Understanding Cryptography
Answers of Homework No.5

Chapter 9

1.

Consider the following elliptic curve:

$$y^2 = x^3 + 2x + 2 \mod 17$$

1.1. Show that the condition $4a^3 + 27b^2 \neq 0 \mod p$ is fulfilled for this curve.

1.2. Calculate $(2,7) + (5,2)$ with only a packet calculator.

1.3. Verify Hasse's theorem for this curve.

1.4. Describe why all elements are primitive elements?

حل:

1.1.

$$y^2 = x^3 + 2x + 2 \mod 17 \Rightarrow a = 2, \; b = 2, \quad p = 17$$

$$4a^3 + 27b^2 = 4 \times 2^3 + 27 \times 2^2 \neq 0 \Rightarrow 140 = 4 \quad mod\ 17$$

$$4 \neq 0 \quad \surd$$

1.2.

$$(2,7) + (5,2) \Rightarrow x_1 = 2, \; x_2 = 5, \quad y_1 = 7, \; y_2 = 2$$

$$S = (y_2 - y_1)(x_2 - x_1)^{-1} \mod 17$$

$$S = (2 - 7)(5 - 2)^{-1} \mod 17$$

$$S = (-5)(3)^{-1} \mod 17$$

$$S = (-5)(6) \equiv 4 \mod 17$$

$$x_3 = S^2 - x_1 - x_2 \mod 17$$

$$\mathbf{x_3 = 4^2 - 2 - 5 \ mod17 = 9}$$

$$\mathbf{y_3 = S(x_1 - x_3) - y_1 \ mod\ 17}$$

$$\mathbf{y_3 = 4(2-9) - 7 \ mod\ 17 = 16}$$

$$\rightarrow \mathbf{(9, 16)}$$

1.3.

$\mathbf{Theorem\ 9.2.2}$: Hasse's theorem

$\boldsymbol{Given\ an\ elliptic\ curve\ E\ modulo\ p, the\ number\ of\ points\ on\ the\ curve\ is\ denoted\ by}$ $\boldsymbol{\#\ E\ \ and\ is\ bounded\ by}$:

$$P + 1 - 2\sqrt{P} \ \leq \#\ E \ \leq P + 1 + 2\sqrt{P}$$

$$17 + 1 - 2\sqrt{17} \leq 19 \ \leq 17 + 1 + 2\sqrt{17} \ \ \rightarrow \ \ 9.7 \ \leq 19 \leq 26.246 \ \ \surd\surd$$

1.4.

طبق قضیه کتاب داریم :

$$Theorem\ 8.2.4\ \ Let\ G\ be\ \ a\ finite\ cyclic\ group\ .Then\ it\ holds\ that$$

$$1. The\ \ number\ of\ primitive\ elements\ of\ G\ is\ \emptyset(|G|)$$

$$2. If\ |G|\ is\ prime\ , then\ all\ elements\ \ a \neq 1 \in G\ are\ primitive.$$

به دلیل اینکه P یک عدد اول است و یک $cyclic\ \ group$ می سازد. بنابراین اعداد گروه نسبت به P اول اند و مولد هستند.

2.

Consider the following elliptic curve:

$$\boldsymbol{y^2 = x^3 + x + 6 \ \ mod\ 11}$$

Consider a $\boldsymbol{DHKE}$ protocol based on this elliptic curve with Alice's private key $\boldsymbol{a\ =\ 6}$. Alice receives Bob's public key $\boldsymbol{B\ = (5, 9)}$. Calculate the session key for this protocol using the $\boldsymbol{double\ and\ add}$ algorithm.

