**Cryptology Workshop**

**Task:**

You are an intern researcher for the government who is tasked with figuring out and comparing different algorithms for cryptography, how they work, and which to use in order to protect your research from getting stolen. You will be experimenting with different algorithms and ciphers to find out this answer and applying them to see how they work.

Cryptology is the study of making information secret by using a secret code, keys, or passwords to encrypt and decrypt information to keep it secret. Julius Caesar used encryption to cipher letters and messages. Encryption played an important role in many wars and throughout the years but is beginning to be used more and more in the private and public sectors. The ancient Greeks were one of the first ones to use cryptography using a stick and strip of cloth. They would wrap the cloth around the stick, write their message, then send the cloth and if you had a stick with similar length you would wrap it around the stick and see your message.

**Outcome:**

After doing this workshop you will understand the basics of cryptology, learn about One Time pad algorithm as well as RSA and apply a cipher to a plain text using Openssl to decrypt and encrypt. As well as understand the fundamentals of cryptology such as substitution, transposition, symmetric, asymmetric, stream, and block ciphers.



Ciphers are like the secret codes or rules used to turn your text into a secret message. There are two types of operations used on ciphers which are Substitution and Transposition. Substitution is when a character is replaced by another character by a code or rule called a key for example, given the following key that we shift each letter in the word over to the next letter. So, if we see A it turns into B if we see Z it turns into A and so on. By applying this word, we are encrypting it.

**Step 1 Learn about encrypting decrypting substitution And Transposition**

**Further reading**

[**https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography**](https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography)

Example

(plain text) bat → cbt (encrypted message)

encryptions move each letter to the letter after it by 1(Substitution)

To decrypt the word, we simply apply the reverse of the key and move each letter to the letter before it by 1.

(encrypted message) cbt→ bat (secret message or plain text from the beginning

Decryption)

1.Apply the same decryption used above to the following text. Hint Positive encouragement

zpv eje ju

\_ \_ \_ \_ \_ \_ \_ \_

Transposition is changing the order in which your supposed to read the message for example a cipher they call the rail fence cipher.

Rail fence cipher

C………O……...A………..I……..

..A …Y…U….E….D….H….S….

…..N……….R……….T…………..

2. What do you get when reading this message left from right?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Guess what the secret message is. HINT Its four words. (Unhighlight for hint)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The above was a cipher text only attack which is an attack given the encrypted message only.

This transposition is read by going diagonally down right ↘then diagonally up right ↗and back down diagonally right ↗ and you keep doing this until you reach the last letter. So, the correct message is Canyoureadthis (unhighlight to see the answer) after answering number 3.

4. Did you guess correctly in number 3.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

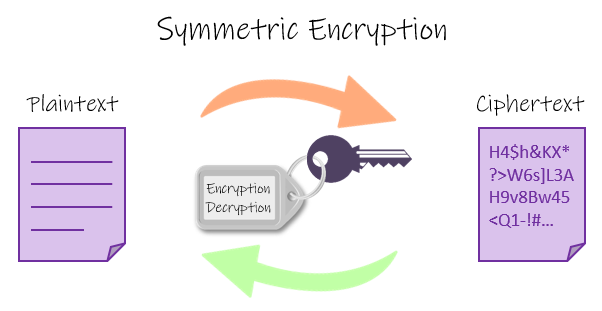
**Step 2 learn about the difference between symmetric vs asymmetric ciphers and stream vs block ciphers**

**Further reading**

[**https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/**](https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/)

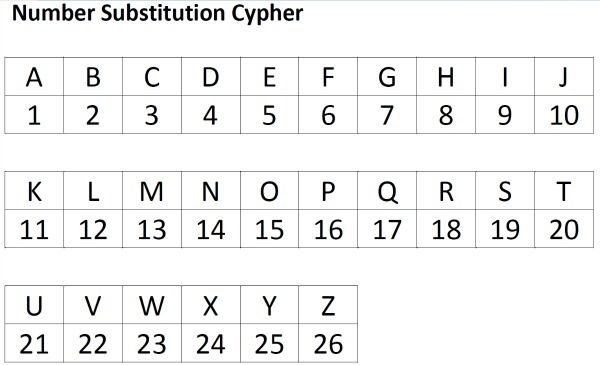
[**https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/#:~:text=The%20main%20difference%20between%20Block,plain%20text%20at%20a%20time.&text=While%20stream%20cipher%20uses%208%20bits**](https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/#:~:text=The%20main%20difference%20between%20Block,plain%20text%20at%20a%20time.&text=While%20stream%20cipher%20uses%208%20bits)**.**

So far, the ciphers we have been looking at have been using the same rule or code to decrypt and encrypt. These rules or code are called keys. And when using the same key to decrypt and encrypt it is called a symmetric cipher like our first example.



