Cryptography

Haris Mouratidis

Learning outcomes

- On completion of this session you should be able to
  - Understand the basic concepts of cryptography;
  - Understand the different types of encryption;
  - Understand the characteristics of good encryption algorithms;
  - Become familiar with industrial used cryptographic solutions.

Lecture Layout

Stockholm University

- Cryptography
  - Definition
  - History
- Cryptosystems
  - Types
  - Commercial systems
- Cryptography for other security properties
  - Hash Functions
  - Digital Certificates

Cryptography

- Cryptography (from Ancient Greek: κρυπτός, *kryptós* "hidden"; and γραφή *graphei*, "to write").
- Encryption is the process of encoding a message so that its meaning is not obvious.

Cryptography history

Stockholm University

- Cryptography has been around for centuries
  - Substitution of information with symbols, numbers, pictures
  - Shift of letters/words
  - Rearrangement of letters
- Why?
  - Assyrians were interested in protecting the secret of making pottery
  - Chinese wanted to protect the process of making milk
  - Germans used cryptography to protect their military secrets
- Today, many governments / organisations / individuals use encryption techniques to protect their information

Cryptography definitions

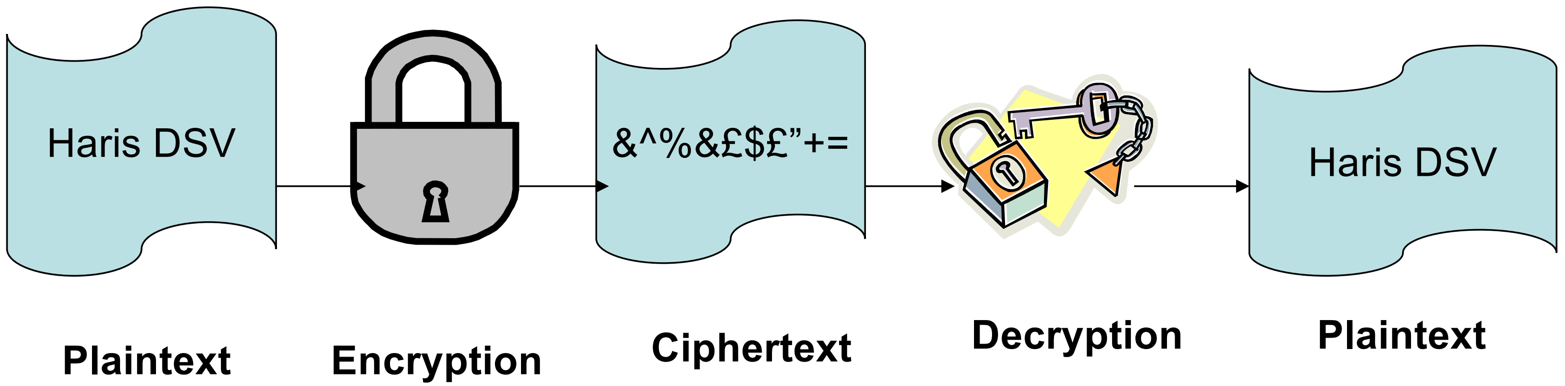
- Encryption
  - The method of disguising plaintext to hide its substance
- Plaintext
  - Data that can be read without any manipulation
- Ciphertext
  - A scrambled (unreadable) message produced as a result of encryption
- Decryption
  - The method of producing the original plaintext
- Cryptosystem
  - A system for encryption and decryption is called a cryptosystem

Cryptosystems

Stockholm University

- Used in modern cryptography to encrypt and decrypt data
- Algorithm: a mathematical function that works in tandem with a key
- The exact substitutions and transformations performed by the algorithm depend on the key
- Same plaintexts encrypted to different ciphertexts with different keys

Graphically



Types of Cryptosystems

- The type of operation used for transforming plaintext to ciphertext
    - **Substitution** in which each element in the plaintext is mapped into another element
    - **Transposition** in which elements in the plaintext are rearranged
- The number of keys used
    - Symmetric or conventional or single key or secret key
    - Asymmetric or public key
- The way in which the plaintext is processed
    - Block cipher processes the input one block of elements at a time producing an output block for each input block
    - Stream cipher processes the input elements continuously, producing output one element at a time as it goes along