حل :

اطلاعات مساله:

$$y^2 = x^3 + x + 6 \mod 11 \quad a = 1, \qquad b = 6, \quad p = 11$$
$$Alice\ private\ key: \quad a = 6$$
$$Bob\ public\ key: \quad B = (5, 9)$$

با استفاده از الگوریتم *double and add*:

Double-and-Add Algorithm for Point Multiplication
Input: elliptic curve E together with an elliptic curve point P
a scalar $d = \sum_{i=0}^{t} d_i 2^i$ with $d_i \in 0, 1$ and $d_t = 1$
Output: $T = dP$
Initialization:
$T = P$
Algorithm:
1 FOR $i = t - 1$ DOWNTO 0
1.1 $T = T + T \mod n$
IF $d_i = 1$
1.2 $T = T + P \mod n$
2 RETURN (T)

در پروتکل *DHKE* داریم:

Diffie–Hellman Key Exchange with Elliptic Curves :

Elliptic Curve Diffie–Hellman Key Exchange (ECDH)

Alice		Bob
choose $k_{prA} = a \in \{2, 3, \ldots, \#E - 1\}$		choose $k_{prB} = b \in \{2, 3, \ldots, \#E - 1\}$
compute $k_{pubA} = aP = A = (x_A, y_A)$		compute $k_{pubB} = bP = B = (x_B, y_B)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
compute $aB = T_{AB}$		compute $bA = T_{AB}$

Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

$$T_{AB} = bA \ , \qquad T_{AB} = aB \quad \rightarrow Session\ Key = T_{AB} = 6(5, 9) = (110)_2(5.9)$$

هم چنین می دانیم:

Elliptic Curve Point Addition and Point Doubling

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}$$

$$b = (\mathbf{110})_2$$

گام یک :

$P + P$
$S = (5,9) + (5,9):$
$S = (3{x_1}^2 + 1)(2y_1)^{-1} \quad mod\ 11 = \ 76/18 \quad mod\ 11 = 10\ \times 18^{-1}\ mod\ 11$
$18^{-1} = \ 18^9\ mod\ 11 = 8 \qquad : \qquad S = 80\ \ mod\ 11 = 3$
$x_3 = \ S^2 - x_1 - \ x_2\ \ mod\ 11 = 3^2 - 5 - 5 \quad mod\ 11 = 10$
$y_3 = S(x_1 - x_3) - \ y_1\ \ mod\ 11$
$y_3 = 3(5 - 10) - \ 9\ \ mod\ 11 = 9$

$$S = 3 \quad \rightarrow \quad P + P = 2P = (10,9)$$

گام دو :

$2P + P$
$2P = (10,9) \qquad P = (5,9)$
$S = (y_2 - \ y_1)(x_2 - x_1)^{-1} \quad mod\ 11 = \ (9 - 9)/(10 - 5)^{-1} \quad mod\ 11 = 0$
$x_3 = \ S^2 - x_1 - \ x_2\ \ mod\ 11 = 0^2 - 5 - 10 \quad mod\ 11 = 7$
$y_3 = S(x_1 - x_3) - \ y_1\ \ mod\ 11$
$y_3 = 0(5 - 7) - \ 9\ \ mod\ 11 = 2$

$$S = 0 \quad \rightarrow \quad 2\,P + P = 3P = (7,2)$$

گام سه :

$3P + 3P$
$S = (7,2) + (7,2):$
$S = (3{x_1}^2 + 1)(2y_1)^{-1} \quad mod\ 11 = \ 148/4 \quad mod\ 11 = 10\ \times 18^{-1}\ mod\ 11$
$4^{-1} = \ 4^9\ mod\ 11 = 3 \qquad : \qquad S = 148 \times 3\ \ mod\ 11 = 4$
$x_3 = \ S^2 - x_1 - \ x_2\ \ mod\ 11 = 4^2 - 7 - 7 \quad mod\ 11 = 2$
$y_3 = S(x_1 - x_3) - \ y_1\ \ mod\ 11$
$y_3 = 4(7 - 2) - \ 2\ \ mod\ 11 = 7$

$$S = 4 \quad \rightarrow \quad 3P + 3P = 6P = (2,7)$$

$$\rightarrow \quad \boldsymbol{Key \;\; Exchange \;\; T_{AB} = (2,7)}$$

Chapter 10

3. Consider an Elgamal signature scheme with $p = 31$, $\alpha = 3$ and $\beta = 6$. You receive the message $x = 10$ twice with two signatures $(17, 5)$ and $(13, 5)$.

