University of the West Indies, Cave Hill Campus
Department of Computer Science, Mathematics and Physics
COMP3230: Network and Computer Security
Dr. Dwaine Clarke, dwaine.clarke@cavehill.uwi.edu
Semester 2, 2017/2018
Cryptography Exercises

*Please record your answers in a **SINGLE TEXT** file. Please include your name, ID number, email address, and lab instructor name at the top of the file. Please consult your lab instructor as to how your lab should be submitted and the deadline for the lab. Please ensure that you keep a copy of your lab submission.*

References

- http://www.asciitable.com/
- http://en.wikipedia.org/wiki/Modular_exponentiation

1. (10 marks) Alice and Bob would like to communicate using the one-time pad scheme to encrypt their messages. Alice is concerned about the inconvenience of establishing a shared key with Bob. The following protocol occurs to her:

   When Alice is ready to send her message m, she randomly selects r_1, and sends Bob $s_1 = m \oplus r_1$. Bob then randomly selects r_2 and sends Alice $s_2 = s_1 \oplus r_2$. Next, Alice computes $s_3 = s_2 \oplus r_1$ and sends it to Bob. Bob may then compute the message as $s_3 \oplus r_2 = m$.

   This idea appears similar to the one-time pad scheme, but does not require prior distribution of a shared key.

   Is Alice's protocol secure against a passive adversary? If yes, describe why you believe it is secure. If no, give a passive attack that breaks the protocol.

2. (a) Consider an RSA crytosystem with (e, n) as the public key and (d, n) as the private key. Suppose that the keys are generated using the primes $p = 101$, $q = 449$.
      i. (2 marks) What is $\phi(n)$?
      ii. (6 marks) Suppose that $e = 17$. What are the public key (e, n) and private key (d, n)?

   (b) (12 marks) Consider the following encoding for encryption in an RSA cryptosystem:
      i. Take the ASCII decimal representation of each character (including spaces), using 2 digits to represent each number; for example, $D \rightarrow 68$.
      (ref: http://www.asciitable.com/)
      ii. Group characters in pairs. If there are an odd number of characters, add an extra space at the end. Thus, each pair of characters is represented as 4 digit number.
      iii. Let α be a single 4 digit number representing a pair of characters.
      Calculate $\alpha^e \bmod n$ to encrypt the pair.
      Represent each encrypted pair using 6 digits, for example, $10000 \rightarrow 010000$.
      iv. Concatenate the resulting encrypted pairs to form the encrypted message.

What is the decrypted message of the following string if the message was encrypted with the public key in Step 2(a)ii using the encoding just described:

```
033579017159010704004008
035066040870031072040179
044616036491029179020540
003864023497022980009092
004008
```

3. Suppose Alice and Bob would like to establish a shared secret key using the Diffie-Hellman key exchange protocol. They agree to use prime number $p = 19$ with generator $g = 3$. Alice chooses her private key $a = 15$. Bob chooses his private key $b = 16$.

   (a) (3 marks) What is Alice's public key (p, g, A)?

   (b) (3 marks) What is Bob's public key (p, g, B)?

   (c) (4 marks) What is the shared secret key that Alice and Bob establish (assume each user obtains an authentic copy of the other user's public key.)

Total: 40 marks