Substitution Ciphers

- Cesar Cipher

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

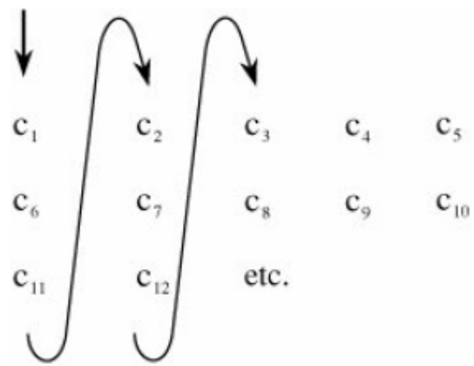
HELLO - khoor

- Simple – advantage
- Obvious pattern - disadvantage

Transpositions

- Encryption in which the letters are rearranged
  - It is also known as permutation
- Columnar transposition

c_1	c_2	c_3	c_4	c_5
c_6	c_7	c_8	c_9	c_{10}
c_{11}	c_{12}	etc.		



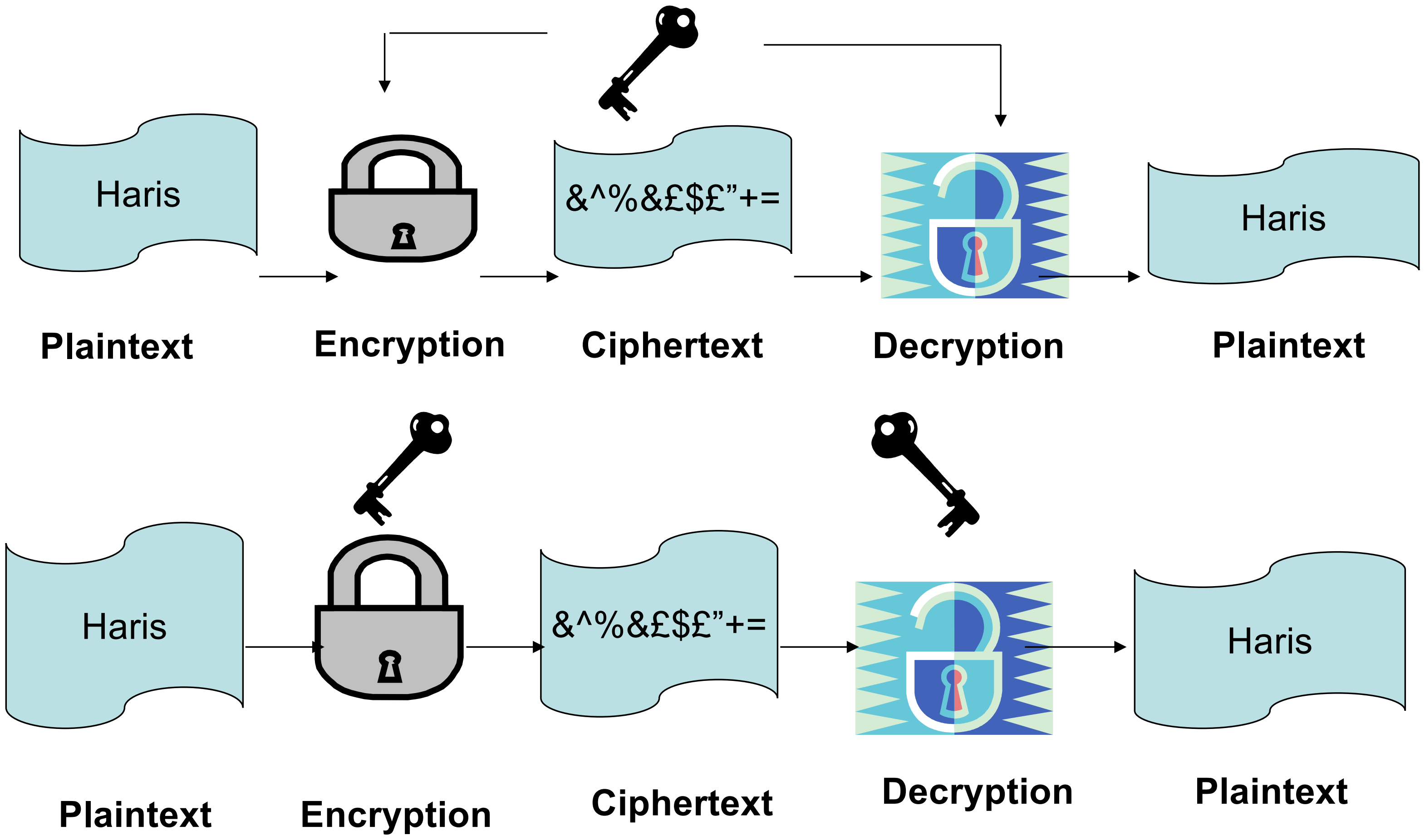
Permutation Example

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

THIS IS A MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS

tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns

Symmetric vs asymmetric



Stream vs block algorithms

- **Stream:** Convert one symbol of plaintext immediately into a symbol of ciphertext
  – Cesar
- **Block**: Encrypts a group of plaintext symbols as one block
  – Columnar transposition

Advantages/Disadvantages

- Stream

  +Speed of transformation

  +Low Error

  -Low diffusion

  -Susceptibility to malicious insertions and modifications

- Block

  +High diffusion

  +Immunity to insertion of symbols

  -Slowness of encryption

  -Error propagation

Cryptanalysis

- The process of attempting to discover the plaintext or key;
- In simple English “breaking of a code”!
- The strategies used by the cryptanalyst depends on the nature of the encryption and the information available.

Types of Attacks

Stockholm University

Type of Attack	Information known
Ciphertext only	▪Encryption algorithm ▪Ciphertext to be decoded ▪One or more plaintext-ciphertext pairs formed with the secret key
Known plaintext	▪Encryption Algorithm ▪Ciphertext to be decoded ▪Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	▪Encryption Algorithm ▪Ciphertext to be decoded ▪Purported cipher chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	▪Encryption Algorithm ▪Ciphertext to be decoded ▪Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key ▪Purported cipher chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Encryption scheme

- An encryption scheme is computational secure
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