3.1. Which one of these signatures is valid?

3.2. How many valid signatures are there for each message x and the specific parameters chosen above?

حل:

3.1.

$$\alpha^x = 3^{10} \;\; mod\, 31 = 25$$

$$(17,5): \;\; r = 17, s = 5,$$
$$t = \beta^r . r^s \;\; mod\, p = 6^{17} . 17^5 \;\; mod\, 31 = 25 \quad \rightarrow valid$$

$$(13,5): \;\; r = 13, \quad s = 5\,,$$
$$t = \beta^r . r^s \;\; mod\, p = 6^{13} . 13^5 \;\; mod\, 31 = 5 \quad \rightarrow invalid$$

3.2.

در کل تعداد امضاهای معتبر برای یک مقدار x بستگی به مقدار k_E دارد و با توجه به اینکه k_E باید در محدوده 0 تا $P-2$ باشد پس $P-1$ امضا می توان داشت که حداکثر برابر ۳۰ است.

4. Given an RSA signature scheme with the public key $(n = 9797\,, e = 131)$, show how Oscar can perform an existential forgery attack by providing an example of such for the parameters of the RSA digital signature scheme.

حل:

Alice		Oscar		Bob
	$\xleftarrow{(n,e)=(9797,131)}$	$S \in Z_n$ (a random number) $S = 11$		$k_{pr} = d$
verification: $x' \equiv S^e \bmod n$	$\xleftarrow{(x,s)=(4755,11)}$	$x = S^e \bmod n$ $x = 4755$	$\xleftarrow{(n,e)}$	$k_{pub} = (n, e)$
$x' = x \rightarrow$ verified				$k_{pub} = (9797, 131)$

در واقع $oscar$ مقدار S را انتخاب می کند و از روی آن مقدار پیام x را می سازد و نمیتواند پیام دلخواه خود را بسازد. x تولید شده توسط $verification$ تایید می شود.

5.
CrypTool

1. Answer the following questions with respect to the Digital Signature Algorithm;
   i. Generate a 2048bit DSA key pair using CrypTool key generation tool, with your own first name, last name, and student id (as your PIN).
   ii. Use this key to sign a text of your choice. What does the resulting file consist of?
   iii. Verify your previous signature using the same key.
   iv. Make a slight change to the signature and repeat the previous part. Explain what happens.

2. Answer the following questions about the elliptic curve cryptosystem;
   i. Create a key pair with a 256-bit prime, using your first name, last name, and student ID (as your PIN).
   ii. Use this key with ECC-AES hybrid encryption algorithm to encrypt an arbitrary document. Why are asymmetric ciphers usually used in tandem with symmetric ones to encrypt files, and why don't we use asymmetric-only encryption?
   iii. Decrypt the resulting cipher text in the previous part with the same key and algorithm.

Programming

Do the following exercise by writing codes in your favorite programming language. Please be noted that you may use available codes on the internet only to draw inspiration but not to copy. Also, please provide brief reports on your codes in which you include your sample inputs and pictures of your program's output to them.

1. Write a program that solves the Elliptic Curve Discrete Logarithm Problem (ECDLP) using Shanks' Baby-Step Giant-Step algorithm; your program should:
   i. Take two coefficients *a* and *b*, a prime number *p*, and coordinates of two points P and Q as input.
   ii. The first three inputs construct an elliptic curve with the following formula:
$$y^2 \equiv x^3 + a.x + b \bmod p$$
   iii. The points P and Q lie on this curve.
   iv. Use the mentioned algorithm to compute the coefficient x such that Q = x.P

حل:

CrypTool

1.

i.

