Name: Zak Rowland
Embedded Security
CST 466
Assignment 5: AES Encryption

1. Is AES a symmetric key encryption/decryption algorithm?

    No, there are four steps in each round of processing and the order of these steps is different for encryption and decryption.

2. Is the AES algorithm a symmetric function?

    No, the algorithm for decryption is substantially different than the algorithm for encryption. They are similar but the implementations are not the same and the order of the steps differs.

3. What are the supported key sizes in AES?

    There are three key sizes for AES: 128-bit, 192-bit, and 256-bit.

4. What is the difference between ECB mode and CBC mode? When should ECB mode be used? When should CBC mode be used?

    ECB stands for electronic code book and is used where simplicity and speed is needed over security. The security is weak because the plaintext is taken 128 bits at a time and encrypted with each key, which also means it can work in parallel. Encrypting with ECB leaves residual information behind.

    CBC stands for cipher block chaining, and this mode is more secure than ECB. A random initialization vector is given to the first block for use in the encryption algorithm, and every consecutive block uses the cipher text from the previous block as the initialization vector. The original initialization vector is needed for decryption.

Name: Zak Rowland
Embedded Security
CST 466
Assignment 5: AES Encryption

5. Given that there is AES 256, what is the practical reason why AES 128 is used? Isn't AES 256 stronger?

   Although AES 256 is stronger, AES 128 has a worst-case time complexity for a brute-force attack of 2^{128}. This means that computers will not have the processing power required to brute force the encryption for many years to come. AES 256 should be used where security is much more important than speed.

6. What is the purpose of the substitution box in AES?

   The goal of the substitution is to reduce the correlation between the input and output bits at the byte level.

7. How many key combinations are there in AES 128?

   2^{128}

8. How many key combinations are there in AES 256?

   2^{256}

9. What is confusion? Why is it important?

   Confusion means that the relationship between the encryption key and the ciphertext must be as complex as possible. Confusion is important because it makes reverse engineering the encryption algorithm and brute force attacks much harder.

10. What is diffusion? Why is it important?

    Diffusion means that each plaintext bit must affect as many ciphertext bits as possible. Diffusion is important because it makes statistical attacks much harder, and extra bits in the ciphertext makes brute force attacks take longer.

Name: Zak Rowland
Embedded Security
CST 466
Assignment 5: AES Encryption

11. The second step in each round permutes the bytes in each row of the state array. What is the permutation formula that is used? (From A. Kak, Lecture 8.)

    The second step is shift rows. Using a state array format, the first row is not shifted at all. The second row is circularly shifted to the left by one byte. The third row is circularly shifted to the left by two bytes. The last row is circularly shifted left by three bytes.

12. Describe the mix columns transformation that constitutes the third step in each round of AES. (From A. Kak, Lecture 8.)

    The mix columns step replaces each byte of a column by a function of all the bytes in the same column. Each byte in a column is replaced with two times that byte, plus three times the next byte, plus the byte that comes next, plus the byte that follows (in the same column.)

13. Let's now talk about the Key Expansion Algorithm of AES. This algorithm starts with how many words of the key matrix and expands that into how many words? (From A. Kak, Lecture 8.)

    The algorithm begins with four words and expands them into forty-four words.

14. Name one advantage of AES over DES and/or Triple DES.

    One advantage of AES over DES is that AES uses key-alternating block ciphers. This means each round first applies a diffusion-achieving transformation operation to the entire incoming block whereas in DES one-half of the block passes through unchanged. This extra diffusion increases security.

Name: Zak Rowland
Embedded Security
CST 466
Assignment 5: AES Encryption

15. Python has support for AES using pycrypto. Encrypt the message

    Iaintgoingdownforthis.Youainttakinmealive

    Use the following AES 128 key in CBC mode.

    2B7E1516 28AED2A6 ABF71588 09CF4F3C

    If on linux use pip install pycrypto
    If on windows use pip install pycryptodome

    https://pycryptodome.readthedocs.io/en/latest/

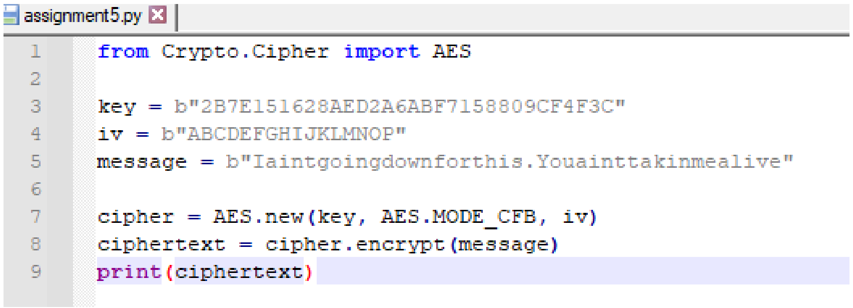
    http://python-docs.readthedocs.io/en/latest/scenarios/crypto.html

    https://pypi.python.org/pypi/pycrypto

    Provide the encrypted output, your initialization vector, and a screenshot of how you used pycrypto. Recall you'll need to import pycrypto before using it. Note that you might need to prefix python strings with b to get the underlying C code to accept the value. Also note that CBC mode does not automatically pad. Try CFB.

Initialization vector = ABCDEFGHIJKLMNOP
Encrypted output =

```
b'?Y\xb2Nd~\x11\xd4&\x9d\xe3eI\xa9\x03"\xa6\xb6Az\xca}
\xb5\x99\xc3\xab\x1a\x14\x1d,\xa6\x92I;d\xb9\xb9\r\x0c
\xd9_'
```



```python
from Crypto.Cipher import AES

key = b"2B7E151628AED2A6ABF7158809CF4F3C"
iv = b"ABCDEFGHIJKLMNOP"
message = b"Iaintgoingdownforthis.Youainttakinmealive"

cipher = AES.new(key, AES.MODE_CFB, iv)
ciphertext = cipher.encrypt(message)
print(ciphertext)
```

Name: Zak Rowland
Embedded Security
CST 466
Assignment 5: AES Encryption

16. Why should you use the built-in cryptofunctions when possible instead of writing your own?

    The built-in cryptofunctions have many experts developing and testing them tirelessly, making them the most secure and efficient to use compared to writing your own (unless you are one of those experts.)