- It is very difficult to estimate the amount of effort required to cryptanalyse ciphertext successfully

Important Parameters

- **Block size:** larger block sizes mean greater security
- **Key Size:** larger key size means greater security
- **Number of rounds:** multiple rounds offer increasing security
- **Subkey generation algorithm:** greater complexity will lead to greater difficulty of cryptanalysis.
- **Fast software encryption/decryption:** the speed of execution of the algorithm becomes a concern

Good Encryption Algorithms

- Different requirements
- Shannon's characteristics
  - The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption;
  - The set of keys and the enciphering algorithm should be free from complexity;
- The implementation of the process should be as simple as possible;
- Errors in ciphering should not propagate and cause corruption of further information in the message;
- The size of the enciphered text should be no longer than the text of the original message

Properties of Trustworthy Encryption Systems

Stockholm University

- It is based on sound mathematics;
- It has been analysed by competent experts and found to be sound;
- It has stood the “test of the time”.

Data Encryption Standard (DES)

Stockholm University

– The algorithm is reffered to the Data Encryption Algorithm (DEA)

– Substitution and transposition

– DES is a block cipher

– The plaintext is 64 bits in length
  - Any larger plaintexts are processed in 64-bit blocks

– The key is 56-bits in length

– Decryption similar to encryption
  - Use the ciphertext as an input to the DES but use the subkeys in reverse order

Triple DES

- Uses three keys and three executions of the Des algorithm
- The function follows an encrypt-decrypt-encrypt (EDE) sequence

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

- C = ciphertext
- P = Plaintext
- EK[X] = encryption of X using key K
- DK[Y] = decryption of Y using key K

3DES future

- Larger length key overcomes the vulnerability to brute-force attack
- No effective cryptanalytic attack has been found

