

Cryptography Assignment

1. Install and configure GNU privacy guard (GNUPG)

```
foram@foram-VirtualBox:~$ gpg --version
gpg (GnuPG) 2.2.19
libgcrypt 1.8.5
Copyright (C) 2019 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/foram/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
foram@foram-VirtualBox:~$ █

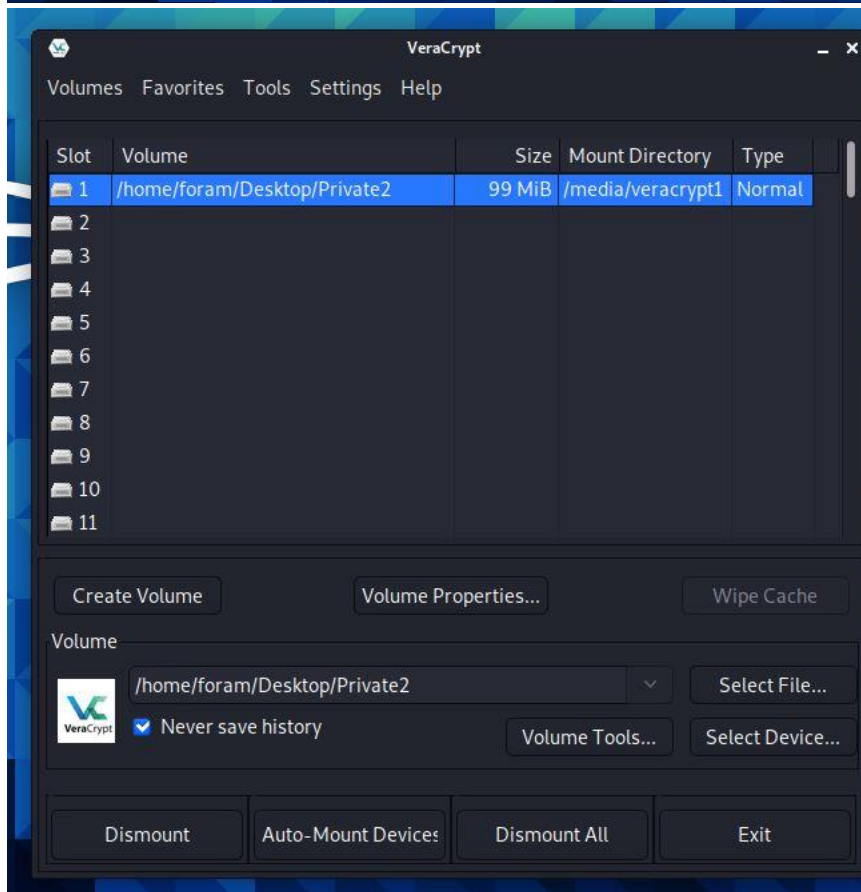
pub   rsa3072 2021-03-05 [SC] [expires: 2023-03-05]
      D8AB2F1546948EAF4D64C308551535839693BA91
uid           Jigar Shah <JS@gamil.com>
sub   rsa3072 2021-03-05 [E] [expires: 2023-03-05]

foram@foram-VirtualBox:~$ █
```

2. Generate a SHA256 hash from the command-line in Linux

```
foram@foram-VirtualBox:~$ sudo sha256sum my_report.txt
c123d1a8621e45082b9f6fd31ff2085a40c560fded119f8a9202c87bfc630042  my_report.txt
foram@foram-VirtualBox:~$
```

3. Install and configure VeraCrypt. Perform a file encryption



4. Send encrypted email (includes exchanging digital certificates and decrypting email)

```
foram@foram-VirtualBox:~$ touch secretinfo.txt
foram@foram-VirtualBox:~$ nano secretinfo.txt
foram@foram-VirtualBox:~$ gpg --encrypt --recipient 'fs@gmail.com' --output confidential.txt.enc secretinfo.txt
gpg: invalid option "--ouput"
foram@foram-VirtualBox:~$ gpg --encrypt --recipient 'fs@gmail.com' --output confidential.txt.enc secretinfo.txt
foram@foram-VirtualBox:~$ ls | grep confi.*
confidential.txt.enc
foram@foram-VirtualBox:~$ cat confidential.txt.enc
00t10q000
a0 0(C0;
 0FDJ00F:00^m[M0a0"l0j0T0e0;00x4000`0 0A0KV0i00u0lQ0L00<00f$A0e0-000M0F0K0t0q0
A0T000/π0001h5000000@)T000h0(10℥ 00FvM0000[k00^x0N0H000000007=
00000-00;40070X=00000.000RB00c0%0090o000 |700-00`0&U0F[$
000t0Q`y00y00p00t0(H0L00R00Nh00c000X@0o0R0&0B0ke00H00s00020P?0o00c0`H0>0x/00800
r/0000000,0?YSJ"6V0+ 00an0T0d0Z0}00v.00000?00Y020f000[000b000Ru00g;0_L00]0Z0
00005;`0zc0s0000@0+Ⅲ~_
@00B0.000N000)00000foram@foram-VirtualBox:~$
```

```
foram@foram-VirtualBox:~$ gpg --decrypt --output secretinfo.txt confidential.txt.enc
gpg: encrypted with 3072-bit RSA key, ID 7431A57F71DDE1F3, created 2021-03-05
"Forum Shah <fs@gmail.com>"
File 'secretinfo.txt' exists. Overwrite? (y/N) y
foram@foram-VirtualBox:~$ cat secretinfo.txt
My secret information
foram@foram-VirtualBox:~$
```