A stream cipher is a cipher that will read bit by bit of data to decrypt and encrypt for example, dealmeal needs to be encrypted. The cipher will encrypt letter by letter d first then encrypt e then a then l and then m then so on one by one.

One time pad is a symmetric cipher that takes the plain text generates a random key of equal length and produces an encrypted message. It is one of the hardest ciphers to decipher when just given the cipher text because the key is random and when given the cipher text it has little to no similarities to the original text. In this workshop we will be using a version of it where the key will tell the amount of shifts to apply to each letter and the letters were chosen randomly. Example given the letter b as plain text with a key of c you shift it 3 over resulting in e



Encrypted text

Iavhcwiyhp

Above is a one pad encryption given by a version of one time pad try guessing the message. Give it your best guess!

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hwurivopsa here is the key for the above encrypted message(unhighlight). What is the decrypted message?

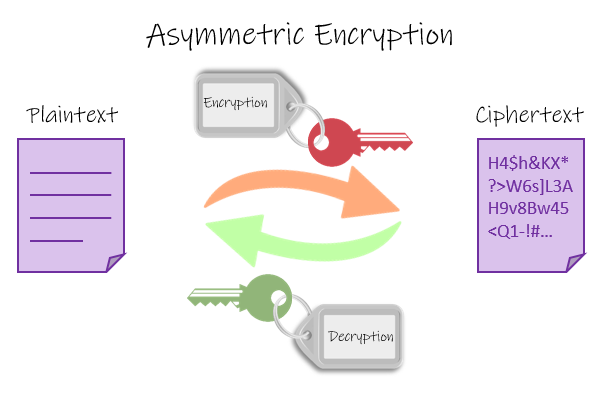
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What are the advantages and disadvantages of this One time pad

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Explain symmetric encryption and stream ciphers in your own words

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



RSA is an asymmetric algorithm that uses block cipher to encrypt and decrypt messages.

Asymmetric is when you use two or more different keys to encrypt and decrypt which is called asymmetric cipher. RSA has a public key and private key. A private key is only known between the person sending the message and receiving it. A public key is a key that can be known and used by anyone to encrypt messages.

A block cipher is a cipher that will read multiple bits of data at once for encryption and decryption for example, Abcdefgh needs to be decrypted. Abcd will be read all at one time and decrypt, then move on to the next block of efgh then be decrypted.

Follow along the algorithm of RSA and fill in the blanks:

The first step is to Choose two prime numbers that are p and q.    
p = 3 q = 11

The second step is Compute the value of  n and  ϕ given the following formulas

n= p \* q= \_\_\_\_\_\_ \*\_\_\_\_\_\_\_\_\_\_\_ =\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ϕ= (p -1) \* (q -1) = (\_\_\_\_\_\_\_\_\_\_\_) \* (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The next step is to find the value of the public key e

You must choose e so that must not be a multiply by factors of ϕ and also not be divisible by ϕ

e=7

Calculate the value of the private key d by doing the following

gcd(ϕ, e) = ϕx +ey = 1 where y is the value of d.

Form a table with four columns i.e., a, b, d, and k.

Set a = 1, b = 0, d = ϕ, k = – in the first row.

Set a = 0, b = 1, d = e, k = ϕ /e in the second row.

From the next row, apply following formulas to find the value of next a, b, d, and k, which is given as

ai = ai -2 – (ai-1 \* ki-1)

bi = bi-2 -(bi-1 \* ki-1)

di = di-2 - di-1 \* ki-1)

ki = (di-1) / (di)

As soon as, d = 1, stop the process and check for

If b> ϕ

b=b mod ϕ

if b<0

b=b+ ϕ

Fiil in the blanks

|  |  |  |  |
| --- | --- | --- | --- |
| A | B | D | K |
| \_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_ | ­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1 | -2 | 6 | 1 |
| -1 | 3 | 1 | - |

Why was the process stopped here?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Last step is to apply the encryption and decryption using the formulas

% is a remainder operation

For example 11/3 =3.66666666 and 6 repeats forever but 11% 3 is the remainder of the division so if we do 11/3 we get 3 \* 3 = 9 11- 9=2 so there is a remainder 2 so in the end 11%3=2

Encryption is

c = t^e % n

Decryption is

t = c^d % n

For the given example, suppose t = 3, so

Encryption is c = 3^7 % 33 =9

Decryption is t = \_^\_ %\_ = \_

Therefore in the final, p = \_\_\_\_\_\_, q = \_\_\_\_\_\_\_\_\_\_, ϕ =\_\_\_\_\_\_\_\_\_\_, n = \_\_\_\_\_\_\_\_, e = \_\_\_\_\_\_\_\_ and d = \_\_\_\_\_\_\_\_\_\_\_\_\_

Diffle keyman algorithm is another asymmetric algorithm with a public key and private key. It is usually used for key exchanges. There are two parties who in this case will be me and you.

