Dept. of EIT, Lund University

Final exam in MATHEMATICAL CRYPTOLOGY

March 05, 2010, 14–19

- 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) If the nonzero element c is a quadratic nonresidue in $\mathbb{F}_p$, then how many solutions are there to the equation $x^2 + 2x + 1 = c$?

1.2) Describe briefly the difference between a Feistel cipher and an SP network.

1.3) Describe how the unicity distance and the number of spurious keys are related.

1.4) For hash functions, what are the differences between properties: preimage resistant, second preimage resistant and collision resistant?

1.5) What is (roughly) the computational complexity of the currently best known algorithms for factoring and (roughly) what size of RSA numbers can be factored.

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

1.7) Give one example of circumstances when a lattice based attack on RSA can work?

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

1.9) Explain the meaning of oblivious transfer.

1.10) Give the definition of co - NP.

(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

Consider triple DES but with two keys k_1, k_2 instead of three,

$$c = DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(m))).$$

Describe a chosen plaintext attack which requires roughly 2^{56} memory and roughly 2^{56} encryptions/decryptions using single DES.

(6 points)

Problem 4

Show that if one knows the secret RSA decryption exponent d corresponding to the public key (N, e), then one can efficiently factor N through a Las Vegas algorithm.

(6 points)

Problem 5

Consider $\mathbb{F}_{647}^*$ generated by the element 5, (ord(5) = 646). Compute the discrete logarithm (base 5) of 201 using Pohlig-Hellman, i.e., find $x \in \mathbb{F}_{647}$ such that $5^x = 201$ in $\mathbb{F}_{647}$.

(6 points)

Problem 6

Consider the problem of constructing a MAC using a keyed hash function. Assume that the hash function h uses a Merkle-Damgaard construction for messages of arbitrary length. A good solution is the so-called HMAC construction. Examples of bad constructions are

$$\text{MAC}_k(M) = h(k||M),$$

and

$$\text{MAC}_k(M) = h(M||k),$$

where $||$ means string concatenation and k is the key and M is the message.

Give your best attacks on the two constructions above. (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
$x = CRT(S)$