Dept. of EIT, Lund University

Final exam in MATHEMATICAL CRYPTOLOGY

March 10, 2011, 9–14

- 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 $\mathbb{F}_{29}^*$. Which values can $ord(x)$ take for $x \in \mathbb{F}_{29}^*$?

1.2) If N is a product of two primes and the element x has a square root, then how many square roots has it?

1.3) Describe CBC mode of operation of a block cipher.

1.4) What is Kerberos and how does it work (very briefly)?

1.5) Define the three problems DLP, DHP, and the DDH problem.

1.6) If you choose a random 512 bit number, what is (roughly) the probability that this number is prime?

1.7) Give the shortest nonzero vector in the lattice spanned by the basis vectors $b_1 = (3\ 0)^T$ and $b_2 = (2\ 1)^T$.

1.8) Explain when an encryption scheme is non-malleable.

1.9) Explain commitment scheme and give an example of such.

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

(20 points)

Problem 2

Consider the elliptic curve $Y^2 = X^3 + 20X + 3$ defined over $\mathbb{F}_{23}$ and the associated group. Let $P = (1, 1)$ be a generator of order 25 and let $[k]P = (11, 6)$. Determine k using a Baby-Step/Giant-Step approach. To help you a bit, we have computed $[5]P = (16, 7)$, $[10]P = (17, 9)$.

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

Assume that we try to strengthen a block cipher by using it twice with two different n-bit keys k_1, k_2 (in total $2n$ bits),

$$c = E_{k_1}(E_{k_2}(m)).$$

Describe a chosen plaintext attack which requires $O(2^n)$ memory and $O(2^n)$ encryptions/decryptions using E.

(6 points)

Problem 4

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

(6 points)

Problem 5

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 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.

Hint: The constant $q = N^{-1} \pmod{R}$ has been precomputed to $q = 1789569707$.

(6 points)

Formulas in Mathematical Cryptology

Ch 1:

CRT: $M = m_1 m_2 \cdots m_r$, $m_1, m_2, \ldots$ pairwise relatively prime. The solution x, $0 \le x \le M$, to $x = a_i \bmod m_i$ for $i = 1, 2, \ldots, r$ is given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$, and $y_i = M_i^{-1} \bmod m_i$.

Legendre and Jacobi Symbols:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

The law of quadratic reciprocity (p, q primes)

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$$

- $\left(\frac{q}{p}\right) = \left(\frac{q \bmod p}{p}\right)$
- $\left(\frac{q \cdot r}{p}\right) = \left(\frac{q}{p}\right) \cdot \left(\frac{r}{p}\right)$
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Computing square roots of a in $\mathbb{F}_p$: When $p = 3 \bmod 4$,

$$x = a^{(p+1)/4} \bmod p,$$

Ch 2:
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 $y_3 = -(\lambda + a_1)x_3 - \mu - a_3$.

Ch 12:
Pohlig-Hellman: solving DLP $g^x = h$ in group of order N.

$S = \{\}$
forall primes p dividing N **do**
Compute largest $T = p^e$ dividing N
$g_1 = g^{N/T}$
$h_1 = h^{N/T}$
$z = \text{DLPOracle}(g_1, h_1, p^e)$
$S = S + \{(z, T)\}$
end
$x = CRT(S)$