Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 5

Exercise 5-1 Consider a variant of CBC mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (as opposed to choosing IV randomly for each message that is being sent). Show that the resulting scheme is not CPA-secure.

Solution (Sketch): Attacker encrypts an arbitrary message to find out IV. Recall that IV is part of the ciphertext in CBC mode. We assume that the length n of IV is known. (If not, then the attacker can encrypt the same message a number of times. Their codes should have the form $IV \,\|\, c_0$, $(IV+1) \,\|\, c_1$, ..., from which it is possible to identify the length of IV with high probability.)

Attacker next encrypts $IV + 1$ (binary addition). The code is $c_0 := (IV + 1) \,\|\, F_k((IV + 1) \oplus (IV + 1)) = (IV + 1) \,\|\, F_k(0^n)$.

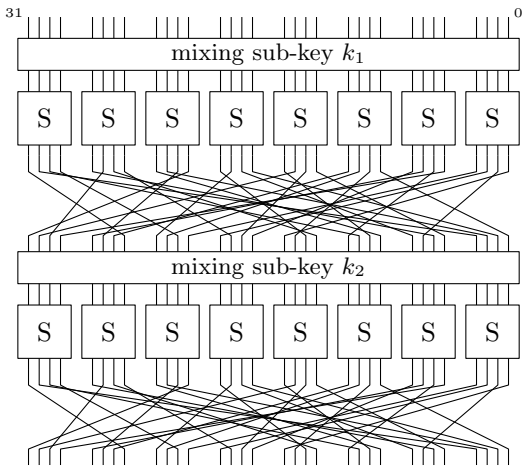
This means that the attacker has found out $F_k(0^n)$.

Attacker then chooses $m_1 = IV + 2$ and another random message m_2 as its two messages.

We now encode one message and give the cipertext c to the attacker.

The attacker can tell if c is the encryption of m_1 or m_2. The code of m_1 will be $c_0 = (IV + 2) \,\|\, F_k(0^n)$, which the attacker can identify.

Exercise 5-2 Assume given a two-round S/P-network for 32-bit inputs, as shown below.



Suppose that the 64-bit key k is obtained by concatenating the two sub-keys, i.e. $k = k_1 \| k_2$.

a) Let $v, w \in \{0,1\}^{32}$ be arbitrary words. Show that there are exactly 2^{32} many keys for which a network of the above form encodes v to w.

Solution (Sketch): Write $f_p \colon \{0,1\}^{32} \to \{0,1\}^{32}$ and $f_S \colon \{0,1\}^{32} \to \{0,1\}^{32}$ for the functions that perform the permutation and the actions of the S-Boxes respectively. The action of the whole network on input x becomes $f_p(f_S(k_2 \oplus f_p(f_S(k_1 \oplus x))))$. Note that f_p and f_S are both invertible.

We show: For all w, v and k_2, there exists a unique k_1, such that $w = f_p(f_S(k_2 \oplus f_p(f_S(k_1 \oplus v))))$ holds. Observe the following equivalences.

$$\begin{aligned} w = f_p(f_S(k_2 \oplus f_p(f_S(k_1 \oplus v)))) &\iff f_S^{-1}(f_p^{-1}(w)) = k_2 \oplus f_p(f_S(k_1 \oplus v))) \\ &\iff f_S^{-1}(f_p^{-1}(w)) \oplus k_2 = f_p(f_S(k_1 \oplus v))) \\ &\iff f_S^{-1}(f_p^{-1}(f_S{-}1(f_p^{-1}(w)) \oplus k_2) = k_1 \oplus v \\ &\iff v \oplus f_S^{-1}(f_p^{-1}(f_S{-}1(f_p^{-1}(w)) \oplus k_2) = k_1 \end{aligned}$$

This means that k_1 is uniquely determined from w, v and k_2, and for any choice of these values there exists a choice of k_1.

As there are 2^{32} possibilities for k_2, this shows the assertion.

b) Let the S-box S be given concretely by the following table (which uses hexadecimal notation for 4-bit values):

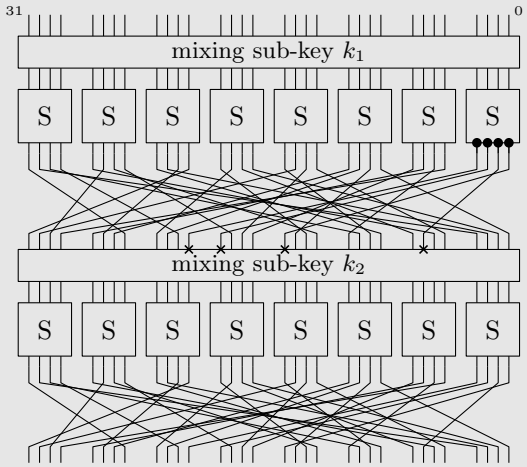
input	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
output	0	1	2	d	4	7	f	6	8	c	e	b	a	9	3	5

Let the permutation in both of the two rounds be given by: `[15 6 19 20 28 11 27 16 0 14 22 25 4 17 30 9 1 7 23 13 31 26 2 8 18 12 29 5 21 10 3 24]`. This means that the permutation maps bit `0` to bit `15`, bit `1` to bit `6`, and generally bit `i` to the bit whose number appears at the `i`-th position in this list.

