Solution to Problem Set 3

Due on Wednesday, October 22, 2008.


**Problem 1: Feistel Network**

Textbook, problem 3.2.

Solution:

In each stage of the Feistel network, it works as follows:

\[
\begin{align*}
L_{i+1} &= R_i \\
R_{i+1} &= L_i \oplus f(R_i, K_i)
\end{align*}
\]

After applying \( n \) stages of the Feistel network to the plaintext \( L_0 \) and \( R_0 \) with the key schedule \( K_0, \ldots, K_{n-1} \), we get the ciphertext \( L_n \) and \( R_n \).

Now we show that the decryption can be done by applying the same encryption algorithm to \( L_n \) and \( R_n \), with the reversed key schedule \( K_{n-1}, \ldots, K_0 \). Switching the two sides of (1) and applying \((\oplus f(R_i, K_i))\) to both sides of (2), we get

\[
\begin{align*}
R_i &= L_{i+1} \\
L_i &= R_{i+1} \oplus f(R_i, K_i)
\end{align*}
\]

Therefore, after applying the algorithm to \( L_n \) and \( R_n \) with key \( K_{n-1} \), we get \( L_{n-1} \) and \( R_{n-1} \). Then applying the algorithm to \( L_{n-1} \) and \( R_{n-1} \) with key \( K_{n-2} \), we get \( L_{n-2} \) and \( R_{n-2} \). Repeating the same procedure for \( n \) times with the key schedule \( K_{n-1}, \ldots, K_0 \), we get \( L_0 \) and \( R_0 \) at the end.

**Problem 2: DES Complementation Property**

Textbook, problem 3.3.

Solution:

\( y = DES(x, K) \) and \( y' = DES(c(x), c(K)) \). The heart of DES is the Feistel network, whose one stage algorithm is described by (1) and (2). For \( DES(L_0R_0, K) \), define \( L'_0 = c(L_0), R'_0 = c(R_0) \) and \( K'_0 = c(K) \), which leads to another instance \( DES(L'_0R'_0, K') \). We will show that for any stage of the Feistel network, \( L'_i = c(L_i) \) and \( R'_i = c(R_i) \).

- **Base**: the case when \( i = 1 \).

  For instance \( DES(L_0R_0, K) \),

\[
\begin{align*}
L_1 &= R_0 \\
R_1 &= L_0 \oplus f(R_0, K_0)
\end{align*}
\]
For instance $\text{DES}(L_0 R_0, K')$,
\begin{align*}
L'_1 &= R'_0 = c(R_0) = c(L_0) \quad (7) \\
R'_1 &= L'_0 \oplus f(R'_0, K'_0) \\
     &= c(L_0) \oplus f(c(R_0), c(K_0)) \quad (8)
\end{align*}

Since $f(R_i, K_i)$ uses the bitwise $\oplus$ operation to combine input bits of $R_i$ (after expansion) and $K_i$ before the permutation in S-boxes, and $\oplus$ operation is associative and commutative,
\[ c(r) \oplus c(k) = r \oplus k \quad (9) \]

Combining (8) and (9) gives
\[ R'_1 = c(L_0 \oplus f(R_0, K_0)) = c(R_1) \quad (10)\]

- Induction: Assume the claim holds for all $i < n$, consider the case when $i = n$.

For instance $\text{DES}(L_0 R_0, K)$,
\begin{align*}
L_n &= R_{n-1} \\
R_n &= L_{n-1} \oplus f(R_{n-1}, K_{n-1}) \quad (11)
\end{align*}

For instance $\text{DES}(L'_0 R'_0, K')$,
\begin{align*}
L'_n &= R'_{n-1} = c(R_{n-1}) \\
R'_n &= L'_{n-1} \oplus f(R'_{n-1}, K'_{n-1}) \\
     &= c(L_{n-1}) \oplus f(c(R_{n-1}), c(K_{n-1})) \\
     &= c(L_{n-1} \oplus f(R_{n-1}, K_{n-1})) \quad (14)
\end{align*}

Therefore, after 16 stages of Feistel network, we can get $L'_{16} = c(L_{16})$ and $R'_{16} = c(R_{16})$.

Concatenating $L'_{16}$ and $R'_{16}$, we conclude
\[ y' = L'_{16} R'_{16} = c(L_{16} R_{16}) = c(y) \quad (15) \]

**Problem 3: DES S-box $S_4$**

Textbook, problem 3.11(a). [Omit part (b).]

