Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 13

Thursday, February 8, 2018

Problem 1. Alice wants to use the triple $(p, a, y) = (137, 3, 97)$ as public ElGamal key.

a) Show that this is a valid ElGamal key.

b) Determine the plaintext to the cryptogram $(c_1, c_2) = (81, 7)$ without calculating the private key x.

Alice utilizes the ElGamal key for signing the messages $h(m_1) = 106$ and $h(m_2) = 99$ with the signatures $(r_1, s_1) = (13, 63)$ and $(r_2, s_2) = (13, 62)$, respectively.

c) What did Alice do wrong?

d) Calculate her private key x.

Problem 2. 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 3.

(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 $0 \leq x, y \leq q - 1$.

(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 4. Consider the equation $E: Y^2 = X^3 + 4X + 1$ over the field $\mathbb{F}_7$.

a) Is E an elliptic curve over $\mathbb{F}_7$? Substantiate your answer.

b) Determine all points on the elliptic curve E.

c) What is the order of the corresponding group?

d) Give a generator for the group.

e) Formulate the elliptic curve Diffie-Hellman-Protocol.

f) Let $P = (0, 1)$. Calculate $2P$, $4P$, and $6P$.

g) Alice and Bob want to execute the elliptic curve Diffie-Hellman protocol. They use $P = (0, 1)$, a generator of the group. Alice chooses the random secret $x = 2$. Bob chooses the random secret $y = 4$. Execute the protocol on the above elliptic curve E.