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

Exercise 11

Friday, January 26, 2018

Problem 1. *(babystep-gaintstep-algorithm on elliptic curves)*

(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 $i = 0, \dots, 4$.

(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 1 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 $a = i + mj \bmod q$.

(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.

Problem 2. 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 $0 \le a \le q - 1$, 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 $0 \le k \le q-1$, 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 3.

a) Show that $\alpha = 5n + 7$ and $\beta = 3n + 4$ are relatively prime for any integer n.
Hint: If $\alpha \cdot x + \beta \cdot y = 1$ for some integers x and y then α and β are relatively prime.

b) Alice and Bob use the RSA cryptosystem and hence need to choose two prime numbers p and q. Using the Miller-Rabin Primality Test, describe a method to generate the prime numbers p and q, such that $n = pq$ has exactly K bits and p and q have $K/2$ bits, provided K is even.

c) Alice and Bob choose prime numbers $p = 11$ and $q = 13$. Moreover, Alice chooses her private key as $e = 7$. Bob receives a ciphertext $c = 31$. What is the message m sent by Alice?.

d) Suppose Alice and Bob use the RSA system with the same modulo n and their public keys e_A and e_B are relatively prime. A new user Claire wants to send a message to both Alice and Bob, so Claire encrypts the message using $c_A = m^{e_A} \mod n$ and $c_B = m^{e_B} \mod n$. Show how an eavesdropper can decipher the message m by intercepting both c_A and c_B.

Consider the RSA signature scheme.

e) Describe the requirements of a *digital signature*.

f) Suppose that Oscar is interested in knowing Alice's signature s for the message m. Oscar knows Alice's signatures for the messages m_1 and $m_2 = (m \cdot {m_1}^{-1}) \mod \text{n}$, where ${m_1}^{-1}$ is the inverse of m_1 modulo n. Show that Oscar can generate a valid signature s on m, using the signatures of m_1 and m_2.