CSci 4554 Assignment 9

Due Friday, April 11 in class

Problem 1 (4 points). Suppose Alice's RSA public key is $N = 77, e = 3$. Mallory (a malicious attacker) happens to know that decryption of a ciphertext $c_1 = 13$ is $m_1 = 5$. Can Mallory send Alice an encryption of a message $m_2 = 25$ without factoring N? If yes, please give the encryption of the message (show your computation). If not, please explain, why.

Problem 2 (16 points). Given $p = 7, q = 19$, and $b = 3$ for Rabin's encryption:

1. compute encryption of $m = 5$
2. check your result by decryption (also show all your computations). Hint: it is easy to find solutions x_p and x_q since N is a Blum integer. After you find the two solutions in each group, for each pair of these solutions you need to solve a system of equations:

   $$x \equiv x_p (\text{mod } p)$$
   $$x \equiv x_q (\text{mod } q)$$

   You may use the Chinese Remainder theorem or just check all possibilities. Please find all four solutions.
3. Using any pair solutions found in part 2, show how N can be factored. Just find one of its prime factors.

Problem 3 (6 points). Given a prime number $p = 73$, a generator $g = 3$, a random $x = 8$ and a random $k = 11$, compute y for ElGamal encryption and use the parameters to encrypt the message $m = 10$ and to decrypt the result to check. Show all your computations.

Problem 4 (6 points). Suppose that the RSA public key is $(77, 3)$. Given the ciphertext $c = 2$, what ciphertext messages need to be given to a parity oracle in order to find out the plaintext message? You don't need to compute the actual messages, just give their formulas. How many messages do you need to narrow down the plaintext to just one value?

Problem 5, Extra credit (up to 10 points; may be done in collaboration). Consider the Coin Flipping Over the Phone protocol. Discuss a possibility for a malicious attacker Mallory to exploit the protocol by providing a "random number service" to Alice. It is assumed that Mallory can observe the results of the coin flip (what the bets were and who "won"). Mallory's goal is to decrypt an earlier message m encrypted with Alice's public key.