**Solution:**

Each S-box $S_i$ maps an input of six bits to an output of four bits, i.e., $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$. $S_i$ can be depicted by a $4 \times 16$ array whose entries are integers in the range $[0, 15]$. Given a six-bit input $B = b_0 b_1 b_2 b_3 b_4 b_5$, we compute $S_i(B)$ as follows. The two bits $b_0 b_5$ determine the binary representation of a row $r$ of $S_i$, where $0 \leq r \leq 3$, while the four bits $b_1 b_2 b_3 b_4$ determine the binary representation of a column $c$ of $S_i$, where $0 \leq c \leq 15$. Then we find the entry corresponding to row $r$ and column $c$ of the $4 \times 16$ array, and use it binary representation as the four-bit output.

For the special property of $S_4$, we need to check the binary representation of each entry one by one. For example, the first entry of the second row is $(13)_{10} = (1101)_2$, and the first entry of the first row is $(7)_{10} = (0111)_2$. Applying the mapping, we have
\[ (0, 1, 1, 1) \mapsto (1, 0, 1, 1) \oplus (0, 1, 1, 0) = (1, 1, 0, 1) \quad (16) \]

We put the results for all the 16 entries in the table below.
Problem 4: Practice with $\mod$

Read pages 3–4 of textbook and then work the following:

(a) Textbook, problem 1.1.

(b) Textbook, problem 1.2.

(c) Textbook, problem 1.3.

(d) Textbook, problem 1.4.

Solution:

- **Problem 1.1**

  (a) By the division theorem, $7503 = 92 \times 81 + 51$, so $7503 \mod 81 = 51$.

  (b) By the division theorem, $-7503 = -93 \times 81 + 30$, so $(-7503) \mod 81 = 30$.

  (c) By the division theorem, $81 = 0 \times 7503 + 81$, so $81 \mod 7503 = 81$.

  (d) By the division theorem, $-81 = -1 \times 7503 + 7422$, so $(-81) \mod 7503 = 7422$

- **Problem 1.2**

  By the division theorem, $a = m \left\lfloor \frac{a}{m} \right\rfloor + (a \mod m)$. Therefore, we have

\[
(-a) \mod m = \left(-m \left\lfloor \frac{a}{m} \right\rfloor - (a \mod m)\right) \mod m \\
= (-(-a \mod m)) \mod m \\
= (m - (a \mod m)) \mod m
\] (17)
Because \( a \not\equiv 0 \pmod{m} \), it is easy to see that \( 0 < a \mod{m} < m \), which implies \( 0 < m - (a \mod{m}) < m \). Therefore, we have

\[
(m - (a \mod{m})) \mod{m} = m - (a \mod{m})
\] (18)

Combining (17) and (18), we reach the conclusion that

\[
(-a) \mod{m} = m - (a \mod{m})
\] (19)

- **Problem 1.3**

By definition, \( a \equiv b \pmod{m} \iff m \mid (a - b) \). By the division theorem,

\[
a = m \left\lfloor \frac{a}{m} \right\rfloor + (a \mod{m})
\] (20)

\[
b = m \left\lfloor \frac{b}{m} \right\rfloor + (b \mod{m})
\] (21)

Subtracting (21) from (20) gives

\[
(a - b) = \left(m \left\lfloor \frac{a}{m} \right\rfloor + (a \mod{m})\right) - \left(m \left\lfloor \frac{b}{m} \right\rfloor + (b \mod{m})\right)
\] (22)

Together with the fact that \( m \mid (mu + v) \iff m \mid v \), we have

\[
m \mid (a - b) \iff m \mid (a \mod{m} - b \mod{m})
\] (23)

Because \( (i \mod{m}) \in \mathbb{Z}_m \), \( m \mid (a \mod{m} - b \mod{m}) \iff a \mod{m} = b \mod{m} \). In sum, we have shown

\[
a \equiv b \pmod{m} \iff a \mod{m} = b \mod{m}
\] (24)

- **Problem 1.4**

By the division theorem, \( a = km + b \), where \( 0 \leq b < m \). It is obvious \( b = a \mod{m} \). Dividing both sides of the first equation by \( m \), we have \( \frac{a}{m} = k + \frac{b}{m} \). \( 0 \leq b < m \) implies that \( 0 \leq \frac{b}{m} < 1 \), and thus \( k \) is the largest integer that is less than or equal to \( \frac{a}{m} \), which is precisely the definition of \( \left\lfloor \frac{a}{m} \right\rfloor \). Therefore,

\[
a \mod{m} = b = a - km = a - \left\lfloor \frac{a}{m} \right\rfloor m
\] (25)

**Problem 5: Extended Euclidean Algorithm**

Textbook, problem 5.3. Show your work.

