HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

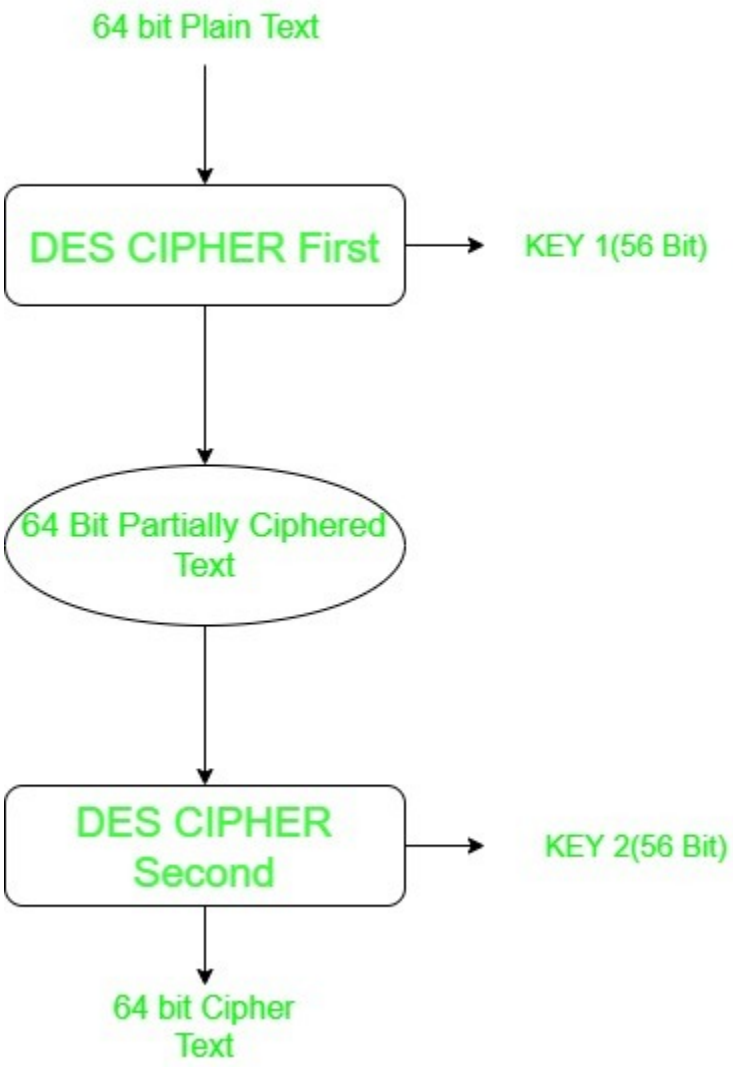
BBM 456 HOMEWORK 1

Mehmet Taha USTA – 21527472

Subject: Why Not Double Des? Explain

1) Double Des

Double DES is a encryption technique which uses two instance of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64 bit plain text goes into first DES instance which than converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.



However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

2) Meet in the middle Attack

The meet-in-the-middle attack is one of the types of known plaintext attacks. The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 2DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

A cipher, which is to be broken using meet-in-the-middle attack, can be defined as two algorithms, one for encryption and one for decryption. Each of them contains two simpler algorithms:

C = Eb(kb, Ea(ka, P))

P = Da(ka, Db(kb, C))

where:

- ➔ C is a ciphertext,
- ➔ P is a plaintext,
- ➔ E is an algorithm for encryption,
- ➔ D is an algorithm for decryption,
- ➔ ka and kb are two secret keys

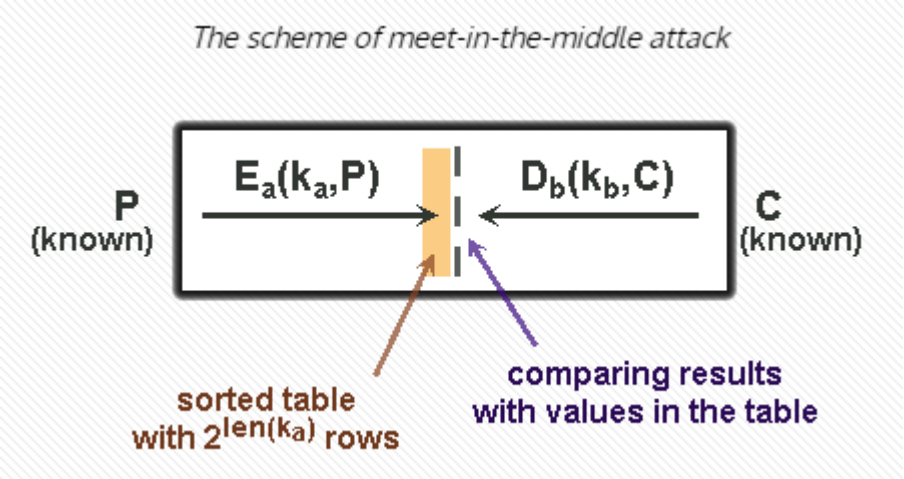
A following equation can be written for the cipher defined above:

Db(kb, C) = Ea(ka, P)

Where C is the ciphertext, known to the intruder, which corresponds to the message P, also known to the intruder.

