Lab Assignment 2: Cryptography

Course Code:	CYB301
Course Name:	Security, Defense, and Response
Time:	90+ minutes in class with additional time on Day 3 if needed
Student name:	Saiprasad Raman
Student ID:	23074624

Materials and Resources

Textbooks:	N/A
Software:	N/A
Websites:	**Activity 1:** • Lookup Tables • NIST Advanced Encryption Standards • Encode-decode.com **Activity 3:** • File Format Info
Videos:	**Activity 2:** • Public Key Cryptography: RSA Encryption Algorithm
Other:	**N/A**

Assignment Description

Cryptography is the practice and science of secure communication and coding techniques. Cryptography provides confidentiality, so only the sender and intended recipient of a message understand it. Confidentiality of files at rest means that only users with the proper authorization can see the files in their intended format. Those without proper authorization can still see the files on the hard drive and even open the files in a hex editor (the files are not hidden), but they will not be able to open the file in the program it was designed to be opened in and see it as anything meaningful.

Assignment Steps

Activity 1: Symmetric Key Encryption and AES

Symmetric key encryption, also known as symmetric key cryptography and private key cryptography, is used for ensuring the confidentiality of messages and files. In symmetric key encryption, the same key is used both to encrypt and decrypt.

1. Your friend just sent you the following 9 bytes:

   ```
   00111111   00001001   00001111   00011001    00011110
   00000101   00011000   00010101   01000111
   ```

   They told you the bytes are ASCII/Unicode characters, encrypted with the XOR cipher, using a single-byte key of 01101100 which repeats for each plaintext/ciphertext byte.
   - OR: If both binary inputs are 0 then the result is 0, otherwise 1.
   - XOR: If both binary inputs are the same, the result is 0, otherwise 1.

2. Use the XOR cipher to decrypt the plaintext.
   a) What is the decrypted binary?

Ans.

```
 00111111   00001001   00001111   00011001    00011110
 01101100   01101100   01101100   01101100    01101100     XOR
______________________________________________________________
 01010011   01100101   01100011   01110101    01110010    <  Ans


 00000101   00011000   00010101   01000111
 01101100   01101100   01101100   01101100      XOR
_________________________________________________
 01101001   01110100   01111001   00101011     < Ans
```

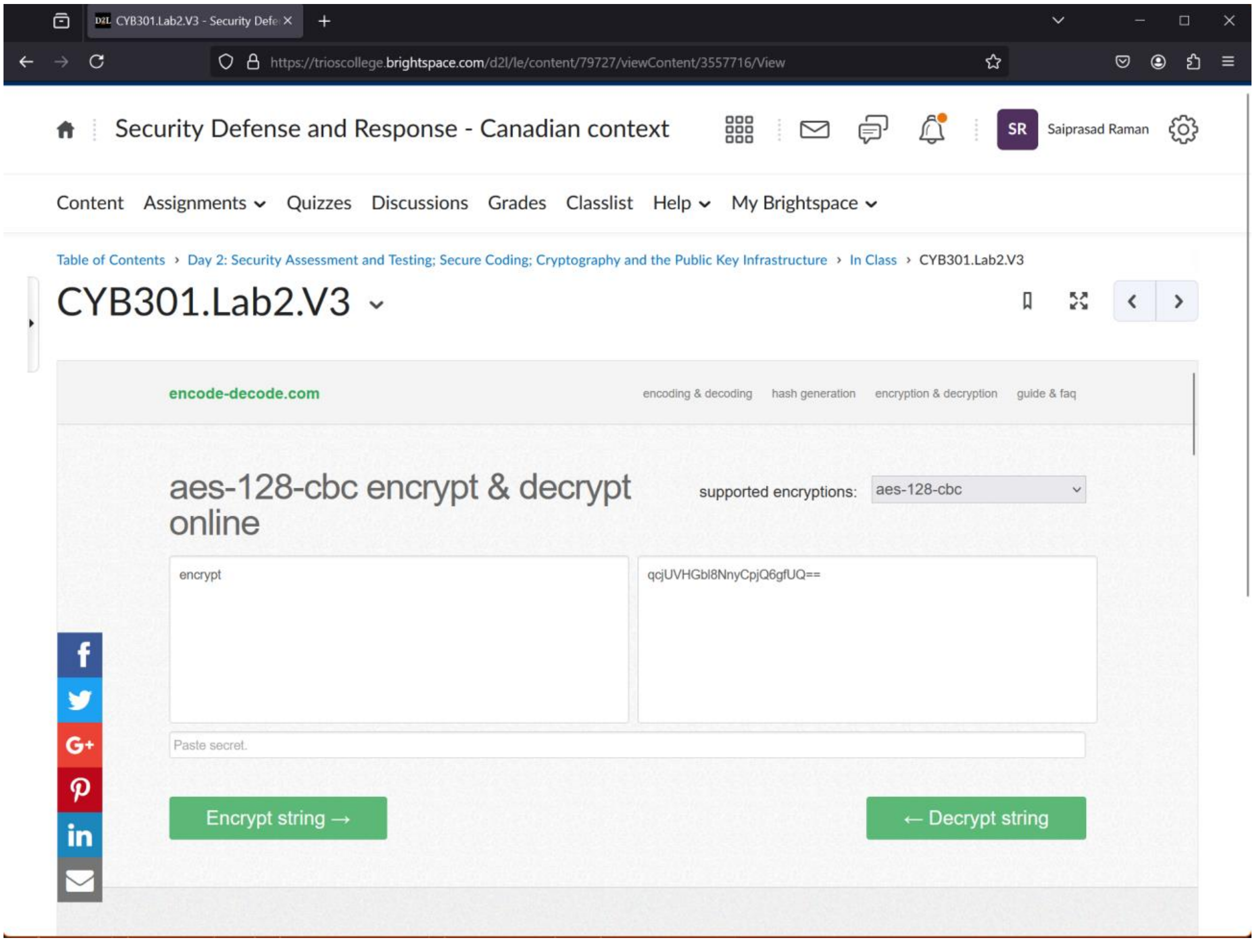
b) Using Lookup Tables, what is the original plaintext?

