POLITECHNIKA BIALOSTOCKA
WYDZIAL INFORMATYKI

Techniki zapewniania poufnosci w internecie

PRACOWNIA SPECJALISTYCZNA 3-4

TEMAT: KRYPTOGRAFIA KRZYWYCH ELIPTYCZNYCH

Elliptic curve cryptography

1. *Elliptic groups*

If two positive integer numbers a and b satisfies to the following relation

$$4a^3 + 27b^2 \neq 0 \ (mod\ \boldsymbol{M}),$$

where $\boldsymbol{M}$ is a prime number and $a< \boldsymbol{M}$ and $b< \boldsymbol{M}$**,** than the elliptic curve can be used to form of the ***elliptic group***.

The elliptic group $E_M(a,b)$ consists of the set of pairs (x,y) of the positive integer numbers less then $\boldsymbol{M}$, which satisfies to the relation:

$$y^2=x^3+ax+b \ (mod\ M),$$

Integer positive pairs of two numbers (x,y) from (0,0) till $(M-1,M-1)$, which satisfies to the above presented relation can be used as elliptic group elements (***points***).

The rule to generate all elements of the elliptic group consists of the next steps

1. For all values of x, $0\le x< M$, the value of x^3+ax+b $(mod\ M)$ should be calculated.

2. For each value from the previous step the square root modulo M as an integer number have to be determined. In a case of the negative answer there are not the element within the elliptic group $E_M(a,b)$. If the root exists the there are two value of y and two elements in a group.

Example For example, let M=5 and $y^2=x^3+4$ *mod* 5, what can be describe as $E_5(0,4)$. In this case a=0, b=4 and $4\times0^3+27\times4^2$ (*mad* 5) = $1 \neq 0$, it means that we can construct the elliptic group $E_5(0,4)$.

Let start with x=0; $y^2=0^3 + 4$ *mod* 5 = 4; $y= +2$ and $y= -2$, Then there are two points (0,2) and (0,-2) = (0,3) within the elliptic group $E_5(0,4)$. Entire set of point are shown below

$$E_5(0,4)=\{O, (0,2), (0,3), (1,0), (3,1), (3,4)\}.$$

Example. For example, let M=23 and $y^2=x^3+x$. In this case a=1, b=0 and $4\times1^3+27\times0^2 = 4 \neq 0$, it means that we can construct the elliptic group $E_{23}(1,0)$.

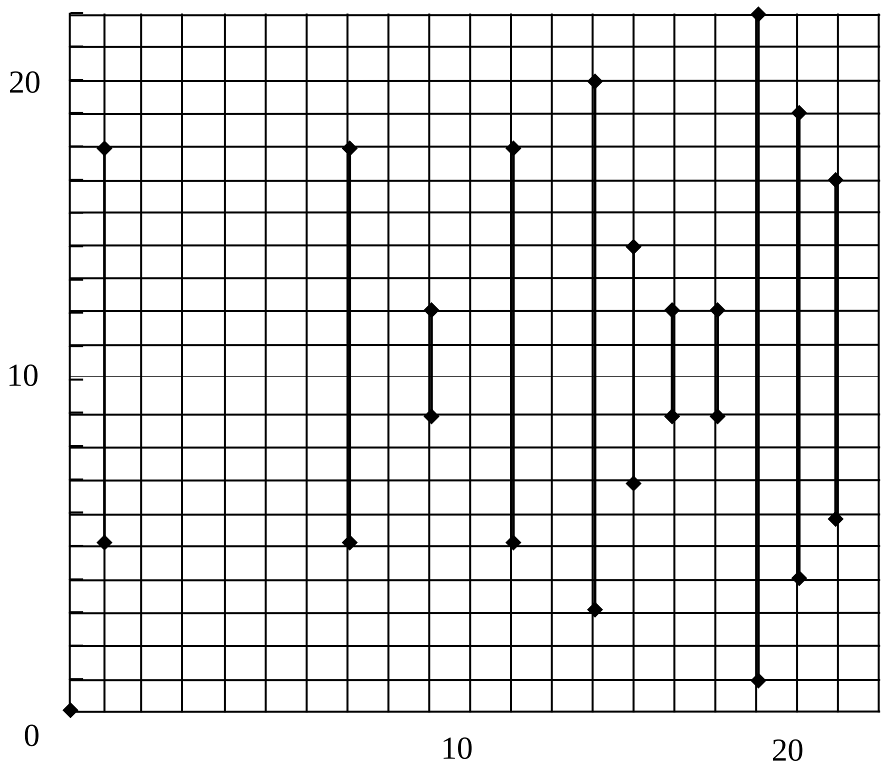
The point (9,5) belongs to this group due to their coordinates satisfies to the elliptic curve equation $y^2=x^3+x$ *mod* 23. Really, substituting the values x=9 and y=5, the next calculation can be done

