Dr. Michael Reyer

Tutorial 13

Wednesday, February 6, 2019

Problem 1. *(Rabin cryptosystem)* Consider a Rabin cryptosystem with public key $n' = p' \cdot q' = 989$.

a) Check that the given parameters satisfy the Rabin cryptosystem requirements.

Consider a Rabin cryptosystem with another public key $n = p \cdot q = 161$ with $p = 7$ and $q = 23$. In order to be able to identify the correct message, we know that the binary representation of the plaintext m ends with 1111.

b) Decipher the cryptogram $c = 116$.

c) Show that the Rabin cryptosystem is vulnerable to chosen-ciphertext attacks.

d) Which vulnerability has the Rabin cryptosystem if $m < \sqrt{n}$ holds? How would you resolve this weakness?

Problem 2. *(Merkle signature scheme)*

a) What are the four main requirements for cryptographic hash functions?

Let $1 < L \in \mathbb{N}$ and $h(m) = m^2 - 1 \mod L$, $m \in \mathbb{Z}$, a hash-function.

b) Let $m \in \mathbb{Z}$. Determine an $m \neq m' \in \mathbb{Z}$ such that $h(m) = h(m')$.

Consider the following hash-based signature scheme to sign messages $m \in \mathbb{N}$. Let $\mathrm{bin}(m)$ denote the binary representation of $m \in \mathbb{N}$. Assume that $\mathrm{bin}(m)$ has n bits.

Key Generation

1) Select $t = n + \lfloor \log_2(n) \rfloor + 1$ random numbers k_i.
2) Compute $v_i = h(k_i)$ for all $i = 1, ..., t$, using a hash function $h : \mathbb{Z} \to \mathbb{Z}_L$ with $L \in \mathbb{N}$.
3) The public key is $(v_1, v_2, ..., v_t)$ and the private key is $(k_1, k_2, ..., k_t)$.

Signature Generation

1) Compute $\hat{c}$, the binary representation of the number of zeros of $\hat{m} = \mathrm{bin}(m)$.
2) Form the concatenated message $\hat{w} = \hat{m} \,||\, \hat{c} = (a_1, a_2, ..., a_n)||(a_{n+1}, ..., a_t)$ with bits a_i, for all $i \leq 1 \leq t$.
3) Determine the positions $i_1 < i_2 < ... < i_u$ in $\hat{w}$, where $a_{i_j} = 1$, for all $1 \leq j \leq u$.
4) Set $s_j = k_{i_j}$ for all $1 \leq j \leq u$.
5) The signature for m is $(s_1, s_2, ..., s_u)$.

Solve the following tasks assuming that $\mathrm{bin}(m)$ has $n = 5$ bits. The private key is given as $(6, 36, 27, 24, 12, 3, 9, 34)$.

c) Describe a verification of the above signature scheme.

d) Sign the decimal message $m = 10$.

e) Eve intercepts a sequence of signatures from Alice. Which knowledge is needed by Eve to impersonate Alice and sign arbitrary messages?

Problem 3. *(ElGamal signature scheme)* Consider an ElGamal signature scheme. The parameters for the signature scheme are given as

$$p = 113,\ x = 66,\ a = 3.$$

a) Show that a is a primitive element modulo p.

b) Calculate the ElGamal signature for the hash value $h(m) = 77$ using the random secret $k = 19$.
Hint: $k^{-1} \equiv 59 \pmod{p-1}$.

From now on we investigate the verification of the ElGamal signature scheme with general parameters.

Assume initially that message m is signed without using a hash function. Oscar chooses $u, v \in \mathbb{Z}$ with $\gcd(v, p-1) = 1$. He computes

$$\begin{aligned} r &= a^u y^v \mod p, \\ s &= -r\, v^{-1} \mod (p-1). \end{aligned}$$

c) Show that (r, s) is a valid signature for the message $m = s\,u \mod (p-1)$.

Oscar knows the signature $(\hat{r}, \hat{s})$ for the hash value $h(\hat{m})$. Let $h(\hat{m})$ and $h(m')$ be invertible modulo $(p-1)$. Oscar computes

$$\begin{aligned} r' &= \hat{r}\,(h(m')\,h(\hat{m})^{-1}\,p - p + 1) \mod (p\,(p-1)), \\ s' &= \hat{s}\,h(m')\,h(\hat{m})^{-1} \mod (p-1). \end{aligned}$$

d) Show that the verification of the signature (r', s') for $h(m')$ provides $v_1 = v_2$.

e) Why does this attack still fail if the verification process is correctly applied?

Problem 4. *(Elliptic Curve Cryptography)* Consider the equation

$$E_a : Y^2 = X^3 + a\,X.$$

You want to uniquely map a message $0 < m < \frac{p}{2}$ to a point (x_m, y_m) on the elliptic curve $E_a(\mathbb{F}_p)$, where p is prime with $p \equiv 3 \pmod 4$ and $x_m \in \{m, p-m\}$.

a) Show that such a point exists. Substantiate your answer.

b) Map the message $m = 6$ to a point on the elliptic curve $E_1(\mathbb{F}_{131})$.
Hint: You may use that $g = 2$ is generator of the field $\mathbb{F}_{131}$ and $2^{114} \equiv 91 \pmod{131}$.

Let $p = 7$.

c) Determine all $a \in \mathbb{F}_7$ such that $E_a(\mathbb{F}_7)$ describes an elliptic curve.

d) For which $a \in \mathbb{F}_7$ does the point $(3, 2)$ lie on $E_a(\mathbb{F}_7)$?

Let $a = 1$.

e) Calculate all points on $E_1(\mathbb{F}_7)$

f) What is the order and the trace t of $E_1(\mathbb{F}_7)$?

g) Prove that $P = (3, 3)$ is a generator of the group.
Hint: Use $2 \cdot (3, 3) = (1, 4)$.