Introduction to Cryptography: Homework #10

Due on August 5, 2019 at 11:59pm

Professor Manuel

ShiHan Chan

Problem 1

8.7??? We need to prove the addition law, commutative law, associative law.

Problem 2

1.
When calculate [2]P, $P_1 = P_2$, so $m = \frac{3x_1^2+b}{2y_1} = \frac{3*8^2+3}{2*9} = 9 \mod 11$
$x_3 = m^2 - x_1 - x_2 = 9^2 - 8 - 8 = 10 \mod 11$
$y_3 = m(x_1 - x_3) - y_1 = 9(8 - 10) - 9 = 6 \mod 11$
$[2]P = (10, 6)$
$[4]P = [2]P + [2]P$
$m = \frac{3x_1^2+b}{2y_1} = \frac{3*10^2+3}{2*6} = 6 \mod 11$ $x_3 = m^2 - x_1 - x_2 = 9^2 - 8 - 8 = 5 \mod 11$
$y_3 = m(x_1 - x_3) - y_1 = 2 \mod 11$
$[4]P = (5, 2)$
$[5]P = [4]P + [1]P$
$[5]P = (1, 0)$
$[10]P = [5]P + [5]P$
$[10]P = (0, 0)$
2.
There are 10 points in total.
3.

$x \mod 11$	$y^2 \mod 11$	$y \mod 11$	Points on E
0	7	x	
1	0	0	(1,0)
2	10	x	
3	10	x	
4	6	x	
5	4	2 or 9	(5,2) or (5,9)
6	10	x	
7	8	x	
8	4	2 or 9	(8,2) or (8,9)
9	4	2 or 9	(9,2) or (9,9)
10	3	5 or 6	(10,5) or (10,6)

There are 10 points in total on elliptic curve, 9 points calculated from equation above and one point O at infinity.

Problem 3

In the ECDLP, we need a curve E, Point $G \in E$ and the order n of G which means $[n]G = \mathcal{O}$. We also need a cryptographic hash function h.
Alice creates a key pair, consisting of a private key integer d_A, randomly selected in the interval [1,n-1], and a public key curve point $Q_A = [d_A]G$.

When Alice wants to sign a message m, the procedure is:
1. Calculate $e = h(m)$.
2. Let z be L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Generate a random integer k in $[1, n-1]$.
4. Calculate $P : (x_1, y_1) = [k]G$.
5. Calculate $r \equiv x_1 \mod n$. If $r = 0$, retry from step 3.
6. Calculate $s \equiv k^{-1}(z + rd_A) \mod n$. If $s = 0$, retry from step 3.
7. The signature is the pair (r, s).

When Bob wants to authenticate Alice's signature, he must have a copy of her public-key curve point Q_A. First he can verify Q_A is a valid curve point as follows:
1. Check that Q_A is not equal to the identity element $\mathcal{O}$.
2. Check that Q_A lies on the curve.
3. Check that $[n]Q_A = \mathcal{O}$.

After that, Bob follows these steps:
1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = h(m)$.
3. Let z be L_n leftmost bits of e, where L_n is the bit length of the group order n.
4. Calculate $w \equiv s^{-1} \mod n$
5. Calculate $u_1 \equiv zw \mod n$ and $u_2 \equiv rw \mod n$.
6. Calculate the curve point $P : (x_1, y_1) = [u_1]G + [u_2]Q_A$. If $P = \mathcal{O}$, the signature is invalid.
7. The signature is valid if $r \equiv x_1 \mod n$, invalid otherwise.

Now we should validate the correctness of the algorithm. Suppose we have $P : (x_1, y_1) = [u_1]G + [u_2]Q_A$ in step 6 of authentication. $P = [u_1]G + [u_2]Q_A$
$= [u_1 + u_2 d_A]G$
$= [zs^{-1} + rd_A s^{-1}]G$
$= [(z + rd_A)s^{-1}]G$
$= [(z + rd_A)(k^{-1}(z + rd_A))^{-1}]G$
$= [k]G$
The benefits of ECDSA is that we can get the same level of security as RSA but with smaller keys. Smaller keys have faster algorithms for generating signatures because the math involves smaller numbers. Smaller public keys mean smaller certificates and less data to pass around to establish a TLS connection. This means quicker connections and faster loading times on websites.

Problem 4

In BB84 scheme, Alice wants to send a private key to Bob. She starts with two bit strings, a and b, each length is n bits. She encodes these two strings as a string of n qubits: $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$
$|\psi_{00}\rangle = |0\rangle$
$|\psi_{10}\rangle = |1\rangle$
$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Alice sends $|\psi\rangle$ to a public and authenticated quantum channel $\mathcal{E}$ to Bob. Because only Alice knows b, it is impossible for either Bob or Eve to distinguish the states of the qubits. In the other hand, after Bob has received the qubits, we know that Eve cannot be in possession of a copy of the qubits sent to Bob.
Bob proceeds to generate a string of random bits bb of the same length as b and then measures the string he has received from Alice, aa. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce bb. Bob communicates over a public channel with Alice to determine which b_i and bb_i are not equal. Both Alice and Bob now discard the qubits in a and aa where b and bb do not match.
From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $\frac{k}{2}$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

Problem 5

1. Quantum channel is used to produce and distribute a key for Alice and Bob, and they use another channel to send message encrypted by the key.
2. When Eve observes the information in the quantum channel, by quantum indeterminacy, measuring an unknown quantum state will change the state. When this happens, Alice and Bob can detect the interaction, so that they can start with another new key which is not disturbed.

Problem 6

1.

$$U_1 \otimes V_1 = \begin{pmatrix} u_{1,1}V_1 & u_{1,2}V_1 & \cdots & u_{1,n}V_1 \\ u_{2,1}V_1 & u_{2,2}V_1 & \cdots & u_{2,n}V_1 \\ \vdots & \vdots & \ddots & \vdots \\ u_{n,1}V_1 & u_{n,2}V_1 & \cdots & u_{n,n}V_1 \end{pmatrix}$$

$$= \begin{pmatrix} u_{1,1}v_{1,1} & \cdots & u_{1,1}v_{1,n} & \cdots & \cdots & u_{1,n}v_{1,1} & \cdots & u_{1,n}v_{1,n} \\ \vdots & \ddots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ u_{1,1}v_{n,1} & \cdots & u_{1,1}v_{n,n} & \cdots & \cdots & u_{1,n}v_{n,1} & \cdots & u_{1,n}v_{n,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{n,1}v_{1,1} & \cdots & u_{n,1}v_{1,n} & \cdots & \cdots & u_{n,n}v_{1,1} & \cdots & u_{n,n}v_{1,n} \\ \vdots & \ddots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ u_{n,1}v_{n,1} & \cdots & u_{n,1}v_{n,n} & \cdots & \cdots & u_{n,n}v_{n,1} & \cdots & u_{n,n}v_{n,n} \end{pmatrix}$$

$W_1 = U_1 \otimes V_1, W_2 = U_2 \otimes V_2, X = W_1 \cdot W_2$
$w_{i,j} = u_{i_1,j_1}v_{i_2,j_2} \quad (i,j \in [1,n^2])$
$x_{i,j} = \sum_{k=1}^{n^2} w_{1,k,j}w_{2,i,k} = \sum_{k=1}^{n^2} u_{1,k_1,j_1}u_{2,i_1,k_1}v_{1,k_2,j_2}v_{1,i_2,k_2} \quad (i,j \in [1,n^2])$

$W_3 = U_1 \cdot U_2, W_4 = V_1 \cdot V_2, Y = W_3 \otimes W_4$
$w_{i,j} \sum_{k=1}^{n} v_{k,j}v_{i,k} \quad (i,j \in [1,n])$
$y_{i,j} = \sum_{k=1}^{n} u_{1,k,j_1}u_{2,i_1,k} \sum_{k=1}^{n} v_{1,k,j_2}v_{2,i_2,k} = \sum_{k=1}^{n^2} u_{1,k_1,j_1}u_{2,i_1,k_1}v_{1,k_2,j_2}v_{1,i_2,k_2} \quad (i,j \in [1,n^2])$

So $(U_1 \otimes V_1) \cdot (U_2 \otimes V_2) = (U_1U_2) \otimes (V_1V_2)$

2.
If there are two vector spaces V,W, and V have a basis $a_1, a_2...a_m$ and W have a basis $b_1, b_2, ..., b_n$, then $U = V \otimes W$ is a vector space with basis $a_i \otimes b_j$. For any vector $v = \sum_{i=0}^{m} v_i a_i \in V$ and $w = \sum_{j=0}^{m} a_j b_j \in V$, we can get $u = v \otimes w = \sum_{i=0}^{m} \sum_{j=0}^{n} v_i w_j (a_i \otimes b_j)$ so that $u \in U$. And we show the operator $\otimes$ is bilinear.