The first step of the attack is to create a table with all possible values for one side of the equation. One should calculate all possible ciphertexts of the known plaintext P created using the first secret key, so Ea(ka,P). A number of rows in the table is equal to a number of possible secret keys. It is good idea to sort the received table based on received ciphertexts Ea(ka,P), in order to simplify its further searching.

The second step of the attack is to calculate values of Db(kb,C) for the second side of the equation. One should compare them with the values of the first side of the equation, computed earlier and stored in the table. The intruder searches a pair of secret keys ka and kb, for which the value Ea(ka,P) found in the table and the just calculated value Db(kb,C) are the same.



HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 2

Mehmet Taha USTA – 21527472

Subject: What is the primitive root? Show an example

Primitive roots

A primitive root b modulo m is a generator for the group $(\mathbb{Z}/m)^\times$. Existence of a primitive root modulo m is equivalent to the cyclic-ness of the multiplicative group $(\mathbb{Z}/m)^\times$. For p prime, $(\mathbb{Z}/p)^\times$ is cyclic, because $\mathbb{Z}/p$ is a field. Relatively elementary arguments then show that there are primitive roots modulo p^ℓ and $2p^\ell$ for $p > 2$ prime, and modulo 4. Non-existence of primitive roots for all other moduli is easier. This was understood by Fermat and Euler.

Because of the cyclic-ness of $(\mathbb{Z}/p)^\times$ for $p > 2$ prime, we have **Euler's criterion**: $b \in (\mathbb{Z}/p)^\times$ is a square modulo p if and only if

$$b^{(p-1)/2} = 1 \bmod p$$

An analogous result holds for q^{th} powers when p is a prime with $p = 1 \bmod q$.

Modulo a prime p, for a fixed primitive root b, for $x \in (\mathbb{Z}/p)^\times$ the **discrete logarithm** or **index** of x modulo p base g is the integer ℓ (uniquely determined modulo $p-1$) such that

$$x = b^\ell \bmod p$$

$$\begin{aligned}
3^1 &= 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7 \\
3^2 &= 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod 7 \\
3^3 &= 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod 7 \\
3^4 &= 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod 7 \\
3^5 &= 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod 7 \\
3^6 &= 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod 7 \\
3^7 &= 2187 = 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7
\end{aligned}$$

On Cryptographic Primitive Roots

We call primitive roots which are small powers of small primes *cryptographic primitive roots*. Without small primitive roots which are a prime power, a prime may have little cryptographic value for stream ciphers. Thus the distribution of primitive roots has cryptographic importance. This distribution has been investigated by many scholars.

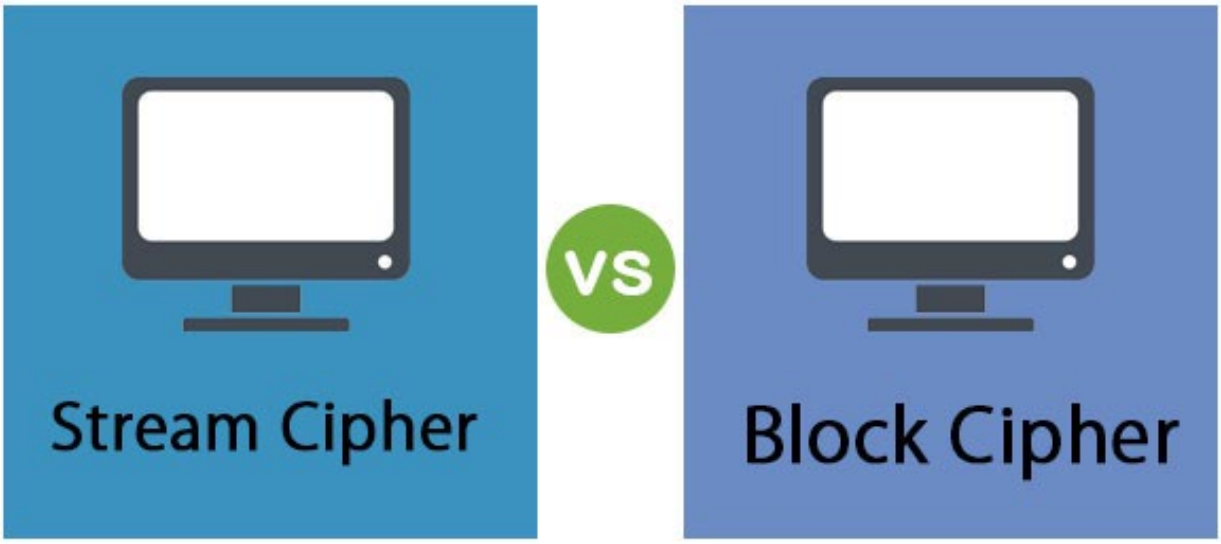
HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 3

Mehmet Taha USTA – 21527472

Subject: Describe Block Ciphers vs. Stream Ciphers Comparing



The important difference between a block cipher and a stream cipher is that the block cipher encrypts and decrypts a block of the text at a time. On the other hand, stream cipher encrypts and decrypts the text by taking the one byte of the text at a time.

Block Cipher:

1. Processing or encoding of plain text is done as a fixed length block one by one.A block for example could be 64 or 128 bits in size.

