MATHEMATICAL CRYPTOLOGY

Lunds Tekniska Högskola
Dept. of EIT
Lund University

March 6, 2008, 8–13

- You are allowed to use a calculator.
- Each solution should be written on a *separate sheet of paper*.
- You must *clearly* show the line of reasoning.
- If any data is lacking, make reasonable assumptions.

Good luck!

Problem 1 Answer each of the following questions using 1- 50 words.

1.1) Consider the multiplicative group $\mathbb{F}_{31}^*$. Which values can $ord(x)$ take for $x \in \mathbb{F}_{31}^*$?

1.2) Let $Q_n = \{x^2 : x \in \mathbb{Z}_n^*\}$ and let J_n be the set of elements in $\mathbb{Z}_n^*$ with Jacobi symbol equal to plus one. When do we have $Q_n = J_n$?

1.3) What is the meaning of *spurious keys*?.

1.4) Describe how CBC-MAC works.

1.5) Describe the relation between the three problems DLP, DHP, and the DDH problem.

1.6) Describe Pollard's Rho algorithm for solving the discrete log problem.

1.7) What is a Carmichael number?

1.8) Give the shortest nonzero vector in the lattice spanned by the basis vectors $b_1 = (30)^T$ and $b_2 = (21)^T$.

1.9) Why is RSA not polynomially secure?.

1.10) Give the definition of an NP complete decision problem.

(20 points)

Problem 2

Consider the elliptic curve $Y^2 = X^3 + X + 4$ defined over $\mathbb{F}_{23}$ and the group generated by $P = (0, 2)$. Alice and Bob are doing a simple DH-EC key exchange. Alice sends Bo $[a]P = (14, 5)$ and Bob sends $[b]P = (11, 9)$ to Alice. Show the computations done by both Bob to determine the shared key $[ab]P$ knowing that $b = 3$. Then do the same for Alice knowing that $a = 8$.

Hint: For the curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (char K not 2 or 3), and $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, we have $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$. Also if $x_1 \neq x_2$ we set $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $\mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$. If $x_1 = x_2$ and $P_2 \neq -P_1$ we set $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$, $\mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$. Now $P_1 + P_2 = P_3 = (x_3, y_3)$ is given by $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = -(\lambda + a_1)x_3 - \mu - a_3$.

(6 points)

Problem 3

Consider $\mathbb{F}_{2663}$ and the multiplicative cyclic group generated by the element 2. Determine its order and then compute the discrete logarithm (base 2) of 413 using Pohlig-Hellman, i.e., find $x \in \mathbb{F}_{2663}$ such that $2^x = 413$ in $\mathbb{F}_{2663}$.

(6 points)

Problem 4

Prove that the two problems FACTORING and SQRROOT are polynomial-time equivalent.

(6 points)

Problem 5

In ElGamal encryption, the private key x is an element of a group G. The public key is given by $h = g^x$, where g is a fixed known element.

In encryption of message m, one generates a random ephemeral key k, sets $c_1 = g^k$ and $c_2 = m \cdot h^k$ and output the ciphertext $c = (_1, c_2)$. Describe the decryption process and prove that it always returns the encrypted message m.

Also prove that assuming that DHP is hard, ElGamal is secure under chosen plaintext attacks (security means it is hard for the adversary, given the ciphertext, to recover the whole of the plaintext). (6 points)

Problem 6

Let modular arithmethic with $N = 1073741827$ be implemented using Montgomery arithmetic with $R = 2^{32} = 4294967296$. Calculate the Montgomery representation of the elements 11 and 13 in $\mathbb{Z}_N$. Then show how their product is computed in a Montgomery fashion, resulting in the element $11 \cdot 13$ in Montgomery representation.