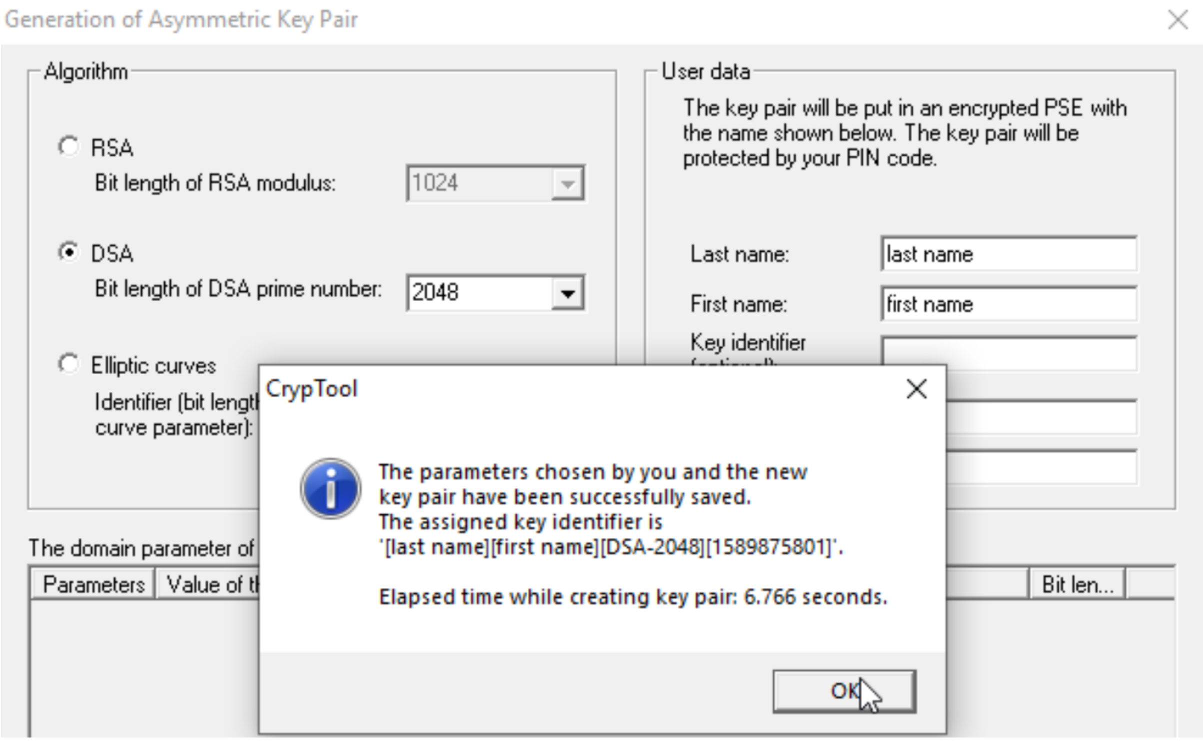

Figure 1: DSA key pair generation

ii.

The file consists of the original document attached to its signature, which is signed using the DSA key.

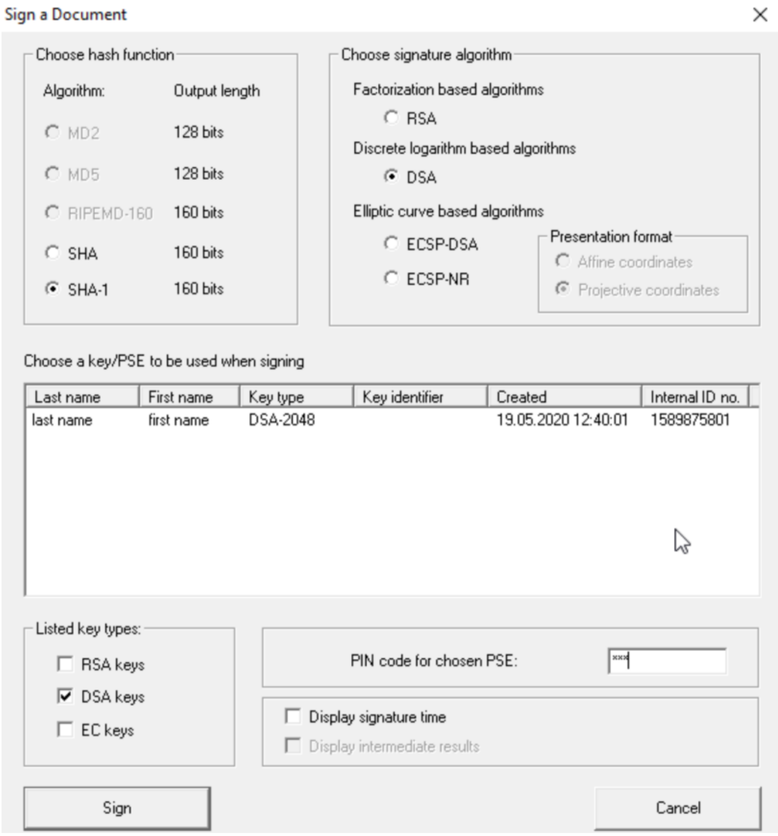

Figure 2: signing an arbitrary document using our key.

iii.