2. The same key is used to encrypt each of the blocks.

3. A pad added to short length blocks.

4. Uses Symmetric Encryption and is NOT used in asymmetric encryption.

5. Confusion factor:The key to the cipher text relationship could be really very complicated.

6. Diffusion factor:output depends on the input in a very complex method.

7. Most block ciphers are based Feistel cipher in structure

8. Looks more line an extremely large substitution and using the idea of product cipher 9. More secure in most cases

10. Usually more complex and slower in operation

11. Examples of Block cipher are:Lucifer/DES,IDEA,RC5,BLOWFISH etc.

Stream Cipher:

1. Processing or encoding of plain text is done bit by bit.The block size here is simply one bit.
2. A different key is used to encrypt each of the bits.
3. Bits are processed one by one in as in a chain.
4. High speed and low hardware complexity.
5. Key is often combined with an initialization vector.
6. Long period with no repetition.
7. Statistically random.
8. Depends on large key and Large Lineer complexity
9. Equality secure if properly designed
10. Usually very simple and much faster
11. Examples of Stream Cipher are: FISH,RC4,ISAAC,SEALİSNOW, etc

HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 4

Mehmet Taha USTA – 21527472

Subject: What is Hill Cipher ? How does it work ? Give an example

Hill Cipher Definition & Working Principle

Hill cipher is one of the primitive encryption algorithms. In this method, block cipher is used. In other words, the plain text to be encrypted is divided into blocks of plain text and the block is encrypted. The character value in the text is multiplied with the key given for each block. The new results are obtained by adding the obtained results.

Places the text to be encrypted in the matrix and creates a random element matrix. Then it multiplies these two matrices and by searching the formed matrix in the alphabet sequence, the encrypted text is obtained.

Invented by Lester S. Hill in 1929, the Hill cipher is a **polygraphic substitution cipher** based on linear algebra. Hill used matrices and matrix multiplication to mix up the plaintext. To counter charges that his system was too complicated for day to day use, Hill constructed a cipher machine for his system using a series of geared wheels and chains. However, the machine never really sold.

Hill's major contribution was the use of mathematics to design and analyse cryptosystems. It is important to note that the analysis of this algorithm requires a branch of mathematics known as number theory. Many elementary **number theory** text books deal with the theory behind the Hill cipher, with several talking about the cipher in detail.

Examples:

```
Input  : Plaintext: ACT
         Key: GYBNQKURP
Output : Ciphertext: POH
```

```
Input  : Plaintext: GFG
         Key: HILLMAGIC
Output : Ciphertext: SWK
```

Encryption

We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

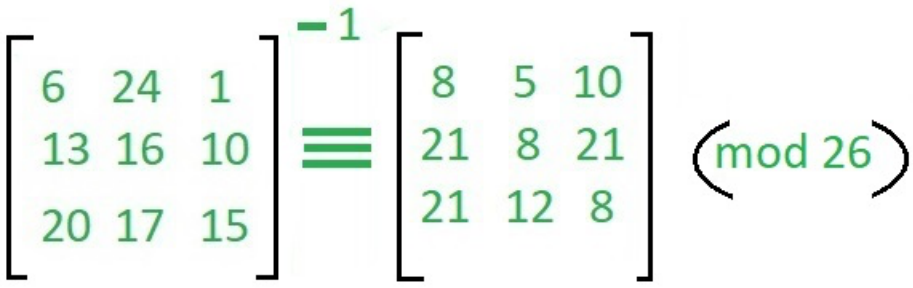
The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} (\text{mod } 26)$$

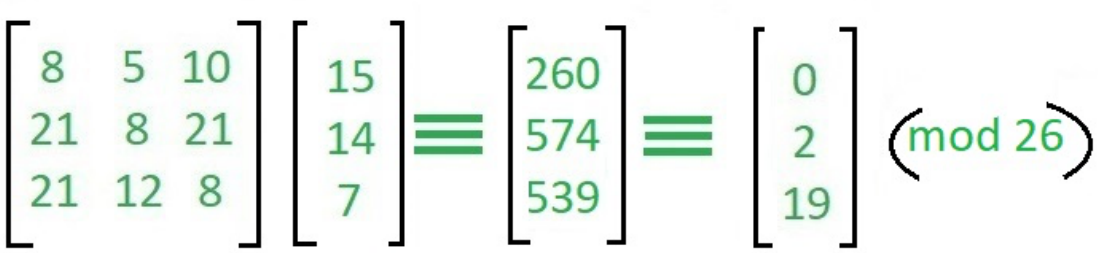
which corresponds to cipher text of ‘POH’

Decryption

To decrypt the message, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). The inverse of the matrix used in the previous example is:



For the previous Cipher text ‘POH’:



which gives us back ‘ACT’.

Assume that all the alphabets are in upper case.

Below is the implementation of the above idea for n=3.

HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 5

Mehmet Taha USTA – 21527472

Subject: Man-in-the-middle attack on Diffie Hellman. Explain

Man In The Middle Attack

In this attack type, various listening operations are carried out by infiltrating between 2 connections and the capture of the desired data is started. There is more than one way to start the listening process to join the network and solve the unencrypted connection between the 2 networks. In some of these methods, the client actually logs on to the server site, but the data transferred while sending the request can be transmitted to the middle attacker. In some attack types, the client accesses a copy of the same page prepared by the attacker before reaching the real site and transfers the information of the site he wants to login to the attacker, if it is not careful, the copy prepared by the attacker can give the site to the site. Attack methods such as MITM can be done without the need for very serious network knowledge, and also we come up with software that integrates into different operating systems. With these softwares, the system to be attacked is determined by just a few clicks, and the listening process is initiated, and then MITM can be implemented, and even the ssl systems can be modified thanks to the built-in certificate system for the vehicle used.

For attackers to succeed in MITM attacks, the victim must direct the victim to the proxy server rather than the actual server.

The following scenarios are implemented in this;

1.LOCAL AREA NETWORK (Local Area Network):

- 1.1.ARP poisoning
- 1.2.DNS spoofing
- 1.3.STP mangling

2.FROM LOCAL TO REMOTE (Remote Local Area Network):

- 2.1.ARP poisoning
- 2.2.DNS spoofing
- 2.3.dhcpspoofing
- 2.4.ICMP redirection
- 2.5.IRDP spoofing - route mangling

3.REMOTE (Remote Network):

- 3.1.DNS poisoning
- 3.2.Traffic tunneling
- 3.3.Route mangling

FOR INSTANCE MAN IN THE MIDDLE ATTACK ON DIFFIE HELLMAN

D-H key exchange revised

Set-up:

- find large prime p
- find primitive element $\alpha \in Z_p$

Protocol:

Alice		Bob
pick $k_{prA} = a_A \in \{2, 3, \ldots, p-2\}$		pick $k_{prB} = a_B \in \{2, 3, \ldots, p-2\}$
compute $k_{pubA} = b_A = \alpha^{a_A} \bmod p$		compute $k_{pubB} = b_B = \alpha^{a_B} \bmod p$
	$\xrightarrow{b_A}$	
	$\xleftarrow{b_B}$	
$k_{AB} = b_B^{a_A} = \alpha^{a_A a_B} \bmod p$		$k_{AB} = b_A^{a_B} = \alpha^{a_A a_B} \bmod p$

Security:

1. passive attacks
   ⇒ security relies on Diffie-Hellman problem thus $p > 2^{1000}$.

2. active attack
   ⇒ *Man-in-the-middle attack:*

Alice		Oscar		Bob
	$\xrightarrow{\alpha^a}$		$\xrightarrow{\alpha^o}$	
	$\xleftarrow{\alpha^o}$		$\xleftarrow{\alpha^b}$	
$k_{AO} = (\alpha^o)^a = \alpha^{ao}$		$k_{AO} = (\alpha^a)^o$		$k_{BO} = (\alpha^o)^b = \alpha^{bo}$
		$k_{BO} = (\alpha^b)^o$		
$y' = e_{k_{AO}}(x)$	$\xrightarrow{y'}$	$x = d_{k_{AO}}(y')$		
		$y'' = e_{k_{BO}}(x)$	$\xrightarrow{y''}$	$x = d_{k_{BO}}(y'')$

- Oscar can read and alter x without detection.
- Underlying Problem: *public keys are not authenticated.*