Signing/Encryption Options...

Identity: Forum Shah <foram7shah@gmail.com>

☒ Enable OpenPGP support (Enigmail) for this identity

☒ Use email address of this identity to identify OpenPGP key
☐ Use specific OpenPGP key ID:

Message Composition Autocrypt

☒ Encrypt messages by default
☒ Sign messages by default
☒ Use PGP/MIME by default

After application of defaults and rules:
☐ Sign non-encrypted messages ☒ Sign encrypted messages

☒ Encrypt draft messages on saving

If both, Enigmail and S/MIME encryption are possible, then:
☐ Prefer S/MIME ☒ Prefer Enigmail (OpenPGP)

☐ Attach my public key to messages

Signing/Encryption Options...

Identity: Foram Shah <foram7shah@gmail.com>

☒ Enable OpenPGP support (Enigmail) for this identity

☒ Use email address of this identity to identify OpenPGP key

☐ Use specific OpenPGP key ID:

Select Key

Message Composition Autocrypt

☒ Encrypt messages by default

☒ Sign messages by default

☒ Use PGP/MIME by default

After application of defaults and rules:

☐ Sign non-encrypted messages ☒ Sign encrypted messages

☒ Encrypt draft messages on saving

If both, Enigmail and S/MIME encryption are possible, then:

☐ Prefer S/MIME ☒ Prefer Enigmail (OpenPGP)