But

- Relatively sluggish in software
- Uses a 64-bit block size
  - Efficiency and security requires larger block

Advanced Encryption Standard (AES)

Stockholm University

- Security Strength equal to or better than 3DES
- Improved efficiency
- Symmetric block cipher with a block length 128 and support for key lengths 128,192,256
- Rijndael as the proposed AES algorithm

AES stages

Stockholm University

- Key length variable (128,192,256)
- **Substitute bytes:** Uses a table, referred to as an S-box, to perform a byte-by-byte substitution of the block
- **Shift rows:** A simple permutation that is performed row by row
- **Mix columns:** A substitution that alerts each byte in a column as a function of all of the bytes in the column
- **Add round key:** a simple bitwise XOR of the current block with a portion of the expanded key

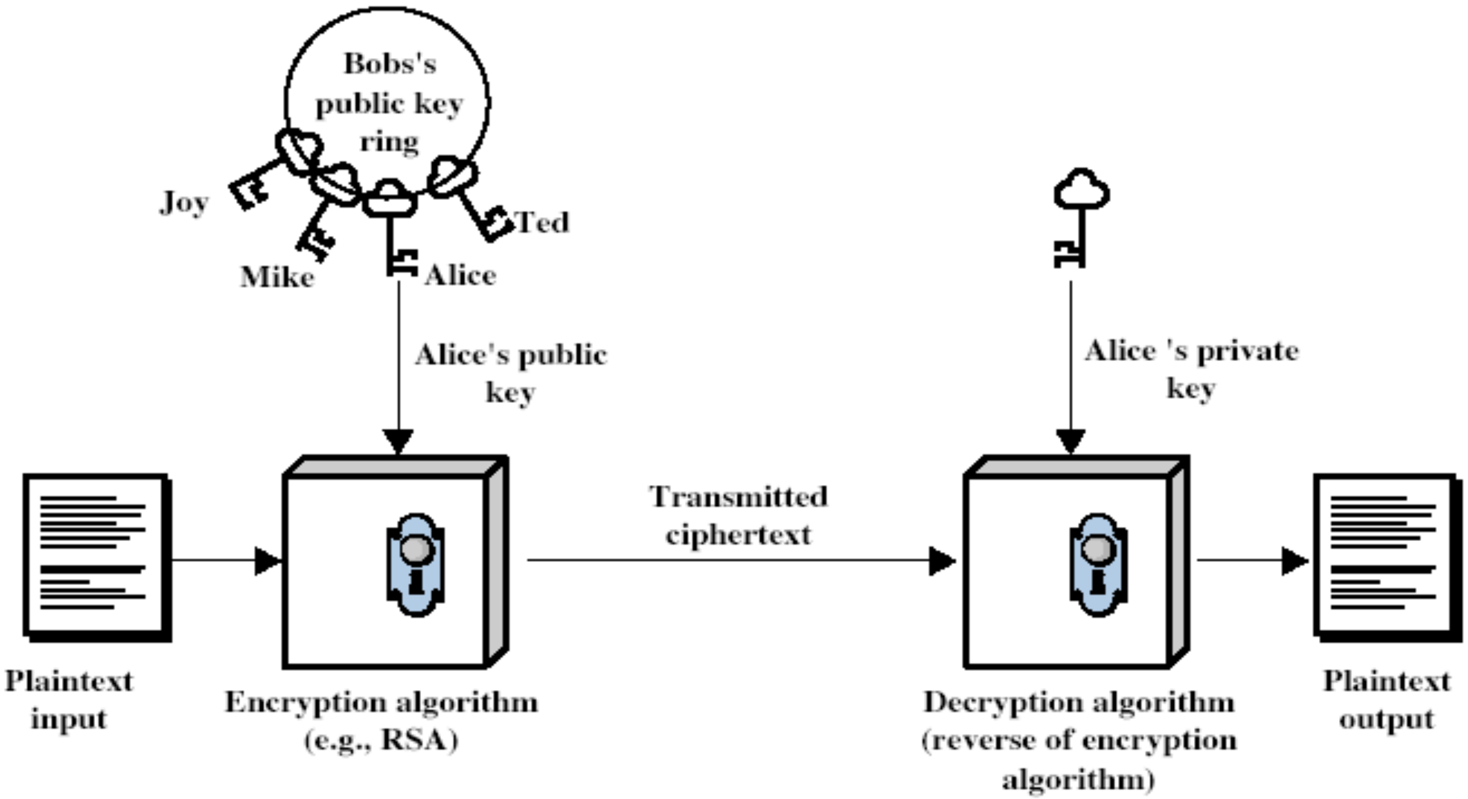
Evaluation

- How strong is it?
- How long would it be until the encrypted code could be routinely cracked?

Public Key cryptography

- First introduced by Diffie and Hellman (1976)
- Uses two keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**
  - a **private-key**, known only to the recipient, used to **decrypt messages**

How it works


Bobs's
public key
ring
Joy
Mike
Alice
Ted
Alice's public
key
Alice 's private
key
Transmitted
ciphertext
Plaintext
input
Encryption algorithm
(e.g., RSA)
Decryption algorithm
(reverse of encryption
algorithm)
Plaintext
output

Public-key Requirements

- Public-Key algorithms rely on two keys. The conditions that such algorithms must fulfil are:
  - It is computationally easy for party B to generate a pair (public key, private key);
  - It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext;
  - It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message;
  - It is computationally infeasible for an opponent, knowing the public key to determine the private key;
  - It is computationally infeasible for an opponent, knowing the public key and a ciphertext to recover the original message
  - (Useful) either of the two related keys can be used for encryption, with the other used for decryption.

Public key cryptography algorithms

- Two main algorithms
- RSA
  - Developed in 1977 by **R**ivest, **S**hamir, and **A**dleman
  - Most widely accepted and implemented approach to public-key encryption
- Diffie-Hellman
  - The first published public-key algorithm appeared in 1976
  - It is refereed to as the key exchange
  - It is used in a number of commercial products

