Exercise Set for Chapter 9: 3CC 2002
Public Key Cryptography

1. Find the inverses of 2 and 5 in $\mathbb{Z}_{17}$.

2. Prove that
   (a) $n^6 - 1$ is divisible by 7 if $\text{gcd}(n, 7) = 1$.
   (b) $n^7 - n$ is divisible by 42 for any integer $n$.
   (c) $n^{12} - 1$ is divisible by 7 if $\text{gcd}(n, 7) = 1$.
   (d) $n^{6k} - 1$ is divisible by 7 if $\text{gcd}(n, 7) = 1$, for any positive integer $k$.
   (e) $n^{13} - n$ is divisible by 2, 3, 5, 7 and 13 for any integer $n$.
   (f) $n^{12} - a^{12}$ is divisible by 13 if $n$ and $a$ are both coprime to 13.
   (g) $n^{12} - a^{12}$ is divisible by 91 if $n$ and $a$ are both coprime to 91.

3. Let $p = 103$. Exactly one of 2 and 5 is a primitive element in $\mathbb{Z}_p$. Find out which one and prove your answer. Call this primitive element $g$.

4. If that was too messy then try a small one. Let $p = 23$. Exactly one of 2 and 5 is a primitive element in $\mathbb{Z}_p$. Find out which one and prove your answer. Call this primitive element $g$.

5. Alice and Bob wish to establish a key $k \mod p$ for secret communication using the Diffie-Hellman procedure and $p$ and the primitive element $g$ (a) from question 1, and (b) from question 2. Alice selects $a \equiv 27 \pmod{p}$ and Bob selects $b \equiv 72 \pmod{p}$. Explain what information Alice sends to Bob, and what Bob sends to Alice, and how each of them finds the key $k \mod p$. Make sure also that you find the key $k$.

6. Suppose that user $U$ has a public key $k_U = (n, e)$ and secret key $\bar{k}_U = (n, d)$ for the RSA cryptosystem, where $n = pq$ with $p$ and $q$ primes, and suppose that someone encrypts a message $x$ such that $\gcd(x, n) \neq 1$, and sends it to $U$. Prove that $d_U(e_U(x)) \equiv x \pmod{n}$.

7. (A ‘baby RSA example’) User Ursula has secret key $\bar{k}_U = (33, 7)$.
   (a) Determine Ursula’s public key $k_U = (n, e)$.
   (b) What is Ursula’s encryption function $e_U(x)$ and decryption function $d_U(y)$?
   (c) Using Table 1 to make each letter A-Z correspond with an integer less than 33, encrypt the message JOHNN.
   (d) Demonstrate how Ursula will decrypt this message.
8. Let $n$ be an odd integer. Prove that $n$ factorises as $n = ab$ ($a \geq b$) if and only if we can write $n$ as $n = t^2 - s^2$ with $t = \frac{1}{2}(a + b)$, $s = \frac{1}{2}(a - b)$.


10. **Protocol Failure:** Suppose that each letter A-Z is replaced by its numerical equivalent (that is, A is replaced by 0, B is replaced by 1, etc).

   (a) Describe how Oscar can easily decrypt a message which is encrypted in this way.

   (b) Illustrate this attack by decrypting the following ciphertext (which was encrypted using an RSA Cryptosystem with $n = 18721$ and user public key exponent $e = 25$): $365, 0, 4845, 14930, 2608, 2608, 0$.

11. **Protocol Failure:** Two users $U_1$ and $U_2$ choose the same modulus $n$ and choose public key encryption exponents $e_1$ and $e_2$ which are relatively prime, that is, $k_{U_1} = (n, e_1)$, $k_{U_2} = (n, e_2)$ with $\gcd(e_1, e_2) = 1$. Alice sends the same message, $x$, to both. Oscar intercepts $y \equiv x^{e_1} \pmod{n}$ and $z \equiv x^{e_2} \pmod{n}$. Oscar then computes $c_1 = e_1^{-1} \pmod{e_2}$, and $c_2 = (c_1 e_1 - 1)/e_2$. (Note that $c_2$ is an integer since $c_1 e_1 \equiv 1 \pmod{e_2}$.) Finally, Oscar computes $y^{c_1} (z^{c_2})^{-1} \pmod{n}$.

   (a) Prove that the last value Oscar computes is $x$. Thus, Oscar can decrypt the message Alice sent, even though the cryptosystem may be "secure".

   (b) Illustrate the attack by computing $x$ by this method if $n = 18721$, $e_1 = 43$, $e_2 = 7717$, $y = 12677$ and $z = 14702$. 

Table 1: Correspondence of alphabet with integers less than 33

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>