Introduction to cryptology
TD#3

2018-W06

Exercise 1: LFSR

Q. 1: Show that the output sequence of an LFSR is periodic. What is the maximal possible period for a binary LFSR with an n-bit state?

Q. 1.5 (bonus): Algebraically speaking, what is the condition on the feedback polynomial $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ of an LFSR $(x_{n-1}, \ldots x_1, x_0) \mapsto (x'_{n-1} = x_{n-2} + a_{n-1}x_{n-1}, \ldots, x'_1 = x_0 + a_1 x_{n-1}, x'_0 = a_0 x_{n-1})$ for it to have a period of maximum length?

Q. 2: Draw schematically the LFSR implemented by the following function:

```
uint8_t mul(uint8_t x)
{
        uint8_t b = (x >> 7);
        if (b)
                b = 0x1B;
        return ((x << 1) ^ b);
}
```

What is the corresponding feedback polynomial?

Q. 3: Give a 3×3 binary matrix with indeterminate coefficients such that applying this matrix to a column vector corresponds to one iteration of a 3-bit LFSR. What is the condition that this matrix must verify to ensure that the LFSR never moves from a non-zero configuration to a zero one?

Exercise 2: MACs

Q. 1: Let $\mathcal{M} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^\tau$ be a "perfect" MAC whose outputs are uniformly and independently random. An adversary is given a single message m and is asked to find the corresponding tag $\mathcal{M}(k, m)$ when k is unknown. What is his success probability (in function of κ and τ)?

Q. 2: Let $\mathcal{M}$ be as above, but with the constraint that it is linear. Give a universal forgery attack on $\mathcal{M}$ with small time and query complexity. Does your attack still work if $\mathcal{M}$ takes an additional "nonce" input r that is never reused from one call to another?

Q. 3: Let $\mathcal{M}$ be as in **Q. 1**. What is the problem with the following scheme

$$k_e, r, k_a, m \mapsto \mathsf{CBC\text{-}Encrypt}(k_e, r, m) || \mathcal{M}(k_a, m),$$

that combines encryption and authentication?

Exercise 3: MACs bis: CBC-MAC

We define a vanilla CBC-MAC with zero IV as $k, m \mapsto \lfloor \mathsf{CBC\text{-}Encrypt}(k, 0, m) \rfloor_{\mathrm{last}}$, where $\lfloor \cdot \rfloor_{\mathrm{last}}$ truncates its input to its last block (for the sake of simplicity, we assume that the input message always has a length multiple the block size).

Q. 1: Why is this scheme not secure?

Hint: Notice that the tag of a single-block message m_0 appears as intermediate value when computing the tag of $m_0||m_1$, for any value of m_1. If you know m_0 and its associated tag t, how can you pick m_1 to ensure that the two-block message $m_0||m_1$ also has tag t?

Q. 2: One proposes to solve the above issue by composing vanilla CBC-MAC with a one-block encryption $\mathscr{E}(k, \cdot)$ with a key k independent from the one used in vanilla CBC-MAC. Do you think that this makes sense?

Q. 3: Is it possible to extract a similar MAC scheme from the CTR mode?

Exercise 4: MACs ter: MAC with a small state

A designer wants to design a MAC using a block cipher $\mathscr{E} : \{0,1\}^{128} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$. He wants to use a variant of CBC-MAC, but with larger tags than what a direct application using $\mathscr{E}$ would allow. Specifically, he wishes for 128-bit tags. The result is the following. On input $(k, k_0, k_1, k_2, k_3, m)$, compute:

$$x := \mathsf{CBC\text{-}Encrypt}[\mathscr{E}](k, 0, m) \quad y_0 := \mathscr{E}(k_0, x) \quad y_1 := \mathscr{E}(k_1, x) \quad y_2 := \mathscr{E}(k_2, x) \quad y_3 := \mathscr{E}(k_3, x),$$

and output $y := y_0||y_1||y_2||y_3$.

Q. 1: How many possible values can be taken by x (for any k, m).

Q. 2: How many possible values can be taken by y, for a fixed MAC key (k, k_0, k_1, k_2, k_3)?

Q. 3: Give a strategy that allows to gather all possible tags for a fixed MAC key, with time, memory and query complexity 2^{32} (assuming for simplicity that if the input message is 32-bit long, no padding is performed in the CBC encryption).

Q. 4 Assuming that the precomputation of the previous question has been performed, what is the forgery probability for a random message? Is this MAC a good MAC?

Q. 5 Is the modified schemen that on input $(k, k_0, k_1, k_2, k_3, m)$ computes:

$$x := \mathsf{CBC\text{-}Encrypt}[\mathscr{E}](k, 0, m) \quad y_0 := \mathscr{E}(k_0, x) \quad y_1 := \mathscr{E}(k_1, y_0) \quad y_2 := \mathscr{E}(k_2, y_1) \quad y_3 := \mathscr{E}(k_3, y_2),$$

and outputs $y := y_0||y_1||y_2||y_3$ protected against the above attack?