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 15 2018

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 You have intercepted the ciphertext AVVLHZF and you believe that the Shift cipher has been used.

Find a plausible decryption.

Problem 2 Consider the group $G = \mathbb{F}_{47}^*$ with generator $g = 5$.

a) Use Shank's Baby-step Giant-step algorithm to show that $\log_5 43 = 13$.

b) You get to know that

$$38^3 \cdot 43^5 = 5^{24}.$$

Use this to find $\log_5 38$.

Problem 3 Let $\mathbb{F}$ be the finite field with 29 elements. We embed the English alphabet in this field in the usual way: A $\mapsto 0$, B $\mapsto 1$, and so on.

Consider the one-time MAC $f : \mathbb{F}^2 \times \mathbb{F}^4 \to \mathbb{F}$ given by

$$f((k_1, k_2), (m_1, m_2, m_3, m_4)) = k_2 + \sum_{i=1}^{4} m_i k_1^i.$$

You intercept two transmissions (KELP, 22) and (HELP, 19). You suspect that the first message was mistyped and that the second message is a correction. You also suspect that the tags were created with the same key (k_1, k_2).

Find (k_1, k_2).

Problem 4 Let $n = 1363$.

a) Given the integer matrix

$$\begin{pmatrix} 2 & 1 & 1 & 0 & 1 \\ 3 & 3 & 0 & 0 & 0 \\ 2 & 0 & 2 & 1 & 0 \\ 3 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

Find two non-empty collections of matrix rows that sum to $\vec{0}$ modulo 2.

Let $\ell_1 = 2$, $\ell_2 = 3$, $\ell_3 = 5$, $\ell_4 = 7$ and $\ell_5 = 11$.

b) Find 5 relations on of the form

$$r^2 \bmod n = \prod_{j=1}^{5} \ell_j^{s_j}.$$

Use 275, 483, 640, 647 and 961 as r.

c) Use the relations you found above and the results from **a)** to find two pairs (r, t) such that

$$r^2 \equiv t^2 \pmod{n}.$$

Use one of these pairs to factor n.

Problem 5 Let p, q be distinct large primes, and let $n = pq$. Let $A, B \in \mathbb{Z}$. Note that as usual we will consider A, B to be elements of $\mathbb{F}_p$, $\mathbb{F}_q$ and $\mathbb{Z}_n$ as needed.

You may assume that the equation $Y^2 = X^3 + AX + B$ defines an elliptic curve over both $\mathbb{F}_p$ and $\mathbb{F}_q$. We denote these curves by E_p and E_q, respectively.

The Chinese remainder theorem gives us a ring isomorphism $\phi : \mathbb{F}_p \times \mathbb{F}_q \to \mathbb{Z}_n$. We can extend this to a ring isomorphism $\phi : \mathbb{F}_p^2 \times \mathbb{F}_q^2 \to \mathbb{Z}_n^2$ as

$$\phi((x_p, y_p), (x_q, y_q)) = (\phi(x_p, x_q), \phi(y_p, y_q)).$$

Define

$$\begin{aligned} U_p &= \{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + Ax + B\} \\ U_q &= \{(x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + Ax + B\} \\ U_n &= \{(x, y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + Ax + B\} \end{aligned}$$

Note that the first two are the sets of non-zero rational points on the elliptic curves E_p and E_q.

a) Show that $\phi(U_p \times U_q) = U_n$, that is, the image of the cartesian product $U_p \times U_q$ under ϕ is U_n.

We shall consider the formula for addition of elliptic curve points with distinct X-coordinates. Given (x_1, y_1) and (x_2, y_2), we define (x_3, y_3) using

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1} \qquad x_3 = \alpha^2 - x_1 - x_2 \qquad y_3 = \alpha(x_1 - x_3) - y_1 \tag{1}$$

When $x_2 - x_1$ is not invertible, (1) cannot be evaluated.

b) Let $P_p, Q_p \in U_p$ and $P_q, Q_q \in U_q$, and define $P = (x_1, y_1) = \phi(P_p, P_q)$ and $Q = (x_2, y_2) = \phi(Q_p, Q_q)$. Suppose $x_1 \neq x_2$.

Show that if (1) can be evaluated, then

$$(x_3, y_3) = \phi(P_p + Q_p, P_q + Q_q).$$

Also show that if (1) cannot be evaluated, then you can use x_1 and x_2 to factor n. In this case, what can you say about the X-coordinates of P_p, Q_p, P_q and Q_q?

c) Let $P_p \in U_p$ be a point on E_p with order a, and let $P_q \in U_p$ be a point on E_q with order b. Suppose b does not divide a. Define $Q_p = (a-1)P_p$ and $Q_q = (a-1)P_q$, and let

$$P = (x_1, y_1) = \phi(P_p, P_q) \qquad Q = (x_2, y_2) = \phi(Q_p, Q_q).$$

Show that $Q_p = -P_p$, that $x_1 \neq x_2$, but that (1) cannot be evaluated.

PS. The above results are interesting, because with just a few more ideas, the above ideas can be turned into a factoring algorithm with very useful properties.