MATH 3094 - Second Practice Midterm

YOUR NAME: _____

P1	P2	P3	P4	P5	Extra	Total

Show all your work. Explain all your answers. Do not use calculator programs.

Problem 1. (25 points) For each problem below, **explain** your steps to find the answer.

(1) *Understand the meaning and how to compute with Legendre symbols.* Find the values of

$$\left(\frac{2}{29}\right), \left(\frac{-1}{29}\right), \left(\frac{17}{29}\right), \left(\frac{29}{17}\right).$$

(2) *Find primes satisfying certain congruence conditions and/or certain Legendre conditions.* Find primes p and q such that $p = 2q + 1$. Both p and q should be > 15.

(3) Find three distinct primes p such that $\left(\frac{p}{7}\right) = 1$.

(4) *Learn how to use the law of quadratic reciprocity.* Compute $\left(\frac{19}{41}\right)$ using Gauss's Law of Quadratic Reciprocity.

Problem 2. (25 points) Let $N = 221$.

(1) *Learn how to use the Fermat primality test.* Is 2 a Fermat witness for the compositeness of N?

(2) *Learn how to use the Miller–Rabin primality test.* Is 2 a Miller–Rabin witness for the compositeness of N?

(3) *Learn how to use Pollard's $p-1$ method to find a factorization of N.* Use Pollard's $p-1$ method to find a factorization of N. Please indicate clearly each step of the algorithm.

Problem 3. (25 points)*Learn how to use RSA.* In this problem, $N = 221$, as in Problem 2. Alice wants to set up an RSA encryption scheme with N as her modulus.

(1) Can Alice choose $e = 3$ as an encryption exponent?

(2) Can Alice choose $e = 7$ as an encryption exponent?

(3) If $e = 7$, what is the decryption exponent d?

(4) Alice sets up RSA with $(N, e) = (221, 7)$. Bob wants to send the message $m \equiv 2 \bmod 221$. What is the encrypted message? How does Alice decrypt the message?

(5) Alice sets up RSA with $(N, e) = (323, 5)$ and Eve intercepts a message from Bob with cipher 11 mod 323. What was Bob's original message?

Problem 4. (25 points) *Learn how to use the Primer Number Theorem, and the confidence probabilities associated to Miller–Rabin tests.*

(1) Consider the number $n = 300001$. According to the prime number theorem, how likely is it that n is a prime number?

(2) Approximately, how many primes are there in the interval $[300000, 400000]$ according to the prime number theorem?

(3) If a is an integer that is *not* Miller–Rabin witness for the compositeness a number p, what is the probability that p is prime? What if we found two integers a and b that are *not* Miller–Rabin witnesses for p, what is the probability that p is prime?

Problem 5. (25 points) *Learn how to use the digital signature algorithms we saw in class: RSA, Elgamal, and DSA.*

(1) Sam sets up an RSA digital signature protocol with $N = 221$. Sam chooses $e = 7$, and the document to be signed is $D \equiv 10 \bmod 221$. Produce a signature for D.

(2) Help Victor verify that the signature in part (1) is legitimate.

(3) Sam sets up an Elgamal digital signature protocol with $p = 43$ and $g = 3$. Sam chooses $a = 5$, $k = 2$, and the document to be signed is $D \equiv 10 \bmod 43$. Produce a signature for D.

(4) Help Victor verify that the signature in part (3) is legitimate.

(5) Sam sets up a DSA digital signature protocol with $p = 43$, $q = 7$, and $g = 41$. Sam chooses $a = 5$, $k = 2$, and the document to be signed is $D \equiv 10 \bmod 43$. Produce a signature for D.

(6) Help Victor verify that the signature in part (5) is legitimate.

Highlights of Chapters 3-4.

Chapter 3: Integer Factorization and RSA

1. **Number theory concepts:**
   (a) Euler's formula for pq: if p and q are distinct primes and $g = \gcd(p-1, q-1)$, then $a^{(p-1)(q-1)/g} \equiv 1 \bmod pq$ for all a with $\gcd(a, pq) = 1$.
   (b) Let p and q be distinct primes and $g = \gcd(p-1, q-1)$, and let d such that $de \equiv 1 \bmod (p-1)(q-1)$. Then, the congruence $x^e \equiv c \bmod pq$ has a **unique** solution $x \equiv c^d \bmod pq$.
   (c) Fermat witness: an integer a is a witness for the compositeness of n if $a^n \not\equiv a \bmod n$.
   (d) Proposition (Miller-Rabin): Let p be an odd prime, with $p - 1 = 2^k q$ where q is odd. Let a be relatively prime to p. Then, one of the following is true:
   - $a^q \equiv 1 \bmod p$, or
   - one of $a^q, a^{2q}, \ldots, a^{2^{k-1}q}$ is $\equiv -1 \bmod p$.

