Problem Set #4

Due Thursday, October 20 @ 11:59 pm

1. Use the square-and-multiply algorithm to compute the following values by hand.

   (a) $5^{21} \mod 9$

   (b) $4^{129} \mod 7$

2. Suppose you are trying to create your own RSA credentials and you have picked primes $p = 401$ and $q = 443$ so that $n = 177\,643$.

   (a) Use the Euclidean Algorithm to show that $e = 17$ is an invalid choice.
   You can use a calculator for arithmetic computations, but show all the steps of the algorithm.

   (b) Use the Euclidean Algorithm to show that $e = 11$ is a valid choice, and use the Extended Euclidean Algorithm to find $k_{pr} = d$.
   You can use a calculator for arithmetic computations, but show all the steps of the algorithm.

   (c) What is public key? What is your private key?

   (d) If Alice wants to encrypt a message to you, how many multiplications are required using the square and multiply algorithm?
   How many multiplications will you need to perform to decrypt the message using the square and multiply algorithm?

3. Suppose that your RSA credentials are $kyou_{pub} = (1\,613\,137, 33)$ and $kyou_{pr} = 829\,701$.
   Notice that $1\,613\,137 = 1223 \cdot 1319$ and that 1223 and 1319 are prime.

   Also suppose that Alice's public RSA credentials are $kal_{pub} = (1\,199\,053, 17)$.

   You may use Mathematica or WolframAlpha for these computations.

   (a) Verify that your credentials are valid.

   (b) Alice sends you messages that are first encrypted using RSA and then signed using a RSA digital signature.
   Determine if the following signatures are valid, and if so, decrypt the message.

      i. $(x, s) = (125\,923, 163\,014)$
      ii. $(x, s) = (84\,402, 357\,255)$

   (c) For your choice of $n = 1\,613\,137$, how many valid choices of e are there?
   This demonstrates that the size of the key space may be quite different from n.

4. For this problem, it will be useful to review the Mathematica notebook from the September 29th in-class work.

   You should also use the sites `http://www.cryptogrium.com/aes-encryption-online-ecb.html` and `https://dencode.com/en/string/hex` as we did in class.

   The setup for this problem is that Alice sends you two messages:

   y_1 is encrypted using your RSA public key.
   After you decrypt y_1, you will get an AES-128 key k.

   y_2 is encrypted using the AES-128 key k.
   The plaintext you obtain after decrypting y_2 is encoded using UTF-16.

Your public RSA key is $k_{pub} = (n, e)$ where $n = p \cdot q$ and $e = 2^{16} + 1$.

The values for y_1, y_2, p and q are given the Mathematica notebook on the course webpage.

(a) What is your RSA private key d?

(b) What is the AES key k that Alice used to encrypt y_2?

(c) What is the plaintext you receive after decrypting y_2 using AES?

(d) The plaintext is a string encoded using UTF-16. What is the string? Any thoughts?

5. This problem involves the *Playfair cipher* with key k ="JAMIETARTT".

   You will need to do some research to understand how the cipher works.
   In this implementation, we are replacing 'J' by 'I'.

   You receive the encrypted message

   ```
   OV KZ HT FB RI AS EP MZ AN DY IU UH PL PQ VA AN AN ID EB RV UG
   ```

   Decrypt the message. Who said this?

   Be sure to explain how you decrypted so that someone else can follow, and recreate, your process.