Solutions to Assignment 11

Barr 4.6: 1, 2.

1. (a) Following Example 4.6.1 (Page 307), we find that $\sigma = 70$.
   (b) Given $(\tilde{x}, \tilde{\sigma}) = (54, 89)$, Bob regards the pair to be likely to be authentic since $54^7 \mod 91 = 89$.

2. (a) Alice’s encrypted pair is (185, 21).
   (b) The original plaintext and signature are: $\tilde{x} = 44$, $\tilde{\sigma} = 86$. This is a valid signature pair since $\tilde{\sigma}^{\tilde{x}} \mod 91 = 86^7 \mod 91 = 44$.

Barr 4.7: 1*, 3, 7*

1.

<table>
<thead>
<tr>
<th>n</th>
<th>$n^2 \mod 39$</th>
<th>n</th>
<th>$n^2 \mod 39$</th>
<th>n</th>
<th>$n^2 \mod 39$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>13</td>
<td>13</td>
<td>26</td>
<td>13</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>14</td>
<td>1</td>
<td>27</td>
<td>27</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>15</td>
<td>30</td>
<td>28</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>16</td>
<td>22</td>
<td>29</td>
<td>22</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>17</td>
<td>16</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>18</td>
<td>12</td>
<td>31</td>
<td>25</td>
</tr>
<tr>
<td>6</td>
<td>36</td>
<td>19</td>
<td>10</td>
<td>32</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>20</td>
<td>10</td>
<td>33</td>
<td>36</td>
</tr>
<tr>
<td>8</td>
<td>25</td>
<td>21</td>
<td>12</td>
<td>34</td>
<td>25</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>22</td>
<td>16</td>
<td>35</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>22</td>
<td>23</td>
<td>22</td>
<td>36</td>
<td>9</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>24</td>
<td>30</td>
<td>37</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>27</td>
<td>25</td>
<td>1</td>
<td>38</td>
<td>1</td>
</tr>
</tbody>
</table>
Thus,
(a) The solutions to \( x^2 \equiv 1 \pmod{39} \) are 1, 14, 25 and 38.
(b) The solutions to \( x^2 \equiv 4 \pmod{39} \) are 2, 11, 28 and 37.
(c) The solutions to \( x^2 \equiv 12 \pmod{39} \) are 18 and 21.

3. | n   | \( n^2 \pmod{31} \) | n   | \( n^2 \pmod{31} \) | n   | \( n^2 \pmod{31} \) |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>13</td>
<td>14</td>
<td>26</td>
<td>25</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>14</td>
<td>10</td>
<td>27</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>15</td>
<td>8</td>
<td>28</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>16</td>
<td>8</td>
<td>29</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>17</td>
<td>10</td>
<td>30</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>18</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>19</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>18</td>
<td>20</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>21</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>19</td>
<td>22</td>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>7</td>
<td>23</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>28</td>
<td>24</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>20</td>
<td>25</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Thus,
The solutions to \( x^2 \equiv 1 \pmod{31} \) are 1 and 30.
The solutions to \( x^2 \equiv 2 \pmod{31} \) are 8 and 17.
The solutions to \( x^2 \equiv 8 \pmod{31} \) are 15 and 16.

7. The password \( s \) in the Fiat-Shamir setup is selected in the range 1 to \( n-1 \). Recall that 
\( n = p \cdot q \), where \( p \) and \( q \) are both large prime numbers. Note that \( n \) is published and \( v \) is 
sent during login – so both are easily obtainable. If the password \( s \) is not relatively prime 
to \( n \), then the greatest common divisor (gcd) of \( v \) and \( n \) is \( p \) or \( q \) (one of the primes!). 
Once \( p \) and \( q \) have been found, it is easy to find \( s \) and the system breaks down.
K1. In the Fiat-Shamir method, it is important to chose a modulus \( n = p \cdot q \) which is hard to factor because once the factorization is known, obtaining \( s = \sqrt{v} \pmod{n} \) is easy to calculate. Similarly, using a large prime \( n \) does not work because \( s = \sqrt{v} \pmod{n} \) is easily calculated if \( n \) is prime.

K2. Using modulus \( P = 10111 \) and base \( B = 12 \), find the dlog of:

(a) \( 2401 = 7^4 \).
\[
\text{dlog}(7) = 3640 \implies 12^{3640} \equiv 7 \pmod{10111}.
\]
\[
\therefore 2401 = 7^4 \equiv (12^{3640})^4 = 12^{14560}.
\] Using Fermat’s Little Theorem, we can reduce the exponent \( 14560 \pmod{10110} = 4450 \).
\[
\therefore \text{dlog}(7^4) = 4450.
\]

(b) \( 1001 = 7 \cdot 11 \cdot 13 \).
\[
\text{dlog}(1001) = \text{dlog}(7 \cdot 11 \cdot 13) = \text{dlog}(7) + \text{dlog}(11) + \text{dlog}(13)
\]
\[
= 3640 + 250 + 4478 = 8368.
\]
\[
\therefore \text{dlog}(1001) = 8368.
\]

(c) \( 10100 \).
\[
10100 \equiv -11 \pmod{10111}.
\]
\[
\text{dlog}(-11) = \text{dlog}(11) + \text{dlog}(-1). \text{ We are given } \text{dlog}(11), \text{ so all we have to do now is calculate } x = \text{dlog}(-1).
\]
\[
\text{Using the definition of dlogs, } 12^x \equiv -1 \pmod{10111} \implies 12^{2x} \equiv 1 \pmod{10111}. \text{ Since } 10111 \text{ is prime, using Fermat’s Little Theorem we know } 12^{10111-1} = 12^{10110} \equiv 1 \pmod{10111}.
\]
\[
\text{Thus, letting } 2x = 10110, \text{ we get } x = 5055.
\]
Thus, \( \text{dlog}(-1) = 5055 \implies \text{dlog}(10110) = \text{dlog}(-1) = \text{dlog}(11) + \text{dlog}(-1)
\]
\[
= 250 + 5055 = 5305.
\]
(d) 9889.

\[ 9889 \equiv 9889 + 10111 \pmod{10111} = 20000 \pmod{10111}. \]
\[ 20000 = 2^5 \cdot 5^4. \]
\[ \therefore \; \text{dlog}(20000) = \text{dlog}(2^5) + \text{dlog}(5^4). \]

\[ \text{dlog}(2^5) \equiv 5 \cdot \text{dlog}(2) \pmod{10110} = 5 \cdot 4918 \pmod{10110} \]
\[ = 24090 \pmod{10110} \equiv 3870. \]
\[ \text{dlog}(5^4) \equiv 4 \cdot \text{dlog}(5) \pmod{10110} = 4 \cdot 9226 \pmod{10110} \]
\[ = 36904 \pmod{10110} = 6574. \]
\[ \therefore \; \text{dlog}(9889) = \text{dlog}(20000) = \text{dlog}(2^5) + \text{dlog}(5^4) = 3870 + 6574 = 10444. \]
Reducing 10444 \pmod{10110}, we obtain \( \text{dlog}(9889) = 334. \)