Topic 2.1 - Introduction to Cryptography

Eric Casanovas

Universitat d'Andorra

9th February, 2022

1. Cryptography and Cryptanalysis
2. Basic Encryption Model
3. Substitution Algorithms
4. Transposition Algorithms
5. One Time Pads (OTPs)

1. Cryptography and Cryptanalysis
2. Basic Encryption Model
3. Substitution Algorithms
4. Transposition Algorithms
5. One Time Pads (OTPs)

Cryptography

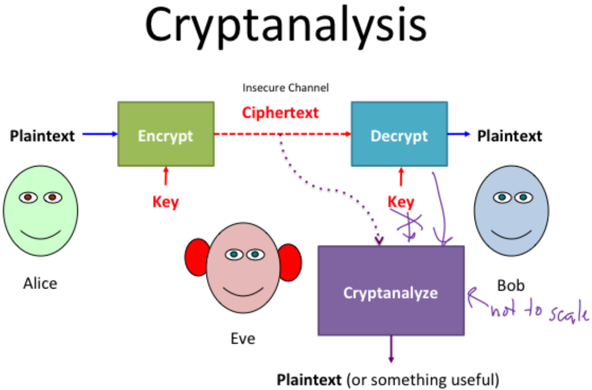
- Cryptography is the science of using mathematics to encrypt and decrypt data
- Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient
- Thanks to cryptography we can send messages over the internet without anyone knowing the content of the messages
- The security in cryptography must reside in the **KEYS** not in the algorithm
- The algorithm can be public, the keys private
- "Do not rely on security through obscurity"

Cryptography vocabulary

- Plaintext: Data that can be read and understood without any special measures.
- Encryption: The method of disguising plaintext in such a way as to hide its substance.
- Cipher text: Result of the encryption of the Plaintext.
- Decryption: The process of reverting cipher text to its original plaintext.
- Key: some secret piece of information

Cryptanalysis

- Cryptanalysis is the "art" of breaking ciphers



Types cryptographic algorithms

- Symmetric key cryptography: It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages
- Asymmetric key cryptography: It is an encryption method where the sender and receiver of a message use 2 pair of keys, one public and one private to encrypt and decrypt messages

Encryption methodologies

- Symmetric key cryptography: It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages
- Asymmetric key cryptography: It is an encryption method where the sender and receiver of a message use 2 pair of keys, one public and one private to encrypt and decrypt messages

1. Cryptography and Cryptanalysis
2. Basic Encryption Model
3. Substitution Algorithms
4. Transposition Algorithms
5. One Time Pads (OTPs)

Basic encryption Model

- Confidentiality encodes the message's content
- Authentication verifies the origin of a message
- Integrity proves the contents of a message have not been changed since it was sent
- Nonrepudiation prevents senders from denying they sent the encrypted message

1. Cryptography and Cryptanalysis
2. Basic Encryption Model
3. Substitution Algorithms
4. Transposition Algorithms
5. One Time Pads (OTPs)

Substitution I

- Substitutions are quite simple, they substitute one thing for another to encrypt plaintext into ciphertext.
- The key is the arrangement of the characters (if we're dealing with an alphabet substitution) that tells us what is exchanged for what.

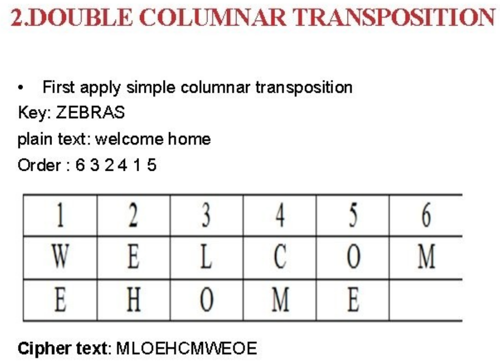
Substitution II

- Consider the alphabet and a rotation cipher of 2 positions
  abcdefghijklmnopqrstuvwxyz -> cdefghijklmnopqrstuvwxyzab
- To encrypt, replace all letters in your plain text with the corresponding letter below it, as given in the box above
  eric wrote this -> gtke ytqvg vjku
- To decrypt, simply replace these letters with the corresponding ones above

1. Cryptography and Cryptanalysis
2. Basic Encryption Model
3. Substitution Algorithms
4. **Transposition Algorithms**
5. One Time Pads (OTPs)

Transposition

- Transposition cipher is the name given to any encryption that involves rearranging the plain text letters in a new order



2.DOUBLE COLUMNAR TRANSPOSITION

- First apply simple columnar transposition

Key: ZEBRAS

plain text: welcome home

Order : 6 3 2 4 1 5

1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Cipher text: MLOEHCMWEOE

1. Cryptography and Cryptanalysis

2. Basic Encryption Model

3. Substitution Algorithms

4. Transposition Algorithms

5. One Time Pads (OTPs)

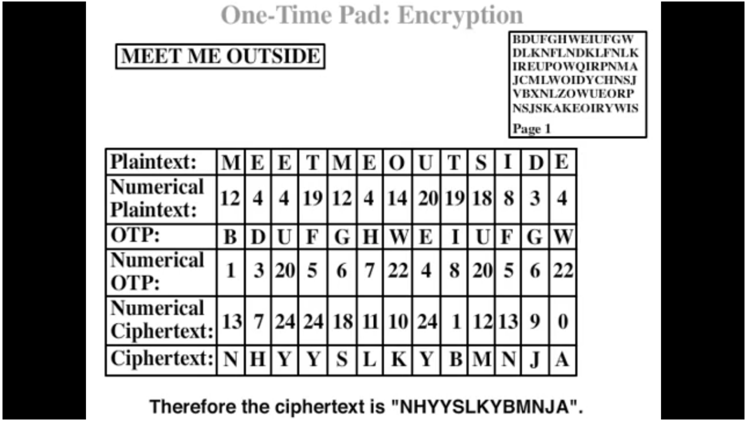
OTPs

- One-time-pad is a system that generates a unique, randomly organized key
- The one-time-use key is used to encrypt a message which is later decrypted by the recipient with the use of a one-time key
- Information encrypted with keys is unbreakable
- Each encryption is unique and shows no relation to another encryption
- The key used is known as the secret key, as they contain crucial information

Properties to be unbreakable

- The key is as long as the given message.
- The key is truly random and specially auto-generated.
- Each key should be used once and destroyed by both sender and receiver.
- There should be two copies of key: one with the sender and other with the receiver.

Example OTP



One-Time Pad: Encryption

MEET ME OUTSIDE

BDUFGHWEIUFGW
DLKNFLNDKLFNLK
IREUPOWQIRPNMA
JCMLWOIDYCHNSJ
VBXNLZOWUEORP
NSJSKAKEOIRYWIS

Page 1

Plaintext:	M	E	E	T	M	E	O	U	T	S	I	D	E
Numerical Plaintext:	12	4	4	19	12	4	14	20	19	18	8	3	4
OTP:	B	D	U	F	G	H	W	E	I	U	F	G	W
Numerical OTP:	1	3	20	5	6	7	22	4	8	20	5	6	22
Numerical Ciphertext:	13	7	24	24	18	11	10	24	1	12	13	9	0
Ciphertext:	N	H	Y	Y	S	L	K	Y	B	M	N	J	A

Therefore the ciphertext is "NHYYSLKYBMNJA".

The END!