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 17/06/2013
Alice uses the DSA signature scheme on the elliptic curve $E : y^2 = x^3 + 3x + 4 \bmod 11$ to sign messages m_i. The curve has $n = 14$ points.
Alice publishes the base point $A = (8,1)$ (of order q) and the point $B = aA = (0,2)$.

1. Verify whether A satisfies the condition required by DSA signature.
2. Find all the points on the curve E with $x = 4,6,7$, if they exist.
3. Alice publishes the signed message $(m_1 \| R_1 \| s_1) = (5 \| (4,6) \| 6)$. Write the equations for signature verification and verify the correctness. Then, verify Alice's signature.
4. Compute a using the BSGS algorithm.
5. Alice signs another message $m_2 = 3$ and publishes $(m_2 \| R_2 \| s_2) = (3 \| (4,6) \| 3)$. Which mistake did she do? Taking advantage from Alice's mistake, compute a.
6. **SAGE** Write the commands to define the elliptic curve, to find how many points it has, and to compute the DSA signature.

Solution. 1. The A order, q, must be a large prime factor of n. It could be 2 or 7. So, we compute $2A = 2(8,1) = (0,9)$ and $7A = 7(8,1) = \infty$. The order of A is 7.

2. $(4,5), (4,6), (7,4), (7,7)$. No points for $x = 6$.

3. $u_1 = s^{-1}m \quad u_2 = s^{-1}x_R$ and $V = u_1 A + u_2 B$ that must be equal to R.
   $u_1 = 2 \quad u_2 = 3$ and $V = 2A + 3B = (0,9) + (8,1) = (4,6)$.

4. $N = \lceil \sqrt{14} \rceil = 4$, $-NA = 4(8,10) = (4,6)$
   $iA = \infty, (8,1), (0,9), (4,6), (4,5)$
   $B + j(-NA) = (0,2), (8,1), \ldots$
   $a = i + jN \bmod n = 1 + 1 \cdot 4 = 5$.

5. The repeated nonce.
   $s_1 k - m_1 = a x_R = s_2 k - m_2$
   $(s_1 - s_2)k = (m_1 - m_2)$
   $k = (m_1 - m_2)(s_1 - s_2)^{-1} \bmod q = (5-3)(6-3)^{-1} \bmod 7 = 2 \cdot 5 \bmod 7 = 3$
   $a = (s_1 k - m_1) x_R^{-1} \bmod q = (6 \cdot 3 - 5) \cdot 4^{-1} \bmod 7 = 5$.

6. **SAGE**
```
E = EllipticCurve(Zmod(11),[3,4]);
E.cardinality();
A = E(8,1); q = 7; k = 3; m = 6; a = 5;
R = k*A; (x,y,z) = R;
kinv = mod(k^(-1), q);
s = mod(kinv*(m + a*int(x)),q);
```

Exercise 2. TDE 25/06/2013
Alice and Bob agree on a common secret using the Diffie-Hellman Key Exchange protocol. They publish the elliptic curve $E : y^2 = x^3 + 9x + 1 \bmod 23$. The curve has $n = 21$ points. They also publish the base point $P = (3,3)$.
Alice sends the message $A = N_A P = (16,20)$ and receives the message $B = N_B P = (2,2)$.
She computes the shared secret S and from that point she obtains a secret key k_A as follows: $k_A = x_S + y_S \bmod q$, where $q = 3$ is the order of B. If S is ∞, then $k_A = 15$.

1. Verify if P is a primitive generator.
2. List all the points on curve E with $x = 9, 18$, if they exist.
3. Compute N_A using the PH algorithm.
4. Compute the shared secret S.
5. Compute the Alice's key k_A. How many keys it's possible to obtain, why? Which are they?
6. **SAGE** Write the commands to define the elliptic curve and the functions to simulate the ECDHKE.

Solution. 1. The order of P should be 21.
   $3P = 3(3,3) = (6,8)$
   $7P = 7(3,3) = (2,2)$.
   The order is 21. P is a primitive generator.

2. $x = 9 \rightarrow (9, \pm 12)$
   $x = 18 \rightarrow nopoints.$

3. $N_A = 5$.

4. $S = N_A * B = 5(2,2) = (2,21)$.

