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

(1) For the following structures, list sizes of the possible cyclic multiplicative groups present in them. These are expected to serve examples for cyclic groups on which ElGamal encryption could be defined.

(a) Integers modulo 31.

(b) Integers modulo 30.

(c) Finite Field of size 128.

(d) Integers modulo 89.

(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.

(3) Use the irreducible polynomial $1 + x + x^4$ to create a table for the finite field $GF(16)$.

(a) Complete the missing entries in the table.

(b) Determine multiplicative order of the elements.

(c) What is the multiplicative inverse of x^3?

(4) Prove that ElGamal decryption equations satisfy as required.

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

(6) 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.

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	x	x	$[0,1,0,0]$	
2	x^2	x^2	$[0,0,1,0]$	
3	x^3	x^3	$[0,0,0,1]$	
4	x^4			
5	x^5			
6	x^6			
7	x^7			
8	x^8			
9	x^9			
10	x^{10}			
11	x^{11}			
12	x^{12}			
13	x^{13}			
14	x^{14}			
15	x^{15}			

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

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}.