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 30/06/2015
Alice uses the DSA signature scheme on the elliptic curve $E : y^2 = x^3 + x + 1 \bmod 19$ to sign messages m_i. The curve has $n = 21$ points.
Alice publishes the base point $A = (10,2)$ (of order q) and the point $B = aA = (14,2)$.

1. Verify whether A satisfies the condition required by DSA signature.
2. Find all the points on the curve E with $x = 2,3,7$, if they exist.
3. Alice publishes the signed message $(m_1 \| R_1 \| s_1) = (6 \| (15,3) \| 6)$. 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 $m_2 = 5$ and publishes $(m_2 \| R_2 \| s_2) = (5 \| (15,3) \| 3)$. Which mistake did she do? Taking advantage from Alice's mistake, compute a.

Solution.
1. The A order, q, must be a large prime factor of n. It could be 3 or 7 So, we compute $3A = 3(10,2) = (14,2)$ and $7A = 7(10,2) = \infty$. The order of A is 7.
2. $(2,7),(2,12),(7,3),(7,16)$. No points for $x = 3$.
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.
   $u_1 = 1 \quad u_2 = 6$ and $V = A + 6B = (10,2) + -(14,2) = (10,2) + (14,17) = (15,3)$.

4. $N = \lceil\sqrt{21}\rceil = 5$, $-NA = 5(10,17) = (15,3)$
   $iA = \infty, (10,2), (15,16), (14,2), (14,17), (15,3)$
   $B + j(-NA) = (14,2), \ldots$
   $a = i + jN \bmod n = 3 + 0 \cdot 5 = 3$.

5. She uses the nonce twice.
   $s_1 k - m_1 = a x_R = s_2 k - m_2$
   $(s_1 - s_2)k = (m_1 - m_2)$
   $k = (m_1 - m_2)(s_1 - s_2)^{-1} \bmod q = (6-5)(6-3)^{-1} \bmod 7 = 1 \cdot 5 \bmod 7 = 5$
   $a = (s_1 k - m_1) x_R^{-1} \bmod q = (6 \cdot 5 - 6) \cdot 15^{-1} \bmod 7 = 3$.

Exercise 2. TDE 30/06/2015
Alice and Bob agree on a common secret using the Diffie-Hellman Key Exchange protocol. They publish the elliptic curve $E : y^2 = x^3 + x + 4 \bmod 7$. The curve has $n = 10$ points. They also publish the base point $P = (0,2)$, that is a primitive generator.
Alice chooses her secret $N_A = 7$ and Bob chooses his secret $N_B = 9$.
Simulate in **SAGE** the DHKE and verify the correctness.

Solution.
```
E = EllipticCurve(Zmod(7),[1,4]);
P = E(0,2); N_A = 7, N_B = 9;
A = N_A * P;
B = N_B * P;
K_A = B * N_A;
K_B = A * N_B;
if K_A == K_B:
-- print correct
else:
-- print error
```

Exercise 3. TDE 14/07/2015
Alice and Bob agree on a common secret using the Diffie-Hellman Key Exchange protocol. They publish the elliptic curve $E : y^2 = x^3 + 5x + 7 \bmod 23$. The curve has $n = 18$ points. They also publish the base point $P = (2,5)$.
Alice sends the message $A = N_A P = (3,16)$ and receives the message $B = N_B P = (1,6)$.
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 $x = 1, 4$, if they exist.

3. Compute N_A using the PH algorithm.

4. Compute the shared secret S. (If you have not find N_A in the previous step use $N_A = 5$).

5. Compute the Alice's key k_A. How many keys it's possible to obtain, why? Which are they?

Solution. 1. The order of P should be 18.
$2P = 2(2,5) = (12,1)$
$3P = 3(2,5) = (11,17)$.
$6P = 6(2,5) = (1,6)$
$9P = 9(2,5) = (6,0)$
The order is 18. P is a primitive generator.

2. $x = 1 \rightarrow (1, \pm 6)$
$x = 4 \rightarrow nopoints$.

3. $N_A = 5$.

4. $S = N_A * B = 5(1,6) = (1,17)$

5. $k_A = 1 + 17 \bmod 3 = 0$. The order of B is 3, so the possible keys are 3.
If $S = (1,17) \rightarrow k_A = 0$. If $S = (1,6) \rightarrow k_A = 2$. If $S = \infty \rightarrow k_A = 15$.

Exercise 4. TDE 14/07/2015
Alice uses the DSA signature scheme on the elliptic curve $E : y^2 = x^3 + 6x + 7 \bmod 11$ to sign messages m_i. The curve has $n = 8$ points.
Alice publishes the base point $A = (2,4)$ (of order $q = 4$), and the point $B = aA = (2,7)$. And keeps secret $a = 3$. Then, she signs the message $m = 6$ using the nonce $k = 3$.
Write the command in **SAGE** to do the following:

1. List all the points on the curve E and verify how many they are.

2. Sign the message m.

3. Verify the signature obtained.

Solution.
```
E = EllipticCurve(Zmod(11),[6,7]);
E.points();
A = E(2,4); q = 4; k = 3; m = 6; a = 3;
R = k*A; (x,y,z) = R;
kinv = mod(k ^(-1), q);
s = mod(kinv*(m + a*int(x)),q);
u_1 = mod(s^(-1)*m,q);
u_2 = mod(s^(-1)*int(x),q);
V = int(u_1) * A + int(u_2) *B;
if V == R:
-- print signature verified
else:
-- print -1
```

Exercise 5. TDE 07/09/2015
Alice wants to send a message to Bob. She uses the public key ElGamal cryptosystem and publishes the curve:

$$E : y^2 = x^3 + 5x + 7 \bmod 11$$

and the point $A = (2,5)$. The curve has $n = 16$ points. Bob chooses a secret number a and publishes the point $B = aA = (2,6)$.
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 $Y_{1,2} = Y_{1,1}, Y_{2,2} = (5,5)$ and obtain $P_{m,2}$.

Solution.
1. The order of A could be 2,4,8,16. $2A = 2(2,5) = (10,10)$; $4A = 4(2,5) = (7,0)$; $8A = 8(2,5) = \infty$. The order is 8.
2. $N = \lceil\sqrt{16}\rceil = 4$, $-NA = -4(2,5) = (7,0)$
   $iA = \infty, (2,5), (10,10), (3,4), (7,0)$
   $B + j(-NA) = (2,6), (3,4), \ldots$
   $a = i + jN \bmod n = 3 + 1 * 4 \cdot 16 = 7$.
3. $Y_{1,1} = kA = 3A = 3(2,5) = (3,4)$; $Y_{2,1} = P_{m,1} + kB = (4,5) + 3(2,6) = (4,5) + (3,7) = (8,3)$.
4. $P_{m,1} = Y_{2,1} - aY_{1,1} = (8,3) - 7(3,4) = (4,5)$
5. $Y_{2,1} - P_{m,1} = kB = Y_{2,2} - P_{m,2}$.
   $P_{m,2} = Y_{2,2} - Y_{2,1} + P_{m,1}$.
   $P_{m,2} = (5,5) - (8,3) + (4,5) = (6,0)$.

Exercise 6. TDE 07/09/2015
Consider a Hill cipher operating in $\mathbb{Z}_{26}$.
First, write the command in **SAGE** to do the following:

1. Encrypt the message $x = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \bmod 26$, by using the key $k = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \bmod 26$. (Remember to the define the matrix).
2. Decrypt the ciphered message y.
3. Suppose to know x and y, write the command to find k.

Secondly, consider an example of Hill cipher over the upper-case letters of the English alphabet. Write the command in **SAGE** to do the following:

1. Define the alphabet AS and the cryptosystem H of block length 3.

2. Generate a random key K. Encode and cipher the message X = "Hello World!".

3. Decipher the message Y and verify the correctness.

Solution.
```
R = Zmod(26)
x = matrix(R, [[1,2], [3,4]])
k = matrix(R, [[1,2], [4,5]])
y = x*k
x = y*k^(-1)
k= x^(-1)*y
----------------
AS = AlphabeticStrings()
H = HillCryptosystem(AS,3)
K = H.random_key()
X = H.encoding("Hello World !")
Y = H.enciphering(K,X)
H.deciphering(K,Y)
H.deciphering(K,Y) == X
- True
```

Exercise 7. TDE 21/09/2015
Alice uses a variation to the ElGamal digital signature on the elliptic curve

$$E : y^2 = x^3 + 9x + 1 \bmod 13$$

to sign a message $h(m_1) = 11$. The curve has $n = 18$ points.

Alice publishes the points $A = (0,1)$ and $B = aA = (0,12)$. Moreover, Alice chooses a nonce $k = 3$ 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 $h(m_2) = 10$ and publishes $(h(m_2) \| R_2 \| s_2) = (10 \| (8,0) \| 8)$. Which mistake did she do? Compute a.

Solution. 1. The order of A could be 2,3,6,9,18.
So, $2A = 2(0,1) = (4,7)$, $3A = 3(0,1) = (8,0)$, $6A = 6(0,1) = \infty$.
The order is 6.

2. $N = \lceil\sqrt{18}\rceil = 5$, $-NA = -5(0,1) = (0,1)$
   $iA = \infty, (0,1), (4,7), (8,0), (4,6), (0,12)$
   $B + j(-NA) = (0,12), \ldots$
   $a = i + jN \bmod n = 5 + 0 \cdot 5 = 5$.

3. $R = 3A = 3(0,1) = (8,0)$,
   $s = a^{-1}(h(m_1) - kx_R) \bmod n = 5^{-1}(11 - 3 \cdot 8) \bmod 18 = 11(11-24) = 11 * 5 = 1$.

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!
   $V_1 = h(m)A = 11A = 5A = 5(0,1) = (0,12)$
   $V_2 = sB + x_r R = (0,12) + 8(8,0) = (0,12) + \infty = (0,12)$.

5. $s_1 a - h(m_1) = -kx_R = s_2 a - h(m_2)$
   $(s_1 - s_2)a = h(m_1) - h(m_2)$
   $(1-8)a = (11-10)$
   $a = 7^{-1} \cdot 1 \bmod 18 = 5$.

Exercise 8. TDE 21/09/2015
Alice uses the public key Elgamal cryptosystem. She publishes the curve $E : y^2 = x^3 + 5x + 7 \bmod 11$ and the point $A = (2,5)$ of order 8. She also chooses a secret number a = 7 and publishes the point $B = aA$. Bob wants to sent to Alice a message corresponding to the point $P_m = (4,5)$.
Write the command in **SAGE** to do the following:

1. Calculate B.

2. Cipher the message using $k = 3$.

3. Decipher the message.

4. Using the repeated nonce, decipher the ciphered message ($Y_{1,2} = (3,4)$, $Y_{2,2} = (5,5)$).

Solution.
```
E = EllipticCurve(Zmod(11),[5,7])
A = E(2,5)
a = 7
B = a *A
-----------
k = 3; P_m =E(4,5)
Y_1 = k * A
Y_2 = P_m + k*B
-----------
P_m = Y_2 - a * Y_1
-----------
Y_22 = E(5,5)
P_m = Y_22 - Y_2 + P_m
```