RSA

- RSA is a block cipher, which is actually a set of two algorithms:
  - **Key Generation**: A key generation algorithm.
  - **RSA Function Evaluation**: A function *F* that takes as input a point *x* and a key *k* and produces either an encrypted result or plaintext, depending on the input and the key.

- Key Generation
  - The key generation algorithm is the most complex part of RSA.
  - The aim of the key generation algorithm is to generate both the *public* and the *private* RSA keys.
  - weak key generation makes RSA very vulnerable to attack. So it has to be done correctly.

RSA key generation

Stockholm University

Key Generation	
Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Discussion about RSA

Stockholm University

- Brute-force approach: try all possible keys
  - The larger the number of bits in e and d, the more secure the algorithm
  - On the other hand, the larger the size of the key, the slower the system will run
- The inventors of RSA offered $100 reward for anyone who could decode a cipher they printed in a scientific journal
  - The key was 428 bits and they predicted it could take more than 40 quadrillion years
  - In 1994 a group working over the internet using 1600 computers broke the cipher
  - It doesn’t prove that it is not safe, but rather that large key sizes should be used

Is encryption enough?

- Encryption protects against passive attacks
- We also need to be protected against active attacks
- Protection against active attacks is known as message authentication
- A message, file, or other collection of data is said to be authentic when it is genuine and came from its alleged source

Hash Function

- Create a shield around the file
  - Detect when it is broken
- Hash/checksum
- One way functions
- Message Digest (MD4, MD5)

Digital Signatures

- Protocol to mimic real signatures
- Two conditions
  - It must be unforgeable
  - It must be authentic
- Also
  - It is not alterable
  - It is not reusable

– Public Key encryption systems are ideal

Digital Certificates

- Used to address the authenticity challenge
- Different types
  - Server, Browser, Personal
- Certificates to Authenticate an Identity
  - A public key and user's identity are bound together in a certificate, which is then signed by certification authority, certifying the accuracy of the binding.

Conclusions

Stockholm University

- Cryptography
  - Symmetric
  - Public Key
- Message Authentication
- Hash Functions
- Public Key Certificates