T-79.5501 Cryptology Spring 2009

Homework 6

Tutor : Joo Y. Cho
joo.cho@tkk.fi

19th March 2009

Q1. Let us consider the Boolean function
$t(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$.

1. Compute the values of the difference distribution table $N_D(a', b')$ of the function t, for $a' = 010$ and $a' = 111$ and $b' \in \{0, 1\}$.
2. A *linear structure* of a Boolean function f of three variables is defined as a vector $w = (w_1, w_2, w_3) \neq (0, 0, 0)$ such that $f(x \oplus w) \oplus f(x)$ is constant. Show that t has exactly one linear structure.
3. Show that t preserves complementation, that is, if each input bit is complemented then the output is complemented.

A1-a). Let $x = (x_0, x_1, x_2)$, $a'_1 = (0,1,0)$, $a'_2 = (1,1,1)$, $b'_1 = t(x) \oplus t(x \oplus a'_1)$, $b'_2 = t(x) \oplus t(x \oplus a'_2)$. We get the table:

x_0	x_1	x_2	$t(x)$	$t(x \oplus a'_1)$	$t(x \oplus a'_2)$	b'_1	b'_2
0	0	0	0	0	1	0	1
0	0	1	0	1	1	1	1
0	1	0	0	0	1	0	1
0	1	1	1	0	0	1	1
1	0	0	0	1	1	1	1
1	0	1	1	1	0	0	1
1	1	0	1	0	0	1	1
1	1	1	1	1	0	0	1

Hence, the difference distribution table $N_D(a', b')$ has the following values for $a' = (0,1,0)$, $a' = (1,1,1)$, and $b' = \{0,1\}$:

$a' \setminus b'$	0	1
010	4	4
111	0	8

A1-b). From the ANF of t we get that

$$\begin{aligned} t(x \oplus w) &= (x_0 \oplus w_0)(x_1 \oplus w_1) \oplus (x_0 \oplus w_0)(x_2 \oplus w_2) \\ &\quad \oplus (x_1 \oplus w_1)(x_2 \oplus w_2) \\ &= t(x) \oplus (w_1 \oplus w_2)x_0 \oplus (w_0 \oplus w_2)x_1 \oplus (w_0 \oplus w_1)x_2 \oplus t(w). \end{aligned}$$

If we want $t(x \oplus w) \oplus t(x)$ to be constant for every x the coefficients of x_0, x_1 and x_2 in the equation above must be zero:

$$\begin{aligned} w_1 \oplus w_2 &= 0 \\ w_0 \oplus w_2 &= 0 \\ w_0 \oplus w_1 &= 0 \end{aligned}$$

or, what is the same, $w_0 = w_1 = w_2$. Since we assumed that $w \neq 0$ we must have $w = (1, 1, 1)$ and this solution is unique.

A1-c). The complement of a bit b is the bit $b \oplus 1$. From A1-a), we get $t(x) \oplus (x \oplus (1,1,1)) = 1$ for all $x = (x_1, x_2, x_3)$. Hence, $t(x \oplus (1,1,1)) = t(x) \oplus 1$ for all $x = (x_1, x_2, x_3)$. This proves the claim.

Q2. Let π_S be an m-bit to n-bit S-box and

$$N_L(a, b) = 2^{m-1} + \frac{1}{2} \sum_{x \in \{0,1\}^m} (-1)^{a \cdot x \oplus b \cdot \pi_S(x)}.$$

1. Problem(Stinson): Show that

$$\sum_{a=0}^{2^m-1} N_L(a, b) = 2^{2m-1} \pm 2^{m-1},$$

   for all n-bit mask values b, where the sum is taken over all m-bit mask values a (enumerated from 0 to $2^m - 1$).
2. Check the result in (a) for the linear approximation table in Fig. 3.2 of the textbook.

A2-a). Using the expression of $N_L(a,b)$ we get

$$\begin{aligned}
\sum_{a=0}^{2^m-1} N_L(a,b) &= \sum_{a\in\{0,1\}^m}\left(2^{m-1}+\frac{1}{2}\sum_{x\in\{0,1\}^m}(-1)^{a\cdot x\oplus b\cdot\pi_S(x)}\right)\\
&= 2^m 2^{m-1}+\frac{1}{2}\sum_{a\in\{0,1\}^m}\sum_{x\in\{0,1\}^m}(-1)^{a\cdot x}(-1)^{b\cdot\pi_S(x)}\\
&= 2^{2m-1}+\frac{1}{2}\sum_{x\in\{0,1\}^m}(-1)^{b\cdot\pi_S(x)}\sum_{a\in\{0,1\}^m}(-1)^{a\cdot x}\\
&= 2^{2m-1}+2^{m-1}(-1)^{b\cdot\pi_S(0)}.
\end{aligned}$$

The last equality follows from the equality

$$\sum_{y\in\{0,1\}^m}(-1)^{y\cdot x}=\begin{cases}2^n, & x=0\\ 0, & x\neq 0\end{cases}$$

given in Lecture 6 and Homework 5. Now $(-1)^{b\cdot\pi_S(0)}=\pm 1$ from which the claim follows.

