Mathematical Cryptology, 2013

Dept. of EIT
Lund University

WEEK 3,

Reading instructions:

- Chapter 12, 13
- Chapter 2

There will be 4 hours of lectures covering the above.

Hand-in exercises:

1) Review exercises: 2.1-2.7, 12.1-12.6, 13.1-13.6

2) Standard exercises: 2.8-2.11, 12.7-12.10, 13.7

3) Programming exercise: 2.12 (maximum 5 hours)

Hand in no later than **February 26, 2013.**

Ch 2: Review exercises:
2.1 When is an elliptiv curve singular?
2.2 If two curves have the same j-invariant, what does it mean?
2.3 Describe the chord-tangent process and how it relates to the elliptic curve group law.
2.4 What is the trace of Frobenius, and what inequality does it satisfy?
2.5 When is an elliptic curve anomalous?
2.6 Why does one use projective coordinates?
2.7 By roughly what precentage does point reduce the amount of bandwith needed to transmit an elliptic curve point?

Ch 2: Standard exercises:
2.8 From the geometric definition of the group law derive the formulae in Lemma 2.2.
2.9 Let E denote the elliptic curve

$$Y^2 = X^3 + aX + b$$

over a field of characteristic greater that three. Describe the possible points of order three on the curve.
2.10 Show that the curves

$$E : Y^2 = X^3 + aX + b,$$
$$E : Y^2 = X^3 + ad^2X + bd^3,$$

defined over the field K are isomorphic over the algebraic closure of K. When are they isomorphic over K.
2.11 Write down an elliptic curve version of the ElGamal encryption scheme.

Ch 2: Programming exercise:
2.12 Implement a software library to perform elliptic curve addition and doubling over the integers modulo p. Implement ElGamal as in 2.11.

Ch 12: Review exercises:
12.1 What is the Fermat primality test and what is the main problem associated with it?
12.2 What is the main difference between a primality testing algorithm like Miller-Rabin, and a primality proving algorithm like ECPP?
12.3 What is meant by a smooth number and how can one use smooth numbers in factoring algorithms. 12.4 Describe the $P - 1$ factoring algorithm.
12.5 Why does finding two numbers x and y such that $x^2 = y^2 \pmod N$ allow us to factor N with probability at least $1/2$?
12.6 What is meant by a sieve and why are they used in modern factoring algorithms?

Ch 11: Standard exercises:
12.7 Show that if a composite number n passes the Fermat test to base a, but fails the Miller-Rabin test for the same base, then we can factor n.
The next three questions discuss Pollard's Rho method to factoring. Define the sequence

$$x_0 = 2, x_{i+1} = x_i^2 + 1 \pmod{N}.$$

12.8 Show that if we find two values of the sequence with $x_i = x_j \pmod{p}$ then we can factor N with high probability by computing $gcd(x_i - x_j, N)$.
12.9 Argue that we must eventually find two indices $i \neq j$ such that $x_i = x_j \pmod{p}$.
12.10 Show how to find two such indices using a small amount of storage.

Ch 13: Review exercises:
13.1 What cryptographic conclusion do we draw from the Pohlig-Hellman algorithm?
13.2 How does the Baby-Step/Giant-Step method work?
13.3 What are the practical problems associated with the Baby-Step/Giant-Step method and how are these overcome when using Pollard's Rho method?
13.4 What cryptographic conclusions can we draw from the existence of the Pollard's Rho method?
13.5 What cryptographic conclusions can we draw from the existence of index-calculus algorithms in finite fields?
13.6 Discuss the statement that elliptic curves offer higher strength per bit than finite fields.

Ch 13: Standard exercises:
13.7 Use a calculator to compute x such that

$$3^x = 5 \pmod{p},$$

where $p - 1 = 2 \cdot 3 \cdot 101 \cdot 103 \cdot 107^2$.