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

(1) For the following structures, list sizes of the possible cyclic multiplicative groups present in them.
   (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 $GF(16)$.

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	$1+x^2$	$[0,0,0,1]$	
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

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

Key Management Questions:

(1) List ways in which secret keys can be distributed to two communicating parties.
(2) What is the difference between a session key and a master key?
(3) What is a nonce?
(4) Explain the problems with key management and how it affects symmetric cryptography?

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