NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4160 Cryptography**

Academic contact during examination: Anders S. Lund

Phone: 73 59 16 25 / 41 45 19 15

Examination date: 10 December 2014

Examination time (from–to): 09:00–13:00

Permitted examination support material: B: All printed and hand-written support material is allowed. A specific basic calculator is allowed.

Other information:
All answers must be justified.

Language: English

Number of pages: 2

Number pages enclosed: 0

Checked by:

Date Signature

Problem 1 (10%) Calculate the Jacobi symbol $\left(\frac{2345}{6789}\right)$.

Problem 2 (10%) Suppose we use the following formula to calculate MACs (Message Authentication Codes).

$$\text{Poly-MAC}(m) = a + bm \pmod{1249}$$

where a and b are positive integers less than 1249. 1249 is a prime.

Explain why this MAC is secure if it is used on only one message, but insecure if it is used on two or more messages.

Problem 3 Let $p = 1249$, $g = 2$ and $h = 30$. You can still use that 1249 is a prime.

a) (10%) Use that $(g^{10}h^{-4})^4(g^{14}h^{15})^2(g^{157}h^{-19}) \equiv 1 \pmod{1249}$ to find $\log_g h$.

b) (10%) Let (p, g, h) be a verification key for an ElGamal signature protokol. Use the answer in a) to find a signature on $m = 4$ with random key $k = 5$.

If you have not solved a), make a signature on $m = 4$ with $h = 79$, $a = 40$ and $k = 5$.

Problem 4 Let $E : y^2 = x^3 + x + 1$ be an elliptic curve over the field $\mathbb{F}_{23}$. $P = (1, 7)$ and $Q = (11, 3)$ are points on the curve, and $Q = aP$ for some integer a. It is known that $2Q = (4, 0)$.

a) (10%) Suppose we are going to use ElGamal on the curve. Let (P, Q) be the public key, and a the secret key. Find the encryption of $M = (6, 19)$ when the randomness is $t = 2$ (you can safely assume that M is a point on the curve).

b) (10%) The order of P is divisible by a prime number greater than 6. Find the order of P. Is E cyclic?

Problem 5 (10%) Suppose we are using ElGamal with public key (g, h, p) to encrypt messages, and that we use the version of ElGamal where $e_K(m) = (g^t, h^t g^m)$ for a randomly chosen t and a small message m of your own choice, e.g. $m = 2047$ or $m = 2048$.

Explain why we should not use the square-and-multiply algorithm to do the exponentiations.

Hint: Suppose you can trick someone to encrypt repeatedly, and that you can measure the time it takes.

Problem 6 (10%) Alice sets up an RSA cryptosystem with public key (n, e), and awaits an important message from Bob. Eve wants to find out what the message Alice receives from Bob is, and manages to obtain the encrypted message. In addition she has a huge advantage: She was allowed to choose a small set of messages that Bob could choose from, but not the precise message.

How can Eve guarantee that she is always able to decide which message Alice receives as long as Alice and Bob uses standard RSA? Could Bob do something to stop Eve from succeeding?

Problem 7 Let $n = 99221$.

a) (10%) Factor n by finding x and y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv y \pmod{n}$.

Hint: Find a y such that $y \not\equiv \pm 2 \pmod{n}$, but $y^2 \equiv 4 \pmod{n}$.

Concider the following protocol between Alice and Bob.

1. Alice chooses an RSA-modulus $n = pq$ (p and q known to Alice, but not to Bob), a public key e, a message m and calculates $c \equiv m^e \pmod{n}$. Alice sends (n, e, c) to Bob.
2. Bob chooses an $x \in \mathbb{Z}_n$ and calculates $y \equiv x^2 \pmod{n}$. Bob sends y to Alice.
3. Alice finds a random z such that $z^2 \equiv y \pmod{n}$. Alice sends z to Bob.

b) (10%) Explain how Bob can find m with probability $1/2$, that he can not get a higher probability of succeeding and that Alice cannot stop him, or know if he finds m or not.