Suppose now that, for some unknown key k, this two-round network encodes `0x40414243` to `0xf82e5109`, `0x84838281` to `0x3291021d`, and `0x12345678` to `0xaefcf8c1`.

What can you say about the key k?

Solution (Sketch): Suppose an input word w is mapped to an output word v. Consider the four bits marked with circles. If we know these four bits, then we can compute the same four bits of k_1 from the input w. Likewise, we can compute the four bits of k_2 marked with crosses from the output word v.



We can try all possibilities for these four bits. For each input-output-pair, we get a possibility for four bits of k_1 and four bits of k_2. But the keys all input-output pairs are encoded using the same key. So only those choices of the four bits are possible that result in the same bits of k_1 and k_2 for all input-output pairs.

We can do this for all blocks ($16 \cdot 8$ many possibilites to try) to narrow down the choices for the key.

In this example we get the following possibilites (`k1` — first four bits of k_1; `k2'` — value of the circled bits).

`0x40414243`	`12345678`	`0x84838281`
$\mapsto$ `0xf82e5109`	$\mapsto$ `aefcf8c1`	$\mapsto$ `0x3291021d`
`k1: f, k2': 0`	`k1: f, k2': 0`	`k1: f, k2': 0`
`k1: 8, k2': 1`	`k1: d, k2': 1`	`k1: 3, k2': 1`
`k1: b, k2': 2`	`k1: c, k2': 2`	`k1: 0, k2': 2`
`k1: e, k2': 3`	`k1: 7, k2': 3`	`k1: 1, k2': 3`
`k1: 9, k2': 4`	`k1: a, k2': 4`	`k1: 4, k2': 4`
`k1: 5, k2': 5`	`k1: 6, k2': 5`	`k1: 6, k2': 5`
`k1: a, k2': 6`	`k1: 8, k2': 6`	`k1: e, k2': 6`
`k1: 0, k2': 7`	`k1: 9, k2': 7`	`k1: 5, k2': 7`
`k1: 1, k2': 8`	`k1: 2, k2': 8`	`k1: a, k2': 8`
`k1: d, k2': 9`	`k1: e, k2': 9`	`k1: d, k2': 9`
`k1: 3, k2': a`	`k1: 1, k2': a`	`k1: c, k2': a`
`k1: 2, k2': b`	`k1: b, k2': b`	`k1: 9, k2': b`
`k1: 4, k2': c`	`k1: 4, k2': c`	`k1: 7, k2': c`
`k1: 6, k2': d`	`k1: 3, k2': d`	`k1: b, k2': d`
`k1: 7, k2': e`	`k1: 0, k2': e`	`k1: 2, k2': e`
`k1: c, k2': f`	`k1: 5, k2': f`	`k1: 8, k2': f`

From the three pairs, only one option remains (`k1=f`, `k2'=0`).

In this example, there are two possibilities for the whole key k_1: `cafebeaf` and `cafebeef`.

Exercise 5-3 Let the S-box S from the lecture (which uses hexadecimal notation for 4-bit values):

input	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
output	e	4	d	1	2	f	b	8	3	a	6	c	5	9	0	7

a) Compute all the input pairs of S that have differential `3` and that are mapped by S to outputs with differential `9`.

Solution (Sketch):

`(1,2), (2,1), (d,e), (e,d)`

b) Consider the following function, which takes two 4-bit inputs m_1, m_2, and in which k is some unknown 4-bit key.

$$f_k(m_1, m_2, d) = \begin{cases} 1 & \text{if differential of } S(m_1 \oplus k) \text{ and } S(m_2 \oplus k) \text{ is } d, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose you know $f_k(\mathtt{b}, \mathtt{8}, \mathtt{9}) = 1$. What can you tell about the key k?

Solution (Sketch): There are only four possible inputs that produce output differential `9` from input differential `3`. Note that $\mathtt{b} \oplus k$ and $\mathtt{8} \oplus k$ have differential `3`. This means that $(\mathtt{b} \oplus k, \mathtt{8} \oplus k)$ must be one of the four pairs of a). This leaves for `k` only the possibilities `a` and `9`.

What can you tell about the key k if you further know $f_k(\mathtt{0}, \mathtt{1}, \mathtt{a}) = 1$?

Solution (Sketch): The pairs `(0,1)` and `(a,b)` are the only outputs with differential `1` that produce output differential `a`. If we proceed as in b), this leaves only the options $\mathtt{k} = \mathtt{0}$ or $\mathtt{k} = \mathtt{a}$.