CSE3230 Algebra and Cryptography
Assignment B

2022-2023

1 Polynomials (2/30)

(1) $x^4 + x + 1$ - is the polynomial (with coefficients in GF(2)) irreducible? What about primitive?
(2) $x^4 + x^3 + 1$ - is the polynomial (with coefficients in GF(2)) irreducible? What about primitive?

2 Diffie-Hellman System (5/30)

Alice and Bob choose (publicly) a prime number p, and a generator g of the cyclic group $\mathbb{Z}_p^*$.
(1) How to select the value p? Or how to make a prime test, please give an example?
(2) Why it is important to set a prime p there?
(3) How do you check what is the order of an element (generator), based on your example?
(4) Consider $\mathbb{Z}_{31}^*$ and $\mathbb{Z}_{33}^*$ and for every possible generator, find what is its order.
(5) Please give an example of Alice and Bob Diffie-Hellman key exchange, based on $\mathbb{Z}_{31}^*$, and a generator $g = 3$?

3 Rabin Cryptosystem (3/30)

In a Rabin cryptosystem, choose two large distinct prime numbers p and q s.t. $p \equiv q \equiv 3 \ mod 4$, and compute $n = p * q$. A message M can be encrypted by first converting it to a number $m < n$ and computing $c = m^2 \ mod \ n$. To decrypt, we compute the square root of c modulo p and q:

$$m_p = c^{\frac{1}{4}(p+1)} \ mod \ p$$

$$m_q = c^{\frac{1}{4}(q+1)} \ mod \ q$$

Then, use the extended Euclidean algorithm to find y_p and y_q s.t. $y_p * p + y_q * q = 1$. Finally, use the Chinese remainder theorem to find the four square roots of $c \ mod \ n$:

$$s_1 = (y_p * p * m_q + y_q * q * m_p) \ mod \ n$$

$$s_2 = n - s_1$$

$$s_3 = (y_p * p * m_q - y_q * q * m_p) \ mod \ n$$

$$s_4 = n - s_3$$

One of these solutions is the original plaintext m.
(1) Why one of the solutions should be the original plaintext, and how many possible solutions we will have?
(2) Why are the formulas for m_p and m_q correct?
(3) Consider $p = 71$ and $q = 23$. Show key generation, message $m = 74$ encryption, and message decryption.

4 RSA (3/30)

Let $p = 73$ and $q = 37$.
(1) Show with Fermat primality testing that the numbers are not composite with probability larger than 30%.

(2) Show key generation for RSA (note that e cannot be equal to 3).

(3) Show how to encrypt and decrypt message $m = 24$. For decryption, use Chinese Remainder Theorem to show how calculations can be done in a more efficient way.

5 ElGamal Signature (3/30)

Consider the Elgamal signature scheme with $p = 47$ and generator $g = 3$ for $\mathbb{Z}_{47}^*$. Moreover, assume that Alice chose the secret value $a = 113$.
(1) Show the key generation.
(2) Suppose Alice wants to sign the message $x = 109$ and chooses $k = 103$ as a random value. Show how to sign the message and the corresponding signature.
(3) Please show the verification for the above signature.

6 Fermat Primality Test (3/30)

Please select a number (which could be random 3-digits number) and run the Fermat primality test for the number. Is the number a composite? If not, how many witnesses you have to make that conclusion? Please show detailed steps.

7 Finite Field Representation (4/30)

- Please construct additive and multiplicative representation of a field $GF(2^3)$ using irreducible polynomial $x^3 + x + 1$.
- Please construct a finite field $GF(2^4)$ using polynomial $X^4 + x + 1$.

8 Groups and Cosets (3/30)

Assume G is a cyclic group of order 20 with generator a.
(1) What are the orders (individually) of a^3, a^4, and a^{14}? Note that the notation a^x refers to the element of a group.
(2) How many distinct cosets are there of $H = \langle a^5 \rangle$?
(3) How many distinct cosets are there of $H = \langle a^7 \rangle$?

9 S-box Calculation (4%)

Consider S-box of size 3×3:

$$F(x) = \frac{(x+1)^2}{x} + b.$$

Note:

$$F(x) = \begin{cases} b & \text{if } x = 0 \\ \frac{(x+1)^2}{x} + b & \text{otherwise.} \end{cases}$$

(1) Show additive, multiplicative, and vector representation of field elements. And show the truth table for this S-Box. Use irreducible polynomial $x^3 + x + 1$ and $b = 2$.
(2) What is the nonlinearity based on the calculated Walsh-Hadamard value? Assume this is the maximal value in the Walsh-Hadamard spectrum.