5. $k_A = 2 + 21 \bmod 3 = 2$. The order of B is 3, so the possible keys are 3.
   If $S = (2,2) \rightarrow k_A = 1$. If $S = (2,21) \rightarrow k_A = 2$. If $S = \infty \rightarrow k_A = 15$.

6. **SAGE**

```
E = EllipticCurve(Zmod(23),[9,1]);
P = E(3,3)
def function1(E,P):
--x = random.randint(2,21)
--X = x * P
--return (x, X)
def function2(x,X):
--S = x * X
--return S
```

Exercise 3. TDE 16/07/2013
Alice uses a variation to the ElGamal digital signature on the elliptic curve

$$E : y^2 = x^3 + 9x + 1 \bmod 31$$

to sign a message $h(m_1) = 12$. The curve has $n = 35$ points.

Alice publishes the points $A = (7,2)$ and $B = aA = (20,20)$. Moreover, Alice chooses a nonce $k = 7$ and sends $R = kA, \quad s = a^{-1}(h(m) - kx_R) \pmod{n}$ to Bob.

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

2. Compute a using the BSGS algorithm.

3. Sign the message $h(m_1)$.

4. Show that the verification $V_1 = h(m)A$, $V_2 = sB + x_r R$ is a valid verification procedure. Then, verify the signature.

5. Alice signs another message $h(m_2) = 15$ and publishes $(h(m_2) \| R_2 \| s_2) = (15 \| (5,27) \| 20)$. Which mistake did she do? Compute a.

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

Solution. 1. The order of A could be 5 or 7.
So, $5A = 5(7,2) = (12,15)$, $7A = 7(7,2) = (5,27)$.
The order is 35.

2. $N = \lceil\sqrt{35}\rceil = 6$, $-NA = 6(7,29) = (20,11)$
   $iA = \infty, (7,2), (19,26), (9,25), (0,1), (12,15), (20,20)$
   $B + j(-NA) = (20,20), \ldots$
   $a = i + jN \bmod n = 6 + 0 \cdot 6 = 6$.

3. $R = 7A = 7(7,2) = (5,27)$,
   $s = a^{-1}(h(m_1) - kx_R) \bmod n = 6^{-1}(12 - 7 \cdot 5) \bmod 35 = 6(12 - 0) = 2$.

4. $h(m)A = sB + x_R R = a^{-1}(h(m) - kx_R)B + x_R R = a^{-1}h(m)aA - a^{-1}kx_R aA + x_R kA = h(m)A$ OK!
   $V_1 = h(m)A = 12A = 6(7,2) + 6(7,2) = (22,11)$
   $V_2 = sB + x_r R = 2(20,20) + 5(5,27) = (22,11) + \infty = (22,11)$.

5. $s_1 a - h(m_1) = -kx_R = s_2 a - h(m_2)$
   $(s_1 - s_2)a = h(m_1) - h(m_2)$
   $(2 - 20)a = (12 - 15)$
   $a = 17^{-1} \cdot 32 \bmod 35 = 33 \cdot 32 = 6$.