- **Man-in-the-middle attack applies to all Public-key schemes.**

HACETTEPE UNIVERSITY DEPARTMENT OF

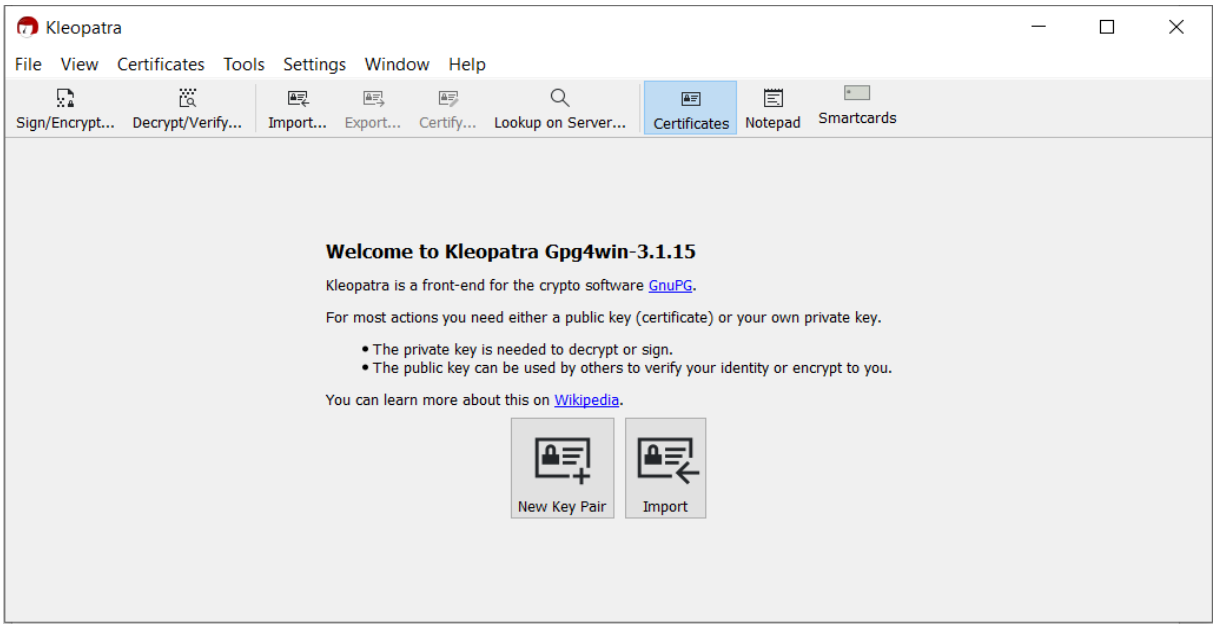
COMPUTER ENGINEERING

BBM 456 HOMEWORK 6

Mehmet Taha USTA – 21527472

Subject: Download and Install PGP. Create Encrypted and signed message traffic. Propare 3-4 page report with screenshot

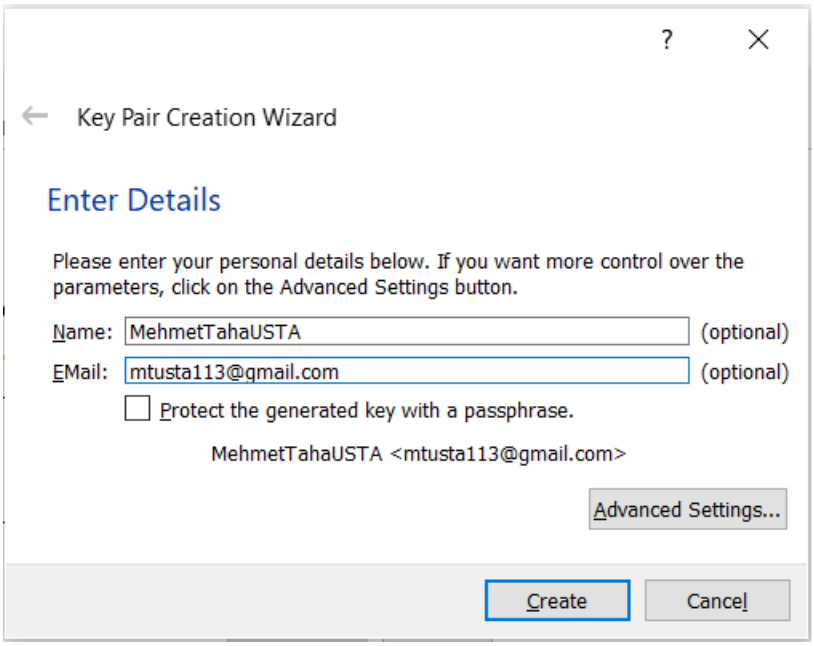
1) Kleopatra program must be installed for Windows



