Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Review

Tuesday, March 15, 2016

Problem 1. The following scheme is used to compute square roots modulo a prime number p.

Algorithm 1 Computing square roots modulo a prime number p.

Input: An odd prime number p and a quadratic residue a modulo p

Output: Two square roots $(r, -r)$ of a modulo p

1) Choose a random $b \in \mathbb{Z}_p$ until $v = b^2 - 4a$ is a quadratic non-residue modulo p.
2) Let $f(x)$ denote the polynomial $x^2 - bx + a$ with coefficients in $\mathbb{Z}_p$.
3) Compute $r = x^{\frac{p+1}{2}} \mod f(x)$ (Use without proof: r is an integer)

return $(r, -r)$

a) Let $p = 11$ and $a = 5$. Compute the square roots of a using Algorithm 1 above. Instead of choosing b at random, begin with $b = 5$. If b is invalid, increment b by one.
Hint: To compute r in step 3), perform the polynomial division.

Consider the Rabin cryptosystem. The prime numbers are given by $p = 11$ and $q = 23$. It is known that the plaintext message m ends with 0100 in its binary representation.

b) Decrypt the ciphertext $c = 225$.

c) Somebody announces that the plaintext message m ends with 1111 in its binary representation. Why is this agreement a bad choice for the given ciphertext c?

Problem 2. Consider the following hash-based signature scheme to sign messages $m \in \mathbb{N}$. Let the hat-symbol denote the binary representation of a variable. Message $\hat{m}$ 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 $h : \mathbb{Z}_L \to \mathbb{Z}_L$ 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 in the message $\hat{m}$.
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 $(s_1, s_2, ..., s_u)$.

Verification

1) Obtain the authentic public key $(v_1, v_2, ..., v_t)$.
2) Steps 2) to 4) are identical to the signature generation procedure 1) to 3) above.
5) Accept the signature if and only if $v_{i_j} = h(s_j)$ for all $1 \leq j \leq u$ holds.

Solve the following tasks. The messag $\hat{m}$ has $n = 5$ bits. The hash-function $h(m) = m^2 - 1 \mod L$, $m \in \mathbb{N}$, is used.

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

b) The given hash function $h(m)$ is insecure. Determine an $m' \in \mathbb{N}$ such that $h(m) = h(m')$.

c) Compute t random keys $k_1, k_2, ..., k_t$ using the following pseudo-random number generator with the initial seed $k_0 = 57$:

$$k_n = k_{n-1}^2 \mod 47.$$

d) Sign the decimal message $m = 10$ and verify the signature.

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

Problem 3. Consider a trusted authority which chooses the following system parameters.

(i) p is a large prime number.

(ii) q is a large prime number dividing $p-1$.

(iii) $\beta \in \mathbb{Z}_p^*$ has order q.

(iv) $t \in \mathbb{N}$ is a security parameter such that $q > 2^t$.

Every user in the network chooses its own private key a, with $0 \leq a \leq q-1$, and constructs a corresponding public key $v = \beta^{-a} \mod p$. The Schnorr Identification Scheme is defined as:

1) Alice chooses a random number k, with $0 \leq k \leq q-1$, and she computes $\gamma = \beta^k \mod p$. She sends her certificate and γ to Bob.

2) Bob verifies Alice's public key v on the certificate. Bob chooses a random challenge r, with $1 \leq r \leq 2^t$, and sends it to Alice.

3) Alice computes $y = k + ar \mod q$ and sends the response y to Bob.

4) Bob verifies that $\gamma \equiv \beta^y v^r \mod p$. If true, then Bob accepts the identification; otherwise, Bob rejects the identification.

Answer the following questions:

(a) On the hardness of which mathematical problem does the Schnorr Identification Scheme rely?

(b) Show that Alice is able to prove her identify to Bob, assuming that both parties are honest and perform correct computations, i.e., the verification in step 4 is correct.

(c) Which operations are computationally hardest in this protocol? Which operations can be done prior to the direct identification process?

(d) Now, the public parameters are $p = 71$, $q = 7$, $\beta = 20$, $t = 2$. Suppose Alice chooses $a = 5$, $k = 10$, and Bob issues the challenge $r = 4$. Compute all steps in the protocol, assuming that Alice's certificate is valid.

Problem 4. Consider the function

$$E_a : Y^2 = X^3 + aX + 2$$

over the field $\mathbb{F}_7$.

(a) Determine all possible values of a, such that E describes an elliptic curve over the field $\mathbb{F}_7$.

Let $a = 3$ in the following.

(b) Determine all points and their inverses for $E_3(\mathbb{F}_7)$.

(c) Give the group order $\#E_3(\mathbb{F}_7)$.

(d) Show that the point $(0, 3)$ is a generator of the group $E_3(\mathbb{F}_7)$ with respect to the corresponding addition.

(e) Give an upper and a lower bound for the cardinality of $E_3(\mathbb{F}_q)$.