University of Notre Dame
Department of Computer Science and Engineering

CSE 40622 Cryptography
Fall Semester, 2021

Mid-term Exam

Instruction

- **You cannot use theorems that did not appear in the lecture notes or did not appear in the lectures.**
- If something is not clear, do ask in the middle of the exam!
- I do not give credits for correct answers alone. I give up to 90% of the credits to wrong answers with logical analysis.

Code of Honor Pledge (must be read and signed)

- I will answer the questions on my own without referring to others who are not teaching staff.
- By writing my name below, I agree to abide by the ND Honor Code.

Name (ALL CAPITAL): PARKER MOORE

NetID (ALL CAPITAL): PMOORE2

Date: October 13th, 2021

Scores of this exam

Question	Maximum Points
1	20
2	20
3	20
4	20
5	20
Total	100

1. (20 pts) **Lecture 03-05, WA02, the Corollary of Euler's Theorem**

   Suppose an algorithm can only take in positive integers a, b, n and compute $a^b \mod n$. It does not accept negative integers. Given that n is a prime number and $\gcd(a, n) = 1$, how can we use this algorithm to compute $a^{-k} \mod n$ when k is a positive integer less than $n - 1$?

   *** Answers using the Extended Euclidean algorithm get 12/20 pts only.**

   Answer:

Since $\gcd(a,n) = 1$, we know that the inverse exists and $a^k \mod n = a^{k \mod \phi(n)} \mod n$ from WA02. We can use the algorithm to $a^k \mod n$ and take the inverse of a^k.

2. (20 pts) **Lecture 06-08, WA03: Finite group and group operators.**

   Suppose $(\mathbb{G}, \circ)$ is a finite cyclic group. Suppose $\mathbb{H} = \{x_1, x_2, \cdots, x_m\}$ is a special subset of $\mathbb{G}$ where $\circ$ is closed in it and also associative. Prove that $|\mathbb{H}|$ divides $|\mathbb{G}|$.

   - Hint:
     - First, prove that, for any $x_i \in \mathbb{H}$, there will be some integer m such that x_i^m is an identity element and it exists in $\mathbb{H}$.
     - Second, show that the inverse of x_i exists in $\mathbb{H}$.
     - Third, prove that $(\mathbb{H}, \circ)$ is a subgroup of $(\mathbb{G}, \circ)$.

   Answer:

- Since the binary Operator is closed in $\mathbb{H}$ we will eventually find an $m = |\mathbb{G}|$ and $x^{|\mathbb{G}|} = e$ so $\mathbb{H}$ has the identity element
- Since we found an $m = |\mathbb{G}|$ where $x^{|\mathbb{G}|} = e$, there exists an $x^{|\mathbb{G}|-1} = x^{-1}$. This is also guaranteed to belong in $\mathbb{H}$ because the binary operator is closed. This means $\mathbb{H}$ has an inverse.
- Because of closure, associativity, identity existence, and invertibility, the subset $\mathbb{H}$ is a group which makes $\mathbb{H}$ a subgroup.
- The order of a subgroup must divide a group according to Lagranges Theorem

3. (20 pts) **Lecture 06-08, WA03: Finite group and group operators.**

In the proof of Lagrange's Theorem, we have a subset $x\mathbb{H}$ of a group $\mathbb{G}$. Prove by contradiction that $x\mathbb{H}$ is not closed with the same group operator.

- Hint: Assume that there are two elements in $x\mathbb{H}$, say xh_i, xh_j, such that $xh_i \circ xh_j \in x\mathbb{H}$. In other words, assume that there is a third element $xh_k \in \mathbb{H}$ such that $xh_i \circ xh_j = xh_k$. Then, derive a contradiction.

Answer:

$$xh_i \circ xh_j = xh_k$$

$$x^{-1}(x^2 h_i h_j) = (xh_k)x^{-1}$$ ← we can ~~take~~ take the inverse of x since x is in $\mathbb{G}$ and $\mathbb{G}$ is a group

$$xh_ih_j = h_k$$

This is a contradiction because $xh_ih_j \in x\mathbb{H}$ and $h_k \in \mathbb{H}$. Since we know that $\mathbb{H} \cup x\mathbb{H} = \emptyset$, we cannot set those two elements equal to each other.

4. (20 pts) **Lecture 09-10, PA02, WA04: QR and QNR**

Taeho tried to develop the ElGamal encryption scheme, and he found the g using the following code and used the group generated by g in his implementation.

```
// initialize the random state
gmp_randstate_t rndstate;
gmp_randinit_default(rndstate);
gmp_randseed_ui(rndstate, (unsigned long)time(NULL));

mpz_t p,q;
mpz_inits(p, q, NULL);

// find a prime p = 2q + 1 with prime q
while(mpz_probab_prime_p(p, 50) == 0){
        mpz_urandomb(q, rndstate, 2048);
        while(mpz_probab_prime_p(q,50) == 0){
                mpz_urandomb(q, rndstate, 2048);
        }
        mpz_mul_ui(p, q, 2);
        mpz_add_ui(p, p, 1);
}

int notFinished = 1;
mpz_t g, g2, gq;
mpz_inits(g, g2, gq, NULL);

// find a generator whose order is exactly 2q=p-1
while(notGenerator){ notFinished
        mpz_urandomm(g, rndstate, p);

        if(mpz_cmp_ui(g,1) == 0) continue;

        mpz_powm_ui(g2, g, 2, p);
        if(mpz_cmp_ui(g2,1) == 0) continue;

        mpz_powm(gq, g, q, p);
        if(mpz_cmp_ui(gq, 1) != 0) continue;

        notFinished = 0;
}
```

4.1. Explain why the g from the code above is not the generator of $\mathbb{Z}_p^*$ (10 pts).
Answer:

mpz_cmp_ui(a,b) returns 0 if a=b. In order to find a generator of Z_p^* we need g != e. Also we want $g^2 \bmod p \neq 1$. The first if should be if(mpz_cmp_ui(g,1) != 0) and the second should be if(mpz_cmp_ui(g2,1) != 0)

4.2. Explain why his implementation will be secure against QR/QNR attacks (10 pts).
Answer:

This will be secure against QR/QNR attacks because g will generate a cyclic group of only QRs. Therefore, an attacker cannot calculate the Legendre symbol and find use the fact that a number is a QR or a QNR to their advantage because they are all QRs.

5. (20 pts) **Lecture 10-13: Formal definitions**

5.1. What does the following mean conceptually in plain language (5 pts)? You do not need to explain your answer.

* Note that $\mathcal{A}$ can be any PPTA algorithm that returns anything.

> The following is true for all PPTA $\mathcal{A}$ and some negligible function $\text{negl}(\kappa)$:
>
> $$\Pr\left[\mathcal{A}(g, g^a, g^b) = g^{ab} | g \in \mathbb{G}, a, b \in \mathbb{Z}\right] \leq \text{negl}(\kappa)$$

(One sentence is enough to get full credits)

Answer:

CDH problem is intractable

5.2. If the DDH problem is intractable in a group $\mathbb{G}$, is the CDH problem intractable in $\mathbb{G}$ as well (5 pts)? Why (10 pts)?

Answer:

DDH intractable → CDH intractable

$\neg$(CDH intractable) → $\neg$(DDH intractable)

CDH is easy → DDH is easy

This is true because CDH says that given g, g^a, g^b find g^{ab}. DDH says given (g, g^a, g^b, X) determine if X is g^{ab} or g^c. If CDH is easy, if we have g^{ab}, we will easily be able to know if X is g^{ab} or g^c because we already have g^{ab}. Because of contraposition we also know that If DDH is intractable, then CDH is intractable