5^2 *mod* 23 = 9^3 + 9 *mod* 23,
25 *mod* 23 = 729 + 9 *mod* 23,
25 *mod* 23 = 738 *mod* 23,
2 = 2.

The elliptic group $E_{23}(1,0)$ has 23 following points

{O (0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5) (13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)}.

Graphical presentation of the above described elliptic group $E_{23}(1,0)$ is shown below.



Note that there are two points for every x value. Even though the graph seems random, there is still symmetry about y=11,5. Recall that elliptic curves over real numbers, there exists a negative point for each point which is reflected through the x-axis. over the finite field, the negative components in the y values are taken modulo 23, resulting in a positive number as a difference from 23. Here $–P=(x_P,(-y_P \; mod \; 23))$. If P=(1,5), then $–P$=(1,(-5 *mod* 23))= (1,18).

The number of points in elliptic group is bounded according to the inequality ***Hassego.***

$M+1-2M^{1/2} \leq \#E_M(a,b) \leq M+1+2M^{1/2}$.

Consider the next example of the elliptic curve group.

Example For example, let M=5 and $y^2=x^3+1 \; mod \; 5$, what can be describe as $E_5(0,1)$. In this case a=0, b=1 and $4\times0^3+27\times1^2$ (*mad* 5) = 2 $\neq$ 0, it means that we can construct the elliptic group $E_5(0,1)$ with the six points.

$$E_5(0,1) = \{O, (0,1), (0,4), (2,2), (2,3), (4,0)\}.$$

$$5 + 1 – 2\times5^{1/2}= 2 \leq \#E_5(0,1) = 6 \leq 5 + 1 + 2\times5^{1/2} = 10.$$

2. *Arithmetic in an Elliptic Curve group*

Elliptic curve group have a finite number of points, which is a desirable property for cryptographic purposes. Since these curves consists of a few discrete points, it is not clear how to “connect the dots” to make their. However, there are algebraic rules for elliptic curve groups.

1. ***Adding distinct points*** $P=(x_P,y_P)$ and $Q=(x_Q,y_Q)$.

If P and Q are distinct points such that P is not $–Q$, then $P+Q=R$ where

$$s = (y_P – y_Q)/(x_P – x_Q) \; mod \; M;$$

$$x_R = s^2 - x_P - x_Q \ mod\ M;$$
$$y_R = -y_P + s(x_P - x_R) \ mod\ M;$$

2. ***Doubling the point*** *P*. Provided that y_P is not 0, $2P=R$ where

$$s = (3x_P^2 + a)/(2y_P) \ mod\ M;$$
$$x_R = s^2 - 2x_P \ mod\ M;$$
$$y_R = - y_P + s(x_P - x_R) \ mod\ M;$$

Recall that *a* is one of the parameters chosen with the elliptic curve.

Example. In the elliptic group $E_{23}(9,17)$ defined by $y^2=x^3+9x+17$ *mod* 23 for the point $P=(16,5)$ determine $2P=P+P$.

$s = (3x_P^2 + a)/(2y_P)$ *mod M* $= (3\times16^2+9)/(2\times5)$ *mod* 23;

then $10s=18$ *mod* 23;

$s=18\times10^{\varphi(23)-1}$ *mod* 23 $= 18\times10^{21}$ *mod* 23 =11.

$x_R = s^2 - 2x_P$ *mod M* $= (11^2 - 2\times16)$ *mod* 23=20;

$y_R = - y_P + s(x_P - x_R)$ *mod M* $= -5+11(16 - 20)$ *mod* 23 = −49 *mod* 23 = −3 *mod* 23 = 20;

As the result $2P=(20,20)$.

For two pints $P=(16,5)$ and $Q=2P=(20,20)$ determine $R=P+Q=3P$.

