POLITECNICO DI MILANO, DEIB

Network Security and Cryptography

Giulia Mauri
email: *giulia.mauri@polimi.it*
website: *http://home.deib.polimi.it/gmauri*

June 10, 2015

Exercise 1. TDE 07/07/09
Consider the following game. Alice and Bob choose the elliptic curve $E : y^2 = x^3 + 9x + 1 \pmod{31}$, with $N = 35$ points. Alice chooses a secret number pair a, a' such that $aa' = 1 \pmod{N}$. Bob chooses a secret number pair b, b' such that $bb' = 1 \pmod{N}$. Moreover, they take two points on the curve $P_1 = (14, 22), P_2 = (5, 4)$.

1. Bob computes $B_1 = bP_1, B_2 = bP_2$. He sends the points to Alice with a random order.
2. Alice chooses one between B_1 and B_2, computes $C = aB$ and sends it to Bob.
3. Bob computes $D = b'C$ and sends it to Alice.
4. Alice computes $E = a'D$. Alice wins if $E = P_2$.

Do the following:

1. Compute, if they exist, all the points with coordinate $x = 20$.
2. What values can E assume and why?
3. What conditions should respect the secret numbers a, b? Knowing that $a = 2$, compute a'.
4. At step 1., Bob presents $B = (25, 17)$ and $B = (15, 16)$. Suppose Alice chooses $B = (25, 17)$. Compute C.
5. Using C from previous step, Bob computes $D = (12, 15)$. Verify if Alice has won.

6. Compute b using BSGS.
7. Compute the order of points P_1, P_2.
8. Alice doesn't know the b value and she can't compute it. Explain how she can cheat.
9. **SAGE** Write the commands to define the elliptic curve, to find how many point it has, and to find the order of the points P_1 and P_2.

Solution.
1. $(20,20)$ and $(20,11)$
2. $E = a'D = a'b'C = a'b'aB_i = a'b'abP_i$
3. a, b should be prime with respect to 31. $a^{-1} = 18$
4. $C = (14,9)$
5. $E = a'D = 18(12,15) = (14,22)$ that isn't equal to P_2. Alice looses.
6. $b = 3$
7. P_1 order is 7, P_2 order is 5.
8. The order of B should be a divisor of the order of P_2.
9. E = EllipticCurve(Zmod(31),[9,1]);
   E.cardinality();
   P_1 = E(14,22);
   P_1.order();
   P_2 = E(5,4);
   P_2.order();

Exercise 2. TDE 04/09/09
Alice uses the following signature scheme like ECDSA. Alice publishes the curve $y^2 = x^3 + 7x + 1 \pmod{31}$, with $N = 26$ points. She chooses the base point A (of order $q = 13$), the secret number a and computes $B = aA$. Alice publishes $A = (1,3), B = (9,7)$. Then Alice signs the message m, she chooses the nonce k and computes $R = (x_R, y_R) = kA, \quad s = k^{-1}(m + ax_R) \bmod q$.

1. Find the smallest x value with $x \geq 7$ which corresponds to a point on the curve. Compute the corresponding y.
2. Compute the order of B.
3. Write the equations for signature verification and verify the correctness.
4. Alice publishes the signed message $(m \| R \| s) = (11 \| (11,13) \| 4)$. Verify the signature.
5. Then, Alice publishes $(m \| R \| s) = (7 \| (11,13) \| 5)$. Solve the equation $B = aA$ usign BSGS. Finally, compute a using the repeated nonce.

6. **SAGE** Write the commands to define the elliptic curve, and to compute the DSA signature.

Solution. 1. The smallest is $x = 9$ which corresponds to $(9,7)(9,24)$.

2. The order is 13.

3. $u_1 = s^{-1}m \quad u_2 = s^{-1}x_R$ and $V = u_1A + u_2B$ and must be equal to R.

4. $u_1 = 6 \quad u_2 = 6 \quad V = 6(1,3) + 6(9,7) = (11,13)$.

5. $a = 7$
   $(s_1 - s_2)k = (m_1 - m_2) \rightarrow k = 9 \rightarrow a = (s_1k - m_1)x_R^{-1} = 7$

6. E = EllipticCurve(Zmod(31),[7,1]);
   A = E(1,3); k = 9; q = 13; m = 11; a = 7;
   R = k * A; (x,y,z) = R;
   kinv = mod(k^(-1),q);
   s = mod(kinv*(m+int(x)*a),q)

Exercise 3. TDE 22/06/10
Consider the elliptic curve E with equation

$$E : y^2 \equiv x^3 + x + 1 \pmod{11}$$

with the base point $P = (4,5)$. The curve has 14 points.
Alice and Bob use the ECDHKE. Alice chooses the secret number $a = 3$ and receives from Bob the point $B = bP = (2,0)$. At the end of the protocol, Alice and Bob share a secret point, S, with coordinates (x_S, y_S). From that point they obtain a secret key, k, as follows:

$$k = 2x_S + (y_S \bmod 2)$$

if $S = \infty$, then $k = 22$.

