Xueyuan Su *October 27, 2008*

Solution to Problem Set 3

Due on Wednesday, October 22, 2008.

In the problems below, "textbook" refers to Douglas R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Chapman & Hall/CRC, 2006.

Problem 1: Feistel Network

Textbook, problem 3.2.

Solution:

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

$$L_{i+1} = R_i \tag{1}$$
$$R_{i+1} = L_i \oplus f(R_i, K_i) \tag{2}$$

After applying n stages of the Feistel network to the plaintext L_0 and R_0 with the key schedule $K_0, \cdots, K_{n-1}$, 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 $K_{n-1}, \cdots, K_0$. Switching the two sides of (1) and applying $(\oplus f(R_i, K_i))$ to both sides of (2), we get

$$R_i = L_{i+1} \tag{3}$$
$$L_i = R_{i+1} \oplus f(R_i, K_i) \tag{4}$$

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 $K_{n-1}, \cdots, K_0$, 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 $K'_i = c(K_i)$, 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 $DES(L_0R_0, K)$,

$$L_1 = R_0 \tag{5}$$
$$R_1 = L_0 \oplus f(R_0, K_0) \tag{6}$$

For instance $DES(L'_0R'_0, K')$,

$$\begin{aligned} L'_1 &= R'_0 = c(R_0) = c(L_0) && (7)\\ R'_1 &= L'_0 \oplus f(R'_0, K'_0) \\ &= c(L_0) \oplus f(c(R_0), c(K_0)) && (8) \end{aligned}$$

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,

$$c(r) \oplus c(k) = r \oplus k \tag{9}$$

Combining (8) and (9) gives

$$R'_1 = c(L_0 \oplus f(R_0, K_0)) = c(R_1) \tag{10}$$

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

  For instance $DES(L_0R_0, K)$,

$$\begin{aligned} L_n &= R_{n-1} && (11)\\ R_n &= L_{n-1} \oplus f(R_{n-1}, K_{n-1}) && (12) \end{aligned}$$

  For instance $DES(L'_0R'_0, K')$,

$$\begin{aligned} L'_n &= R'_{n-1} = c(R_{n-1}) && (13)\\ R'_n &= L'_{n-1} \oplus f(R'_{n-1}, K'_{n-1}) \\ &= c(L_{n-1}) \oplus f(c(R_{n-1}), c(K_{n-1})) \\ &= c(L_{n-1} \oplus f(R_{n-1}, K_{n-1})) && (14) \end{aligned}$$

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

$$y' = L'_{16}R'_{16} = c(L_{16}R_{16}) = c(y) \tag{15}$$

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., $S_i : \{0,1\}^6 \to \{0,1\}^4$. S_i can be depicted by a 4×16 array whose entries are integers in the range $[0, 15]$. Given a six-bit input $B = b_0b_1b_2b_3b_4b_5$, we compute $S_i(B)$ as follows. The two bits b_0b_5 determine the binary representation of a row r of S_i, where $0 \le r \le 3$, while the four bits $b_1b_2b_3b_4$ determine the binary representation of a column c of S_i, where $0 \le c \le 15$. Then we find the entry corresponding to row r and column c of the 4×16 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

$$(0,1,1,1) \mapsto (1,0,1,1) \oplus (0,1,1,0) = (1,1,0,1) \tag{16}$$

We put the results for all the 16 entries in the table below.

c	first row	mapping	second row
0	$(7)_{10} = (0111)_2$	$(0,1,1,1) \mapsto (1,0,1,1) \oplus (0,1,1,0) = (1,1,0,1)$	$(13)_{10} = (1101)_2$
1	$(13)_{10} = (1101)_2$	$(1,1,0,1) \mapsto (1,1,1,0) \oplus (0,1,1,0) = (1,0,0,0)$	$(8)_{10} = (1000)_2$
2	$(14)_{10} = (1110)_2$	$(1,1,1,0) \mapsto (1,1,0,1) \oplus (0,1,1,0) = (1,0,1,1)$	$(11)_{10} = (1011)_2$
3	$(3)_{10} = (0011)_2$	$(0,0,1,1) \mapsto (0,0,1,1) \oplus (0,1,1,0) = (0,1,0,1)$	$(5)_{10} = (0101)_2$
4	$(0)_{10} = (0000)_2$	$(0,0,0,0) \mapsto (0,0,0,0) \oplus (0,1,1,0) = (0,1,1,0)$	$(6)_{10} = (0110)_2$
5	$(6)_{10} = (0110)_2$	$(0,1,1,0) \mapsto (1,0,0,1) \oplus (0,1,1,0) = (1,1,1,1)$	$(15)_{10} = (1111)_2$
6	$(9)_{10} = (1001)_2$	$(1,0,0,1) \mapsto (0,1,1,0) \oplus (0,1,1,0) = (0,0,0,0)$	$(0)_{10} = (0000)_2$
7	$(10)_{10} = (1010)_2$	$(1,0,1,0) \mapsto (0,1,0,1) \oplus (0,1,1,0) = (0,0,1,1)$	$(3)_{10} = (0011)_2$
8	$(1)_{10} = (0001)_2$	$(0,0,0,1) \mapsto (0,0,1,0) \oplus (0,1,1,0) = (0,1,0,0)$	$(4)_{10} = (0100)_2$
9	$(2)_{10} = (0010)_2$	$(0,0,1,0) \mapsto (0,0,0,1) \oplus (0,1,1,0) = (0,1,1,1)$	$(7)_{10} = (0111)_2$
10	$(8)_{10} = (1000)_2$	$(1,0,0,0) \mapsto (0,1,0,0) \oplus (0,1,1,0) = (0,0,1,0)$	$(2)_{10} = (0010)_2$
11	$(5)_{10} = (0101)_2$	$(0,1,0,1) \mapsto (1,0,1,0) \oplus (0,1,1,0) = (1,1,0,0)$	$(12)_{10} = (1100)_2$
12	$(11)_{10} = (1011)_2$	$(1,0,1,1) \mapsto (0,1,1,1) \oplus (0,1,1,0) = (0,0,0,1)$	$(1)_{10} = (0001)_2$
13	$(12)_{10} = (1100)_2$	$(1,1,0,0) \mapsto (1,1,0,0) \oplus (0,1,1,0) = (1,0,1,0)$	$(10)_{10} = (1010)_2$
14	$(4)_{10} = (0100)_2$	$(0,1,0,0) \mapsto (1,0,0,0) \oplus (0,1,1,0) = (1,1,1,0)$	$(14)_{10} = (1110)_2$
15	$(15)_{10} = (1111)_2$	$(1,1,1,1) \mapsto (1,1,1,1) \oplus (0,1,1,0) = (1,0,0,1)$	$(9)_{10} = (1001)_2$