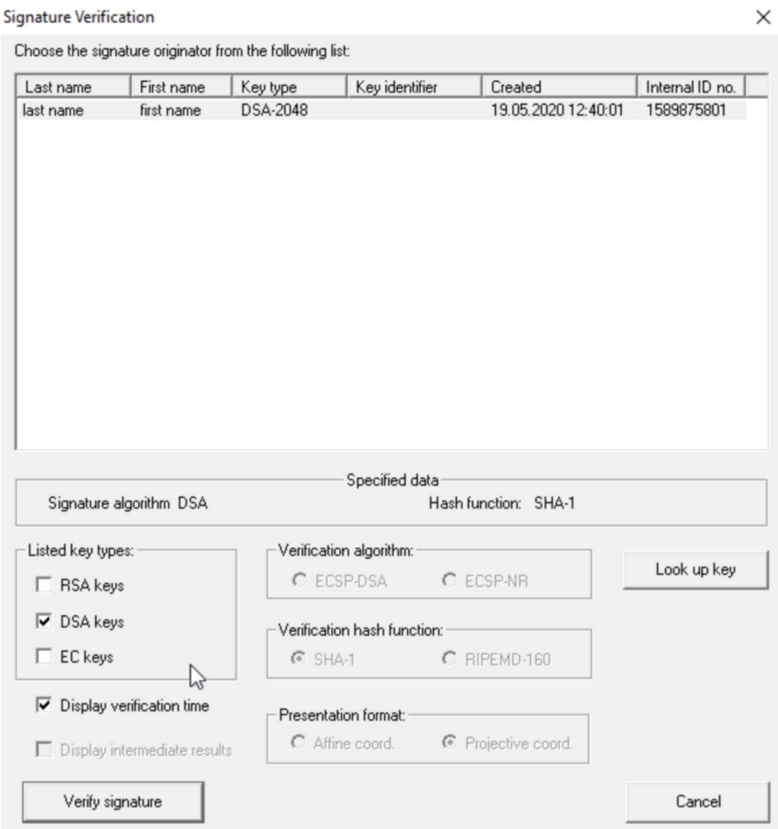

Figure 3: signature verification with the same key.

Figure 4: signature has been verified successfully.

iv.

Signatures will be computed using one's private key. Consequently, they can be decrypted using the same person's public key. As the public key is available to every other party, but the private key is unique to any individual, only that specific person, who has the private key, can sign his own documents. By signing files, we want to guarantee their integrity. Thus, if a document doesn't match the decrypted version of its attached signature, we assume it's been modified.

Here, by changing the signature we invalidate its soundness.

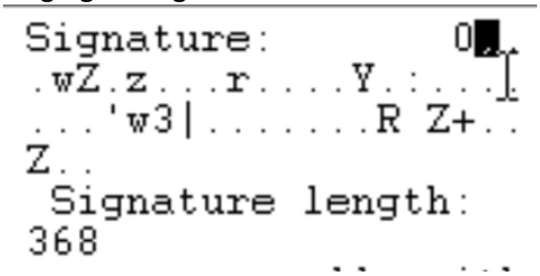

Figure 5: the original signature

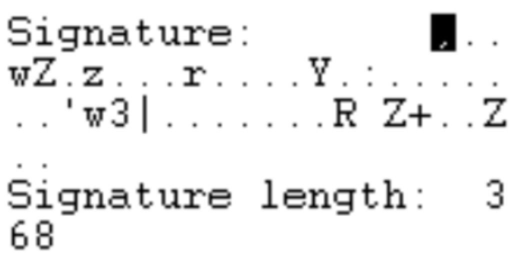

Figure 6: the altered version of the signature.