   (e) Let n be an odd composite number. Then at least 75% of the numbers between 1 and $n-1$ are Miller-Rabin witnesses for n.
   (f) The Prime Number Theorem: Let $\pi(x)$ be the number of primes in the interval $[1, x]$. Then, $\lim_{x\to\infty} \pi(x)/(x/\ln(x)) = 1$.
   (g) Quadratic residues: a is a QR mod p if $x^2 \equiv a \bmod p$ has a solution, a QNR otherwise. There are $(p-1)/2$ QR's and $(p-1)/2$ QNR's mod p.
   (h) Quadratic residue symbol, or Legendre symbol: $\left(\frac{a}{p}\right)$ is 1 is a is a QR, -1 if a is a QNR, and 0 if $p|a$.
   (i) Quadratic Reciprocity for distinct odd primes p and q:
   - $\left(\frac{-1}{p}\right)$ is 1 if $p \equiv 1 \bmod 4$, and -1 if $p \equiv 3 \bmod 4$.
   - $\left(\frac{2}{p}\right)$ is 1 if $p \equiv \pm 1 \bmod 8$, and -1 if $p \equiv \pm 3 \bmod 8$.
   - $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if p or $q \equiv 1 \bmod 4$, and $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ if $p \equiv q \equiv 3 \bmod 4$.

2. **Cryptography:**
   (a) RSA:
   - Bob picks secret primes p, q, and e with $\gcd(e, (p-1)(q-1)) = 1$. Publishes $N = pq$ and e. Bob also computes d such that $ed \equiv 1 \bmod (p-1)(q-1)$.
   - Alice chooses plaintext m, computes $c \equiv m^e \bmod N$, sends c to Bob.
   - Bob computes $m \equiv c^d \bmod N$.

   (b) Person-in-the-middle attacks.
   (c) Fermat's primality test using Fermat witnesses.
   (d) Miller-Rabin primality test using Miller-Rabin witnesses.
   (e) Pollard's $p-1$ factoring algorithm:
   - N is to be factored. Set $a = 2$ (or some other value).
   - Compute $a^2, (a^2)^3, (a^6)^4, \ldots \bmod N$, and $d = \gcd(a^{j!} - 1, N)$.
   - If $1 < d < N$, then d is a proper divisor of N and we have factored N into smaller numbers.

   (f) Goldwasser-Micali cryptosystem:
   - Bob chooses secret p and q, choose a with $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$, and publishes $N = pq$ and a.
   - Alice chooses $m = 0$ or 1, chooses $1 < r < N$, and computes $c = r^2 \bmod N$ if $m = 0$ and $c = ar^2 \bmod N$ if $m = 1$. Sends c to Bob.
   - Bob computes $\left(\frac{c}{p}\right)$, and $m = 0$ if $\left(\frac{c}{p}\right) = 1$ and $m = 1$ if $\left(\frac{c}{p}\right) = -1$.

Chapter 4: Digital Signatures

1. **Number theory concepts:**
   (a) If p is a prime and q divides $p-1$, then there are elements $g \bmod p$ of exact order q.
2. **Cryptography:**
   (a) RSA digital signatures:
   - Sam chooses secret primes p, q. Chooses verification exponent e with $\gcd(e,(p-1)(q-1))=1$, and d with $de \equiv 1 \bmod (p-1)(q-1)$. Publishes $N=pq$ and e.
   - Chooses document $D \bmod N$, and signs document $S \equiv D^d \bmod N$. Sends (D,S) to Victor.
   - Victor verifies $S^e \equiv D \bmod N$.

   (b) Elgamal digital signature:
   - A trusted party chooses large prime p and a primitive root $g \bmod p$.
   - Sam chooses secret signing key $1 \le a \le p-1$. Compute $A \equiv g^a \bmod p$, and publishes A.
   - Chooses $1 < k < p$ with $\gcd(k,(p-1))=1$, a document $D \bmod p$, and computes signature $S_1 \equiv g^k \bmod p$ and $S_2 \equiv (D-aS_1)k^{-1} \bmod (p-1)$. Sends (D,S_1,S_2) to Victor.
   - Victor verifies $A^{S_1}S_1^{S_2} \equiv g^D \bmod p$.

   (c) DSA digital signature:
   - A trusted party chooses large primes p and q such that $p \equiv 1 \bmod q$ and an element $g \bmod p$ of exact multiplicative order q.
   - Sam chooses secret signing key $1 \le a \le q-1$. Compute $A \equiv g^a \bmod p$, and publishes A.
   - Chooses $1 < k < q$, a document $D \bmod q$, and computes signature $S_1 \equiv (g^k \bmod p) \bmod q$ and $S_2 \equiv (D+aS_1)k^{-1} \bmod q$. Sends (D,S_1,S_2) to Victor.
   - Victor computes $V_1 \equiv DS_2^{-1} \bmod q$ and $V_2 \equiv S_1S_2^{-1} \bmod q$ and
   - Victor verifies $(g^{V_1}A^{V_2} \bmod p) \bmod q = S_1$.