MathCrypto Final (20 points)

Instructions

Instructions

- The Final Exam will be on THURS MAY 11 2-3 PM
- The exam will be an open book exam. Printed materials, textbooks, and handwritten notes are allowed. Calculators are allowed . Phones, laptops, tablets , and other electronic devices are not allowed.
- The weight of Final exam is 20%.
- The content of Final exam includes all content from this course.
- No make-up exams will be allowed.

Question 1

Consider the following public key system:
Alice chooses two large primes primes p and q, and publishes $N = pq$.
Alice chooses three random numbers $g, r_1, r_2 \in Z_N$ such that $gcd(g, N) = 1$ and publishes g_1, g_2 where
$g_1 \equiv g^{r_1(p-1)} \bmod N$
$g_2 \equiv g^{r_2(q-1)} \bmod N$.

So, Alice's public parameters are N, g_1, g_2 and Alice's private parameters are p, q.

Bob wants to send message $m \in Z_N$ to Alice.
Bob chooses two random integers $s_1, s_2 \in Z_N$ and computes
$c_1 \equiv mg_1^{s_1} \bmod N$
$c_2 \equiv mg_2^{s_2} \bmod N$
Bob sends the ciphertext (c_1, c_2) to Alice.

To decrypt the ciphertext, Alice uses the Chinese Remainder Theorem to solve the congruences:
$x \equiv c_1 \bmod p$
$x \equiv c_2 \bmod q$

(a) Given the following values: $p = 5, q = 7$. What is the message m sent from Bob to Alice given the ciphertext $(3, 27)$?

(b) Prove that for any values of public and private parameters, Alice's solution x is equal to Bob's plaintext m. That is, show that m satisfies the congruences

$$x \equiv c_1 \bmod p$$
$$x \equiv c_2 \bmod q$$

Hint: What is $g_1 \bmod p$ and what is $g_2 \bmod q$? Use Fermat's little theorem.

(c) Suppose g_1 is such that $g_1 \bmod q = 1$, prove that c_1 is equal to m.

(d) Suppose g_1 is such that $g_1 \bmod q$ is not equal to 1, show that $gcd(g_1 - 1, N) = p$.
Hint: $gcd(g_1 - 1, N)$ can only be $1, p, q, pq$. Is $g_1 - 1$ divisible by p? Is $g_1 - 1$ divisible by q?

Remarks: This cryptosystem was proposed in a cryptography conference. However, as shown in part (c) and part (d) that this cryptosystem is insecure.

Question 2.1

Let p be an odd prime and g be a generator of Z_p^*.
Let A be the set of all g^i where i is even.
Let B be the set of all g^i where i is odd.
(a) The size of A is the same as the size of B. True or False?
(b) All elements in A are quadratic residue. True or False?
(c) All elements in B are quadratic non-residue. True or False?

Question 2.2

Let $p = 5$ and $h = 3$.
(a) Compute $J_p(h)$.
(b) Is h a quadratic residue modulo p?
(c) Let g be the generator of Z_p^*. Suppose $g^x = h$. Should x be even or odd? Justify your answer? Hint: Use Question 2.1.

Remarks: Consider the discrete logarithm problem: Given p is prime and $g, h \in Z_p$ such that $g^x = h$, find x. If p is large safe prime, it is computationally intractable to compute the value of x.
However, by computing whether h is quadratic residue modulo p, we can discover some information about x. In particular, we know whether x is even or odd as shown in part (c).

Question 3

Recall Rabin encryption scheme. The public parameter is just the modulus N which is a product of two large primes.
Suppose the same message m is encrypted using Rabin encryption scheme with two different moduli N_1, N_2 where N_1 and N_2 are coprime.
If Eve sees the ciphertexts c_1, c_2 where $c_1 = m^2 \bmod N_1$ and $c_2 = m^2 \bmod N_2$, show how Eve can compute the message m in linear time.

Hint 1: Recall in the lecture we discussed the same problem using RSA encryption scheme with $e = 3$ and the same message m is encrypted using different moduli N_1, N_2, N_3 where N_1, N_2, N_3 are pairwise coprime.
Hint 2: Finding integer square root can be done efficiently using binary search.

Remarks: This question illustrate one limitation of textbook Rabin and RSA encryption scheme. This attack is easily prevented by using randomized padding schemes.

Question 4

Let F_3 be the field consists of integers modulo 3.

(a) Prove that $f(x) = x^2 + x + 2$ over F_3 is irreducible.

(b) Is $F_3[x]/(f(x))$ a field? How many elements does this field have?

(c) Consider the set of non-zero elements in $F_3[x]/(f(x))$. We know that it is a cyclic multiplicative group with respect to multiplication. How many generators does this group have? Hint: Use Euler totient function.

Question 5.1

Consider the $(3, 3)$-Shamir's secret sharing scheme over Z_8.

(That is, the secret key and the coefficients of the secret polynomials are in Z_8 and all computations are done modulo 8).

Let $f(x) = a_0 + a_1 x + a_2 x^2$ be the secret polynomial over Z_8 with degree 2.

(a) Is Z_8 a field?

(b) Suppose participant 1 has share value 6, participant 2 has share value 3. In this question, we aim to explore whether participant 1 and participant 2 can derive information about the secret key with only two share values?

(i) What is $f(2) - f(1)$ (modulo 8)?

(ii) Show that $a_1 + 3a_2 = 5 \bmod 8$.

(iii) Show that the secret value a_0 can't be even. Hence, participant 1 and participant 2 can rule out even numbers from Z_8 to be the secret key.

Question 5.2

Consider the $(3, 3)$-Shamir's secret sharing scheme over Z_{11}.

Let $f(x) = a_0 + a_1 x + a_2 x^2$ be the secret polynomial over Z_{11} with degree 2.

(a) Is Z_{11} a field?

(b) Just like Question 5.1, participant 1 and participant 2 can rule out some values from Z_{11} to be the secret key. True or False? Justify your answers.

Remarks: This questions illustrates the application of Finite Field. Over a finite field, a (t, n)-Shamir's secret sharing scheme guarantees that less than t participants will not gain information about the secret key. On the other hand, if Shamir's secret sharing scheme was to implemented over an arbitrary ring, there is no such guarantee.