Figure 7: signature has not been verified.

2.

i.

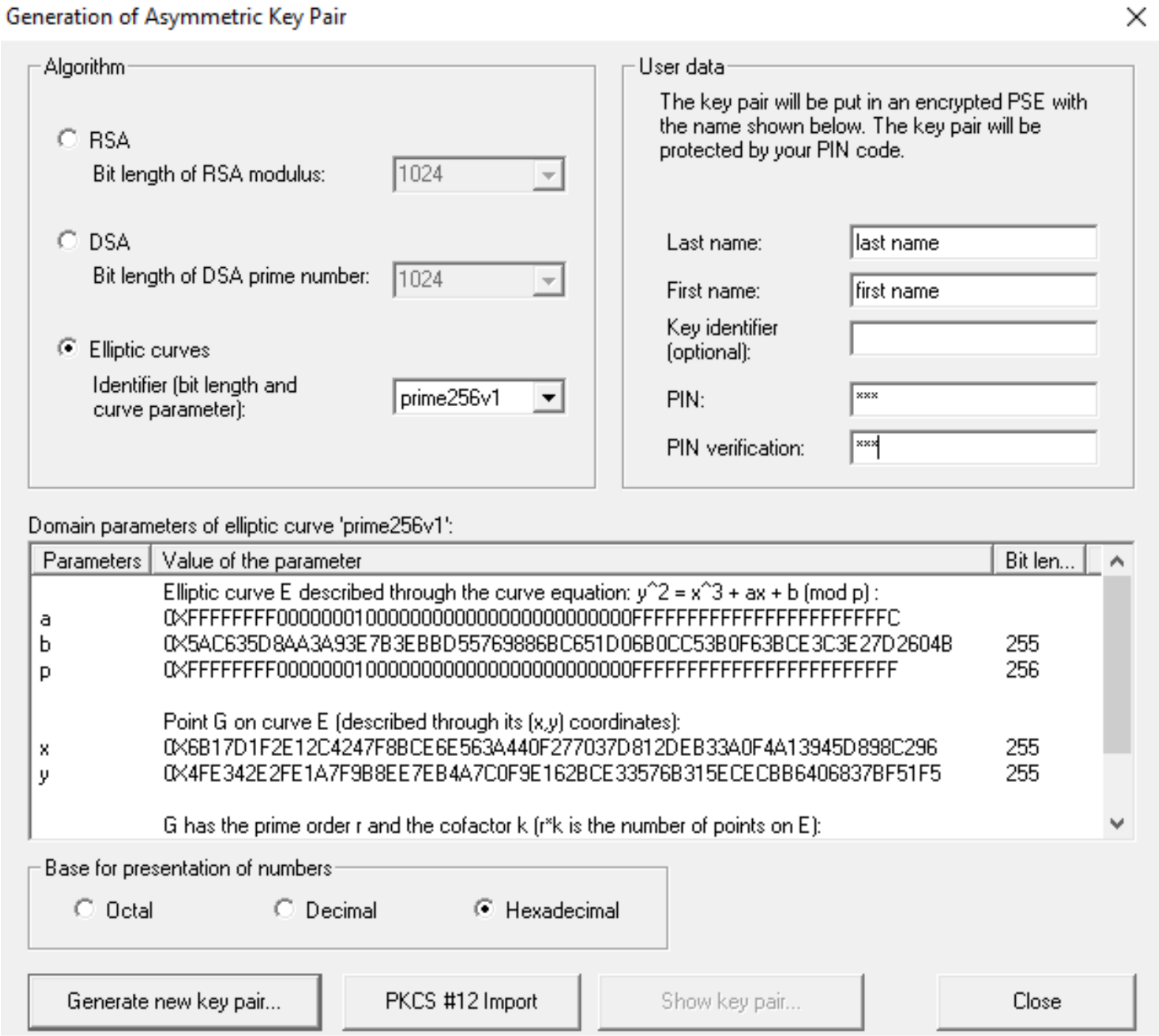

Figure 8: creating an elliptic curve key pair with a 256-bit prime.

ii.