Ans. 83 101 99 117 114 105 116 121 43

Security+

3. For a general idea of how involved AES is, check out the official AES documentation. You will see that XOR, as mentioned, is a part of AES.

4. Encrypt some plaintext with an online AES tool from encode-decode.com. Notice in the tool there are many modes for AES which handle the influence one encrypted block has on the next block.



CYB301.Lab2.V3 - Security Defe

https://trioscollege.brightspace.com/d2l/le/content/79727/viewContent/3557716/View

Security Defense and Response - Canadian context

Table of Contents › Day 2: Security Assessment and Testing; Secure Coding; Cryptography and the Public Key Infrastructure › In Class › CYB301.Lab2.V3

CYB301.Lab2.V3

aes-128-cbc encrypt & decrypt online

supported encryptions: aes-128-cbc

encrypt

qcjUVHGbl8NnyCpjQ6gfUQ==

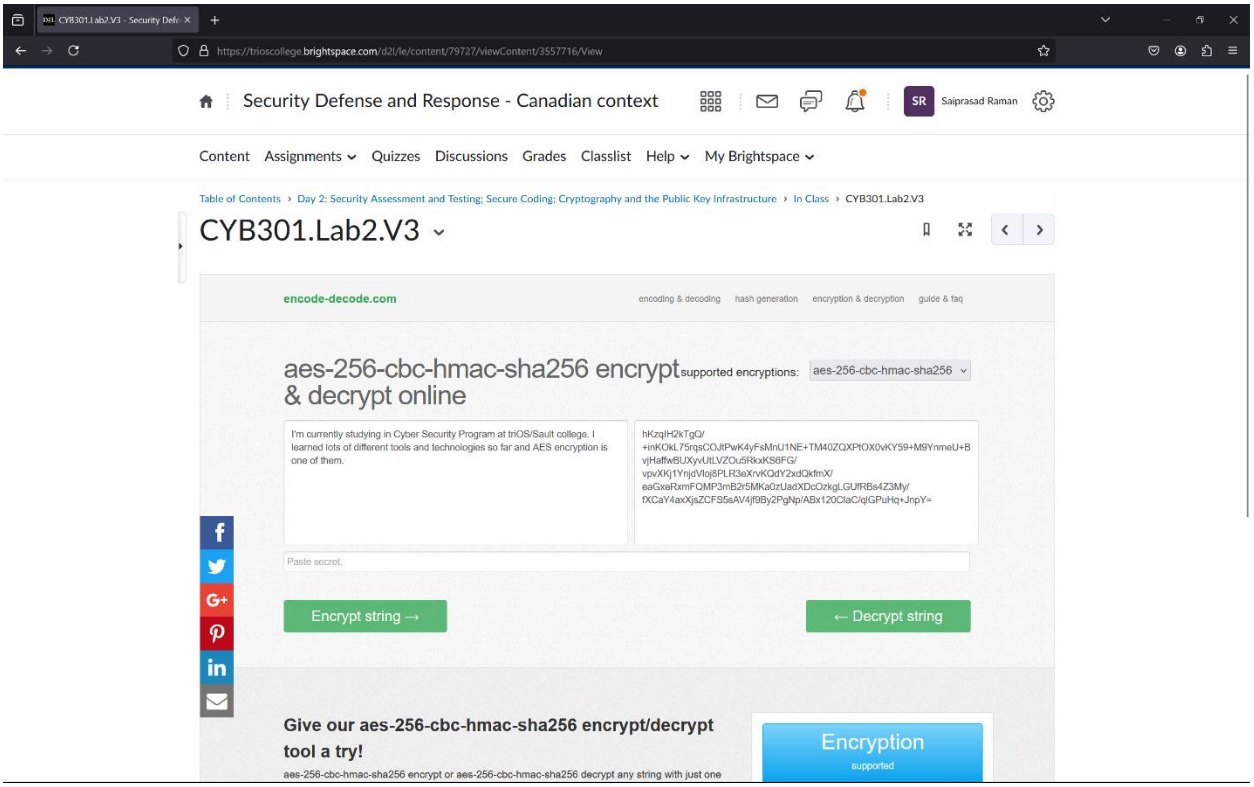
Paste secret.

5. Name the AES mode is used to encrypt and decrypt the following string. *(Hint: AES encryption more than 128 bits)*

Encrypted String:
hKzqIH2kTgQ/+inKOkL75rqsCOJtPwK4yFsMnU1NE+TM40ZQXPtOX0vKY59+M9YnmeU+BvjHaffwBUXyvUtLVZOu5RkxKS6FG/vpvXKj1YnjdVloj8PLR3eXrvKQdY2xdQkfmX/eaGxeRxmFQMP3mB2r5MKa0zUadXDcOzkgLGUfRBs4Z3My/fXCaY4axXjsZCFS5sAV4jf9By2PgNp/ABx120CIaC/qlGPuHq+JnpY=

Decrypted String:
