Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam:
Kristian Gjøsteen 73 55 02 42

EXAM IN TMA4160 CRYPTOGRAPHY

English
Friday, December 21, 2012
Time: 0900-1300
Grades due: January 21, 2013
Any printed or hand-written material is allowed during the exam.
An approved, simple calculator is allowed.

All problems have equal weight. Show your work.

Problem 1 You have got hold of the cipher text

```
lqgbtnlyuolobbynvluxqgjnxclv
```

You think this is a message encrypted with the affine cipher. You also think baboons are somehow involved. Find the message.

Problem 2 Let $E : y^2 = x^3 + 48x + 12$ be an elliptic curve over the field $\mathbb{F}_{61}$.

a) Show that the polynomial $x^3 + 48x + 12$ has three zeros over $\mathbb{F}_{61}$. How many points of order 2 are there on the elliptic curve?

b) Show that the point $Q = (15, 52)$ lies on the curve and has order 5.

c) How many points are there on the curve? Is the group $E(\mathbb{F}_{61})$ cyclic?

Problem 3 Let q be a big prime power, let $\mathbb{F}_q$ be the field with q elements and let $x_1, x_2, \ldots, x_n$ be distinct, non-zero elements in $\mathbb{F}_q$.

a) Let $f(x) \in \mathbb{F}_q[x]$ have degree at most t, and let S be a subset of $\{1, 2, \ldots, n\}$. Suppose that $a_i = f(x_i)$ for $i \in S$. Prove that when $|S| > t$, then

$$f(x) = \sum_{i \in S} a_i e_i(x), \qquad \text{where } e_i(x) = \prod_{j \in S \setminus \{i\}} \frac{x - x_j}{x_i - x_j}.$$

b) Let $f(x) \in \mathbb{F}_q[x]$ have degree exactly t, and let S be a subset of $\{1, 2, \ldots, n\}$. Suppose you know t and $a_i = f(x_i)$ for $i \in S$, but otherwise you know nothing about $f(x)$.

Show that if $|S| \leq t$, then $f(0)$ can take any value as far as you know, but if $|S| > t$, then you can compute $f(0)$.

Let $q = 11$. Let $x_1 = 1$, $x_2 = 2$, $x_3 = 3$ and $x_4 = 4$.

c) Alice has a secret $k \in \mathbb{F}_{11}$. She has chosen a polynomial $f(x) \in \mathbb{F}_{11}[x]$ of degree at most 2 such that $f(0) = k$. The she has computed $a_i = f(x_i)$, $i = 1, 2, 3$, and given a_1 to Bob, a_2 to Carol and a_3 to David.

Given that $a_1 = 1$, $a_2 = 10$ and $a_3 = 1$, find k.

Alice has another secret $l \in \mathbb{F}_{11}$. She has chosen a polynomial $g(x) \in \mathbb{F}_{11}[x]$ of degree 1 such that $g(0) = l$. Then she has computed $b_i = g(x_i)$, $i = 1, 2, 3, 4$, and given b_1 to Bob, b_2 to Carol, b_3 to David and b_4 to Eve.

Bob says he got $b_1 = 9$, Carol says she got $b_2 = 4$, David says he got 0, and Eve says she got 7. Bob and Carol may be lying. What is l?

Problem 4 Let p and q be big primes such that $(p-1)/2$ and $(q-1)/2$ both are prime, and let $n = pq$. Let $g \in \mathbb{Z}_n$ have maximal order and Jacobi-symbol -1. We can now define a hash function $h : \mathbb{Z} \to \mathbb{Z}_n$ by

$$h(x) = g^x.$$

a) Show that a collision in the hash function can be used to factor n.

Let $n = 517$ and $g = 2$.

b) Compute $h(26)$ and $h(256)$ using a fast exponentiation algorithm.

c) Use the collision you discovered above to factor n.