Asymmetric ciphers are really slow compared with symmetric ciphers, decryption speed is even much lower, for them, than encryption speed.
Another problem is with their padding; the cipher text is expanded using particular padding schemes, and the size of the encrypted block is less than the modulus. Padding schemes may cause such amount of overhead that depletes our memory resources.
A second problem with padding is that it requires the use of a random number generator. It may adversely affect our system's performance and speed, if the encrypter keeps asking random numbers to encrypt numerous blocks of a file.

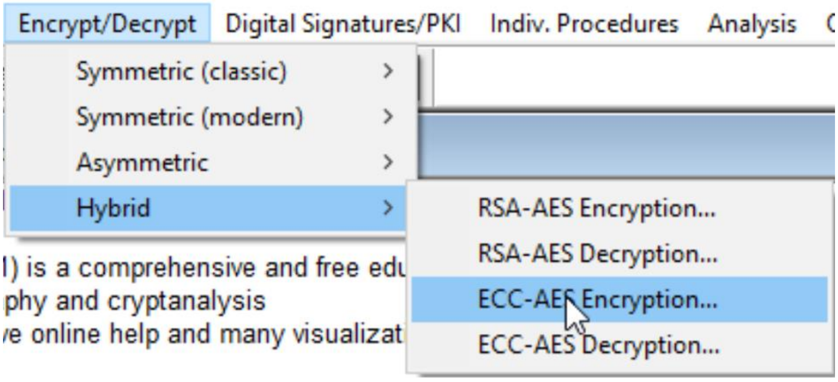

Figure 9: ECC-AES encryption in the menu

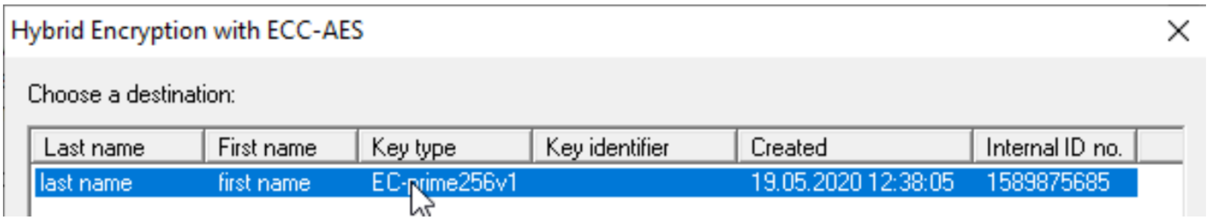

Figure 10: choosing our generated key

iii.

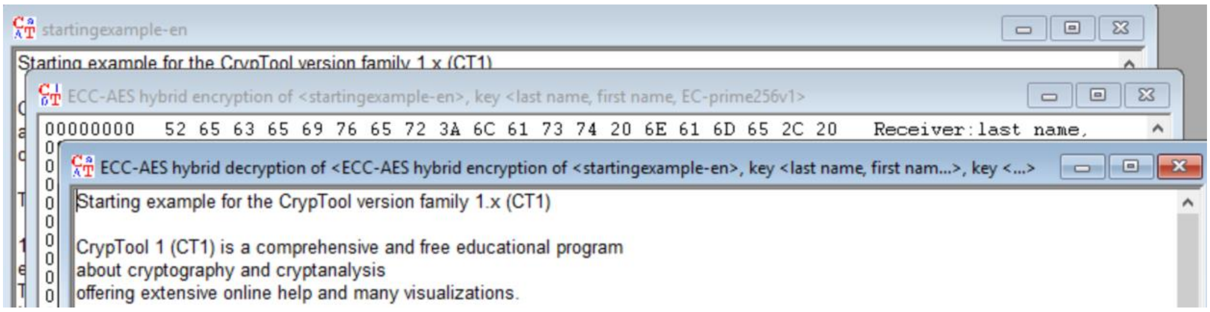

Figure 11: decrypting the encrypted file using the same key and algorithm.