Cryptology I (spring 2014) Prof. Dr. Dominique Unruh

Exercise Sheet 3

Out: March 30, 2014 Due: April 7, 2014

Problem 1: One-time-pad in CBC mode

Assume someone uses the one-time pad in CBC mode. That is, the block cipher is $E(k, m) := k \oplus m$, and that block cipher is used in CBC mode.

(a) Assume a message $m = m_1 \| m_2 \| m_3 \| m_4$ is encrypted where all $m_1 = m_2 = m_3 = m_4$ are blocks consisting only of only zeroes.

What is the resulting ciphertext?

(b) Assume a message $m = m_1 \| m_2 \| m_3 \| m_4$ is encrypted. What is the resulting ciphertext? (Give a formula in terms of the m_1, m_2, m_3, m_4, simplified as much as possible.)

(c) Explain how to compute $m_3 \oplus m_4$ from the resulting ciphertext. (Without using the key.)

(d) Explain why the above implies that the one-time pad in CBC mode is not IND-CPA secure (not even IND-OT-CPA).

Problem 2: "Inverse" CBC

Consider the following mode of operation (which I call "inverse CBC"):

To encrypt a message m consisting of blocks $m_1, \ldots, m_n$ with key k, pick a random initialization vector iv and then compute $c_1 := E_0(k, m_1) \oplus iv$ and $c_i := E_0(k, m_i) \oplus m_{i-1}$ for $i = 2, \ldots, n$. Here E_0 is the block cipher. And $E(k, m) := iv \| c_1 \| \ldots \| c_n$.

The adversary has intercepted a ciphertext $c = E(k, m)$. He happens to know the last block m_n of m (e.g., because that one is prescribed by the protocol).

(a) Explain how the adversary can completely decrypt m. He can make chosen plaintext queries (i.e., he can ask for encryptions of arbitrary message m'). He cannot make decryption queries.

(b) Suggest how to fix the mode of operation so that it becomes secure at least again this attack (and simple modifications thereof). You do not need to prove security.

Problem 3: Encoding messages for ElGamal

The message space of ElGamal (when using the instantation that operates modulo a prime $p > 2$ with $p \equiv 3 \bmod 4$ [1]) is the set $\mathrm{QR}_p = \{x^2 \bmod p : x = 0, \ldots, p-1\}$.

The problem is now: if we wish to encrypt a message $m \in \{0,1\}^\ell$ (with $\ell \leq |p| - 2$), how do we interpret m as an element of QR_p?

One possibility is to use the following function $f : \{1, \ldots, \frac{p-1}{2}\} \to \mathrm{QR}_p$:

$$f(x) := \begin{cases} x & \text{if } x \in \mathrm{QR}_p \\ -x \bmod p & \text{if } x \notin \mathrm{QR}_p \end{cases}$$

Once we see that f is a bijection and can be efficiently inverted, the problem is solved, because a bitstring $m \in \{0,1\}^\ell$ can be interpreted as a number in the range $1, \ldots, \frac{p-1}{2}$ by simply interpreting m as a binary integer and adding 1 to it. (I.e., we encrypt $f(m+1)$.)

We claim that the following function is the inverse of f:

$$g(x) := \begin{cases} x & \text{if } x = 1, \ldots, \frac{p-1}{2} \\ -x \bmod p & \text{if } x \neq 1, \ldots, \frac{p-1}{2} \end{cases}$$

We thus need to show the following: the range of f is indeed QR_p, and that $g(f(x)) = x$ for all $x \in \{1, \ldots, \frac{p-1}{2}\}$.

(a) Show that $f(x) \in \mathrm{QR}_p$ for all $x \in \{1, \ldots, \frac{p-1}{2}\}$.

Hint: You can use (without proof) that $-1 \notin \mathrm{QR}_p$ (this only holds in QR_p for p prime with $p \equiv 3 \bmod 4$). And that the product of two quadratic non-residues is a quadratic residue (this only holds in QR_p, but not in QR_n for n non-prime).

(b) Show that $g(f(x)) = x$ for all $x \in \{1, \ldots, \frac{p-1}{2}\}$.

(This then shows that f is injective and efficiently invertible. Bijectivity follows from injectivity because the domain and range of f both have the same size.)

Hint: Make a case distinction between $x \in \mathrm{QR}_p$ and $x \notin \mathrm{QR}_p$. Show that for $x \in \{1, \ldots, \frac{p-1}{2}\}$ it holds that $-x \bmod p \notin \{1, \ldots, \frac{p-1}{2}\}$.

[1] You do not actually need to use this fact, but the hint that $-1 \notin \mathrm{QR}_p$ below is only true in this case.