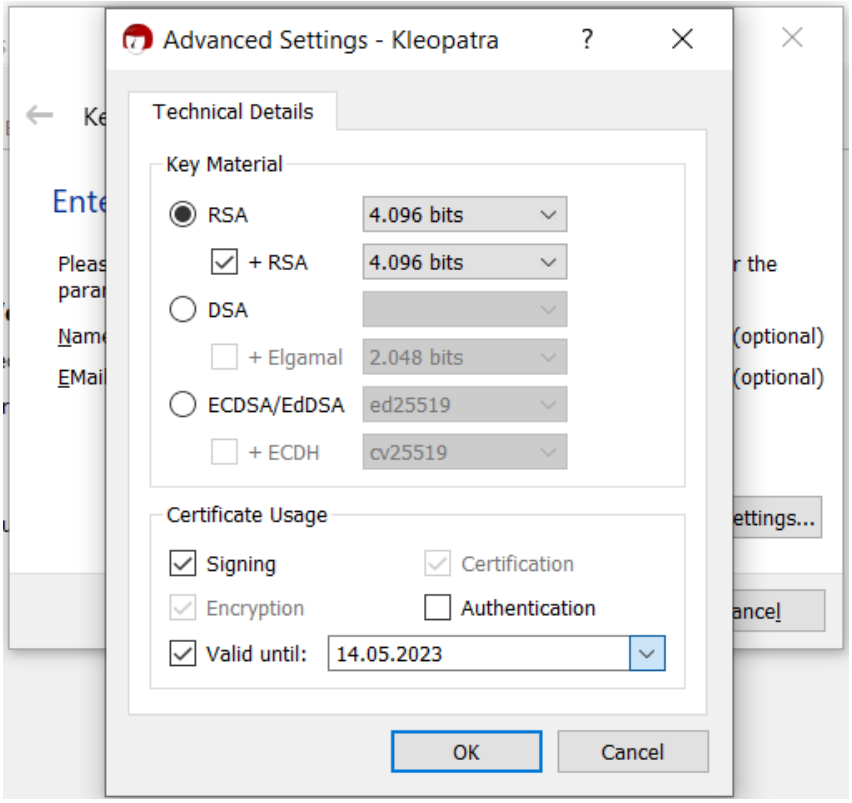
2) Encryption

2.1) New Key Pair

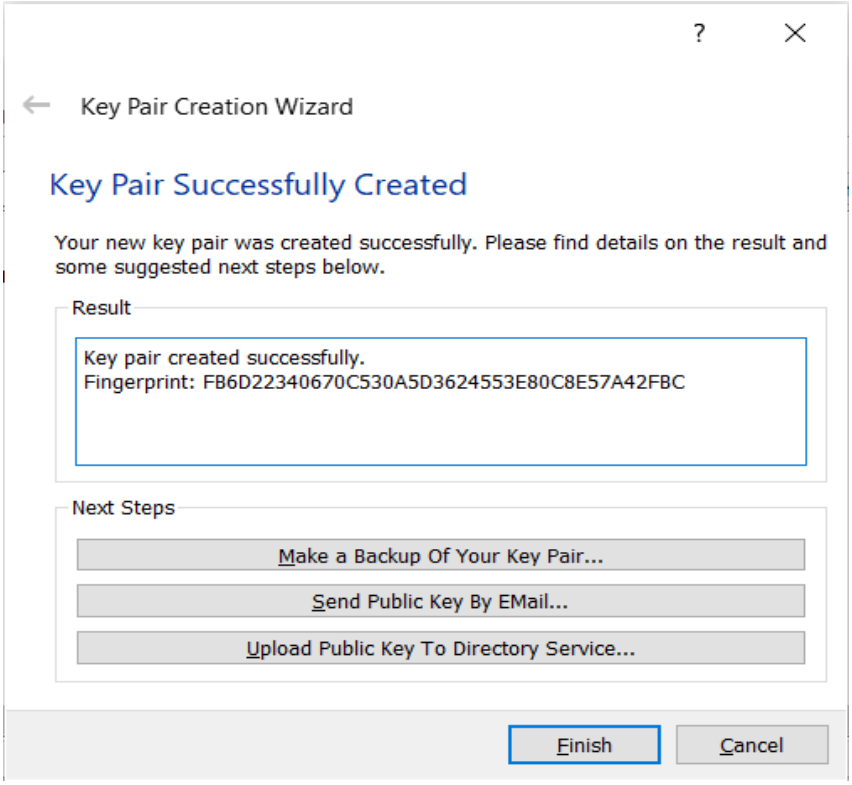
In Encryption, we first need to generate our keys by pressing the New Key Pair button.



2.2) Key Pair Settings



2.3) Generated Keys



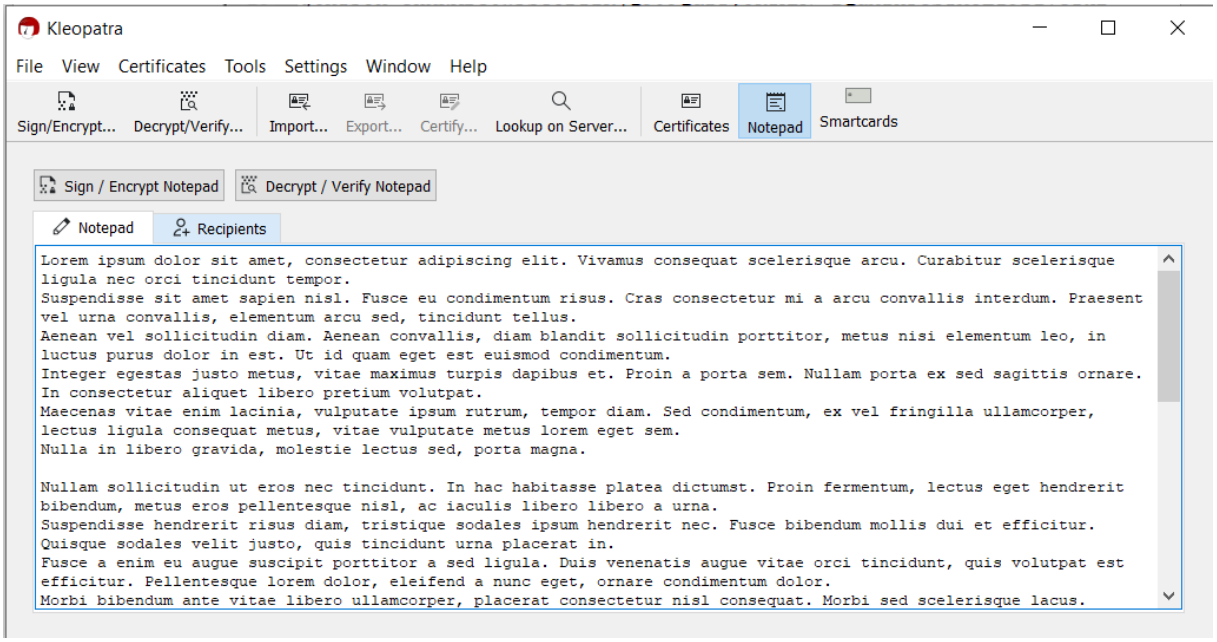
2.4) Exported Public Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID:   MehmetTahaUSTA <mtusta113@gmail.com>
Comment: Created:   12.05.2021 19:26
Comment: Expires:   14.05.2023 12:00
Comment: Type:  4.096-bit RSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint:   FB6D22340670C530A5D3624553E80C8E57A42FBC