$s = (y_P - y_Q)/(x_P - x_Q)$ *mod M* $= (5-20)/(16-20)$ *mod* 23; then $4s = 15$ *mod* 23;

$s=15\times4^{\varphi(23)-1}$ *mod* 23 $= 15\times4^{21}$ *mod* 23 = 2.

$x_R = s^2 - x_P - x_Q$ *mod M* $= (2^2 - 16 - 20)$ *mod* 23 = −9 *mod* 23 = 14;

$y_R = -y_P + s(x_P - x_R)$ *mod M* $= - 5 + 2(14-16)$ *mod* 23= −9 *mod* 23 = 14;

As the result $R = 3P = (14,14)$.

Example. Consider the addition of two points $P=(0,1)$ and $Q=(2,2)$, belonging to the elliptic group $E_5(0,1)$. The following conditions are holds true $(0,1)\neq(2,2)$ and $(2,2) \neq -(0,1)$, the first case for addition should be used. Then $s = (y_P - y_Q)/(x_P - x_Q)$ *mod M* $= (1-2)/(0-2)$ *mod* 5. As the result $2s=1$ *mod* 5 and $s=3$.

The resulting point $R=(x_R,y_R)$ has the coordinates:

$x_R = s^2 - x_P - x_Q$ *mod M* $= (3^2-0-2)$ *mod* 5=2;

$y_R = -y_P + s(x_P - x_R)$ *mod M* $= -1+3(0-2)$ mod 5 = −7 mod 5=3.

The final result is $R = (x_R,y_R) = (2,3)$.

Example. Consider the doubling of the point $P = (2,2)$, belongs to group $E_5(0,1)$. Due to (2,2)=(2,2), the second case for addition should be chosen. Then $s = (3x_P^2 + a)/(2y_P)$ *mod M* $= (3\times2^2+0)/(2\times2)$ *mod* 5 = 3. The resulting point $2P = R=(x_R,y_R)$ is:

$x_R = s^2 - 2x_P$ *mod M* $=(3^2-2\times2)$ *mod* 5=0;

$y_R = - y_P + s(x_P - x_R)$ *mod M* $= -2+3(2-0)$ *mod* 5 = 4.

$R=(x_R,y_R) = (0,4)$.

Example. Consider the addition of two points $P = (2,2)$ and $-P = (2,3)$, belonging to the elliptic group *E*5(0,1). The following conditions is true (2,2) = − (2,3). The resulting point is *O*. Formally this results can be recognized from first step of calculation:

$s = (y_P - y_Q)/(x_P - x_Q)$ *mod M* $= (2-3)/(2-2)$ *mod* $5=\infty$.

Then (2,2) + (2,3) = *O*.

3. *The Point Order Determination*

In a case of the elliptic group $E_5(0,1)$ with the six points {*O*, (0,1), (0,4), (2,2), (2,3), (4,0)}all possible results for both operation addition and doubling are shown in the table

+	O	(0,1)	(0,4)	(2,2)	(2,3)	(4,0)
O	O	(0,1)	(0,4)	(2,2)	(2,3)	(4,0)
(0,1)	(0,1)	(0,4)	O	(2,3)	(4,0)	(2,2)
(0,4)	(0,4)	O	(0,1)	(4,0)	(2,2)	(2,3)
(2,2)	(2,2)	(2,3)	(4,0)	(0,4)	O	(0,1)
(2,3)	(2,3)	(4,0)	(2,2)	O	(0,1)	(0,4)
(4,0)	(4,0)	(2,2)	(2,3)	(0,1)	(0,4)	O

If we carry on computing $P+P+P+\ldots$ for long enough, since the number of curve points is finite, we must eventually get a result O. We will certainly have $\delta P=\beta P$ for some a and b with $\beta>\delta$. This implies that $cP=O$ where $c=\beta-\delta$The least c for which this is true is called the ***order of the point***.

Results of the addition points $P+P+P+\ldots$ for $E_5(0,1)$.

