Introduction to cryptology
TD#2

2019-W05,...

Exercise 1: Arithmetic in $\mathbb{Z}/2^8\mathbb{Z}$ and $\mathbb{F}_{2^8}$

Q. 1: Compute the following in $\mathbb{Z}/2^8\mathbb{Z}$:

— 153 + 221

— 29 + 8

— 64 + 31

Q. 2: Compute the following in $\mathbb{F}_2^8$ (where a decimal representation is used for the elements, i.e. the addition corresponds to the bitwise XOR):

— 153 + 221

— 29 + 8

— 64 + 31

Q. 3: Under what condition on their operands are the additions in $\mathbb{Z}/2^8\mathbb{Z}$ and $\mathbb{F}_{2^8}$ equivalent? (Prove it.)

Exercise 2: Bit-vector arithmetic

Q. 1: Write a small "naïve" C function that computes the scalar product of two vectors of $\mathbb{F}_2^{32}$. This function must have the following prototype:

```
uint32_t scalar32_naive(uint32_t x, uint32_t y).
```

Q. 2: Write another implementation of the same function, of prototype

```
uint32_t scalar32_popcnt(uint32_t x, uint32_t y),
```

that uses a *bitwise and* instruction "`&`" and the *population count* function for 32-bit words "`__builtin_popcount()`".

Q. 3 Explain why in C, assuming that `x` is of type `uint32_t`, `x << 1` computes the multiplication of `x` by two in $\mathbb{Z}/2^{32}\mathbb{Z}$.

Q. 4 Explain why in C, assuming that `x` is of type `uint32_t`, `x >> 1` is equivalent to `x / 2`.

Q. 5 Write the matrix M of dimension 8 over $\mathbb{F}_2$ such that $M\mathbf{x} = \texttt{mul2(x)}$, where `mul2` is defined as:

```
uint8_t mul2(uint8_t x)
{
  return ((x << 1) & 0xFF);
}
```

and $\boldsymbol{x}$ and `x` are in natural correspondence (with the encoding convention that $\boldsymbol{x} = (\boldsymbol{x}_0 \quad \boldsymbol{x}_1 \quad \ldots \boldsymbol{x}_7)^t \mapsto \boldsymbol{x}_7 2^7 + \boldsymbol{x}_6 2^6 + \ldots + \boldsymbol{x}_0 2^0$). Is this matrix invertible?

Q. 6 What are the logical formulas computed by the following functions on their inputs?

```
uint32_t f1(uint32_t x, uint32_t y, uint32_t z)
{
  return ((x & y) | (~x & z));
}

uint32_t f2(uint32_t x, uint32_t y, uint32_t z)
{
  return ((x & y) | (x & z) | (y & z));
}

uint32_t f2(uint32_t x, uint32_t y, uint32_t z)
{
  return (z ^ (x & (y ^ z)));
}
```

Which of these functions can be computed as matrices?

Exercise 3: PRPs

Let $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher for which there is a subset $\mathcal{K}' \subset \{0,1\}^\kappa$ of *weak keys* of size 2^w such that if $k \in \mathcal{K}'$, $\mathcal{E}(k, \cdot) : x \mapsto x$.

Q. 1: Give a lower-bound for $\mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(1,1)$.

Q. 2: Some mode of operation of block ciphers rely on the fact that $\mathcal{E}(k, 0)$ is an unpredictable value when k is random and secret (with 0 denoting the all-zero binary string).

Show that this is a reasonable assumption. More precisely, give a lower-bound on $\mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(1,1)$ assuming that one can predict this value with unit time and success probability p.

Q. 3: Assume that $\mathcal{E}$ is a “good” block cipher. Define a related cipher $\mathcal{E}'$ for which $\mathcal{E}(k, 0)$ is trivially predictable for any key (several constructions are possible).

Exercise 4: CTR mode

Let $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. The CTR encryption of a message $m = m_0||m_1||\ldots$ (where all of the m_is are n-bit long) with $\mathcal{E}$ and a key k is given by $m_0 \oplus \mathcal{E}(k, t_0)||m_1 \oplus \mathcal{E}(k, t_1)\ldots$, where the t_is are n-bit pairwise-distinct values (for instance one can take $t_0 = 0$, $t_1 = 1$, etc.). In other words, one is encrypting a message with a pseudo-random keystream generated by $\mathcal{E}$.

Q. 1 : Show that the keystream used to encrypt a message of 2^n blocks (that is $n2^n$-bit long) is not perfectly random, if it is generated with a single key.

Hint: Exploit the fact that $\mathcal{E}(k, \cdot)$ is invertible.

We may try to solve the problem of the previous question by defining $\mathcal{E}'(k, x) := \mathcal{E}(k, x) \oplus x$. This makes $\mathcal{E}'$ non-injective. One may then still encrypt a message $m = m_0||m_1|| \ldots$ as $m_0 \oplus \mathcal{E}'(k, t_0)||m_1 \oplus \mathcal{E}'(k, t_1) \ldots$.

Q. 2 : Show that if the t_i values are public, then $\mathcal{E}'$ suffers from the same problem as $\mathcal{E}$ in Q. 1.

(However, it can be shown that if the t_is are secret and "random" enough (for instance $t_i = \mathcal{E}''(k, t'_i)$ where the t'_is are pairwise distinct), then $\mathcal{E}'$ does achieve better security than $\mathcal{E}$ in CTR mode.)

Exercise 5: ECB, toy modes

Let $\mathcal{E} : \{0, 1\}^\kappa \times \{0, 1\}^n \to \{0, 1\}^n$ be a block cipher. The ECB encryption of a message $m = m_0||m_1|| \ldots$ (where all of the m_is are n-bit long) with $\mathcal{E}$ and a key k is given by $\mathcal{E}(k, m_0)||\,\mathcal{E}(k, m_1) \ldots$.

Q. 1: Explain why ECB is not a good mode (in particular why it is not IND-CPA).

We modify ECB to the following toy mode, that uses *domain separation* to solve some of the issues of ECB: the encryption of a message $m = m_0||m_1|| \ldots$ (where all of the m_is are $n - b$-bit long) with $\mathcal{E}$ and a key k is given by $\mathcal{E}(k, m_0||t_0)||\,\mathcal{E}(k, m_1||t_1) \ldots$, where the t_is are b-bit pairwise-distinct values (for instance one can take $t_0 = 0$, $t_1 = 1$, etc.).

Q. 2: Give an upper-bound for the maximum message length that can be securely encrypted with this toy mode before having to change the key.

Q. 3: Are messages encrypted as above authenticated?

We modify again the toy mode. The encryption of a message $m = m_0||m_1|| \ldots$ (where all of the m_is are $n{-}b{-}r$-bit long) with $\mathcal{E}$ and a key k is given by $\mathcal{E}(k, m_0||t_0||0^r)||\,\mathcal{E}(k, m_1||t_1||0^r) \ldots$, where the t_is are b-bit pairwise-distinct values and 0^r is a string or r zeros.

Q. 4: What is the probability that a uniformly random ciphertext corresponds to a message encrypted with the above toy mode? Explain how this allows to perform some authentication of the ciphertexts. Give a trivial (but limited) attack that may still be performed by an adversary.