PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

Lecture 5

Classical cryptography

Most of them not in use nowadays

Classical transposition cipher

- Is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.
- Transposition cipher, simple data encryption scheme in which plaintext characters are shuffled in some regular pattern to form cipher text.
  - Rail Fence cipher
  - Columnar transposition
  - Double transposition

Rail fence cipher

- The **rail fence cipher** (sometimes called zigzag cipher) is a **transposition cipher** that jumbles up the order of the letters of a message using a basic algorithm.
- The rail fence cipher works by writing your message on **alternate lines** across the page, and then reading off each line in turn.

Rail fence example

- Plaintext: “this is a secret message”
- Key =2
- Cipher system: rail fence
- Ciphertext:

T		I		I		A		E		R		T		E		S		G	
	H		S		S		S		C		E		M		S		A		E

- TIIAERTESGHSSSCEMSAE

Columnar transposition cipher

- In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
- Both the width of the rows and the permutation of the columns are usually defined by a keyword.
- For example, the keyword ZEBRAS is of length 6, and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".
- In a regular columnar transposition cipher, any spare spaces are filled with nulls;

Encryption:

- For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE.

6	3	2	4	1	5
Z	E	B	R	A	S
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	X-Q	X-K	X-J	X-E	X-U

- providing five nulls (QKJEU), these letters can be randomly selected as they just fill out the incomplete columns and are not part of the message.
- The cipher text is then read off as:
- EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

Columnar transposition decryption

- To decipher it, the recipient must work out the column lengths by dividing the message length by the key length.
- Then, write the message out in columns again, then re-order the columns by reforming the key word.

Double transposition Cipher

- **Double Transposition** consists of two applications of columnar transposition to a message. The two applications may use the same key for each of the two steps, or they may use different keys.

Example

- Plaintext “We are discovered flee at once”
- Key1: zebras
- Key2: help
- Ciphertext after key1:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

- Ciphertext after key2:

EVAKAFEWEEETEODUELCEQOEIKNDSRJCRG

2	1	3	4
H	E	L	P
E	V	L	N
E	A	C	D
T	K	E	S
E	A	Q	R
O	F	O	J
D	E	E	C
U	W	I	R
E	E	X-K	X-G

Steganography

Uses of Steganography

- **Governments**
- **Businesses:** *Digital Watermarking*
- **Individuals**

Steganography & Cryptography

- Steganography and Cryptography are closely related
- The difference is in their goals...
  - Cryptography: although encypted and unreadable, the existence of data is not hidden
  - Steganography: no knowledge of the existence of the data
- Steganography and Cryptography can be used together to produce better protection

Digital Watermarking

Image “painted” with the watermark: “Invisible Man” © 1997, Neil F. Johnson

Digital Watermarking

- Used primarily for identification
- Embedding a unique piece of information within a medium (typically an image) without noticeably altering the medium
- Almost impossible to remove without seriously degrading an image

Types of Digital Steganography

- **Hiding a Message inside Text**
- **Hiding a Message inside Images**
  - Most popular technique
- **Hiding a Message inside Audio and Video Files**

Hiding a Message inside Text

- **Partially effective**

randoM capitalosis is a rarE disEase ofTen contrAcTed by careless inTernet users. tHis sad illnEss causes the aFfected peRsON To randomly capitalize letters in a bOdy oF texT. please do not confuse this disease witH a blatant attEmpt aT steganogRAPhy.

Reveals: MEET AT THE FRONT OF THE TRAP

Hiding a Message inside Text

- First-letter algorithm
- Every n-th character
- Altering the amount of whitespace
- Using a publicly available cover source

Hiding a Message inside Images

- The most popular medium!

- ***Least-significant bit (LSB) modifications***
  - *24-bit vs. 8-bit images*
  - *Tools to implement LSB: EzStego and S-Tools*
- ***Masking and Filtering***
- ***Algorithms and Transformations***

Hiding an Image within an Image

- Removing all but the two least significant bits of each color component produces an almost completely black image. Making that image 85 times brighter produces the image below

- source: wikipedia.org

Next Class

- ☞ Mandatory reading for the next class
- ☞ https://users.encs.concordia.ca/~youssef/Publications/Papers/Cryptanalysis%20of%20Simple%20Substitution%20Ciphers%20Using%20Particle%20Swarm.pdf

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT

PESU Center for Internet of Things