6. **SAGE**

```
E = EllipticCurve(Zmod(31),[9,1]);
N = ceil(sqrt(35));
A = E(7,2); B = E(20,20);
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 4. TDE 05/09/2013
Alice wants to send a message to Bob. She uses the public key ElGamal cryptosystem and publishes the curve:

$$E : y^2 = x^3 + 5x + 4 \bmod 7$$

and the point $A = (2,6)$. The curve has $n = 10$ points. Bob chooses a secret number a and publishes the point $B = aA = (2,1)$.
Then, Alice sends to Bob a message corresponding to the point $P_{m,1} = (4,5)$.

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

2. Compute a using the BSGS algorithm.

3. Cipher the message $P_{m,1}$, using $k = 3$ and obtain $Y_{1,1}, Y_{2,1}$.

4. Decipher the message and obtain $P_{m,1}$.

5. Using the repeated nonce, decipher the message $Y_{1,2} = Y_{1,1}, Y_{2,2} = (3,5)$ and obtain $P_{m,2}$.

6. **SAGE** Write the commands to define the elliptic curve, to cipher and decipher the message.

Solution. 1. The order of A could be 2,5,10. $2A = 2(2,6) = (0,5)$; $5A = 5(2,6) = \infty$. The order is 5.

2. $N = \lceil\sqrt{10}\rceil = 4$, $-NA = -4(2,6) = (2,6)$
   $iA = \infty, (2,6), (0,5), (0,2), (2,1)$
   $B + j(-NA) = (2,1), \ldots$
   $a = i + jN \bmod n = 4 + 0 \cdot 4 = 4$.

3. $Y_{1,1} = kA = 3A = 3(2,6) = (0,2)$; $Y_{2,1} = P_{m,1} + kB = (4,5) + 3(2,1) = (3,2)$.

4. $P_{m,1} = Y_{2,1} - aY_{1,1} = (3,2) - 4(0,2) = (4,5)$

5. $Y_{2,1} - P_{m,1} = kB = Y_{2,2} - P_{m,2}$.
   $P_{m,2} = Y_{2,2} - Y_{2,1} + P_{m,1}$.
   $P_{m,2} = (3,5) - (3,2) + (4,5) = (5,0)$.

6. **SAGE**
```
E = EllipticCurve(Zmod(7),[5,4]);
k = 3; A = E(2,6); a = 4; B = a*A; P = E(4,5)
Y1 = k * A ; Y2 = P + k*B;
Pm = Y2 - a*Y1;
```

Exercise 5. TDE 19/09/2013
Consider the Diffie-Hellman key exchange over the Elliptic Curve:

$$E : y^2 = x^3 + 4x + 3 \bmod 13$$

with $n = 16$ points and the basepoint $P = (8,1)$. Alice chooses a secret number a and send the point $A = aP = (10,4)$. Bob chooses a secret number $b = 6$ and sends the point $B = bP = (7,7)$. At the end of the protocol, Alice and Bob use the key k to cipher a message m as follows: $Enc(m) = x_k + y_k + m$. Eve is an active attacker that makes a Man-in-the-Middle attack. Suppose the attack is successful. Eve choose its secret number $e = 2$.

1. Compute the order of the group generated by P.

2. Compute a using the BSGS algorithm.

3. Depict what happens in the message exchange. Compute the shared keys.

4. Alice wants to send the message $m = 7$, that Eve does not modify. Write the corresponding ciphered message sent by Alice and received by Bob.

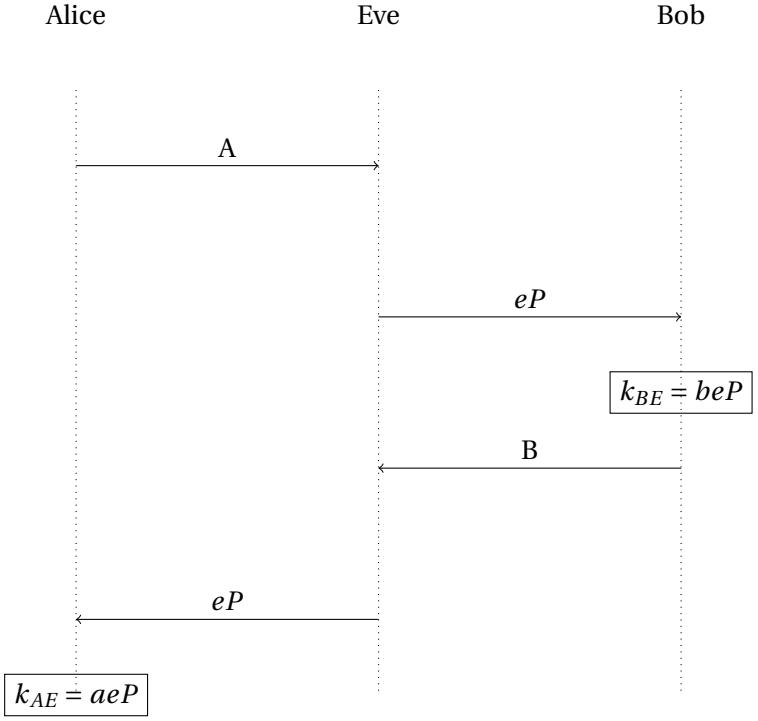
5. To avoid the attack, A and B are pre-distributed to the participants. What are the lacks of this choice? Explain how to avoid the attack with no pre-distribution.

6. **SAGE** Write the commands to define the elliptic curve and the functions to simulate the ECDHKE.

Solution. 1. The order of P could be 2,4,8,16. $2P = 2(8,1) = (7,6)$; $4A = 2(7,6) = (11,0)$; $8A = 2(11,0) = \infty$. The order is 8.

2. $N = \lceil\sqrt{16}\rceil = 4$, $-NA = -4(8,1) = (11,0)$
   $iP = \infty, (8,1), (7,6), (10,9), (11,0), (10,4), ..$
   $A + j(-NP) = (10,4), ...$
   $a = i + jN \bmod n = 5 + 0 \cdot 4 = 5$.

3. $k_{AE} = aeP = 2(10,4) = (7,6)$; $k_{BE} = beP = 2(7,7) = (11,0)$.



4. $C_{AE} = 7 + 6 + 7 = 20$; $C_{BE} = 11 + 0 + 7 = 18$.

5. K_{AB} remains the same, it does not change. If there are many participants, the pre-distribution requires a considerable abount of time. Adding a mutual authentication as the full STS protocol does. However, this requires a digital signature scheme and a public key infrastructure.

6. **SAGE**
   `E = EllipticCurve(Zmod(23),[9,1]);`