A2-b). Since $m = 4$, we check $\sum_{a=0}^{15} N_L(a, b) = 128 \pm 8$ for any b.

a	b: 0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	10	6
A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	6	8
F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8

FIGURE 3.2
Linear approximation table: values of $N_L(a, b)$

In this way, each of the 256 random variables is named by a (unique) pair of hexadecimal digits, representing the input and output sum.

3.3.3 A Linear At

Linear cryptanalysi
that can be used to d
last round). We wi
The diagram in Fig
use. This diagram c
random variables w
S-boxes are the one
boxes in the approx
This approximati

- In S_2^1, the r
- In S_2^2, the r
- In S_2^3, the r
- In S_4^3, the r

The four random va
value. Further, we
"intermediate" ranc
If we make the a
then we can compu
3.1). (The random
cannot provide a m
the approximation s
fore hypothesize th

Q3. Let $\mathbb{F}$ be a finite field with q elements and β a primitive element in $\mathbb{F}$. Consider the function $f : \mathbf{Z}_{q-1} = \{0, 1, \ldots, q-2\} \to \mathbb{F}^*$, $f(x) = \beta^x$.

1. Show that f is a bijection.
2. For $a' \in \mathbf{Z}_{q-1}$ and $b' \in \mathbb{F}$, let us denote

   $$N_D(a', b') = \#\{x \in \mathbf{Z}_{q-1} | f((x + a') \bmod q - 1) - f(x) = b'\}.$$

   Show that $N_D(a', b') = 1$, for all $a' \neq 0$ and $b' \neq 0$.

A3.

1. As β is primitive, we know $\beta^0 \neq \beta^1 \neq \ldots \neq \beta^{q-2}$ and f is clearly one-to-one (injective). Also $\mathrm{ord}(\beta) = \#\mathbb{F}^\times = \#\mathbf{Z}_{q-1}$: the domain and codomain have the same cardinality, and it follows that f is in fact bijective.
2. Primitive β implies $\mathrm{ord}(\beta) = q - 1$ so we write equivalently

$$\begin{aligned} N_D(a', b') &= \#\{x \in \mathbf{Z}_{q-1} | \beta^{x+a'} - \beta^x = b'\} \\ &= \#\{x \in \mathbf{Z}_{q-1} | \beta^x = b'(\beta^{a'} - 1)^{-1}\} \\ &= \#\{x \in \mathbf{Z}_{q-1} | \beta^x = c\} \text{ where } c = b'(\beta^{a'} - 1)^{-1} \in \mathbb{F}^\times \end{aligned}$$

For all $a' \neq 0$ and $b' \neq 0$, we can see that c is distinct. Hence, the exact number of x such that $\beta^x = c$ holds is one. That is, given the stated restraints $N_D(a', b') = 1$ holds.

Q4. Bob is using the RSA cryptosystem and his modulus is $n = pq = 67 \cdot 41$. Show that if the plaintext is 2009 then the ciphertext is equal to 2009.

A4. The task is to show $2009^e \equiv 2009 \bmod 67 \cdot 41$ for any public exponent e. First we observe e must be an odd number as $gcd(e, 66 \cdot 40) = 1$. Then we can obtain $2009^e \mod pq$ using the chinese remainder theorem:

$$\begin{aligned} 2009^e &\equiv (-1)^e = -1 \bmod 67 \\ 2009^e &\equiv 0^e = 0 \bmod 41 \end{aligned}$$

Since $41^{-1} \equiv 18 \bmod 67$, we get

$$2009^e \mod 67 \cdot 41 = -1 \cdot 18 \cdot 41 = -738 \equiv 2009 \mod 67 \cdot 41.$$

Hence, the claim holds.

Q5. (Stinson 5.14) The aim is to prove that the RSA Cryptosystem is not secure against a chosen ciphertext attack.