We agree on a prime number 17 (P)and g a base

P = 17 g = 3

I pick a secret number 5(my secret key)x= 5

And apply the formula

X = g^x % p

X = 3^5%17

X=243%17

X = 5

Now you pick a secret number 2- 7 to make it simple(y= your number goes here)(secret key)

Apply the formula

 Y = g^y % p

Y= \_^\_ % \_

Y=\_%\_

Y= \_

Then you send me Y and I send you X

I use the formula with what you sent me

K = Y^x % p

K = \_^4%17

K=\_%17

K=\_

You use the formula with what I send you

K = X^y % p

K= \_^\_ % \_

K= \_ % \_

K=\_

**Step 4 compare and contrast differences**

What are the differences between symmetric and asymmetric cryptography? What are the advantages and disadvantages of each?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the difference between stream and block ciphers? What are the advantages and disadvantages of each?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which is more secure symmetric or asymmetric cryptography and why?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What are some advantages of RSA and Disadvantages?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 5 Use open ssl

Now we will use some encryptions and decryption using openssl

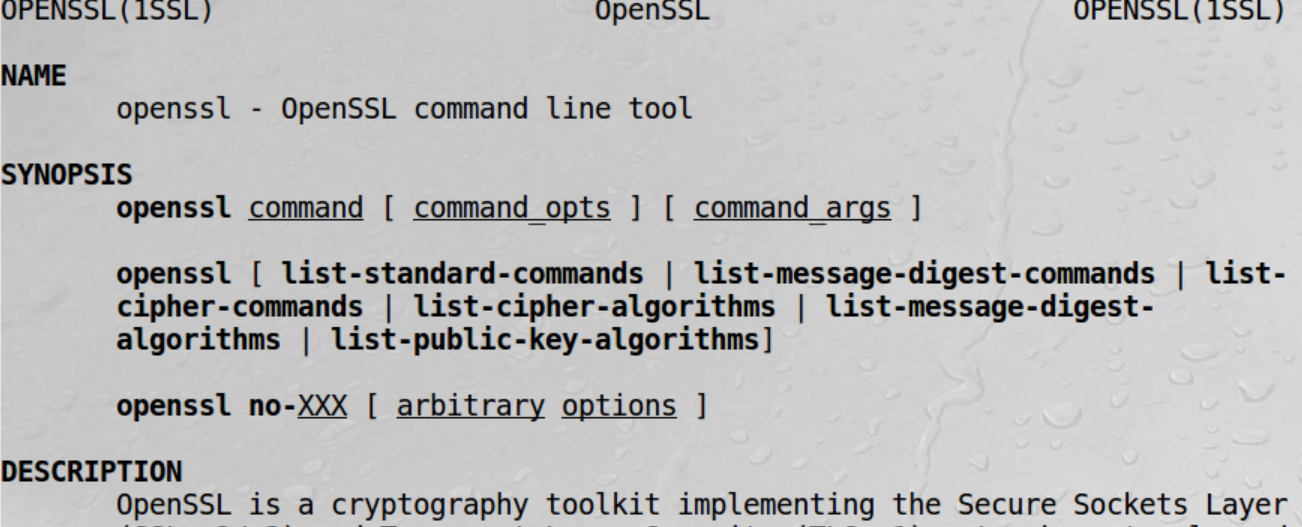
Open the command terminal



Next man openssl



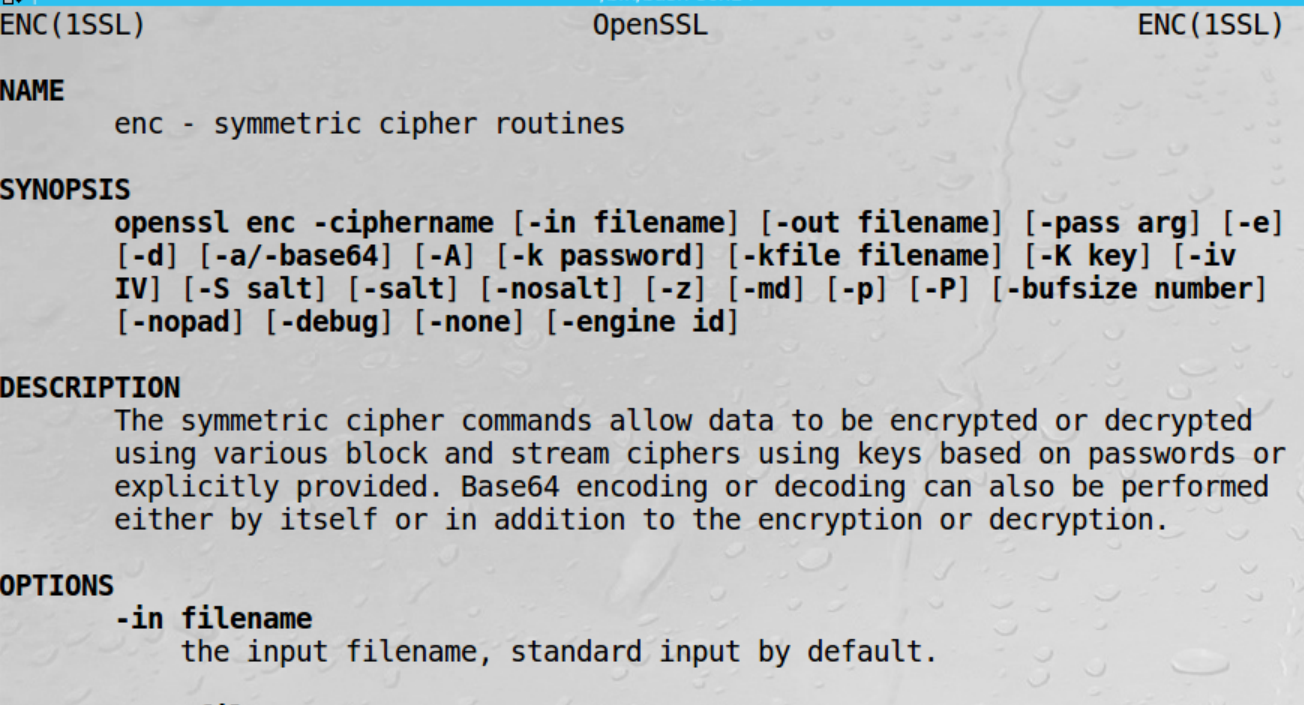
And you should see something similar to this



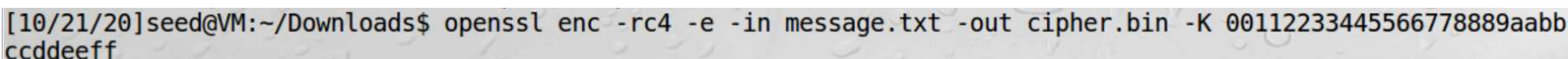
What is openssl?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now man enc and you should see something similar to this below



Here is a sample command using enc



