COMP90043: Cryptography and security: Week 10, El-Gamal Signatures, a sample solution

(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 elements in $\mathbf{Z}_8$ divide 0, eg. $2 * 4 = 0$.

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

Both the above structures are identical when m is a prime number.

(3) For any finite field of size p^k, p is a prime number, and k is an integer ≥ 1, show that

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

where $a \in \mathbf{GF}(p^k)$ and $a \neq 0$.

As any non-zero element has inverse in a finite field, the result follows from a similar arguements done for proving Fermat's Euler's theorems.

(4) Use the above 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 $aa^{p^m-2} = a^{p^m-1} = 1$.

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

Read the slides $4, 5$ and 9 and first consider 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 $\ = 13$,$m = 7$, calculate the signature and verify it.

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

Lets choose $X_A = 12$

Then $Y_A = \alpha^{X_A} \bmod q = 13^{12} \bmod 19 = 7$

So Private key = {12}, Public key = {19,13,7}

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

Then, $S_1 = \alpha^K \bmod q = 13^5 \bmod 19 = 14$, and

$S_2 = K^{-1}(m - X_A S_1) \bmod (q-1) = 11\ (7 - 12 * 14) \bmod 18 = 11$

So the signature for this message is {14,11}

Let's very this now at the receivers end

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

and $V_2 = (Y_A)^{S_1}(S_1)^{S_2} \bmod q = 7^{14}14^{11} \bmod 19 = 10$

(7) Show that verification equations of Schnorr's signature scheme follows from signing equation. Use te similar steps as in the above questions.

(8) 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.