**Solution:**

a) \( 17^{-1} \mod{101} = 6 \)

<table>
<thead>
<tr>
<th>( i )</th>
<th>( r_i )</th>
<th>( u_i )</th>
<th>( v_i )</th>
<th>( q_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>101</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>17</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>1</td>
<td>-5</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-1</td>
<td>6</td>
<td>16</td>
</tr>
</tbody>
</table>
b) \(357^{-1} \mod 1234 = 1234 - 159 = 1075\)

<table>
<thead>
<tr>
<th>(i)</th>
<th>(r_i)</th>
<th>(u_i)</th>
<th>(v_i)</th>
<th>(q_i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1234</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>357</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>163</td>
<td>1</td>
<td>-3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>31</td>
<td>-2</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>11</td>
<td>-38</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>-35</td>
<td>121</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>46</td>
<td>-159</td>
<td>1</td>
</tr>
</tbody>
</table>

c) \(3125^{-1} \mod 9987 = 1844\)

<table>
<thead>
<tr>
<th>(i)</th>
<th>(r_i)</th>
<th>(u_i)</th>
<th>(v_i)</th>
<th>(q_i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9987</td>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3125</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>612</td>
<td>1</td>
<td>-3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>65</td>
<td>-5</td>
<td>16</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>27</td>
<td>46</td>
<td>-147</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
<td>-97</td>
<td>310</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>240</td>
<td>-767</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>-577</td>
<td>1844</td>
<td>1</td>
</tr>
</tbody>
</table>

**Problem 6: Linear Diophantine Equations**

Textbook, problem 5.4. Show your work.

**Solution:**
\[
gcd(57, 93) = 3
\]

\[
\begin{array}{c|c|c}
\hline
a & b \\
93 & 57 \\
57 & 36 \\
36 & 21 \\
21 & 15 \\
15 & 6 \\
6 & 3 \\
3 & 0 \\
\hline
\end{array}
\]

\(s = -13, t = 8\)

<table>
<thead>
<tr>
<th>(i)</th>
<th>(r_i)</th>
<th>(u_i)</th>
<th>(v_i)</th>
<th>(q_i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>31</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>19</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>2</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>-3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>5</td>
<td>-3</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>-13</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>
Problem 7: RSA Encryption


Suppose your RSA modulus is \( n = 55 = 5 \times 11 \) and your encryption exponent is \( e = 3 \).

(a) Find the decryption modulus \( d \).

(b) Assume that \( \gcd(m, 55) = 1 \). Show that if \( c \equiv m^3 \pmod{55} \) is the ciphertext, then the plaintext is \( m \equiv c^d \pmod{55} \). Do not quote the fact that RSA decryption works. That is what you are showing in this specific case.

Solution:

(a) Since \( n = 55 = 5 \times 11 \), we have \( \phi(n) = (5 - 1) \times (11 - 1) = 40 \). Now we apply the Extended Euclidean algorithm to find \( d \) given that \( e = 3 \).

\[
\begin{array}{c|ccc|c}
 i & r_i & u_i & v_i & q_i \\
 1 & 40 & 1 & 0 & 13 \\
 2 & 3 & 0 & 1 & 13 \\
 3 & 1 & 1 & -13 & 1 \\
\end{array}
\]

Therefore, we have \( d = 40 - 13 = 27 \).

(b) The question asks us to prove \( m \equiv c^{27} \pmod{55} \), given \( c \equiv m^3 \pmod{55} \) and \( \gcd(m, 55) = 1 \). Starting from the first condition, we have

\[
c \equiv m^3 \pmod{55} \Rightarrow c^{27} \equiv (m^3)^{27} \equiv (m^{40})^2 \times m \pmod{55} \quad (26)
\]

Euler’s theorem says, if \( \gcd(x, n) = 1 \), then

\[
x^{\phi(n)} \equiv 1 \pmod{n} \quad (27)
\]

Since \( \phi(55) = 40 \) and \( \gcd(m, 55) = 1 \), combining (26) and (27) gives

\[
c^{27} \equiv (m^{40})^2 \times m \equiv m \pmod{55} \quad (28)
\]

Because congruence is commutative, (28) implies

\[
m \equiv c^{27} \pmod{55} \quad (29)
\]