HW 8 CMSC 456. Morally DUE Nov 16

1. (25 points) Alice and Bob do DH with $p = 47$ and $g = 2$.

   (a) (6 points) Alice picks $a = 4$ and Bob picks $b = 5$. What is the shared secret?

   (b) (6 points) Alice picks $a = 5$ and Bob picks $b = 4$. What is the shared secret?

   (c) (13 points) You should have gotten THE SAME ANSWER for the last two parts.

   PROVE OR DISPROVE THE FOLLOWING:

   Let Alice and Bob do DH with prime p and Generator g. Let s_{xy} be the message if Alice picks $a = x$ and Bob picks $b = y$. Then $s_{xy} = s_{yx}$.

2. (25 points) Alice and Bob use the El Gammal encryption scheme with prime p and generator g (which Eve knows). The first day of the month they establish a shared secret key which they use for that month.

   (a) (10 points) On November 2 Eve finds out that, on Nov 1, plaintext m codes into ciphertext c. Show how Eve can use this to find the secret key and hence be able to decode messages until December 1.

   (b) (15 points) How can Alice and Bob modify their scheme so that Eve cannot use what she did in the answer to part a?

3. (25 points BASED ON the Guest Lecture on Cheating in Bridge) Alice and Bob are bridge partners. And they cheat! Here is their scheme:

   - If the first card is placed horizontally then the person placing it has 0 or 1 Ace.
   - If the first card is placed vertically then the person placing it has 2 or 3 or 4 Aces.

   In this problem we will both (1) help Alice and Bob and (2) help the bridge community.

   (a) (15 points) Alice and Bob will be playing 20 games and are worried that their cheating may be discovered. Show how they can use a 1-time pad to make their cheating harder to discover.

   (b) (10 points) Give advice to the Bridge Association to PREVENT this kind of cheating. (You cannot recommend banning-for-life or the death penalty or any other kind of penalty for cheating—we want to make it hard to cheat in the first place.)

4. (25 points) This is a programming assignment where you will code up RSA. The same programming languages and file naming conventions from previous homeworks apply.

   You will need 3 subroutines.

   ALICE-KEYGEN takes integer L and performs the following steps:

   (a) Generate two L-bit primes p, q for $L < 5000$.

   (b) Compute $R = (p-1)(q-1)$, $N = pq$.

   (c) Generate two numbers e, d such that $e \in \{\frac{R}{3}, \frac{2R}{3}\}$, e is rel prime to R, and $ed \equiv 1 \pmod{R}$.

   (d) Print on a single line your p, q, separated by spaces, no commas.

   (e) On the next line, print N, d the same way. (This is your PRIVATE key.)

   (f) On the next line, print N, e . (Note that Bob and Eve will only see (N, e). This is your PUBLIC key.)

   BOB-ENCRYPT will take a public key (N, e) and a integer m representing the plaintext, where $m < \lfloor N/1000 \rfloor$.

   (a) Pad m with a random 3-digit integer $0 \leq r < 1000$ by
   $m' \leftarrow 1000m + r \pmod{N}$.

   (b) Print, on a new line, the ciphertext.

   ALICE-DECRYPT will take a private key (N, d) and a ciphertext c.

   (a) Decrypt RSA to get a padded plaintext. Reverse the padding you did in BOB-ENCRYPT to get the unpadded plaintext.

   (b) Print, on a new line, the plaintext.

Combine these into a single program. Your program will recieve as input 3 integers a,b,c, each on their own line.

On the next a lines you will recieve one integer L on each line, you should run ALICE-KEYGEN a times, once on each line.

On the next b lines you will recieve 3 integers N, e, m separated by spaces, one triplet on each line. You should run BOB-ENCRYPT on each set of parameters.

On the next b lines you will recieve 3 integers N, d, c separated by spaces on each line. You should run ALICE-DECRYPT on each set of parameters.

In total you will receive $3 + a + b + c$ lines. You will print $3a + b + c$ lines (3 lines per keygen, 1 line per encrypt/decrypt.)

As stated earlier, each line you print should either be just an integer, or two integers separated by a space.

Just like previous assignments, print and read from stdout/stdin.