NTNU

Department of Mathematical Sciences

Examination paper for **TMA4160 Cryptography**

Academic contact during examination: Kristian Gjøsteen
Phone: 73 55 02 42

Examination date: December 17, 2013
Examination time (from–to): 15:00–19:00
Permitted examination support material: B: All printed and hand-written support material is allowed. A specific basic calculator is allowed.

Other information:

Language: English
Number of pages: 2
Number pages enclosed: 0

Checked by:

Date Signature

Problem 1 (i) Show that the matrices

$$\begin{pmatrix} 7 & 4 \\ 11 & 11 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 9 & 18 \\ 17 & 1 \end{pmatrix}$$

are inverses modulo 26.

(ii) Alice sent a ciphertext to Bob that begins with `tusdrfrf`. You think Alice has used the Hill cipher with block size 2 and that the plaintext begins with `hello`.

Find the secret key and decrypt the rest of the ciphertext.

The message that was sent is in English, the alphabet has 26 letters and the usual correspondence between numbers and letters has been used.

Problem 2 In this problem we shall consider RSA encryption with public encryption key $(n, e) = (28673, 7)$.

a) Use Pollard's ρ-method to factor n. Start with the number 14 and use the iteration function $f(x) = x^2 + 1$.

b) Find a decryption key for (n, e).

c) Compute the decryption of $c = 2$.

Problem 3 In this problem we shall work with the elliptic curve E given by the equation $Y^2 = X^3 + X + 46$ over the field $\mathbb{F}_{101}$. We use ∞ for the point "at infinity".

a) Use the Chinese remainder theorem to find all possible solutions to the equations

$$\begin{aligned} N &\equiv 1 \pmod 3 \text{ and} \\ N &\equiv 4 \pmod 5. \end{aligned}$$

You get to know that the number of points N on the elliptic curve is prime and satisfies the above equations. Explain why $N = 109$.

b) The points $P = (2, 37)$, $Q = (54, 2)$ and $R = (64, 19)$ are on the curve. Show that

$$6P + 2Q + R = \infty \text{ and}$$
$$2P + Q + 2R = \infty.$$

c) Find $\log_P R$.

Problem 4 ElGamal over the group $\mathbb{F}^*_{28019}$ with generator $g = 2$ was used to encrypt either 1 or -1. The ciphertext is $(x, w) = (144, 6789)$. Decide which message was encrypted.

Problem 5 Let G be a group of prime order $q = 53$. Let g be a generator and let y be an element in the group.

a) Given that $g^3y^3 = g^{35}y^5$, find $\log_g y$.

Schnorr signatures based on the group G and a hash function $H : \{0,1\}^* \times G \to \{0, 1, 2, \ldots, q-1\}$ work as follows:

- A signing key is a number a. The corresponding verification key is $y = g^a$.
- We sign a message $m \in \{0,1\}^*$ as follows:
  1. Choose random r from $\{1, 2, \ldots, q-1\}$.
  2. Compute $v = H(m, g^r)$.
  3. Compute $w = r + av \bmod q$.

  The signature is the pair (v, w).
- We verify a signature (v, w) on a message $m \in \{0,1\}^*$ by verifying the equation
$$H(m, g^w y^{-v}) = v.$$

b) Given the Schnorr signatures $(50, 3)$ and $(48, 35)$ on two distinct messages under the same signing key, find the secret signing key and the random numbers used to sign.

What went wrong during signature creation?