I'm currently studying in Cyber Security Program at triOS/Sault college. I learned lots of different tools and technologies so far and AES encryption is one of them.

Ans. aes-256-cbc-hmac-sha256


CYB301.Lab2.V3 - Security Defe
https://trioscollege.brightspace.com/d2l/le/content/79727/viewContent/3557716/View
Security Defense and Response - Canadian context
SR
Saiprasad Raman
Content
Assignments
Quizzes
Discussions
Grades
Classlist
Help
My Brightspace
Table of Contents › Day 2: Security Assessment and Testing; Secure Coding; Cryptography and the Public Key Infrastructure › In Class › CYB301.Lab2.V3
CYB301.Lab2.V3
encode-decode.com
encoding & decoding
hash generation
encryption & decryption
guide & faq
supported encryptions:
aes-256-cbc-hmac-sha256
Paste secret.
Encrypt string →
← Decrypt string
Encryption
supported

aes-256-cbc-hmac-sha256 encrypt & decrypt online

I'm currently studying in Cyber Security Program at triOS/Sault college. I learned lots of different tools and technologies so far and AES encryption is one of them.

```
hKzqIH2kTgQ/
+inKOkL75rqsCOJtPwK4yFsMnU1NE+TM40ZQXPtOX0vKY59+M9YnmeU+B
vjHaffwBUXyvUtLVZOu5RkxKS6FG/
vpvXKj1YnjdVloj8PLR3eXrvKQdY2xdQkfmX/
eaGxeRxmFQMP3mB2r5MKa0zUadXDcOzkgLGUfRBs4Z3My/
fXCaY4axXjsZCFS5sAV4jf9By2PgNp/ABx120ClaC/qlGPuHq+JnpY=
```

