There are 6 problems on this exam. Please take a photo/scan your solution of each problem done on paper (not necessarily the printed exam) and upload the problem on the Moodle course web page on wolfware.ncsu.edu.

By taking the exam, you agree that you will not consult with others about the solution. You can consult your notes/book.

You have until noon today, Tuesday, April 7, to upload the photos/scans. Good luck!
Problem 1 (16 points)

(a, 4pts) True or false: \( \forall n \in \mathbb{Z}_{\geq 2}, a, b, c \in \mathbb{Z}_n, b \neq 0: ab \equiv cb \pmod{n} \implies a \equiv c \pmod{\frac{n}{\gcd(b, n)}}. \)
Please explain.

(b, 4pts) True or false: 101101 = 7 \cdot 11 \cdot 13 \cdot 101 is a pseudo-prime. Please explain.

(c, 4pts) Please compute \( 2^{80} \pmod{100} \), showing your work.

(d, 4pts) Please show how to compute \( a^{15} \pmod{n} \) for \( a \in \mathbb{Z}_n \) with 5 multiplications modulo \( n \).
Problem 2
(5 points): Please compute residues \(x, y \in \mathbb{Z}_7\), or prove that none exist, such that

\[
6x + 2y \equiv 2 \pmod{7}
\]
and

\[
2x + 3y \equiv 2 \pmod{7}.
\]

Problem 3
(5 points) Let \(p, q\) be two prime numbers \(\geq 2, p \neq q\). Please verify that

\[
\sum_{d \text{ divides } pq \text{ and } d \geq 1} \phi(d) = p^2 q.
\]
Problem 4 (8 points): Consider $1716 = 11 \cdot 12 \cdot 13$ and let $a \in \mathbb{Z}_{1716}$ with

$$a \equiv 10 \pmod{11},$$
$$a \equiv 4 \pmod{12},$$
$$a \equiv 12 \pmod{13}.$$

Please compute $y_0 \in \mathbb{Z}_{11}$, $y_1 \in \mathbb{Z}_{12}$ and $y_2 \in \mathbb{Z}_{13}$ such that

$$a = y_0 + y_1 \cdot 11 + y_2 \cdot 11 \cdot 12.$$

Then compute $a$. Please show all your work.
Problem 5 (5 points): Please consider the following (toy) instance of the RSA: the public modulus is $n = 51$ and the private (deciphering) exponent is $j = 13$. Please compute the public enciphering exponent $k$ such that $(m^k)^{13} \equiv m \pmod{51}$ for all messages $m$ with $\gcd(m, 51) = 1$. Please decipher the message $m$ from the cipher text $c = (m^k \mod 51) = 2$ that was encoded with the computed $k$. Please show your work.

Problem 6 (5 points): Consider the following table of indices (discrete logarithms) for the prime number 19 with respect to the primitive root $g = 10$:

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{ind}_{10}(a)$</td>
<td>0</td>
<td>17</td>
<td>5</td>
<td>16</td>
<td>2</td>
<td>4</td>
<td>12</td>
<td>15</td>
<td>10</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td>14</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

Please list all primitive roots modulo 19.