Review Exercise Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

31.07.2012, WSH 24 A 407, 10:30h

Problem 4. A prime number $p \equiv 5 \pmod 8$, a quadratic residue a modulo p and the following algorithm are given.

Algorithm 1 SQR

Input: Prime number p with $p \equiv 5 \pmod 8$ and quadratic residue a modulo p
Output: Square roots $(r, -r)$ of a modulo p

$d \leftarrow a^{\frac{p-1}{4}} \mod p$
if $(d = 1)$ **then**
  $r \leftarrow a^{\frac{p+3}{8}} \mod p$
end if
if $(d = p - 1)$ **then**
  $r \leftarrow 2a(4a)^{\frac{p-5}{8}} \mod p$
end if
return $(r, -r)$

a) Show that the variable d in algorithm SQR can only take the values 1 or $p - 1$.

b) Suppose that $2^{\frac{p-1}{2}} \equiv -1 \pmod p$ holds. Prove that algorithm SQR computes both square roots of a modulo p.

A variant of the Rabin cryptosystem uses algorithm SQR and is accordingly defined for prime numbers $p, q \equiv 5 \pmod 8$ with $n = p \cdot q$.
The prime numbers $p = 53$, $q = 37$, and the ciphertext $c = 1342 = m^2 \mod n$ are given. By agreement the message m ends on 101 in its binary representation.

c) Compute the square roots of 17 modulo 53 and 10 modulo 37.

d) Decipher the message m. You may use $7 \cdot 53 - 10 \cdot 37 = 1$ for your computation.

Problem 5.

(a) Compute the probability that in a group of 6 students at least two students have their birthday on the same day in this year (year 2012 has 366 days) assuming that birthdays are independent and uniformly distributed.

(b) What are the four basic requirements of cryptographic hash functions?

The *discrete logarithm hash function* $h : \mathbb{Z}_{q^2} \to \mathbb{Z}_p$ is defined by:

$$h(m) = h(x, y) = u^x v^y \mod p,$$

with numbers $p = 2q + 1$ and q both prime, numbers u and v primitive elements modulo p, and a message given as $m = x + yq$ with $0 \le x, y \le q - 1$.

(c) Compute the hash value $h(x, y)$ for the message $m = 1073$ with the parameters $u = 37$, $v = 131$, and $p = 167$.

(d) What values can $\gcd(a, p - 1)$ attain for $a \in \mathbb{N}$?

(e) Assume that $h(x_1, y_1) = h(x_2, y_2)$ with $x_1 \neq x_2$, $y_2 > y_1$, and $2 \nmid y_2 - y_1$ holds. Compute the discrete logarithm $\log_u(v)$ depending on x_1, y_1, x_2 and y_2.

(f) Find a collision to $h(1073)$ for the given discrete logarithm $\log_{37}(131) = 101$.

The hash function is now applied on two messages m_1 and m_2. Alice wants to sign both hashed messages with the Digital Signature Algorithm (DSA).

(g) What are the three basic requirements for signature schemes?

(h) Assume Alice uses the same session key k for both signatures. Derive her secret key x.

Problem 6.

(a) Show that $E_\alpha : Y^2 = X^3 + \alpha X + 1$ is an elliptic curve over the finite field $\mathbb{F}_{13}$ for $\alpha = 2$.

(b) Compute the points iP for $P = (0, 1)$ on E_2 with $i = 0, \ldots, 4$.

(c) The group order of E_2 is $\#E_2(\mathbb{F}_q) = 8$. Show that P is a cyclic generator for E_2.

Consider the following algorithm to compute the discrete logarithm on elliptic curves:

Algorithm 2 The Babystep-Giantstep-Algorithm on Elliptic Curves

Require: An elliptic curve $E_\alpha(\mathbb{F}_q)$ and two points $P, Q \in E_\alpha(\mathbb{F}_q)$

Ensure: $a \in \mathbb{F}_q$, i.e., the discrete logarithm of $Q = aP$ on E_α

(1) Fix $m \leftarrow \lceil \sqrt{q} \rceil$.

(2) Compute a table of *babysteps* $b_i = iP$ for indices $i \in \mathbb{Z}$ in $0 \le i < m$.

(3) Compute a table of *giantsteps* $g_j = Q - j(mP)$ for all indices $j \in \mathbb{Z}$ in $0 \le j < m$ until you find a pair (i, j) such that $b_i = g_j$ holds.

return $a = i + mj \mod q$.

(d) Show that the given algorithm calculates the discrete logarithm on elliptic curves.

(e) Compute the discrete logarithm of $Q = aP$ with points $P = (0, 1)$ and $Q = (8, 3)$ on the elliptic curve E_2 using this algorithm.