1. First, show that the encryption operation is multiplicative, that is, $e_K(x_1 x_2) = e_K(x_1)e_K(x_2)$, for any two plaintexts x_1 and x_2.
2. Next, use the multiplicative property to construct an example about how to decrypt a given ciphertext y by obtaining the decryption $\hat{x}$ of a different (but related) ciphertext $\hat{y}$.

A5.

1. RSA encryption is the function $e_K(m) = m^K \mod n$. For $m = m_1 m_2$ we have $e_K(m_1 m_2) = (m_1 m_2)^K = m_1^K m_2^K = e_K(m_1) e_K(m_2)$.
2. We want to obtain the decryption of ciphertext $y = x^e \mod n$. We choose ciphertext $\hat{y} = ys^e \mod n$ with a random $s \in \mathbf{Z}_n$. Note e is public. We then ask for the decryption of $\hat{y}$ and obtain $\hat{y}^d \equiv (ys^e)^d \equiv x^{ed} s^{ed} \equiv xs \pmod{n}$ and we obtain the plaintext x as $xss^{-1} \equiv x \pmod{n}$.

Q6.

1. What are the quadratic residues modulo 5?
2. What are the quadratic residues modulo 7?
3. What are the quadratic residues modulo 35?

Note that $\#QR_p = \#QNR_p = (p-1)/2$ for $p > 2$.

A6.

1. Since $1^2 = 1, 2^2 = 4, 3^2 \equiv 4, 4^2 \equiv 1$, we get $QR_5 = \{1, 4\}$.
2. Since $1^2 = 1, 2^2 = 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1$, we get $QR_7 = \{1, 2, 4\}$.
3. Suppose there exists x such that for some a and b

$$x^2 = a \bmod 5, \text{ and } x^2 = b \bmod 7.$$

By CRT, we get

$$x^2 = a \cdot 7 \cdot u + b \cdot 5 \cdot v = 21a + 15b \bmod 35$$

since $u = 7^{-1} = 3 \bmod 5$ and $v = 5^{-1} = 3 \bmod 7$. Therefore, for $a \in QR_5$ and $b \in QR_7$, we have $(21a + 15b) \bmod 35 \in QR_{35}$. Note that either a or b can be zero (but not both). Using (a) and (b), we get

$$QR_{35} = \{1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30\}$$

Q7.

1. Evaluate the Jacobi symbol

$$\left(\frac{801}{2005}\right).$$

You should not do any factoring other than dividing out powers of 2.

2. Let n be a composite integer and a an integer such that $1 < a < n$. Then n is called *Euler pseudoprime* to the base a if

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}.$$

Show that 2005 is an Euler pseudoprime to the base 801.

A7-a). We iteratively apply the rules from the textbook.

$$
\begin{aligned}
\left(\frac{801}{2005}\right) &= \left(\frac{2005}{801}\right) = \left(\frac{403}{801}\right) \text{ by property 4 then 1} \\
&= \left(\frac{801}{403}\right) = \left(\frac{398}{403}\right) \text{ by property 4 then 1} \\
&= \left(\frac{2}{403}\right)\left(\frac{199}{403}\right) = -\left(\frac{199}{403}\right) \text{ by property 3 then 2} \\
&= \left(\frac{403}{199}\right) = \left(\frac{5}{199}\right) \text{ by property 4 then 1} \\
&= \left(\frac{199}{5}\right) = \left(\frac{4}{5}\right) \text{ by property 4 then 1} \\
&= \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1 \text{ by property 3 then 2}
\end{aligned}
$$

A7-b). Let us set $n = 2005$ and $a = 801$. From A7-(a), we know that $\left(\frac{a}{n}\right) = 1$. Hence, we show $a^{\frac{n-1}{2}} \bmod n = 801^{1002} = 1 \bmod 2005$ by using CRT as above (Problem 1) here.

$$\begin{aligned} 801^{1002} &\equiv 1^{1002} \equiv 1 \mod 5 \\ 801^{1002} &\equiv (-1)^{1002} \equiv 1 \mod 401 \end{aligned}$$

BY the extended Euclidean algorithm, we get $401^{-1} \equiv 1 \bmod 5$ and $5^{-1} \equiv 321 \bmod 401$. Hence,

$$801^{1002} = 1 \cdot 401 \cdot 1 + 1 \cdot 5 \cdot 321 \equiv 1 \mod 2005.$$

Therefore, $n = 2005$ is a pseudoprime to the base $a = 801$.