Homework 2

CSE 594: Modern Cryptography
Stony Brook University, Spring 2017

Due: Monday, April 24, 2017 by 11:59 PM ET.

Problem 1. This problem is an example run for the RSA function. Suppose that $p = 3$ and $q = 5$ so that the RSA modulus is $N = pq = 15$. For this value of N:

1.1 (3 points) What is the value of $\phi(N)$?

1.2 (3 points) Write down all elements of the set $\mathbb{Z}_N^*$.

1.3 (3 points) In the RSA system, you want to pick numbers e and d such that (N, e) is public key and (N, d) is the secret key. What is the relationship between e, d, and N?

1.4 (3 points) For $N = 15$ above, give an example value of e and the corresponding value of d for the RSA system. (In particular, e, d, N should satisfy the relation in 1.3).

1.5 (3 points) Every element $x \in \mathbb{Z}_{15}^*$ has a unique inverse. Write down all pairs (x, y) such that x and y are mutual inverses modulo 15 i.e. $x \cdot y = 1 \mod 15$.

Problem 2. This problem has three parts. Each sub-problem builds upon the one before it.

(2.1) [2 points] Let a be a natural number. Prove that 3 divides one of the numbers in the sequence $a, a + 1, a + 2$.

(2.2) [5 points] Let $p > 3$ be a prime number. Prove that 6 divides either $p - 1$ or $p + 1$.

(2.3) [3 points] Let $p > 3$ be a prime number. Prove that 12 divides $p^2 - 1$.

Problem 3. (10 points) Suppose that Alice and Bob have never met. Alice wants to send a private letter to Bob through a common friend Eve. Eve cannot be trusted with not reading the contents of the letter. Design a protocol using the physical items given below so that Alice can send the letter to Bob using Eve without giving Eve the ability to open and read the letter:

(a) Alice has a physical padlock A and its key K_A
(b) Bob also has a physical padlock B and its key K_B
(c) Alice also has a non-transparent metal box M which can be locked with multiple locks.
(c) Only Alice can open A, and only Bob can open B.
(d) If M has any lock on it, nobody can see what is inside the box.

Problem 4. Recall the interactive proof for the *Graph Non-Isomorphism* problem from the class. In this proof, the statement $x := (G_0, G_1)$ is a pair of graphs which are not isomorphic. The honest verifier V, picks one of the two graphs at random, and permutes it randomly to get a new graph H. It sends H to the prover P. The prover then sends back 0 if H is isomorphic to G_0 and 1 if H is isomorphic G_1.

(4.1) [8 points] Prove that this protocol is **honest verifier zero-knowledge**. I.e., (a) construct a PPT simulator algorithm S, which on input x, simulates the distribution obtained by the (honest) verifier algorithm V in the real execution; and (b) prove that the output of the simulator is distributed identically to that of V's view in a random execution of the protocol.

(4.2) [7 points] Prove that the protocol is **not** zero-knowledge against a *cheating verifier* who may not follow the protocol. Show an example verifier who learns extra information by deviating from the protocol. (Note: assume that if the verifier sends invalid messages, such as messages longer than the protocol has specified, or any other deviation detected by the prover, the prover responds by sending a special "abort" symbol denoted by $\perp$).