

# Homework 3 of CS549 Cryptography and Network Security

ASSIGNED: OCT 23RD, 2010

DUE DATE: 5PM, NOV 23, 2010.

EXTENSION DATE (WITH 10% DEDUCTION ON GRADING): 5PM, NOV 30, 2010

FALL 2010, CS DEPARTMENT, IIT

There are 4 questions in HW3. Please type your answer. You have to do the following (all)

- print it and give TA the hardcopy (for on-campus students),
- upload the electronic file in PDF or Postscript format to blackboard at IIT. Put your name on your solution and name your file as "lastname-HW3.pdf", where lastname is your last name. Do Not forget to write your name also in your solution.

Notice: We do not accept MS WORD file and we prefer electronic submission.

1. (25 points) Suppose Bob uses the DSA signature scheme with prime numbers  $q = 101$ ,  $p = 7879$ , and the primitive root  $g = 170$ . And Bob selects his private key as  $x = 75$ , and publishes his public key as  $y = g^x \pmod p = 4567$ .
  - (a) Determine Bob's signature on a message with hashed value  $h(M) = 5001$  when using a random number  $k = 49$ .
  - (b) Assume Alice wants to verify this signature, show the procedure Alice used to verify the signature.
2. (25 points) Elgamal signature scheme works as follows. Let  $p$  be a large prime number and  $g \in Z_p^*$  be a primitive element. Suppose Bob is using the ElGamal Signature Scheme, Bob picks a random integer  $0 < a < p$  and publishes  $\beta = g^a \pmod p$ , but keep  $a$  secret. Bob signs a message  $m$  as follows
  1. Bob picks a random integer  $k < p$ , and computes  $(\gamma, \delta)$ , where  $\gamma = g^k \pmod p$ ,
  2. Bob computes the hash value, say  $x = h(m)$ , of the message  $m$ , and computes

$$\delta = k^{-1}(x - a\gamma) \pmod{(p-1)}.$$

The pair  $(\gamma, \delta)$  is the signature of the message  $m$ .

When Alice receives the signature  $(\gamma, \delta)$  for the message  $m$ , Alice also computes the hash value, say  $x = h(m)$ , of the message  $m$ . Alice then verifies the signature by checking if

$$\beta^\gamma \gamma^\delta = g^x \pmod p.$$

- (a) Prove that Alice accepts the signature if the signature is indeed created by Bob.
  - (b) Suppose Bob signs two messages  $x_1$  and  $x_2$  with signatures  $(\gamma, \delta_1)$  and  $(\gamma, \delta_2)$ , respectively. (The same value for  $\gamma$  occurs in both signatures.) Suppose also that  $\gcd(\delta_1 - \delta_2, p - 1) = 1$ . Describe how the signature scheme can then be broken. In other words, how to find number  $a$ ?
3. (25 points) Prove that having an algorithm to solve the Diffie-Hellman problem in polynomial time is equivalent of having an algorithm breaking the ElGamal Encryption Cryptosystem. Notice that the two problems are defined as follows:
    - **Diffie-Hellman Problem:** We are given four positive integers  $p$ ,  $\alpha$ ,  $\beta_1$ , and  $\beta_2$ , where  $p$  is a prime number,  $\alpha$  is a primitive root  $\pmod p$ ,  $\beta_1 = \alpha^{x_1} \pmod p$ , and  $\beta_2 = \alpha^{x_2} \pmod p$ . Here  $x_1$  and  $x_2$  are some integers we do not know. We want to find the value  $\alpha^{x_1 \cdot x_2} \pmod p$  using the given four positive integers  $p$ ,  $\alpha$ ,  $\beta_1$ , and  $\beta_2$ .
    - **ElGamal Encryption Cryptosystem:** We are given five positive integers  $p$ ,  $\alpha$ ,  $\beta$ ,  $y_1$ , and  $y_2$ , where  $p$  is a prime number,  $\alpha$  is a primitive root  $\pmod p$ ,  $\beta = \alpha^x \pmod p$ ,  $y_1 = \alpha^k \pmod p$ , and  $y_2 = m \cdot \beta^k \pmod p$ . Here  $x$ ,  $k$ , and  $m$  are some positive integers we do not know. We want to find the value  $m$  using the given five positive integers  $p$ ,  $\alpha$ ,  $\beta$ ,  $y_1$ , and  $y_2$ .

4. (25 points) Assume that you are given an integer  $n$ , which is the product of two large prime numbers. You are also given two integers  $e$  and  $d$  such that  $e \cdot d = 1 \pmod{\phi(n)}$ . Notice that you do NOT know the value of  $\phi(n)$ . Implement a program to factorize  $n$  with high probability, using the information  $n$ ,  $e$  and  $d$ . Your code should be able to deal with large integers as in HW1.
- You have to submit the code of your program.