Hassan Hage Hassan
CMSI 662 – HW 4 Exercises

1. What is the difference between a code and a cipher?
   - A code is a method of changing a message or text by replacing each word with another word whose meaning is different than the original word.
   - Ciphers use algorithms to transform text-based data into a seemingly random string of characters.

2. In the course notes, we demonstrated an Auto-Key Vigenère cipher using the plaintext following the keyphrase. Repeat the example encryption in the notes by following the keyphrase with the *ciphertext*.
   - From the course notes:

```
Keyphrase:      QUARK
Plaintext:      TAKEACOPYOFYOURPOLICYTONORMAWILCOXONTHETHIRDFLOOR
Key:            QUARKTAKEACOPYOFYOURPOLICYTONORMAWILCOXONTHETHIRD
Ciphertext:     JUKVKVOZCOHMDSFUMZCTNHZVQPFOJWCOOTWYVVBHUBYHYSWFU
```

   - Encryption with the keyphrase followed by the ciphertext above:

```
Keyphrase:      QUARK
Plaintext:      TAKEACOPYOFYOURPOLICYTONORMAWILCOXONTHETHIRDFLOOR
Key:            QUARKJUKVKVOZCOHMDSFUMZCTNHZVQPFOJWCOOTWYVVBHUBYH
Ciphertext:     JUKVKLIZTYAMNWFWAOAHSFNPHETZRYAHCGKPHVXPFDMEMFPMY
```

3. Write a Node.js command line application that takes in four command line arguments. The first is either `-e` or `-d` (for encrypt and decrypt, respectively). The second is either a message to encrypt or a ciphertext to decrypt. The third is the key. The fourth is an initialization vector. If encrypting, the program assumes the string argument is a utf-8 encoded string and outputs the AES256-CBC encoding of the input, as a hexadecimal string. If decrypting, the string argument is assumed to be a hexadecimal representation of a byte sequence, and the output should be the decrypted string.
   - GitHub Link to aes256cbc.mjs file

4. Simulate RSA-512 encryption and decryption (WITH THE USUAL DISCLAIMERS THAT THIS SIZE IS TOO SMALL AND IS ONLY USED FOR EDUCATIONAL PURPOSES AND DO NOT DO THIS STUFF YOURSELF) where p=10039208923731615832357098500868790785326998100564056903945758400791312964008 1 and q=90392089237316158323570985008687907853269981005640569039457584007913129640041 and e=65537. Use a 60-byte block size.
   a. What is N?

      $$N = p * q \Rightarrow$$

      - 907465068906008924819930740099105546809886210332140338904744327029102958514943741289978823030747746151835429180153466090494042443181096594841193141608332 1
   b. What is d?

      $$d = \text{modular inverse of } e \text{ relative to } (p-1)(q-1) \Rightarrow$$

      - 344060485407884244990244274684263463801090262818454051010956971451533489680315669363057815101204131681549469289738402961975530391324982830754051026040627 3

c. Given the message "Scaramouche, Scaramouche, will you do the Fandango? 💃", what is the resulting ciphertext? Show your answer as a byte sequence written in hex.
   - Message ASCII to Hex
     53636172616d6f756368652c2053636172616d6f756368652c2077696c6c2079
     6f7520646f207468652046616e64616e676f3f20f09f9283f09f8fbd
   - Hex to Decimal:
     10168633209541050849814010853602863428045530534764754206969156 0
     01588546537764111850907612301243212079604529047969231878421680 4
     1473417435720683453
   - Decimal encrypted with RSA512:
     11032240857587152234440648069952176593031456774545029468240418 0
     00863112809234657168138849814196807203518797601503545249808063 3
     18161403531226003541429172 27
   - Encrypted decimal to **Encrypted Hex**:
     1510726EC4756E595C4B5CE1F3A1974798A34369EB8F43F7462D4093F3
     0973994849A5B63D6B28E33C2200BFEA7F7005BD7642E74302832B739
     BE60D966A926B

d. Decrypt the ciphertext. What did you get back? Yes, you should get back the original message. But be honest. Show your work, as they say.
   - I got back the original message: “Scaramouche, Scaramouche, will you do the Fandango? 💃” I used python to simulate this encryption/decryption exercise. Here are links to my work GitHub Link Repl Link

5. What is the sha384 digest of the phrase "Російський військовий корабель, іди нахуй"?
   - c358ff602ada470dfb85fad41bd1fe277d587ace98d09c7eb70f48ef1048b76a2ec1103f6
     7d54871cd18046cbd6fe816