on the plaintext letters.
- Example: Rail fence of depth 2

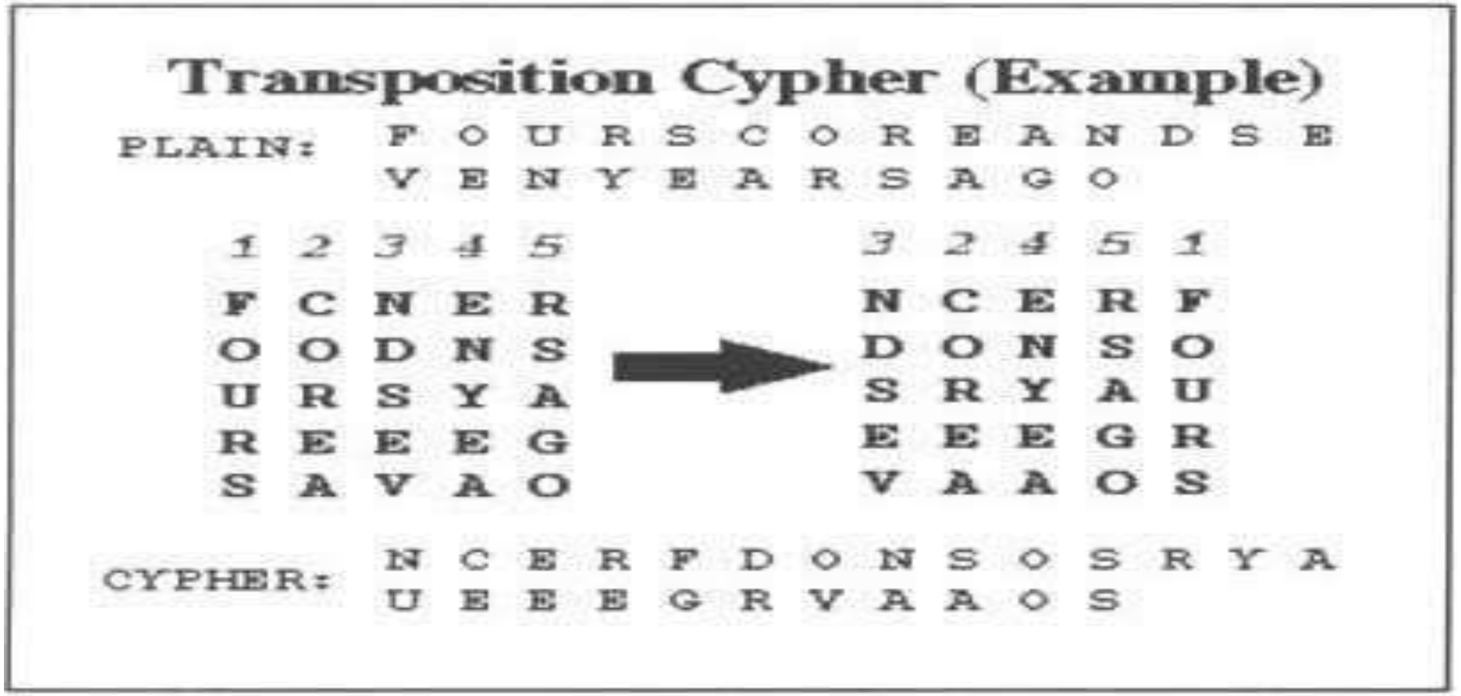
  text : meet me after the toga party

  m e m a t r h t g p r y

  e t e f e t e o a a t

  cipher: MEMATRHTGPRYETEFETEOAAT

Rail fence of depth 2



Transposition Cypher (Example)

PLAIN: F O U R S C O R E A N D S E
V E N Y E A R S A G O

1	2	3	4	5
F	C	N	E	R
O	O	D	N	S
U	R	S	Y	A
R	E	E	E	G
S	A	V	A	O

3	2	4	5	1
N	C	E	R	F
D	O	N	S	O
S	R	Y	A	U
E	E	E	G	R
V	A	A	O	S

CYPHER: N C E R F D O N S O S R Y A
U E E E G R V A A O S

Figure 21. Example of a basic transposi

Thank You