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 7 2016

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:

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 A message in English beginning with the two letters `OR` has been encrypted using the affine cipher, resulting in the following ciphertext:

`VKDQH ZUDQP ITDQT VUMXK QDLX` .

Find the key and the decryption of the message. (The letters of the ciphertext are in groups of five.)

Problem 2 Let E be the elliptic curve defined by $Y^2 = X^3 - X + 15$ over $\mathbb{F}_{19}$. The point $P = (3, 1)$ is on the curve.

a) Compute $16P$ using a fast exponentiation (point multiplication) algorithm, showing that $16P = -P$.

b) Determine the number of rational points on the curve. Is the curve cyclic?

Problem 3 The number 247237 is a product of two primes p and q. Compute p and q using Fermat factoring.

Problem 4 A single random number is used in the creation of a Schnorr signature. Suppose you know a message m, a signature σ on m and the random number r used to create the signature. Explain how you can use this information to easily compute the Schnorr signing key.

Problem 5 In this problem, G is a group of order p, where p is a large prime, g is a generator and x is a group element. We want to study a method of computing $\log_g x$.

Let $\{S_1, S_2, S_3\}$ be a partition of G and let $f : G \to G$ be the function

$$f(z) = \begin{cases} xz & z \in S_1 \\ z^2 & z \in S_2 \\ zg & z \in S_3 \end{cases}$$

Let D be a subset of G with r elements such that p/r is small compared to $\sqrt{p}$. We shall now generate m sequences of group elements (of varying length):

$$\begin{aligned} &y_{11}, y_{12}, \ldots, y_{1,n_1} \\ &y_{21}, y_{22}, \ldots, y_{1,n_2} \\ &\vdots \\ &y_{m1}, y_{2m}, \ldots, y_{m,n_m} \end{aligned}$$

For all k, the following are satisfied:

1. y_{k1} has been sampled from the uniform distribution on G;
2. $y_{k,i+1} = f(y_{ki})$ for all $i < n_k$; and
3. $y_{ki} \in D$ if and only if $i = n_k$ (only the last element in each sequence is in D).

You may assume that n_k is approximately p/r for all k, that $\sum_k n_k \approx mp/r \approx \sqrt{p}$, and that m is not too large.

a) Show that if $y_{ki} = y_{lj}$ for some $k, l \leq m$, $i \leq n_k$, $j \leq n_l$, then $y_{k,n_k} = y_{l,n_l}$.

b) Describe an easy-to-compute function $h : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ such that if $z = x^a g^b$ and $h(a, b) = (c, d)$, then $f(z) = x^c g^d$.

Show that if you know a_{k1} and b_{k1} such that $y_{k1} = x^{a_{k1}} g^{b_{k1}}$, then you can compute a_{k,n_k} and b_{k,n_k} such that $y_{k,n_k} = x^{a_{k,n_k}} g^{b_{k,n_k}}$, using at most n_k evaluations of f and h.

c) You have been given $(y_{1,n_1}, a_{1,n_1}, b_{1,n_1}), (y_{2,n_2}, a_{2,n_2}, b_{2,n_2}), \ldots, (y_{m,n_m}, a_{m,n_m}, b_{m,n_m})$, where a_{k,n_k} and b_{k,n_k} are as in b) above. Suppose that $y_{k,n_k} = y_{l,n_l}$ for some (unknown) $k \neq l$, but $a_{k,n_k} \not\equiv a_{l,n_l} \pmod{p}$. Show how you can now easily compute $\log_g x$.

d) The above implies an algorithm for computing discrete logarithms. Describe, using plain English or Norwegian, how this algorithm works. Estimate how many steps is required (counting only group and arithmetic operations) in terms of m, r and p.

It is for some purposes reasonable to assume that f is "random-looking", which allows us to pretend that the y_{ki} are all sampled from the uniform distribution.

e) Assume that f is "random-looking". Derive a reasonable approximation for the probability that $y_{ki} = y_{lj}$ for some $k \neq l$, in terms of m, r and p.

Also give an informal argument for why it is unlikely that $a_{k,n_k} \equiv a_{l,n_l} \pmod{p}$ when $y_{ki} = y_{lj}$.

The following is not a problem, but an explanation of why the above is important for cryptography: Since each of the sequences can be computed independently, the workload for the above algorithm can be distributed among μ (independent, but communicating) processors, such that they compute discrete logarithms almost μ times faster than a single processor using ordinary Pollard ρ. We get nearly *linear speedup* for a *parallel algorithm.*

Parallel algorithms are important because today most of the increase in raw computing power comes from have more processors, not faster processors.