+	(0,1)	(0,4)	(2,2)	(2,3)	(4,0)	(4,0)
P	(0,1)	(0,4)	(2,2)	(2,3)	(4,0)	(4,0)
2P	(0,4)	(0,1)	(0,4)	(0,1)	O	(2,2)
3P	O	O	(4,0)	(4,0)	(4,0)	(2,3)
4P	(0,1)	(0,4)	(0,1)	(0,4)	O	(0,1)
5P	(0,4)	(0,1)	(2,3)	(2,2)	(0,4)	(0,4)
6P	O	O	O	O	O	O

For ***example*** point P = (0,1) has the order c=3.

4. *Elliptic curve discrete logarithm problem*

In the multiplicative group, the discrete logarithm problem is:

Given elements r and q of the group, and a prime p, find a number k such that $r=q^k \mod p$.

If the elliptic curve groups is described using multiplicative notation, then the elliptic curve discrete logarithm problem is:

Given points *P* and *Q* in the group, find a number *k* that *kP=Q;*
***k* is called the discrete logarithm of *Q* to the base *P*.**

Example In the elliptic group defined by $y^2=x^3+9x+17 \mod 23$ What is the discrete logarithm k of Q=(4,5) to the base P=(16,5)?

One (naive) way to find k is to compute multiples of P until Q is found. The first multiples of P are: P=(16,5), 2P=(20,20), 3P=(14,14), 4P=(19,20), 5P=(13,10), 6P=(7,3), 7P=(8,7), 8P=(12,17), 9P=(4,5). Since 9P=(4,5)=Q, the discrete logarithm of Q to the base P is k=9.

In real application, *k* would be large enough such that it would be infeasible to determine *k* in this manner.

Example. Based on elliptic curve $y^2=x^3+10x+10$ and M=23 define the elliptic group $E_{23}(10,10)$ with the generating point $G = G(x,y) = G(5,1)$. The result of the operation kG in $E_{23}(10,10)$ are shown below

k	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
kG	(5,1)	(8,21)	(11,5)	(10,11)	(12,8)	(7,20)	(15,19)	(9,1)	(9,22)
k	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*
kG	(15,4)	(7,3)	(12,15)	(10,12)	(11,18)	(8,2)	(5,22)	(*O*)	(5,1)

5. *Key Exchange in Elliptic Curve Group*

First of all the prime number $M \approx 2^{180}$ as well as the parameters of a and b for the elliptic curve to define the elliptic group $E_M(a,b)$ Then the generating point $G = G(x,y)$ should be chosen such a way that c, for which $cG=O$, is a very lager prime number. The parameters $E_M(a,b)$ and G with c are open for everybody.

Key exchange procedure in between the user A and B.

1.User ***A*** takes the integer number n_A, that $n_A < c$. n_A is ***secret key*** for user ***A***. Then ***A*** generate an ***open key*** $P_A = n_A G$, Note, that P_A is the point over $E_M(a,b)$.

2. User ***B*** repeats the same to get their own secret key n_B and open P_B key.

3. User ***A*** sends to ***B*** his open key P_A, and ***B*** to ***A*** his P_B.

4. User ***A*** generates common secrete key as $K= n_A\, P_B$, as well as user ***B*** generate the same common secrete key as $K= n_B\, P_A$.

It is easy to show that $n_A\, P_B = n_A\, (n_B\, G) = n_B\, (n_A\, G) = n_B\, P_A$.

To break this system the third part should calculate the value k (n_A or n_B) based on G and kG, where k is n_A or n_B

Example. Let M=23 and $E_{23}(10,10)$ and generating point is $G=G(5,1)$ with the order c equal to 17.

1. Secret key for user ***A*** is $n_A = 2 < c = 17$, the open key $P_A = n_A\, G = 2(5,1) = (8,21)$.

2. Secret key for user ***B*** is $n_B = 3 < c = 17$, the open key $P_B = n_B\, G = 3(5,1) = (11,5)$.

3. Based the open communication channel the user ***A*** sends to ***B*** $P_A = (8,21)$ and ***B*** to ***A*** his key $P_B = (11,5)$.

4. Common secrete key $K= n_A\, P_B = n_B\, P_A = 2(11,5) = 3(8,21) = (7,20)$.

6. *Elliptic Curve Group Cryptosystem*

There are several approaches to apply the Elliptic Curve Group to modern Cryptographic systems. The most straightforward solution can be described as follows.

First step is the coding the message to be send m as a point $Pm=Pm(x,y)$ of the Elliptic group. The first problem is the limitation of the Elliptic group point values. There are not all possible meaning of x and y within the defined Elliptic group $E_M(a,b)$.

As in the key exchange algorithm: The parameters $E_M(a,b)$ and G with the value of c are open for everybody. Both users ***A*** and ***B*** generate their keys: secret (n_A ,n_B), and public (P_A, P_B), where $P_A = n_A\, G$, and $P_B = n_B\, G$.

<u>Enciphering</u>

To send the message $Pm=Pm(x,y)$ from ***A*** to ***B.***

1. User ***A*** generates random integer number $k < c$.

2. User ***A*** calculates the point kG.

3. User ***A*** calculates the point kP_B based on open key P_B of the user B.

4. User ***A*** calculates the sum $Pm+ kP_B$ based on two points Pm and P_B. The user ***A*** masked their message Pm by the addition to the point kP_B

5. User ***A*** determines the ciphertext as $Cm = (kG, Pm+ kP_B)$, which also consists of two points.

<u>Deciphering</u>

To decipher ciphertext $Cm = (kG, Pm+ kP_B)$ ***B*** have to calculate.

1. User ***B*** multiply the first point kG of Cm by their secret key n_B to get n_B (kG).

2. User ***B*** subtract the result $n_B(kG)$ from the second point of Cm. Then,

$Pm + kP_B - n_B(kG)=Pm + k(n_BG) - n_B(kG) = Pm.$

Example. Let M=23 and $E_{23}(10,10)$ and generating point is $G=G(5,1)$ with the order c equal to 17. User ***A*** sent to ***B*** the message encoded as a point P_m=(15,4).

User ***B*** ***Secret key*** is n_B = 3, and ***Public key*** – P_B= n_BG=3(5,1)=(11,5)

<u>Enciphering</u>

1. User ***A*** randomly generates $k = 7 < c = 17$.

2. Using the point G ***A*** obtained kG = 7(5,1) = (15,19).

3. Based on user's ***B*** public key P_B = (11,5), user A calculate kP_B= 7(11,5) = (10,11).

4. User ***A*** determine the value P_m+kP_B = (15,4) + (10,11) = (11,18).

5. User ***A*** sends to user ***B*** ciphertext C_m=((15,19), (11,18)).

<u>Deciphering</u>

To decipher ciphertext C_m = ((15,19), (11,18)) ***B*** have to calculate.

1. User ***B*** based on the first point kG = (15,19) elliptic group $E_{23}(10,10)$ and his own secret key n_B=3 determine $n_B(kG)$ = 3(15,19) = (10,11).

2. User ***B*** subtract the result $n_B(kG)$=(10,11) from the second point of C_m. Then, $(P_m+kP_B) - (n_B(kG))$ = (11,18) − (10,11) = (11,18) + (10,-11) = (11,18) + (10,12) = (15,4).

7. *Digital Signature Algorithm ECDSA*

The digital signature algorithm ***ECDSA*** is standardized in 2005.

1.***Preparation Phase***

The ***open parameter*** for everybody are: Elliptic group $E_M(a,b)$ and generating point G of order c. The Hash function $H(M)$ also is an open

The sender has to generate:

Private key n_A and ***Public key*** P_A

2. ***Signing***

The user ***A*** signs the message M.

1. User ***A*** chooses a random number k, $1<k<c$-1.

2. ***A*** computes $kG=(x_1,y_1)$ and $r=x_1$ *mod c*. The number r is an integer number $0 \le r \le c$-1. In a case when r=0 ***A*** returns again to step 1.

3. ***A*** computes k^{-1} *mod c*.

4. On the bases of function $H(M)$ and the message M, ***A*** computes $m = H(M)$.

5. ***A*** computes $s=k^{-1}(m+n_Ar)$ *mod c*. If s=0, then ***A*** returns again to step 1.

6. ***A***'s signature for M is the pair (r,s).

3.***Signature Verification***

The verifier ***B*** have got the message M with the signature (r,s). He has the access to elliptic group $E_M(a,b)$, and generating point G of order c. The Hash function $H(M)$ also is available for him.

1. Based on the Hash function $H(M)$ user ***B*** calculate $m = H(M)$.

2. ***B*** verifies that the integers (r,s) belongs to interval from 1 to c-1.

3. ***B*** computes $w=s^{-1}$ *mod c.*

4. ***B*** computes $u_1=mw$ *mod q* and $u_2=rw$ *mod c.*

5. ***B*** computes $u_1G+u_2P_A=(x_1^*,y_1^*)$ and $r^*=x_1^*$ *mod c.*

6. If $r^* \neq r$ the signature is rejected and if $r^* = r$ the signature is adopted.

Example. Let the Elliptic group is define by the elliptic curve $y^2=x^3+10x+10$ *mod* 23. Then $E_{23}(10,10)$ with the generating point G=(5,1) of order c=17.

The user A generates his secret key n_A=7 and open key $P_A=n_AG$=7(5,1) as follows:

$2G=2(5,1) \rightarrow \{s=(3x_G^2+a)/(2y_G)$ *mod* $23 = (3\times5^2+10)/(2\times1)$ *mod* $23=8$. $x_R=s^2-2x_G$ *mod* $23=8^2-2\times5$ *mod* $23=8$. $y_R= - y_G+s(x_G - x_R)$ *mod* $23= -1 + 8(5-8)$ *mod* $23 =21\}$. $2G=7(5,1)=(8,21)$. $4G = 2(2G) = 2(8,21) = (10,11)$. $6G = 4G + 2G = (10,11) + (8,21) = (7,20)$; $7G = 6G + G = (7,20) + (5,1) = (15,19)$.

Public key $P_A = n_AG = 7(5,1) = (15,19)$.

2. *Signing*

The user ***A*** signs the message M.

1. User ***A*** chooses a random number $k = 3$, $1< k = 3<c-1 = 16$.
2. ***A*** computes $kG = 3G = 3(5,1) = (11,5)$ and $r=x_1$ *mod* $c=11$ *mod* $17 = 11$, $(r=11)$.
3. A computes k^{-1} *mod* $c=3^{-1}$ *mod* $17 =6$.
4. On the bases of function $H(M)$ and the message M, ***A*** computes $m = H(M)$. Let $m = 5$.
5. ***A*** computes $s=k^{-1}(m+n_Ar)$ *mod* $c = 6(5 + 7\times11)$ *mod* $17 = 16$.
6. ***A***'s signature for M is the pair $(r,s) = (11,16)$.

3. *Signature Verification*

The verifier ***B*** have got the message M with the signature $(r,s)=(11,16)$. He has the access to elliptic group $E_M(a,b)=E_{23}(10,10)$, and generating point $G=(5,1)$ of order $c=17$. The Hash function $H(M)$ also is available for him.

1. Based on the Hash function $H(M)$ user ***B*** calculate $m = H(M) = 5$.
2. ***B*** verifies that the integers $(r,s) = (11,16)$ belongs to interval from 1 to 16.
3. ***B*** computes $w = s^{-1}$ *mod* $c = 16^{-1}$ *mod* $17 = 16$.
4. ***B*** computes $u_1=mw$ *mod* $c = 5\times16$ *mod* $17 = 12$ and $u_2=rw$ *mod* $c = 11\times16$ *mod* $17 = 6$.
5. ***B*** computes $u_1G+u_2P_A= 12(5,1) + 6(15,19) = (x_1^*,y_1^*) = (11,5)$ and $r^* = x_1^*$ *mod* $c = 11$ *mod* $17 = 11$.
6. $r^* = r$ then signature is adopted.

PS_#3 (2 hours)

Problems to be solved:

1. For given $M = 23$ and $a =$ design the Elliptic Group.
2. Select the random value of $b < M$ for which two positive integer numbers given a and randomly chosen b, are satisfying to the inequality $4a^3 + 27b^2 \neq 0$ (*mod* ***M***),
3. For your value of a and b, implement the software application for Elliptic Group elements (points) generation (see section 1).
4. Implement the Arithmetic (***Adding distinct points*** $P = (x_P,y_P)$ and $Q = (x_Q,y_Q)$ and ***Doubling the point*** $P=(x_P,y_P)$) in an Elliptic Curve group (see section 2).
5. Determine the generation point G with the order c represent by big prime number (see section 3).

PS_#4 (2 hours)

Problems to be solved:

Based on the results have been obtained within the framework of the PS_#3.

1. Implement the ***Key Exchange procedure in Elliptic Curve Group*** (see section 5).
2. Implement ***Digital Signature Algorithm ECDSA*** (see section 7).