1. Find, if they exists, the point with coordinates $x = 5$ and $x = 8$.

2. Compute the order of point P.

3. Compute the point A sent by Alice.

4. Compute the key k.

5. Using PH algorithm, compute the secret number b.

6. Given B from Bob, how many different keys is it possible to obtain? Which are they?

7. **SAGE** Write the commands to define the elliptic curve, to list all the points on the curve, and to define the infinity point. Which is the output of the last command?

Solution. 1. For $x = 5$, we have $y^2 = 10$. Since $10^5 \bmod 11 = -1$, there are no corresponding value. For $x = 8$, we have $y^2 = 4$. Since $4^5 \bmod 11 = 1$, there are two points with coordinate $y = 4^3 \bmod 11 = \pm 9$.

2. The order of P could be 2, 7, 14.

$$2P = (6,5)$$
$$7P = (2,0)$$

So the order of P is 14.

3. $A = aP = 3(4,5) = (1,6)$.

4. $S = aB = 3(2,0) = (2,0)$ from that $k = 4$.

5. $b = 7$.

6. The order of B is 2, so two keys are possible $k = 22$, $k = 4$.

7. E = EllipticCurve(Zmod(11),[1,1]);
E.points();
inf = E(0); » (0 : 1 : 0)

Exercise 4. TDE 20/07/09
Alice uses a cryptosystem like ECIES. She publishes the curve $E : y^2 = x^3 + 3x - 1 \pmod{23}$, with $N = 33$ points and the base point $A = (2,6)$. Alice chooses a secret number $a = 4$ and publishes the point $B = aA = (14,5)$. Bob chooses a nonce k and computes $R = kA = (21,13)$, $S = kB$, the point S is the session key. Bob sends the point R and the message m ciphered with the session key to Alice. Alice uses the same curve and the same points A, B for the ElGamal digital signature. Alice chooses a nonce k and sends $R = kA$, $s = k^{-1}(h(m) - ar) \bmod N$, where r is the x_R coordinate and the hash function is cryptographically secure.

1. Find the points corresponding to the coordinates $x = 4, 7, 15$, if they exist.

2. Compute the order of the group generated by A.

3. Write the formulas used by Alice to compute session key. Then compute S.

4. Compute k using Pohlig-Hellman.

5. Eve chooses two random numbers u, v and computes $R = vB + uA$, $s = -rv^{-1} \bmod N$. Verify that R, s is a valid signature for the hash $h(m) = su \bmod N$.

6. Supposing $u = 7$, $v = 1$, compute $h(m)$.

7. Supposing Eve wants to falsify a signature for the message m'. Compute the success probability of the attack.

8. **SAGE** Write the command to define the elliptic curve, to compute the order of A, and to compute the session key.

Solution. 1. $x = 4 \rightarrow (4,12), (4,11)$
$x = 7 \rightarrow (7,8), (7,15)$
$x = 15 \rightarrow nopoints$.

2. The order of A is 33.

3. $S = (20,3)$.

4. $k = 12$.

5. $rB + sR = h(m)A \rightarrow rB - rv^{-1}vB + suA = suA$ is verified.

6. $h(m) = 26$
$R = vB + uA = (1,7)$

7. $h(m) \in \mathbb{Z}_N$ so the success probability is $1/33 = 3\%$.

8. E = EllipticCurve(Zmod(23),[3,-1]);
A = E(2,6); B = E(14,5);
A.order();
k = random.randint(2,q);
S = k*B

Exercise 5. TDE 23/06/10
Alice uses a DSA digital signature scheme. She chooses the elliptic curve:

$$E : y^2 \equiv x^3 - 5x - 3 \pmod{23}$$

with the base point $A = (18,9)$, of order 11. Alice chooses a secret number a, and computes the public number $B = aA = (4,15)$.
Alice signs the message $m = 4$ and obtains the signature $\{R = (10,21), s = 7\}$.

1. Compute the point with $x = 5$ and $x = 3$.

2. Verify Alice's signature.

3. Compute the order of point B.

4. Using Baby Step Giant Step compute a.

5. Knowing that Alice signs another message $m' = 6$ obtaining the signature $\{R' = (10,21), s' = 4\}$, find a using the repeated nonce attack.

6. **SAGE** Write the commands to define the elliptic curve, to compute the babysteps and the giantsteps.

