Name: Joaquim Miguel Conceição Espada

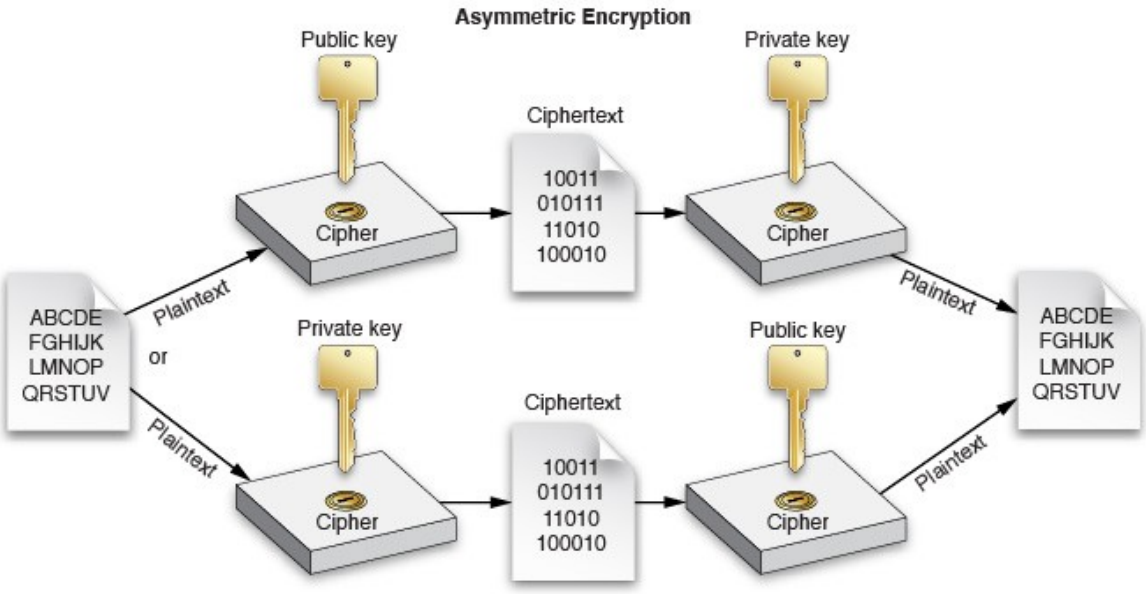
Login: con0004

Date: 22nd November of 2016

Report of measuring

Title: Data Encryption – Secure Communications

Task: Using symmetric and asymmetric methods, encrypt e decrypt data.



Introduction to problematics:

The main objective of this class is to learn about data encryption and it's different methods as well their strengths and weaknesses.
Data encryption is used to turn a legible message into a complete unreadable nonsense.
Data encryption started thousand years ago during the Caesar's Empire. The Caesar cypher was used because if a message was intercepted the enemies they could not read the real content of the message. Nowadays data encryption has the same role against unwanted eavesdroppers.

Elaboration:

Encryption

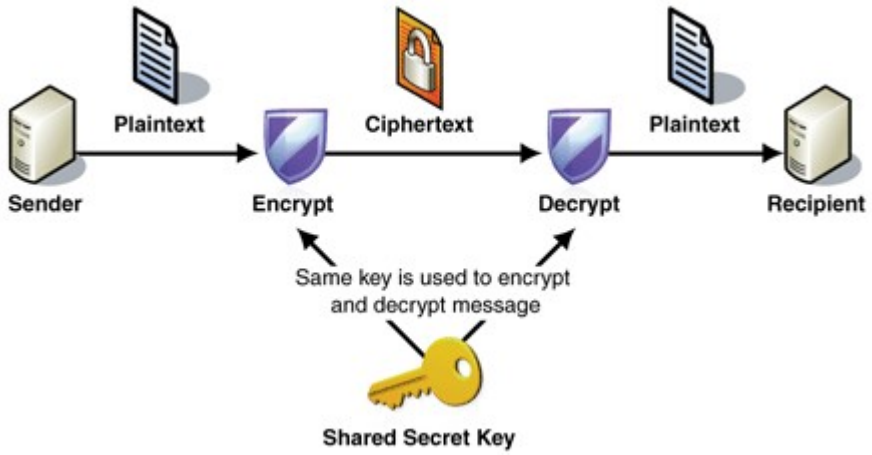
Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security.
To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
Unencrypted data is called plain text and encrypted data is referred to as cipher text.
There are two main types of encryption:

- symmetric encryption.
- asymmetric encryption

Symmetric Encryption

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plain text and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement

that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to asymmetric key encryption.



Transposition Cypher

A transposition cipher is a method of encryption by which the positions held by units of plain text (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cypher text constitutes a permutation of the plain text. That is, the order of the units is changed (the plain text is reordered).

Example

Plain text- HELLO WORLD!!

Rule : Write the message in rows and then get the cypher text by ordering by columns.

H	E	L	L
O	W	O	R
L	D	!	!

Cypher text - HOLEWDLO!LR!

Caesar's Cypher

The Caesar cipher, also known as a shift cipher, is one of the simplest forms of encryption. It is a substitution and symmetric cipher where each letter in the original message (called the plain text) is replaced with a letter corresponding to a certain number of letters up or down in the alphabet.

In this way, a message that initially was quite readable, ends up in a form that can not be understood at a simple glance.

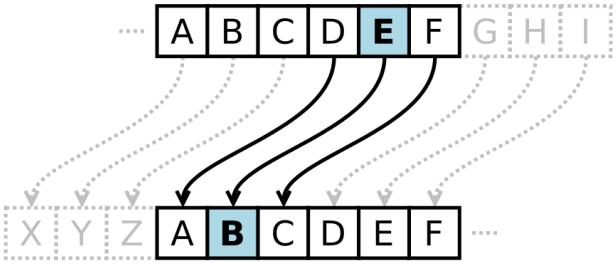
For example, here's the Caesar Cipher encryption of a message, using a right shift of 3.

Plain text:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Cypher text:

QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD



Vernam Cypher

Vernam cipher is a symmetrical, stream cypher and substitution chyper in which the plain text is combined with a random or pseudo random stream of data (the "key stream") of the same length.

Example:

Step 1 : Convert the letter to their numerical equivalents

V	E	N	A	M
21	4	13	0	12
76	48	16	82	44

Step 2: Assume random 2 digits values and add the numeric equivalent and corresponding random number

V	E	N	A	M
21	4	13	0	12
76	48	16	82	44
124	52	29	82	56

Random values

Random values + letter numerical equivelent

Step 3: Perform sum mod26

V	E	N	A	M
21	4	13	0	12
76	48	16	82	44
124	52	29	82	56
20	0	3	4	4
U	A	C	D	D

Random values

Random values + letter numerical equivelent

Cypher Text or Encripted message

Vigenère Cypher

The Vigenère cipher is symmetric and substitution cypher, a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.

Algorithm Implementation example :

Step 1:

Plain text to be encrypted is the following “ATTACKATDAWN”.

Step 2:

The person sending the message chooses a keyword and repeats it until it matches the length of the plain text, for example, the keyword "LEMON".
Key : “LEMONLEMONLE”

Step 3:

Now we must search in the Vigenère table in order to find the interception between the first letter of the plain text and first letter of the repeated keyword in order to obtain the cypher text.