What does -e do?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What does -in do?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What does – out do?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What does -k do?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

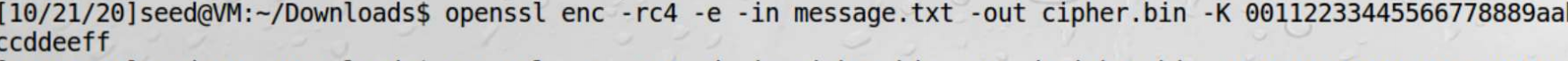
What does -d do? Hint if you don’t know go back to man enc

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Use leafpad at text editor to create an appropriate secret message and save it as message.txt



Then do the following command



What did this command do to your message?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now enter a similar command to decrypt your message to decipher.bin? Hint decryption not encryption

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If you see your original message before encryption in decipher.bin then CONGRATULATIONS, YOU HAVE FINSHED THIS WORKSHOP!!!

Hw Apply a different cipher in openssl encryption and decryption

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Challenge (extra credit)

Explain step by step a different encryption\decryption algorithm?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**References/Further Reading**

https://www.geeksforgeeks.org/how-to-solve-rsa-algorithm-problems/

<https://www.freecodecamp.org/news/understanding-encryption-algorithms/>

https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/#:~:text=The%20main%20difference%20between%20Block,plain%20text%20at%20a%20time.&text=While%20stream%20cipher%20uses%208%20bits.

<https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography>