COMP90043: Cryptography and security: Week 8: ElGamal Encryption and Signatures

(1) For the following structures list the possibe cyclic multiplicative groups present in them.

(a) Integers modulo 31.
$\phi(31) = 30 = 5 \times 3 \times 2$, hence possible group orders are $30, 5, 3, 2, 15, 6, 10, 1$.

(b) Integers modulo 30.
$\phi(30) = \phi(5) * \phi(3) * \phi(2) = 4 \times 2 \times 1 = 8 = 2^3$,hence possible group orders are $1, 2, 4, 8$.

(c) Finite Field of size 128.
$128 - 1 = 127$, hence possible group orders are $127, 1$.

(d) Integers modulo 89.
$\phi(89) = 88 = 2^3 \times 11$, hence possible group orders are $88, 11, 22, 44, 2, 4, 8, 1$.

(2) Consider a finite field Z_{11}; determine the multiplicative order of all nonzero elements of the field.
Note: A multiplicative order of an element α is the smallest integer $j \geq 1$ such that $\alpha^j = 1$. Note that 1 is the multiplicative identity.
$11 - 1 = 10 = 2 \times 5$. Possible orders are $1, 5, 10, 2$.

(3) Use the irreducible polynomial $1 + x + x^4$ to create a table for finite field $GF(16)$. Complete the table:
(a) Complete the missing entries in the table.
(b) Determine multiplicative order of the elements.
(c) What is the multiplicative inverse of x^3? x^{12}.

(4) Prove that ElGamal decryption equations work as required. Study the lectue slides before answering the question.
Method: Consider the defning equation for the signing equation. Take the power of α, the generator, of both LHS and RHS. The regroop the computations based on public parameters. The results then follow, as explained in the lectures. The following two properties are crictical in understaning the ideas:

$$a^m = 1\, mod\, q, \text{if and only if} m = 0\, mod\, (q-1). a^i = a^j\, mod\, q, \text{ if and only if} i = j\, mod\, (q-1).$$

i	Elements:x^i	As Polynomials	As Vectors	Multiplicative Order
$-\infty$	0	0	$[0,0,0,0]$	
0	1	1	$[1,0,0,0]$	1
1	x	x	$[0,1,0,0]$	15
2	x^2	x^2	$[0,0,1,0]$	15
3	x^3	x^3	$[0,0,0,1]$	5
4	x^4	$1+x$	$[1,1,0,0]$	15
5	x^5	$x+x^2$	$[0,1,1,0]$	3
6	x^6	x^2+x^3	$[0,0,1,1]$	5
7	x^7	$1+x+x^3$	$[1,1,0,1]$	15
8	x^8	$1+x^2$	$[1,0,1,0]$	15
9	x^9	$x+x^3$	$[0,1,0,1]$	5
10	x^{10}	$1+x+x^2$	$[1,1,1,0]$	3
11	x^{11}	$x+x^2+x^3$	$[0,1,1,1]$	15
12	x^{12}	$1+x+x^2+x^3$	$[1,1,1,1]$	5
13	x^{13}	$1+x^2+x^3$	$[1,0,1,1]$	15
14	x^{14}	$1+x^3$	$[1,0,0,1]$	15
15	x^{15}	1	$[1,0,0,0]$	1

TABLE 1. Elements of $GF(2^4)$ as powers of x

(5) What are the hard problems on which the security of the ElGamal encryption is based on?

Discrete Logarithms, Computational Diffie Helman problems.

(6) Derive the verification equations of the ElGamal signature using the defining equations of signing.

Note: Please read slides $4, 5$ and 9 before attempting this question.

(7) Discuss Elgamal digital signature scheme with an example. Say, for $q = 19$ and $= 13$,$m = 7$, calculate the signature and verify it.

$$q = 19, \alpha = 13, m = 7$$

Let $X_A = 12$, then $Y_A = \alpha^{X_A} \mod q = 13^{12} \mod 19 = 7$. So, private key $= \{12\}$, public key $= \{19, 3, 7\}$.

Let $K = 5$, which is relatively prime to $q - 1$, that is 18. Using extended gcd algorithm, we can calculate K^{-1} to be 11.

Then, $S_1 = \alpha^K \mod q = 13^5 \mod 19 = 14$, and $S_2 = K^{-1}(m = X_A S_1) \mod (q-1) = 11(7 - 12 * 14) \mod 8 = 11$. So, the signature for this message is $\{14, 11\}$.

Verify this at receiver's end:

$$V_1 = \alpha^m \mod q = 13^7 \mod 19 = 10$$

and

$$V_2 = Y_A^{S_1} S_1^{S_2} \mod q = 7^{14} 14^{11} \mod 19 = 10$$

(8) Show that verification equations of Schnorr's signature scheme follows from signing equation.

(9) How do you determine primes p and q as required for the Schnorr's signature scheme? Suggest a method. Given an example in small primes.

Method: Choose a large prime q of required size. Then Let $p = 1 + 2^l * r * q$, such that p is a prime for some integers l and an a large odd random number r.

Key Management Questions:

(1) List ways in which secret keys can be distributed to two communicating parties. For two parties A and B, key distribution can be achieved in a number of ways, as follows:
1. A can select a key and physically deliver it to B.
2. A third party can select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

(2) What is the difference between a session key and a master key?

A session key is a temporary encryption key used between two principals. A master key is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys. Typically, the master keys are distributed by noncryptographic means.

(3) What is a nonce? A nonce is a value that is used only once, such as a timestamp, a counter, or a random number; the minimum requirement is that it differs with each transaction.

(4) Explain the problems with key management and how it affects symmetric cryptography?

The primary weakness of symmetric encryption algorithms is keeping the single key secure. Known as key management, it poses a number of significant challenges. If a user wants to send an encrypted message to another using symmetric encryption, he must be sure that she has the key to decrypt the message. How should the first user get the key to the second user? He would not want to send it electronically through the Internet, because that would make it vulnerable to eavesdroppers. Nor can he encrypt the key and send it, because the recipient would need some way to decrypt the key. And if he can even get the get securely to the user, how can be he certain that an attacker has not seen the key on that persons computer? Key management is a significant impediment to using symmetric encryption.

Home work:
Study the correctness of DSA signing and verification algorithms from the textbook.