Give our aes-256-cbc-hmac-sha256 encrypt/decrypt tool a try!

aes-256-cbc-hmac-sha256 encrypt or aes-256-cbc-hmac-sha256 decrypt any string with just one

Activity 2: Asymmetric Key Encryption and RSA

Asymmetric key encryption, also known as asymmetric key cryptography and public key encryption, is used for confidentiality, like symmetric key encryption. Unlike symmetric key encryption, however, asymmetric encryption uses two different keys: a public key, which can (and should) be seen by anyone, and a private key, which should never be seen by anyone but the user or organization the key belongs to.

When a public key/private key pair is created, the keys are mathematically linked to each other. When you encrypt using one of them (it does not matter which one), the ciphertext can only be decrypted by the other.

To learn about RSA encryption, watch this great video (16m:30s) that illustrates both how and why RSA works, as well as the history of the algorithm, which predates Rivest, Shamir, and Adlem. The video starts off explaining RSA with colours and then gets into modular arithmetic. If you do not follow all the math, do not worry. As long as you understand the colour example, you will be fine!

Keep the following fundamentals of RSA in mind:

- In RSA, to encrypt, the algorithm is simply x^e mod n.
- In RSA, to decrypt, the algorithm is simply y^d mod n.
- x is the plaintext.
- y is the ciphertext.
- (n, e) is the public key.
- d is the private key.

Step 1: Apply what you have learned so far by walking through an example of an RSA encryption algorithm.

a) For PGP encryption, assume the symmetric key that will encrypt and decrypt the email is 4.
b) To encrypt this symmetric key with RSA so it can be sent securely over an insecure channel, you need the public key of the person you are sending

the email to. Assume the other person sends it to you and it is 33, 3 (as noted, the public key consists of two values).

c) To encrypt, the RSA algorithm takes x and raises it to the power of e, which is 3 in this case: 4^3 is 64. The RSA algorithm divides that 64 by n (the modulus), which in this case is 33. The quotient is 1, which is not relevant to us. What is relevant to us is the remainder, which is 31. That is the ciphertext! Welcome to the world of modular arithmetic, which is a large part of cryptography.

d) **Prove that the ciphertext is 31. (Show your work in detail.)**

Ans.

The recipient sends a public key for the sender to create a cipher text to the symmetric key.

Symmetric key = x = 4

Public key = (33,3) where n = 33 and e = 3

We use RSA encryption algorithm to determine the cipher text.

RSA encryption algorithm = x^e mod n

Cipher text = x^e mod n = 4^3 mod 33

= 64 mod 33

Cipher text = 31

Step 2: Put yourself in the role of the email recipient. You have just received the email sent in the previous step. It is time to go through the RSA decryption algorithm.

a) To decrypt, the RSA algorithm will take the 31, the ciphertext, and raise it to the power of the email recipient's private key. Assume it is 7.

b) Then 31^7 will be divided by the modulus. The remainder is the plaintext, which in this case is 4.

c) **Prove that the plaintext is 4. (Show your work in detail.)**

d) PGP takes that 4 and decrypts the email with that symmetric key, which was protected as it was transmitted with asymmetric encryption.

This example used small numbers, but as you might imagine, these values are usually at least 1024 bits long in practice.

Ans.

The recipient then decrypts the cipher text to determine the symmetric key using the private key and RSA decryption algorithm.

Cipher text = Y = 31

Private key = d = 7

RSA decryption algorithm = y^d mod n

= 31^7 mod 33

= 4

Step 3: Now it is your turn to practice both RSA encryption and decryption.

a) You received someone's public key as (55, 7) and you want to encrypt the plaintext value of 8. Using RSA encryption, what is the corresponding ciphertext? You may use any tool, including Google, to do the math.

Ans.

Symmetric key = x = 8

Public key = (55,7) where n = 55 and e = 7

RSA encryption algorithm = x^e mod n

Cipher text = x^e mod n = 8^7 mod 55

= 2097152 mod 55

Cipher text = 2

b) **What is the RSA decryption algorithm needed** (using the required values) **to decrypt the ciphertext back into the original plaintext with a private key of 23?** You may use any tool, including Google, to verify the math.

