

PESU Center for Information Security, Forensics and Cyber Resilience



#### Welcome to

# **PES University**

Ring Road Campus, Bengaluru

10 June 2020



PESU Center for Information Security, Forensics and Cyber Resilience



## **APPLIED CRYPTOGRAPHY**

Lecture 4



# Classical cryptography

Most of them not in use nowadays





- 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?





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





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





 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





- Simple monoalphabetic substitution cipher
- Substitute one letter for another



 A in plaintext is replace 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



В	Ε	G	I	N	Т	Н	Ε	Α	Т	T	Α	С	K	N	0	W
Ε	Н	J	L	Q	W	K	Н	D	W	W	D	F	N	Q	R	Z

• Ciphertext: EHJLQWKHDWWDFNQRZ



### 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





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

E	N	С	R	Y
P	T	Α	В	D
F	G	Н	I/J	K
L	M	0	Q	S
U	V	W	X	Z





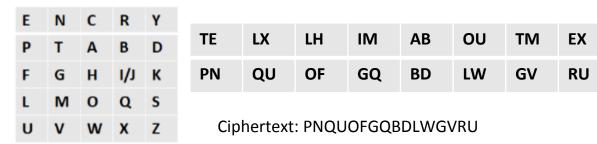
- Two letters at a time
  - Plaintext: "tell him about me"



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



Step2-step4



### **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





Example1:

Plain text: I attack

Key: 2 3 4

Ciphertext: KDXVDGM

Example 2:

Plain text: I attack

Key: exam

Ciphertext: NYRGFAL

L	Α	T	T	Α	С	K
2	3	4	2	3	4	2
K	D	X	V	D	G	M

L	Α	Т	Т	Α	С	K
E	X	Α	M	E	X	Α
N	Υ	R	G	F	Α	L

## Polygraphic substitution cipher



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





- Depends on the concept  $m.m^{-1}=1$
- I is the identity

• If 
$$M = \begin{bmatrix} 3 & 0 & 2 \\ 2 & 0 & -2 \\ 0 & 1 & 1 \end{bmatrix}$$

• 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 my multiplying matrix M by values of plaintext grouped 3 letters at a time

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





Decryption achieved by multiplying ciphertext with inverse of the matrix

Plaintext= 
$$M^{-1}$$
.  $C = \begin{bmatrix} 0.2 & 0.2 & 0 \\ -0.2 & 0.3 & 1 \\ 0.2 & -0.3 & 0 \end{bmatrix}$ 



### **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