NTNU
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4160 Cryptography**

Academic contact during examination: Kristian Gjøsteen

Phone: 73 55 02 42

Examination date: December 17 2019

Examination time (from–to): 9:00-13:00

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

Other information:

Language: English

Number of pages: 3

Number of pages enclosed: 0

Checked by:

Informasjon om trykking av eksamensoppgave	
Originalen er:	
1-sidig ☐	**2-sidig** ☒
sort/hvit ☒	**farger** ☐
skal ha flervalgskjema ☐	

Date Signature

Problem 1 Let $n = 1333$.

a) Use the Fermat test to prove that n is not prime.

Hint: $2^{333} \equiv 70 \pmod{n}$.

b) Use Pollard's $p-1$ method to factor n.

Problem 2 Let $p = 173$ and consider the elliptic curve

$$E: \qquad Y^2 = X^3 + 2X + 2$$

over $\mathbb{F}_p$. The point $P = (2, 35)$ is on the curve.

a) You get to know that $32P = (101, 109)$ and $128P = (137, 26)$. Compute $95P$.

b) In the previous task, you found that $95P = (3, 143)$. Now you also get to know that $291P = (3, 30)$.

Find the number of points on the curve.

Problem 3 We shall now study some ideas that will lead to *ring signatures*.

Suppose we have a collection of RSA public keys $\{(n_1, e_1), (n_2, e_2), \ldots, (n_r, e_r)\}$. Suppose also that b is such that 2^b is much, much larger than any of the RSA moduluses ($2^b \ggg n_i$ for all i). Let $f_i : \{0, 1, \ldots, n_i - 1\} \to \{0, 1, \ldots, n_i - 1\}$ be the bijection $f_i(x) = x^{e_i} \bmod n_i$.

Let $T = \{0, 1, \ldots, 2^b - 1\}$. For each i, define a function $g_i : T \to T$ as

$$g_i(m) = \begin{cases} q_i n_i + f_i(r_i) & \text{if } (q_i + 1)n_i \leq 2^b, \text{ and} \\ m & \text{if } (q_i + 1)n_i > 2^b. \end{cases}$$

where $r_i = m \bmod n_i$ and q_i is such that $m = q_i n_i + r_i$.

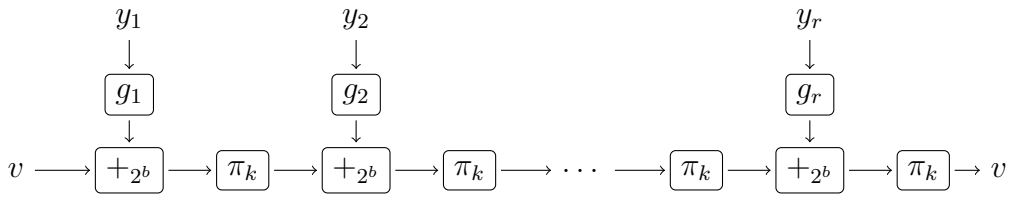
a) Show that g_i is a bijection on T for all i. Also show that $g_i(m) \neq m$ for most $m \in T$.

b) Explain why it is easy to invert g_i if you know the prime factors of n_i.

Explain why it is probably hard to invert g_i if you do not know the prime factors of n_i.

Let K be a set of keys and let $\pi, \pi^{-1} : K \times T \to T$ be a block cipher. As usual, for $k \in K$ denote by π_k the function that takes x to $\pi(k, x)$.

Let $v \in T$ and $k \in K$. Consider the equation in r unknowns $y_1, y_2, \ldots, y_r$ in diagram form:



Or as an equation:

$$v = \pi_k\left(g_r(y_r) +_{2^b} \pi_k\left(\ldots \pi_k\Big(g_2(y_2) +_{2^b} \pi_k(g_1(y_1) +_{2^b} v)\Big)\ldots\right)\right)$$

Here, $+_{2^b}$ denotes addition modulo 2^b, that is, $a +_{2^b} b = (a + b) \bmod 2^b$.

c) Show that if you know the prime factors of some n_i, you can find a solution to the equation for any $v \in T$, $k \in K$ and block cipher π, π^{-1}.

d) Show that for any $v \in T$, $k \in K$ and block cipher π, π^{-1}, the above equation has exactly $(2^b)^{r-1}$ solutions.

A brief explanation of what this can be used for: The above mathematical structure can be used to create a *ring signature*. The owner of any of the RSA private keys involved can easily find solutions to the above equation (c.), while someone who does not know any of the private keys cannot find solutions. It is impossible to reveal which private key was used to create the solution (d.).

A ring signature can be used to prove that a member of a given group of people (government ministers) leaked a given document, proving the document's authenticity, without giving away any information about who leaked to document. A more recent application is to get some anonymity in Bitcoin-like payment systems.

Problem 4 In this task, we shall study *electronic voting*. In particular, we shall consider a straight *yes/no* vote.

The electoral board will publish an encryption key and two distinct values, u and v. The idea is that the voters will encrypt u to vote *yes*, and v to vote *no*. Each voter sends their ciphertext and name to the electoral board. After voting ends, the electoral board will decrypt the ciphertexts one by one using a special secure computer: they will feed each ciphertext to the computer, which will decrypt it and immediately output the decryption.

The election will use ordinary ElGamal over a group G of prime order p with generator g. The secure computer has an ElGamal decryption key a, and it has computed and output the public key $y = g^a$. It is believed to be impossible to extract the decryption key from the special computer.

An encryption of a message m is a pair $(g^r, y^r m)$ for some r.

Just before the decryption is to start, the manufacturer reveals that due to a bug in their software, the special secure computer can only decrypt **one** ciphertext. After decrypting this ciphertext, the decryption key will be permanently destroyed.

a) Explain how the electoral board can still get the election result.

Hint: If the ciphertext (x_1, w_1) decrypts to m_1, and the ciphertext (x_2, w_2) decrypts to m_2, what does the ciphertext $(x_1 x_2, w_1 w_2)$ decrypt to?

b) On the plus side: Explain why this may be good for privacy, in the sense that it should be secret exactly which ballot a voter cast. (That is, explain why this was not true originally, but is true now.)

On the minus side: If a single voter knew this would happen, explain how that voter could have cheated to favor their desired result.