Midterm 1 (July 3rd)

Please put away all electronic devices. You are permitted to refer to a single sheet of notes (two-sided, standard 8×11).

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>B1</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>B2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>B3</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Instructions: Complete problems 1–6, two of problems A1–A4, and two of problems B1–B3. Indicate exactly two problems of A1–A4 and exactly two of problems B1–B3 which you want graded by circling them below:

A1  A2  A3  A4

B1  B2  B3
1a. Which $x \in \{0, \ldots, 10\}$ satisfies $2^{124} \equiv x \mod 11$? (Hint: FLT.)

1b. Which $y \in \{0, \ldots, 70\}$ satisfies $3^{493} \equiv y \mod 71$?

2b. What is the order of 2 in the group $(\mathbb{F}_7^*, \cdot)$?
4. Alice and Bob are using the Diffie–Hellman protocol to establish a key for a symmetric cipher. After obtaining a suitable prime $p$ and $g \in \mathbb{F}_p^*$ from Tom, Alice and Bob choose secret values $a, b \in \mathbb{Z}$. Alice sends Bob $g^a$ and Bob sends Alice $g^b$. What is the value of their shared secret?

5. Fiona is attempting to solve a DLP of the form $g^x = h$ where $g$ has order 10000. If Fiona decides to use the baby step–giant step algorithm (as described in class), how long will each of her lists be?

6a. Use the congruence $81^2 \equiv 4 \mod 6557$ to factor 6557.

6b. If $G$ is a group of order 6557 and the order of $g \in G$ is $k$, what are the possible values of $k$?
Problem A1

a. Let $N$ be an odd integer. Prove that if $N \equiv 3 \mod 4$, then there is a prime $p$ such that $p \mid N$ and $p \equiv 3 \mod 4$.

b. Prove that there are infinitely many primes $p$ such that $p \equiv 3 \mod 4$. 
Problem A2

Eve has put her not-so-bright partner Doofus in charge of solving the DLP $4^x = 6$ in $\mathbb{F}_{19}^*$. Eve told Doofus that the order of 4 in $\mathbb{F}_{19}^*$ is 9. Thinking himself a clever man, Doofus raises both sides to the 3rd power:

$$(4^x)^3 = 6^3,$$

$$(4^3)^x = 6^3,$$

$$7^x = 7$$

(in $\mathbb{F}_{19}^*$). Excited, Doofus tells Eve “The answer is $x = 1$, boss!” Eve sighs

a. Explain what Doofus has done wrong.

b. Find the correct answer. (Hint: $4^4 = 9$.)
Problem A3

a. Let $b$ be an integer, $b \geq 2$. What are the possible values of $\gcd(b - 1, b + 1)$?

b. Suppose that $p$ is an odd prime, $e$ is an integer, and $e \geq 1$. Prove that if $b^2 \equiv 1 \mod p^e$, then either $b \equiv 1 \mod p^e$ or $b \equiv -1 \mod p^e$. 
Problem A4

Suppose Bob has encrypted some important files with the “Discreet” system, whose security is equivalent to the hardness of the DLP modulo a prime $p$ (which Bob chooses).

Bob knows two large primes off the top of his head,

$$p_1 = 48947 \quad \text{and} \quad p_2 = 15502033,$$

and he also knows the factorizations

$$p_1 - 1 = 2 \cdot 24473 \quad \text{and} \quad p_2 - 1 = 2^4 \cdot 3^2 \cdot 7^2 \cdot 13^3.$$

a. Bob knows that Eve will try to use the baby step–giant step algorithm to access his files, and so he chooses $p_2$ to encrypt. Qualitatively speaking, why might Bob think this is a better choice than $p_1$?

b. In a panic, Alice calls up Bob and says “Eve managed to quickly break into my encrypted files! She’s using the Pohlig–Hellman algorithm now!” Bob quickly decides that he should maybe encrypt his files using the prime $p_1$ instead. Why?
Problem B1

Suppose that Eve’s (evil) robot friend Gustavo can solve the DHP quickly.

If Bob sends Alice a message encrypted with ElGamal, and Eve intercepts this message, show that Eve can decrypt the message with Gustavo’s assistance.

[As usual, you may assume Eve knows the publicly available encryption parameters \((p, g, A)\).]
Problem B2

Captain Alice of the Starship Enterprise thinks she’s finally thwarted the nefarious Space Pirate Eve! After a long space battle, Eve’s forces boarded the Enterprise, but Alice managed to press the big red SELF-DESTRUCT button before escaping on a shuttlecraft. Eve can cancel the self-destruct sequence, but only with the correct authorization code!

- Eve knows that Alice’s authorization code is a number \( n \in \{0, \ldots, 9999\} \).
- Eve somehow managed to learn the values of \( n \% 2 \), \( n \% 3 \), \( n \% 5 \), \( n \% 7 \), and \( n \% 11 \).
- Eve can make exactly five attempts to cancel the self-destruct before the Enterprise computer locks her out.

