”Obligatorisk - I - 2013”
INF 240 - Basic Codes
(Counts 10 % towards final grade of INF 240)
Deadline: Wednesday, October 16, 2013 at 13:00

Remember always to justify your answers. You must hand in your solution individually no later than **October 16, by 13.00!** You can submit the solutions electronically via “MiSide”. Alternatively you can hand in a hard copy of the solutions to the group leader Mohsen Toorani. Question can be addressed to group leader Mohsen.Toorani@ii.uib.no

Problem 1 (15%)

a) What is the theorem of Fermat? Explain how we can apply this theorem to show that n=55 is a composite number.

b) Use the Miller-Rabin test to show that n=341 is a composite number.

c) Explain how to use a relation of the type

$$x^2 \equiv y^2 \pmod{n}$$

to possibly factor a number n? Find a relation that you can use to factor n=341 and give the factorization.

Problem 2 (20%)

a) Let p be a prime and c a nonzero element (mod p) and consider the following equation

$$x^2 \equiv c \pmod{p}.$$

Explain why the equation only has a solution when $c^{(p-1)/2} = 1 \pmod{p}$.

b) Explain how to find the solutions in the special case when $p \equiv 3 \pmod{4}$? Find using this method all the solutions of each of the equations

$$x^2 \equiv 5 \pmod{11} \text{ and } x^2 \equiv 12 \pmod{23}.$$

c) Explain the Chinese remainder Theorem? Use this theorem to find all the solutions of

$$x^2 \equiv 104 \pmod{253}.$$

d) Find a value of c such that $x^2 \equiv c \pmod{253}$ has no solution.

Problem 3 (10%)

Construct a public key cryptosystem, RSA, using the two secret primes p=19 and q=23.

a) Let the public exponent be e=7? Use the Extended Euclidean algorithm to find the secret key d? Explain how you will encrypt the message m=5.

b) Select a different RSA key for signing messages using the same module and sign the message m=2. Explain also how the receiver verifies the signature.

Problem 4 (20%)

Given the discrete logarithm problem

$$3^x = 5 \pmod{29}.$$

a) Solve this problem by using the Pohlig-Hellman algorithm.

b) Solve the same problem using the index-calculus method.

c) Alice and Bob want to use the Diffie-Hellman key exchange. Show in detail how it works on an example (mod 29).

Problem 5 (20%)

a) In the ElGamal signature scheme, let $p = 29$ be a prime number and $\alpha = 3$ a primitive root (mod p).

- Choose a private key and compute your public key.
- Use your key to sign the message $m = 11$.
- Go through the verification procedure to verify your signature.

b) Describe the ElGamal cryptosystem. Let $p=29$ and select a public and secret key and give an example of encryption and decryption of the message $m=7$.

Problem 6 (15%)

a) What is a (t,w)-threshold scheme? Describe Shamir's threshold scheme.

b) In Shamir's threshold scheme the secret is hidden as the constant term in a second-degree polynomial (mod 29). The three participants Alice, Bob and Charlie want to reconstruct the secret. Their shares are (2, 9), (3, 13) and (4, 15). What is the secret?

c) Suppose you are the dealer in a (4,6) Shamir threshold scheme (mod 29). Distribute the shares to all the users assuming the shared secret is M=17.