```
P = E(3,3)
def function1(E,P):
--x = random.randint(2,21)
--X = x * P
--return (x, X)
def function2(x,X):
--S = x * X
--return S
```

Exercise 6. Alice uses the DSA signature scheme on the elliptic curve $E : y^2 = x^3 + 2x + 1 \bmod 23$ to sign messages m_i. The curve has $n = 30$ points.
Alice publishes the base point $A = (16,9)$ (of order q) and the point $B = aA = (17,7)$.

1. Verify whether A satisfies the condition required by DSA signature.
2. Find all the points on the curve E with $x = 2, 11$, if they exist.
3. Alice publishes the signed message $(m_1 \| R_1 \| s_1) = (5 \| (17,16) \| 3)$. Write the equations for signature verification and verify the correctness. Then, verify Alice's signature.
4. Compute a using the BSGS algorithm.
5. Alice signs another message $m_2 = 3$ and publishes $(m_2 \| R_2 \| s_2) = (3 \| (17,16) \| 4)$. Which mistake did she do? Taking advantage from Alice's mistake, compute a.
6. **SAGE** Write the commands to define the elliptic curve, to find how many points it has, and to compute the DSA signature.

Solution.

1. The A order, q, must be a large prime factor of n. It could be 2, 3, 5. So, we compute $2A = 2(16,9) = (17,7)$, $3A = 3(16,9) = (17,16)$ and $5A = 5(16,9) = \infty$. The order of A is 5.
2. $(2,6), (2,17)$. No points for $x = 11$.
3. $u_1 = s^{-1}m \quad u_2 = s^{-1}x_R$ and $V = u_1A + u_2B$ that must be equal to R.
   $u_1 = 3^{(-1)} \cdot 5 = 0 \quad u_2 = 2 \cdot 17 = 4$ and $V = 0A + 4B = 4(17,7) = (17,16)$.
4. $N = \lceil \sqrt{30} \rceil = 6$, $-NA = 6(16,14) = (16,14)$
   $iA = \infty, (16,9), (17,7), (17,16), (16,14)$
   $B + j(-NA) = (17,7), \ldots$
   $a = i + jN \bmod n = 2 + 0 \cdot 6 = 2$.
5. The repeated nonce.
   $s_1k - m_1 = ax_R = s_2k - m_2$
   $(s_1 - s_2)k = (m_1 - m_2)$
   $k = (m_1 - m_2)(s_1 - s_2)^{-1} \bmod q = (5-3)(3-4)^{-1} \bmod 5 = 2 \cdot 4 \bmod 5 = 3$
   $a = (s_1k - m_1)x_R^{-1} \bmod q = (3 \cdot 3 - 5) \cdot 17^{-1} \bmod 5 = 2$.

6. **SAGE**

```
E = EllipticCurve(Zmod(23),[2,1]);
E.cardinality();
A = E(16,9); q = A.order(); k = 3; m = 5; a = 2;
R = k*A; (x,y,z) = R;
kinv = mod(k^(-1), q);
s = mod(kinv*(m + a*int(x)),q);
```