Prove that Eve has enough information to cancel the self-destruct sequence!
Problem B3

Alice and Bob have agreed to encrypt their messages using an affine cipher modulo a (publicly known, large) prime number \( p \). The cipher is set up as follows:

- The key space is \( \mathbb{F}_p^* \times \mathbb{F}_p \) (each key is a pair \((k, k')\) where \( k \in \mathbb{F}_p^* \) and \( k' \in \mathbb{F}_p \)).
- The message space and ciphertext space are both \( \mathbb{F}_p \).
- The encryption function is defined by \( e((k, k'), m) = km + k' \).

a. What is the decryption function?

b. Is this a symmetric cipher or an asymmetric cipher? Why?

c. Show that this cipher is vulnerable to a chosen plaintext attack.
Midterm 2 (July 23rd)

Name:

Please put away all electronic devices. You are permitted to refer to a single sheet of notes (two-sided, standard 8×11).

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Instructions: Complete all problems.
1 Three steps to factorization (14 pts.)

In the quadratic sieve and related methods, we are attempting to factor $N$ by producing a nontrivial _____ modulo $N$.

One of the first steps is to choose a smoothness bound $B$. Expressed in terms of $N$ and elementary functions familiar from calculus, a good approximate value for $B$ is _____.

Once enough congruences between squares and $B$-smooth numbers have been obtained, we perform the elimination step using linear algebra over the field _____.


2 Computing Legendre Symbols (7 pts.)

Compute the value of the Legendre symbol \( \left( \frac{234}{199} \right) \).

(Advice: The correct answer is worth only 1 pt. Justify each step!)
3 Pollard’s $p - 1$ (7 pts.)

Eve is trying to factor Alice’s public RSA modulus $N = 577 \cdot 617$ using Pollard’s $p - 1$ method. Using the factorizations $576 = 2^6 \cdot 3^2$ and $616 = 2^3 \cdot 7 \cdot 11$, determine the least positive integers $n_1$ and $n_2$ such that $576 \mid n_1!$ and $616 \mid n_2!$. 
4  Miller–Rabin Witnesses (14 pts.)

Alice is preparing a new set of RSA keys so that she and Bob can communicate without that dastardly Eve spying on them. In considering the integer 

\[ n = 1000000000039 = 10^{12} + 39, \]

Alice checks that none of \( i = 2, \ldots, 100 \) are Miller–Rabin witnesses modulo \( n \), and thereby convinces herself that \( n \) must be prime.

Explain why Alice’s check does not prove that \( n \) is prime.

Gustavo the robot verifies (for fun) that none of \( i = 2, \ldots, 0.3 \times 10^{12} \) are Miller–Rabin witnesses modulo \( n \). Explain why this proves that \( n \) is prime. (Hint: Gustavo’s proof does not rely on the generalized Riemann hypothesis.)
7 YOSO (7 pts.)

Eve is attempting to factor the integer $N = 1751$. Having chosen a factor base of $\{2, 3, 5\}$, she eventually obtains the congruences

\[
\begin{align*}
95^2 &\equiv 2 \cdot 3^3 \cdot 5 \quad \text{mod } 1751 \\
113^2 &\equiv 2^9 \quad \text{mod } 1751 \\
139^2 &\equiv 2^2 \cdot 3 \cdot 5 \quad \text{mod } 1751
\end{align*}
\]

Using this information, Eve computes $\gcd(1751, a - b)$ in an attempt to factor 1751 for what values of $a$ and $b$? (You may express $a$ and $b$ as unsimplified arithmetic expressions.)
8 Rhonda Fights for Cryptographic Freedom (15 pts.)

The totalitarian Tom has decided that all of his citizens will use the same public modulus \( N = 116843 \) but that they are not allowed to know the prime factorization of \( N \). Instead, Tom provides each citizen of his (small) country a pair \((e, d)\) where \( ed \equiv 1 \text{ mod } \phi(N) \).

Tom gives the rebellious Rhonda the encryption key \( e = 11111 \) and the decryption key \( d = 92951 \). After a moment of thought, Rhonda suspects that she can find the flaw in Tom’s implementation of RSA.

Rhonda computes \( ed - 1 = 1032778560 \).
What is the value of \( 3^{1032778560} \text{ mod } 116843 \)?

Next, Rhonda computes \( \frac{ed - 1}{2} = 516389280 \).
What is the value of \( 3^{516389280} \text{ mod } 116843 \)?

Finally, Rhonda computes \( \frac{ed - 1}{4} = 258194640 \) and is excited to find that \( 3^{258194640} \equiv 106252 \text{ mod } 116843 \). Explain why Rhonda now has enough information to factor \( N \) quickly.