Ans.

Cipher text = Y = 2

Private key = d = 23

RSA decryption algorithm = y^d mod n

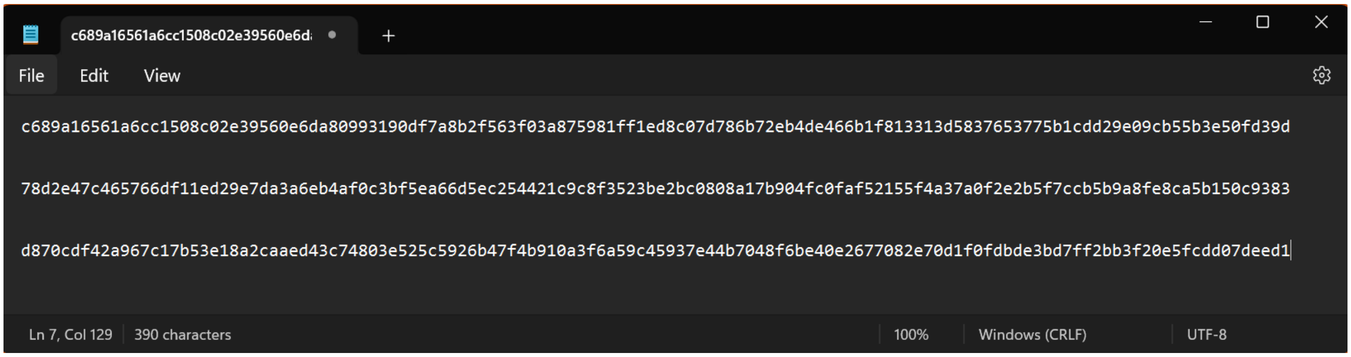
= 2^{23} mod 55

= 8388608 mod 55

= 8

Activity 3: Hashtag

1. Go to File Format Info.
2. In the **String Hash** textbox type **[your first name]** using small letters only and then click the **Hash** button.
3. Scroll down to see all the message digests that were simultaneously calculated. The longer the output, the more secure the hash function because with longer outputs it is harder to find a collision for multiple inputs.
4. Open Notepad by typing Notepad in the Windows search box. Then click the **Notepad** icon. Copy and paste the SHA-512 hash calculated in **Step c** into Notepad.
5. Go to any website and copy a bunch of text (highlight the text and press **CTRL-C**).
6. Paste (press **CTRL-V**) the text into the String Hash textbox from **Step b** and click the **Hash** button.
7. Copy and paste the SHA-512 hash into Notepad below the first hash. As you can see, even though the first input was significantly shorter than the second output, the size of the message digests in the output of the hash function are the same.
8. Back in the String Hash textbox, type **[Your First Name] using first letter as capital and remaining small** and click the **Hash** button. Scroll down to see all the message digests that were simultaneously calculated.
9. Copy and paste the SHA-512 hash into Notepad, on the third line. **Take a screenshot.**



```
c689a16561a6cc1508c02e39560e6da80993190df7a8b2f563f03a875981ff1ed8c07d786b72eb4de466b1f813313d5837653775b1cdd29e09cb55b3e50fd39d

78d2e47c465766df11ed29e7da3a6eb4af0c3bf5ea66d5ec254421c9c8f3523be2bc0808a17b904fc0faf52155f4a37a0f2e2b5f7ccb5b9a8fe8ca5b150c9383

d870cdf42a967c17b53e18a2caaed43c74803e525c5926b47f4b910a3f6a59c45937e44b7048f6be40e2677082e70d1f0fdbde3bd7ff2bb3f20e5fcdd07deed1
```

10. Compare the hash of [your first name] all small letters to the hash of [Your First Name] using first letter as capital and remaining small, and answer the following questions:
    a) Are both hashes of your first name the same?

Ans. No, both are different.

    b) How many bits are different in the binary representation of the first letter of your name as a capital letter and first letter of your name as a small letter?

Ans. 1 Bit, Binary of Capital letter = 010 and binary of small letter = 011.

    c) Choose True or False for the following statement and support your answer with a reason or an explanation:
    If the hash is put back into the function, the original input will be received.

Ans. False, hashing is a one way function. It doesn't reverse to the original input unlike Encryption which is a two way function.