COMP90043 Cryptography and Security
Semester 2, 2021, Workshop Week 11 Solutions

1. What are differences between $\mathbf{GF}(8)$ and $\mathbf{Z}_8$?

   $\mathbf{GF}(8)$ is a finite field, represented as polynomials over $\mathbf{GF}(2)$ (binary field) and of characteristic 2. Whereas Z_8 is a is a finite ring. All non-zero elements of $\mathbf{GF}(8)$ have inverses. Some non-zero elements in $\mathbf{Z}_8$ does not have inverse.

2. Describe the conditions under which $\mathbf{GF}(m)$ and $\mathbf{Z}_m$ are identical.

   They are identical when m is a prime number.

3. For any finite field of size p^k, p is a prime number, k is an integer ≥ 1, $a \in \mathbf{GF}(p^k)$ and $a \neq 0$, we have

   $$a^{p^k-1} = 1.$$

   Use this result to derive a function for determining inverse of an element in $\mathbf{GF}(p^k)$.

   As $a^{p^m-1} = 1$, a^{p^m-2} is inverse of a, because $aa^{p^m-2} = a^{p^m-1} = 1$.

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

   (a) Complete the missing entries in the table. (see table above)

   (b) Determine multiplicative order of elements. (see table above)

   (c) What's the multiplicative inverse of $x^3 + x^2$?
   $x^3 + x$

5. Derive the verification equations of the ElGamal signature using the defining equations of signing.

   Read the slides and first consider the signing equation. Then consider taking a^{th} power on both sides of the signing equation and simplifying the equation using public parameters.

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

13.2 ELGAMAL DIGITAL SIGNATURE SCHEME

Before examining the NIST Digital Signature Algorithm, it will be helpful to understand the Elgamal and Schnorr signature schemes. Recall from Chapter 10, that the Elgamal encryption scheme is designed to enable encryption by a user's public key with decryption by the user's private key. The Elgamal signature scheme involves the use of the private key for digital signature generation and the public key for digital signature verification [ELGA84, ELGA85].

Before proceeding, we need a result from number theory. Recall from Chapter 2 that for a prime number q, if α is a primitive root of q, then

$$\alpha, \alpha^2, \ \ldots \ , \alpha^{q-1}$$

are distinct (mod q). It can be shown that, if α is a primitive root of q, then

1. For any integer m, $\alpha^m \equiv 1 \pmod{q}$ if and only if $m \equiv 0 \pmod{q-1}$.
2. For any integers, i, j, $\alpha^i \equiv \alpha^j \pmod{q}$ if and only if $i \equiv j \pmod{q-1}$.

As with Elgamal encryption, the global elements of **Elgamal digital signature** are a prime number q and α, which is a primitive root of q. User A generates a private/public key pair as follows.

1. Generate a random integer X_A, such that $1 < X_A < q - 1$.
2. Compute $Y_A = \alpha^{X_A} \bmod q$.
3. A's private key is X_A; A's pubic key is $\{q, \alpha, Y_A\}$.

To sign a message M, user A first computes the hash $m = \mathrm{H}(M)$, such that m is an integer in the range $0 \leq m \leq q - 1$. A then forms a digital signature as follows.

1. Choose a random integer K such that $1 \leq K \leq q - 1$ and $\gcd(K, q - 1) = 1$. That is, K is relatively prime to $q - 1$.
2. Compute $S_1 = \alpha^K \bmod q$. Note that this is the same as the computation of C_1 for Elgamal encryption.
3. Compute $K^{-1} \bmod (q - 1)$. That is, compute the inverse of K modulo $q - 1$.
4. Compute $S_2 = K^{-1}(m - X_A S_1) \bmod (q - 1)$.
5. The signature consists of the pair (S_1, S_2).

Any user B can verify the signature as follows.

1. Compute $V_1 = \alpha^m \bmod q$.
2. Compute $V_2 = (Y_A)^{S_1}(S_1)^{S_2} \bmod q$.

The signature is valid if $V_1 = V_2$. Let us demonstrate that this is so. Assume that the equality is true. Then we have

$\alpha^m \bmod q = (Y_A)^{S_1}(S_1)^{S_2} \bmod q$	assume $V_1 = V_2$
$\alpha^m \bmod q = \alpha^{X_A S_1}\alpha^{KS_2} \bmod q$	substituting for Y_A and S_1
$\alpha^{m - X_A S_1} \bmod q = \alpha^{KS_2} \bmod q$	rearranging terms
$m - X_A S_1 \equiv KS_2 \bmod (q - 1)$	property of primitive roots
$m - X_A S_1 \equiv KK^{-1}(m - X_A S_1) \bmod (q - 1)$	substituting for S_2