Dept. of EIT, Lund University

Final exam in MATHEMATICAL CRYPTOLOGY

March 5, 2012, 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) If N is a product of *three* different primes and the nonzero element x has a square root, then how many square roots has it?

1.2) Give an outline of AES encryption using the abstract functions AddRoundKey(), ShiftRows(), SubBytes() and MixColumns().

1.3) Describe the Merkle-Damgård construction for hash functions.

1.4) What is meaning of "nonce" used in many (key distribution) protocols?

1.5) Give an example of a number larger than 200 that is 12-power smooth.

1.6) Describe the relation between the three problems FACTORING, SQRROOT, RSA problem.

1.7) A good hash function outputs a 160 bit hash value. What is roughly the complexity of a generic attack to find a preimage. Secondly, what is roughly the complexity to find a collision.

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

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

1.10) Explain why RSA-OAEP encryption is better than plain RSA encryption.

(20 points)

Problem 2

Consider the elliptic curve $Y^2 = X^3 + X + 3$ defined over $\mathbb{F}_{199}$ and the associated group of order 197. Let $P = (1, 76)$ be a generator. Compute $[29]P$.

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

Let modular arithmethic with $N = 1073741827$ be implemented using Montgomery arithmetic with $R = 2^{32} = 4294967296$. Calculate the Montgomery representation of the elements 3 and 5 in $\mathbb{Z}_N$. Then show how their product is computed in a Montgomery fashion, resulting in the element $3 \cdot 5 = 15$ in Montgomery representation.

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

(6 points)

Problem 5

Consider $\mathbb{F}_{2663}$ and the multiplicative cyclic group generated by the element 3 of order 1331. Compute the discrete logarithm (base 3) of 152 using Pohlig-Hellman, i.e., find $x \in \mathbb{F}_{2663}$ such that $3^x = 2019$ in $\mathbb{F}_{2663}$.

(6 points)

Problem 6

Let $B(m)$ be defined as $B(m) = m \bmod 2$. Show that $B(m)$ is a hard predicate for the RSA problem (defined as $c = m^e \pmod{N}$).

(6 points)