Solution. 1. $(3, \pm 3)$

2.

$$u_1 = 10$$
$$u_2 = 3$$
$$u_1 A + u_2 B = (10,21) = R$$

3. The order can be only 11.

4. $a = 5$

5. From $k(s-s') = (m-m')$ we have $k = 3$. From $ar = ks - m$ we have $a = 5$.

6. E = EllipticCurve(Zmod(23),[-5,-3]);
   N = ceil(sqrt(11));
   A = E(18,9); B = E(4,15);
   C = N*(-A);
   babystep = 0*(N+1) #define a zeros vector
   for i in range(1,N+1):
   ——babystep[i] = A + babystep[i-1]
   giantstep = 0*(N+1) #define a zeros vector
   giantstep[0] = B
   for j in range (1,N+1):
   ——giantstep[j] = giantstep[j-1] + C

Exercise 6. TDE 24/07/08
Alice and Bob use the ECDHKE protocol on the elliptic curve:

$$E : y^2 = x^3 + 2x + 5 \bmod 11$$

and choose the point P = (0, 4) on the curve with $n = 10$ points. Alice chooses the secret number $a = 7$ and sends to Bob the point $A = aP = (3,7)$. Bob sends to Alice the point $B = bP = (8,7)$. After the exchange, Alice sends to BoB the message $m = 11$, signed with the ElGamal digital signature, where $R = A = aP = (3,7)$ and $s = a^{-1}(m - bx_R) \bmod n = 7$.

1. List the points on the curve, if they exist, that correspond to the coordinate $x = 3, 8, 10$.
2. Compute the coordinates of the secret point SS obtained by Alice and Bob at the end of the protocol.
3. Using Pohlig-Hellman algorithm, find the value of b.
4. Verify the Alice signature.
5. **SAGE** Write the functions to simulate the ECDHKE.

Solution. 1. $x = 3 \rightarrow (3,4), (3,7)$
$x = 8 \rightarrow (8,4), (8,7)$
$x = 10 \rightarrow nopoints.$

2. $SS = (9,9)$

3. $b = 4$

4. $V_1 = xB + sR = (0,4)$
   $V_2 = mP = (0,4)$.

5. def function1 (E,P):
   ——x = random.randint(2,10)
   ——X = aP
   ——return x, X

   def function2 (x,X):
   ——sharedsecret = x * X
   ——return sharedsecret

   E = EllipticCurve(Zmod(11),[2,5]);
   P = E(0,4)
   Alice: (a,A) = function1(E,P)
   Bob: (b,B) = function1(E,P)
   Alice: ss_A = function2(a,B)
   Bob: ss_B = function2(b,A)

Exercise 7. TDE 12/07/10
Consider the Diffie-Hellman key exchange with $q = 47$ and $g = 5$. Alice sends the message $A = 31$. Bob sends the message $B = 23$. At the end of the protocol, Alice and Bob use the key k to cipher the messages with a shift cipher.
Eve is an active attacker that makes a Man-in-the-Middle attack. Suppose the attack is successful. Eve chooses his secret number $o = 4$.

1. What properties should q, g have? Verify the properties.

2. Alice wants to send the message $m = 1$, that Eve doesn't modify. Write the corresponding ciphered message sent by Alice and received by Bob.

3. To avoid the attack, A and B are pre-distributed to the participants. What are the lacks of this choice?

4. Explain how to avoid the attack with no pre-distribution

5. **SAGE** Write the functions to simulate the DHKE.

Solution. 1. q should be a large prime: it is a prime (verify with Fermat) but it is small. g should be a primitive generator of $\mathbb{Z}_q$ so it should have the same order of q. The order is 46 so it is a generator.

2. See corresponding TDE for the picture.
   $K_{AO} = 18, K_{OB} = 3$.
   $C_{AO} = K_{AO} + m = 19, C_{OB} = K_{OB} + m = 4$.

3. K_{AB} reamains the same, it doesn't change.
   If there are many participants, the pre-distribution requires a considerable amount of time.

4. Adding a mutual authentication as the full STS protocol do. However, this requires a digital signature scheme and a public key infrastructure.

5. def function1 (q, g):
   ——x = random.randint(2, q-1)
   ——X = mod(g^x, q)
   ——return x, X

   def function2 (x,X):
   ——sharedsecret = mod(X^x, q)
   ——return sharedsecret

   q = 47; g = 5
   Alice: (a,A) = function1(q,g)
   Bob: (b,B) = function1(q,g)
   Alice: ss_A = function2(a,B)
   Bob: ss_B = function2(b,A)

Exercise 8. TDE 12/07/10
Alice uses an ElGamal digital signature. Alice publishes $p = 113, \alpha = 3, y = \alpha^a = 54$. Then, Alice signs the message $m_1 = 7$ and obtains $(r_1, s_1) = (21, 28)$.

1. Compute the order of the group generated by α
2. Verify the signature.
3. Compute a using BSGS.
4. Compute a using PH.
5. **SAGE** Write the commands to simulate PH.

Solution. 1. The order is 112.

2. $v_1 = y^r r^s = 40$
   $v_2 = \alpha^m = 40$.
   The signature is verified.

3. $a = 15$

4. $a = 15$

5. p = 113; q = p-1; g = 3; y = 54;
   q.factor() »2^4*7
   qi = [16,7];
   x = 0;
   xi = 0*2; zi = 0*2; yi = 0*2;
   for i in range (2):
   ——xi[i] = log(mod(y,p),mod(g,p))
   ——print xi
   »15 1
   for i in range (2):
   ——zi[i] = q/qi[i]
   ——yi[i] = mod(zi[i]^(-1),qi[i])
   ——x = x + zi[i] * yi[i] * xi[i]
   a = mod(x,q)