



PESU Center for
Information Security,
Forensics and
Cyber Resilience



Welcome to
PES University
Ring Road Campus, Bengaluru



PESU Center for
Information Security,
Forensics and
Cyber Resilience



APPLIED CRYPTOGRAPHY

Lecture 4

Classical cryptography

Most of them not in use nowadays

Olden days cryptography

- Used historically
- Practically computed and solved by hand
- Most of it was “the art of writing or solving codes”
 - Letter coding
 - Number coding
 - Mixed coding

Letter coding

- If TAP is coded as SZO then how is freeze coded

Number Coding

- If P A I N T is coded as 74128 and E X C E L is coded as 93596, then how would you encode A C C E P T?

Example

- If 'tee see pee' means 'drink fruit juice' 'see kee mee' means 'juice is sweet' and 'fee ree mee' means 'he is intelligent' which word means 'sweet'?

cryptosystem

- A practical cryptosystem should satisfy

Each encryption function e_k and each decryption function d_k should be efficiently computable.

An opponent, upon seeing the ciphertext string y , should be unable to determine the key k that was used, or the plaintext string x

Classical cipher

- The classical algorithms are those invented pre-computer up until around the 1950's.
- Mainly
 - Substitution ciphers
 - Transposition cipher
 - Combined

Substitution cipher

- Encrypt the plaintext by swapping each letter or symbol in the plaintext by a different symbol as directed by the key.
- Monoalphabetic cipher
- Polyalphabetic cipher
- polygraphic cipher

Substitution example

- If cook is called butler, butler is called manager, manager is called teacher, teacher is called clerk and finally clerk is called principal, who will teach in class

Monoalphabetic substitution cipher

- Simple substitution cipher
- Fixed substitution over the entire message
- Example:
 - Caesar cipher

Caesar cipher

- Simple monoalphabetic substitution cipher
- Substitute one letter for another

Index	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	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
Ciphertext	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

- A in plaintext is replaced with D in ciphertext, B in plaintext is replaced with E in ciphertext

Caesar cipher example

- Plaintext “begin the attack now”
- Key: Shift index by 3
- Cipher: Caesar cipher

solution

B	E	G	I	N	T	H	E	A	T	T	A	C	K	N	O	W
E	H	J	L	Q	W	K	H	D	W	W	D	F	N	Q	R	Z

- Ciphertext: EHJLQWKHDWWDFNQZRZ

Polyalphabetic substitution cipher

- Cipher alphabet for the plain alphabet may be different at different places during the encryption process.
 - Examples:
 - Playfair cipher
 - Vigenere cipher

Playfair cipher

- Encrypting and Decrypting:
- Plaintext encrypted two letters at a time:
 - STEP1: if a pair is a repeated letter, insert a filler like 'X', eg. "balloon" encrypts as "ba lx lo on"
 - STEP2: If both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
 - STEP3: if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
 - STEP4: otherwise each letter is replaced by the one in its row in the column of the other letter of the pair

Playfair example

- Plain text = classical ciphers are easily breakable.
- Key = ENCRYPT
- Cipher system = playfair

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

Playfair cipher steps:

- Two letters at a time

- Plaintext: “tell him about me”

TE	LL	HI	MA	BO	UT	ME
----	----	----	----	----	----	----

- Step1: if a pair is a repeated letter, insert a filler

TE	LX	LH	IM	AB	OU	TM	EX
----	----	----	----	----	----	----	----

- Step2-step4

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

TE	LX	LH	IM	AB	OU	TM	EX
PN	QU	OF	GQ	BD	LW	GV	RU

Ciphertext: PNQUOFGQBDLWGV RU

Vigenere Cipher

- Idea: Uses Caesar's cipher with various shifts, in order to hide the distribution of the letters.
- A key defines the shift used in each letter in the text
- A key word is repeated as many times as required to become the same length

Vigenere Cipher examples

Example 1:

Plain text: I attack

Key: 2 3 4

Ciphertext: KDXVDGM

I	A	T	T	A	C	K
2	3	4	2	3	4	2
K	D	X	V	D	G	M

Example 2:

Plain text : I attack

Key: exam

Ciphertext: NYRGFAL

I	A	T	T	A	C	K
E	X	A	M	E	X	A
N	Y	R	G	F	A	L

Polygraphic substitution cipher

- Works on multiple letters at the same time
 - Hill cipher

Hill cipher

- Depends on the concept $m \cdot m^{-1} = I$

- I is the identity

- If $M =$

3	0	2
2	0	-2
0	1	1

- Then $M^{-1} =$

0.2	0.2	0
-0.2	0.3	1
0.2	-0.3	0

To encrypt plaintext using matrix M

- Plaintext='abc'
- Key = matrix M
- Cipher = Hill cipher considering a=1, b=2, c=3
- Encryption achieved by multiplying matrix M by values of plaintext grouped 3 letters at a time

$$\text{Ciphertext } C = \begin{bmatrix} 3 & 0 & 2 \\ 2 & 0 & -2 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 4 \\ -4 \\ 3 \end{bmatrix}$$

Decryption hill cipher

- Decryption achieved by multiplying ciphertext with inverse of the matrix

$$\text{Plaintext} = M^{-1} \cdot C = \begin{bmatrix} 0.2 & 0.2 & 0 \\ -0.2 & 0.3 & 1 \\ 0.2 & -0.3 & 0 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ -4 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$$

Next Class

👉 Mandatory reading for the next class

<https://ieeexplore.ieee.org/document/8686758>

S Rajashree

Computer Science and Engineering

PES University, Bengaluru



PESU Center for
Information Security,
Forensics and
Cyber Resilience



PESU Center for
**Internet
of Things**