COMP90043: Cryptography and security: Week 9 Part B: ElGamal Encryption

(1) For the following structures list the possibe cyclic multiplicative groups present in them.
   (a) Integers modulo 31. $\phi(31) = 30 = 5x3x2$, hence possible group orders are $30, 5, 3, 2, 15, 6, 10, 1$.
   (b) Integers modulo 30. $\phi(30) = \phi(5)*\phi(3)*\phi(2) = 4*2*1 = 8 = 2^3$,hence possible group orders are $1, 2, 4, 8$.
   (c) Finite Field of size 128. $\phi(128) = 127$, hence possible group orders are $127, 1$.
   (d) Integers modulo 89. $\phi(89) = 88 = 2^3 * 11$, 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.
   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}: See the table.

(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:

$a^m = 1 \, mod \, q$, if and only if$m = 0 \, mod \, (q-1)$.$a^i = a^j \, mod \, q$, 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}	$1+x^2x^3$	$[1,0,1,1]$	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) (4 points) A variant of ElGamal cryptosystem over the prime field $GF(q)$ given as follows. Assume the parameters as given in the ElGamal.pdf. Let $y_A = a^{x_A} \mod q$, be the public address of Alice, where $x_A, 1 < x_A < q-1$, is Alice's private key. Encryption function is defined as follows:

$$E(M) = C_1, C_2,$$

where $C_1 = a^k \bmod q$, where k is a random integer $1 \leq k \leq q-1$, $C_2 = K \oplus M$, where $K = y_A^k \bmod q$ and $\oplus$ is binary exclusive or function applied to binary representation of K and M.

a. Describe the Decryption Function $D(C_1, C_2)$ that Alice can use to recover the message.

b. Show how the security of the encryption function is based on Computational Diffie-Hellman (CDH) problem.

CDH Problem: Let q be a prime number and a be a generator of the cyclic multiplicative group of modulo q. Given a^x, a^y, the CDH problem computes a^{xy}.

For the given encryption function, the decryption function D(C1;C2) that recovers the message is defiened as follows:
Key K = C1^XA 1 modq and
Plaintext M = (C2 XOR K) mod q

For recovering the plaintext, the operation done is the XOR of the ciphertext C2 and the recovered key K modulo q. This is because, the function used here for obtaining the cipher text C2 is XOR and we know that for XOR operation, if
c = a XOR b, we have b = a XOR c

Suppose that there exists a probabilistic polynomial time attacker $\mathcal{A}$ that breaks the CDH problem with probability ϵ. Then attacker $\mathcal{B}$ breaks the cryptosystem as follows.

(a) $\mathcal{A}$ receives ciphertext (C_1, C_2) as input.
(b) Run $\mathcal{A}(1^\lambda, \langle a \rangle, C_1, y_A) \to y_A^k$.
(c) Output $M = C_2 \oplus y_A^k$.

$\mathcal{B}$ runs in polynomial time and succeeds iff $\mathcal{A}$ succeeds, thus has success probability ϵ. By assumption this is non-negligible, therefore the CDH problem is a necessary condition for the security of the cryptosystem.