mQINBGCcAboBEAC/fpHxRA3p8pVr5KBShd/PjelIK1Hd7Tc0nigwTXTXit1y3ucQ
fUds+dxPh5AzF2joED3EpeARsweDSL0S4m2ZaYaAD61wW03e/Sturz7dinXYAY6Z
s8TCGmY5bYFMZlgfUyLz2Pe8Y/qv21kP/5WbR4G0DQc7yDTgDebzdX4dsTyozzCl
VnJhbxjwjbD52mJKYOXOdIn/NP1gmvVTYZX7EWNpEiy75F0qbuFbDI+A01S4qxYN
4Z1+tS7dyEGi5ikLPAEBD3Y12AYDiSmLfbDx1/kI9D5xs73n3fBmnkBH42xza2CD
SIiS5iZWY0X2Nzzp3NYydkRSiJuJFucNKnAMRl2/VI5UFjLSL1C4OgNkBlYSiVwS
N3O0IheDWqCgQmdM6RA3u8Ek8FIR1xlzaMfcH0383rqEMlZgwVkyP5J9VVivYWnu
QLvg5EiWjlXNkZc9ENY5mBiwfW7RAUzxi8ISBwVOUTKkPlCofWomRXqwXi4tpidx
WsM9MmPx3ndtS+9QRTY7ZRlHwXg3d+1DZsQ1qSuwa6lj4TYYNTDeIT+lEyhWVzsv
g6nTFJx+oHXNADG0WFSGUDYzKjQJ09QdfYy8KTMM7+fQuXIhF3STX5L19DzVoTkB
jVhsloXEydNnuFRWomMmL80VqhF4XbzqjJE/DOLqH0wFQBmEoldFHhfzhwARAQAB
```

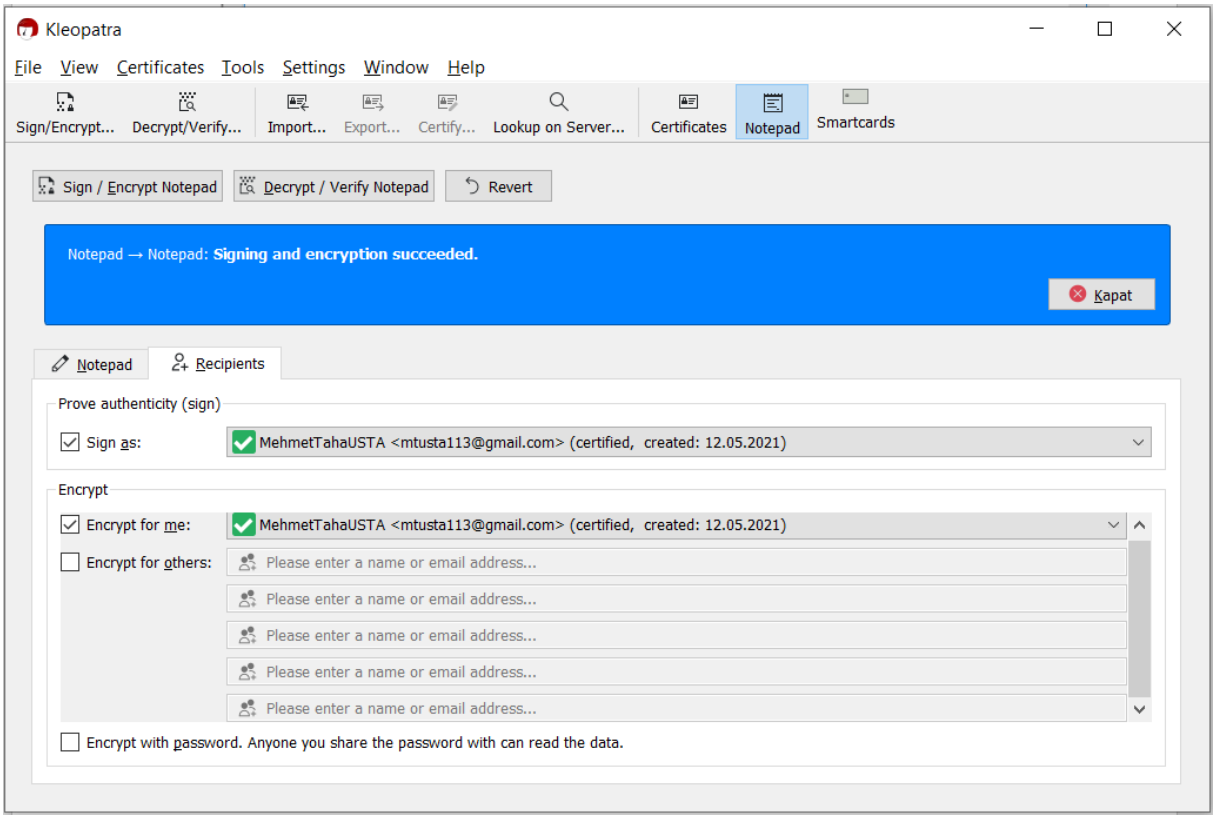
2.5) Exported Private Key