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 $7503 \bmod 81 = 51$.

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

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

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

- Problem 1.2

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

$$\begin{aligned}
(-a) \bmod m &= \left(-m \left\lfloor \frac{a}{m} \right\rfloor - (a \bmod m)\right) \bmod m \\
&= (-(a \bmod m)) \bmod m \\
&= (m - (a \bmod m)) \bmod m \qquad (17)
\end{aligned}$$

Because $a \not\equiv 0 \pmod{m}$, it is easy to see that $0 < a \bmod m < m$, which implies $0 < m - (a \bmod m) < m$. Therefore, we have

$$(m - (a \bmod m)) \bmod m = m - (a \bmod m) \tag{18}$$

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

$$(-a) \bmod m = m - (a \bmod m) \tag{19}$$

- Problem 1.3

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

$$a = m \left\lfloor \frac{a}{m} \right\rfloor + (a \bmod m) \tag{20}$$

$$b = m \left\lfloor \frac{b}{m} \right\rfloor + (b \bmod m) \tag{21}$$

  . Subtracting (21) from (20) gives

$$(a - b) = \left(m \left\lfloor \frac{a}{m} \right\rfloor + (a \bmod m) \right) - \left(m \left\lfloor \frac{b}{m} \right\rfloor + (b \bmod m) \right) \tag{22}$$

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

$$m \mid (a - b) \Leftrightarrow m \mid (a \bmod m - b \bmod m) \tag{23}$$

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

$$a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m \tag{24}$$

- Problem 1.4

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

$$\begin{aligned} a \bmod m &= b \\ &= a - km \\ &= a - \left\lfloor \frac{a}{m} \right\rfloor m \end{aligned} \tag{25}$$

Problem 5: Extended Euclidean Algorithm

Textbook, problem 5.3. Show your work.

Solution:

a) $17^{-1} \bmod 101 = 6$

i	r_i	u_i	v_i	q_i
1	101	1	0	
2	17	0	1	5
3	16	1	-5	1
4	1	-1	6	16

b) $357^{-1} \bmod 1234 = 1234 - 159 = 1075$

i	r_i	u_i	v_i	q_i
1	1234	1	0	
2	357	0	1	3
3	163	1	-3	2
4	31	-2	7	5
5	8	11	-38	3
6	7	-35	121	1
7	1	46	-159	

c) $3125^{-1} \bmod 9987 = 1844$

i	r_i	u_i	v_i	q_i
1	9987	1	0	
2	3125	0	1	3
3	612	1	-3	5
4	65	-5	16	9
5	27	46	-147	2
6	11	-97	310	2
7	5	240	-767	2
8	1	-577	1844	

Problem 6: Linear Diophantine Equations

Textbook, problem 5.4. Show your work.

Solution:

$\gcd(57, 93) = 3$

a	b
93	57
57	36
36	21
21	15
15	6
6	3
3	0

$s = -13, t = 8$

i	r_i	u_i	v_i	q_i
1	19	1	0	
2	31	0	1	0
3	19	1	0	1
4	12	1	0	1
5	7	2	-1	1
6	5	-3	2	1
7	2	5	-3	2
8	1	-13	8	

Problem 7: RSA Encryption

[This is problem 6.8.2 from Trapp & Washington, "Introduction to Cryptography with Coding Theory, Second Edition", Pearson Prentice Hall, 2006.]
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 $e = 3$.

i	r_i	u_i	v_i	q_i
1	40	1	0	
2	3	0	1	13
3	1	1	-13	

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

$$c \equiv m^3 \pmod{55} \Rightarrow c^{27} \equiv (m^3)^{27} \equiv (m^{40})^2 \times m \pmod{55} \tag{26}$$

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

$$x^{\phi(n)} \equiv 1 \pmod{n} \tag{27}$$

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

$$c^{27} \equiv (m^{40})^2 \times m \equiv m \pmod{55} \tag{28}$$

Because congruence is commutative, (28) implies

$$m \equiv c^{27} \pmod{55} \tag{29}$$