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

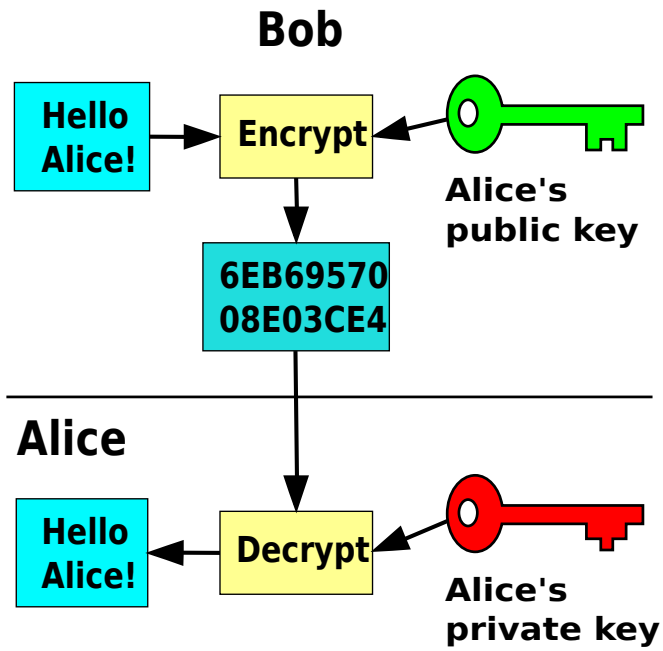
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Illustration 1: Vigenère table

Asymmetric Encryption

Asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

In a public key encryption system, any person can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key. The strength of a public key cryptography system relies on the degree of difficulty (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Security then depends only on keeping the private key private, and the public key may be published without compromising security.



Stenography

Stenography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

The advantage of stenography over cryptography alone is that the intended secret message does not attract attention to itself as an object of "interest".

Experiment Part

1. Hide a message in a image

```
student@eb215-desktop:~$ steghide embed -ef message -cf fox.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "message" in "fox.jpeg"... done
```

2. Getting the concealed message of an image

```
student@eb215-desktop:~$ steghide extract -sf fox.jpeg  -xf privateMessage
Enter passphrase:
wrote extracted data to "privateMessage".
```

3.Hide a message in a text file

```
student@eb215-desktop:~$   stegsnow -C -m "I am lying" -p "Secret" message secretMessage
```

4.Getting the concealed message of an text file

```
student@eb215-desktop:~$ stegsnow -C -p "Secret" secretMessage
```

5.Encryption using AES-256

```
student@eb215-desktop:~$ openssl enc -aes256 -in a.txt -out enc.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
student@eb215-desktop:~$
```

6.Decryption of AES-256 encrypted message

```
student@eb215-desktop:~$ openssl enc -d -aes256 -in enc.txt
enter aes-256-cbc decryption password:
My Hello World
```

7. Asymmetric Encryption

```
student@eb215-desktop:~$ openssl genrsa -out privateX.key 2048
student@eb215-desktop:~$ openssl rsa -in privateX.key -pubout > publicX.key

student@eb215-desktop:~$ openssl rsautl -encrypt -inkey publicX.key -pubin -in a.txt > cipher.txt
student@eb215-desktop:~$ openssl rsautl -decrypt -inkey privateX.key -in cipher.txt
My Hello World
```

8. Generate Certificates

```
student@eb215-desktop:~$ openssl req -new -x509 -days 365 -out cert.pem -keyout privateX.key
```

Conclusion:

After studying cryptographic methods and algorithms I concluded that they can be divided in two big sets the symmetric and asymmetric. The main difference between this is that the symmetric algorithms only use one encryption key and asymmetric algorithms use a pair of encryption keys, a public key that can be shared with everyone and a private key that must be kept safe.

I also concluded that the Caesar's cypher is the simplest, followed by the Vigenère and Vernam. Vigenère algorithm is superior to Caesar's because it uses a key and the Vigenère table that a table with multiple shifts like Caesar's cypher. Vernam is better than Vigenère because the key is a random value but with the size of the original message while in Vigenère the key word must be repeated until it gets with the message length.

References:

- Ing. Pavel Nevlud lectures
- https://en.wikipedia.org/wiki/Symmetric-key_algorithm
- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
- http://www.webopedia.com/TERM/E/encryption.html
- https://en.wikipedia.org/wiki/Cryptography
- https://learncryptography.com/classical-encryption/caesar-cipher