Review Exercise Cryptography II

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

22.02.2013, WSH 24 A 407, 11:00h

Problem 4.

Alice and Bob use a Rabin cryptosystem. Bob's public key is $n = 189121 = p\,q$ with primes $p = 379$ and $q = 499$. By agreement the message is divisible by 8. Alice sends the cryptogram $c = 5$ to Bob.

a) Determine the message m. You may use the following information without proof:

- $79 \cdot 379 - 60 \cdot 499 = 1$
- $449^2 \mod 499 = 5$

Oscar wants to find out the factorization of n. Therefore, he claims that Bob does not know the factorization of n either, and suggests that Bob shall proof this fact by the following protocol.

1) Oscar sends a quadratic residue y modulo n to Bob.
2) Bob calculates a square root x modulo n and returns it to Oscar.
3) Oscar verifies that $x^2 \equiv y \pmod{n}$ holds.

Oscar and Bob exchange the values $y = 625$ and $x = 15943$ following the above protocol.

b) Determine p and q and answer the following questions:
   - i) Why is this task easier for Oscar than for you?
   - ii) What is the probability of success for Oscar to factorize n, if Bob chooses each square root with the same probability?

Problem 5.

Consider an ElGamal signature scheme.

a) Assume the same session key k is used for two signatures. Derive the secret key x.

The public key is $(p, a, y) = (149, 2, 63)$.

b) Show that this key is a valid ElGamal public key.

c) Show that $x = 20$ is the corresponding private key.

Additionally, the hash funktion $h : \mathbb{Z} \to \mathbb{Z}_p$ defined by $h(z) = z^2 + z + 1 \mod p$ is used.

d) Show that for this hash function infinitely many $z \in \mathbb{Z}$ exist with

$$h(z) \equiv h(z-1) \pmod{p}.$$

e) What are the requirements of cryptographic hash functions in general? Which of these requirements is/are violated by means of the property given in (d)? Substantiate your answer.

f) Determine the ElGamal signature for the message $m = 22$. Choose the session key $k = 25$.

Problem 6.

Consider the following elliptic curve over the finite field $\mathbb{F}_7$:

$$E : Y^2 = X^3 + 3X + 2.$$

a) Show that E is an elliptic curve.

b) Determine all points on the elliptic curve E and determine the order of the group.

c) Compute the product $2 \cdot (0, 3)$ on the elliptic curve E.

Now, consider the following encryption scheme based on the discrete logarithm problem:

Shamir's No-Key protocol:

(1) Publish a group $\mathbb{Z}_p^*$ of order $p - 1$ with p prime.
(2) A chooses a plaintext $m \in \mathbb{Z}_p^*$.
(3) A, B choose secret random numbers with $\gcd(a, p-1) = 1$, $\gcd(b, p-1) = 1$.
(4) A, B calculate the inverses a^{-1}, $b^{-1} \in \mathbb{Z}_{p-1}^*$, respectively.
(5) $A \to B$: $c_1 = m^a \mod p$.
(6) $B \to A$: $c_2 = {c_1}^b \mod p$.
(7) $A \to B$: $c_3 = {c_2}^{a^{-1}} \mod p$.

d) How can Bob decrypt c_3?

e) Formulate the given protocol in a group of $\mathbb{F}_q$-rational points over an elliptic curve $E(\mathbb{F}_q)$.

f) Decipher the cryptogram $C_3 = (4, 1)$ in the given elliptic curve $E(\mathbb{F}_7)$ knowing Bobs private key $b = 7$.