```
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQcYBGCcAboBEAC/fpHxRA3p8pVr5KBShd/PjelIK1Hd7Tc0nigwTXTXit1y3ucQ
fUds+dxPh5AzF2joED3EpeARsweDSL0S4m2ZaYaAD61wW03e/Sturz7dinXYAY6Z
s8TCGmY5bYFMZlgfUyLz2Pe8Y/qv21kP/5WbR4G0DQc7yDTgDebzdX4dsTyozzCl
VnJhbxjwjbD52mJKYOXOdIn/NP1gmvVTYZX7EWNpEiy75F0qbuFbDI+A01S4qxYN
4Z1+tS7dyEGi5ikLPAEBD3Y12AYDiSmLfbDx1/kI9D5xs73n3fBmnkBH42xza2CD
SIiS5iZWY0X2Nzzp3NYydkRSiJuJFucNKnAMRl2/VI5UFjLSL1C4OgNkBlYSiVwS
N3O0IheDWqCgQmdM6RA3u8Ek8FIR1xlzaMfcH0383rqEMlZgwVkyP5J9VVivYWnu
QLvg5EiWjlXNkZc9ENY5mBiwfW7RAUzxi8ISBwVOUTKkPlCofWomRXqwXi4tpidx
WsM9MmPx3ndtS+9QRTY7ZRlHwXg3d+1DZsQ1qSuwa6lj4TYYNTDeIT+lEyhWVzsv
g6nTFJx+oHXNADG0WFSGUDYzKjQJ09QdfYy8KTMM7+fQuXIhF3STX5L19DzVoTkB
jVhsloXEydNnuFRWomMmL80VqhF4XbzgjJE/DOLqH0wFQBmEoldFHhfzhwARAQAB
AA/9G0lTTXA3lVb6QLIGwEuQPTiI/b4if7+OBsLkkiFvXUlNzdECVuCrHVWrNW/p
NcaHrc2mp49FUvBSSTxDqN235UzanAPf4Gs6OOSVXEO/bv0MVre+FJu/lTMCzvsS
GgtZUjlb+Sg5ANC0R3u3gKaYMFSroDbdCYE5O5Xvi1B6JIv9S0aetWiQit60TI68
IZYjPFr7VARaJ5Hq6umZvIRixTBQnIe49RsQxXugRAORrTcv0tKaJWc5NHVn1LV0
2Nv4DEBEGl0UKI78KGPSlixWWte+Bi8beMM2c8Q1vcGeAkBfU0EBMyPSRjBiVRv3
```

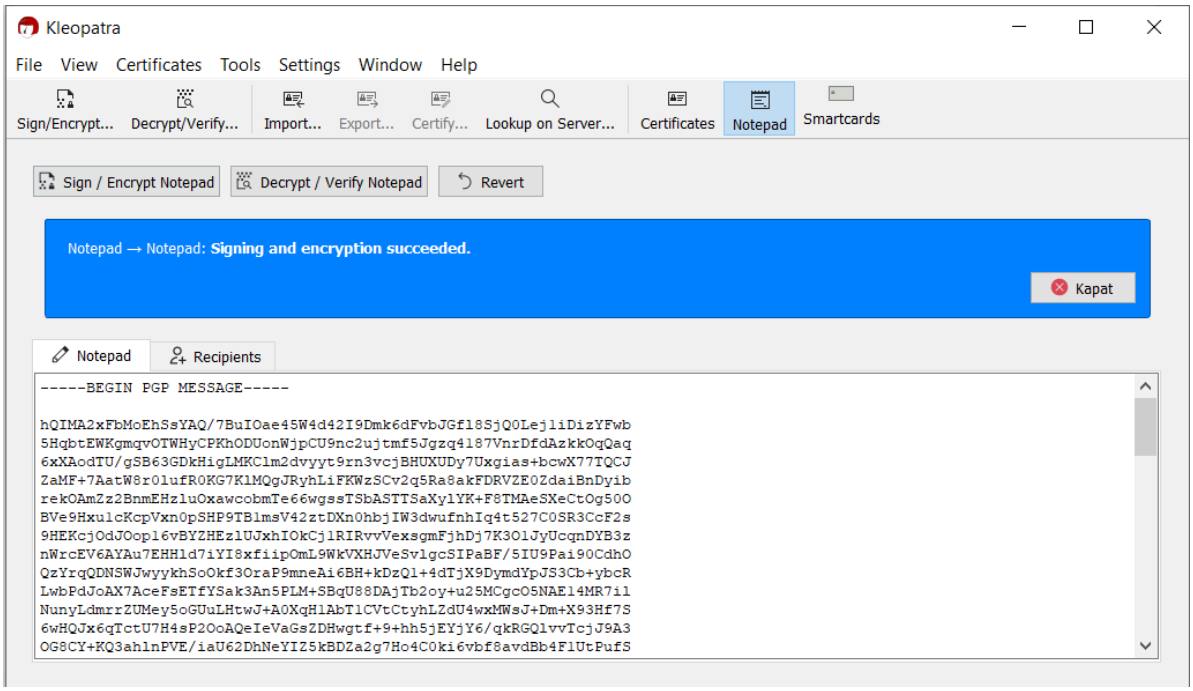
2.6) Message to be encypted



2.7) The message is encrypted with the selected Public Key



2.8) Encrypted Message



2.9) The decrypted message is obtained by pressing the “Decrypt/Verify Notepad” button. The text obtained is the same as the original message.