☐ Attach my public key to messages




... **Inbox**






Foram Shah 2:58 PM
to me ▾






 **encrypted.asc**  

 **noname**  

 Reply

 Reply all

 Forward



content://com.google.androi

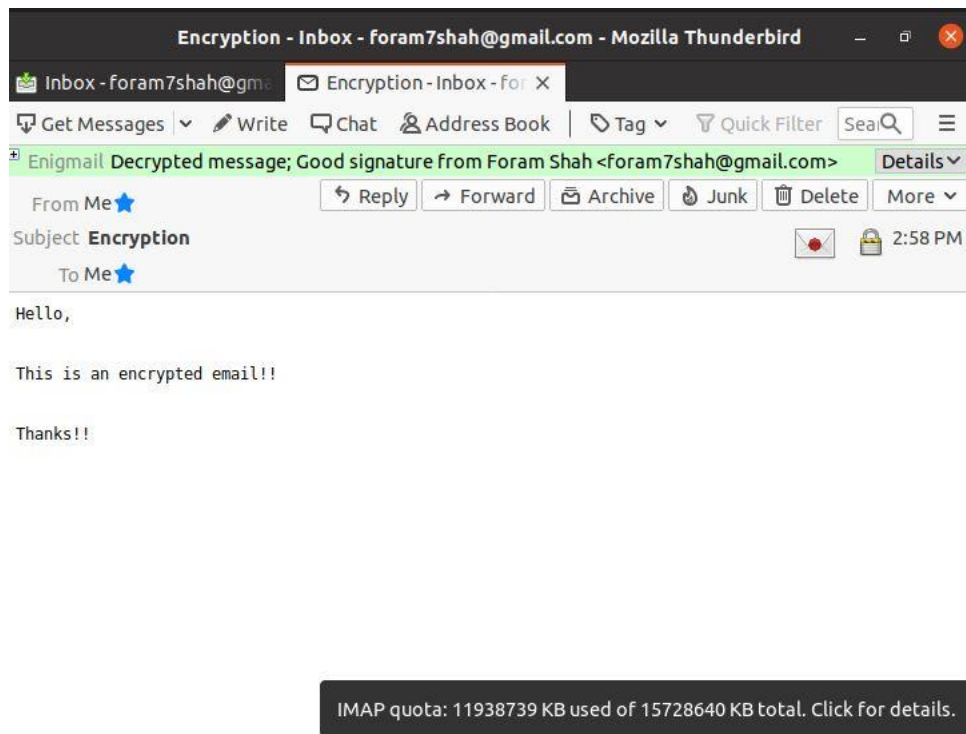


-----BEGIN PGP MESSAGE-----

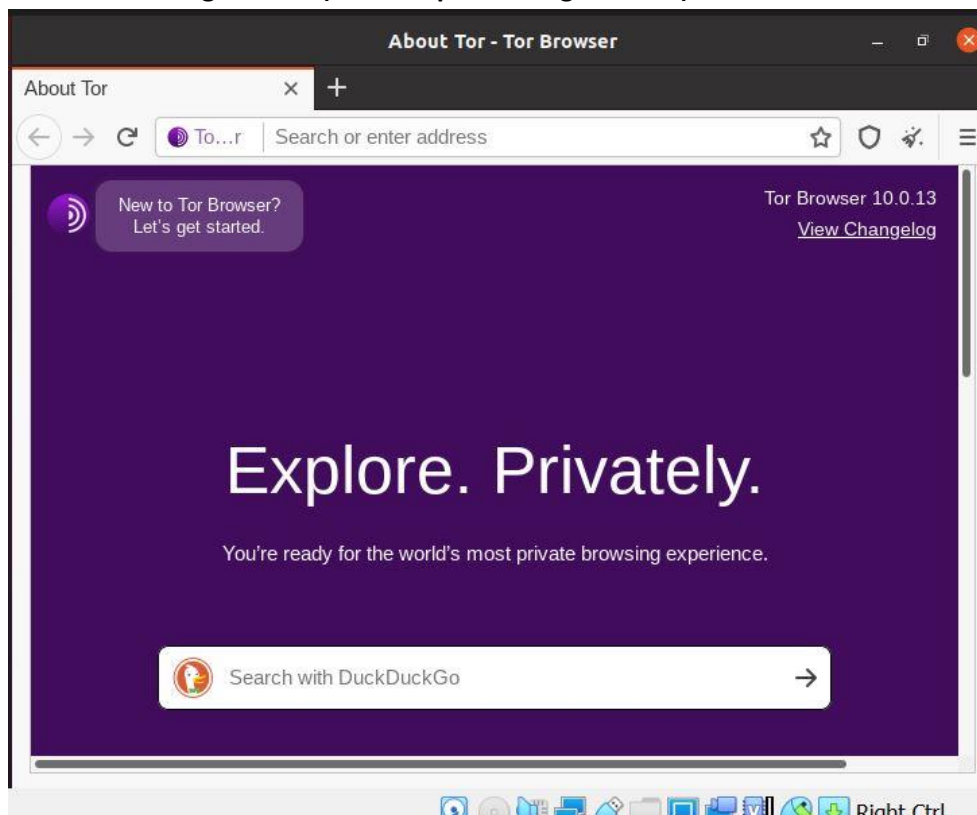
hF4DvVMdnIImItISAQdAEFz2WF0NjxzF2o3puLYDCuNrx9Bvx
8u2IqRfb6VapAcw
g49trdAmneY6FNz68uSk78tVkJn5b27XivChR6GsH0xEX+u4N
yAsC4aXfRL/byia
0ukBIhaE15sL1AgcKkC1uVaPusing/d6MtyOYDb3bCi8RyaR5
uX06PAZ2jMBQAqV
f11JMXSvF9001Snow25IWe3FPH0e/h2GwAgcvSMismie0JSbB
kwPNB56R5qx9joE
ir2lo7XCuYtc02c/RVY9Lp52EPNurDBE9C4xE0JzqmwPjqYDg
q+IzdkBDlmD0uHL
l6Zl8PnQvYWU5mWnrhY0JLNYWiP0HXN/xqINZgVfMvJnEXd7b
auv4Dtcpt0BYxvW
i/GA7DVveQZE184j39NI54evT2AkaTnJo8D2nCQ7pBS1MUGmf
feslYBhX0Fcyfgi
vbtF0iF1DzVaQXCS/GeQIOUBH0rN7vFVKldADV15Br0tAuhcd
pEXM0SXFneMB0Uu
mk5S2FRHfq6IvxrhIzUnvIFCcqaWTZ3HUfdsIPSdeHHG0gBLq
AkRCXuVaEGDYGtq
vKw+lIP/eR6IPNXLX/qtGVZ0b7X8uNuzJhBSmF0BTLczUP20Y
ihIi82+3cW6x9V0
Yn7HDUE5Z3N1mNdUEpR6lKJWlKy/pzmCdoU50vWIs4fFIg39
F8ZvQ6t7NEL1988
Y19Id20uME5RjGGmhW3UFt/uSDlW5Xxha3sVoe5vWNZk0Pnmt
wMWLRbz06MZQkB3
nkis7lQeqUlwF+jfAb1AcuZRjUDwIJ/NBBEpBpaqPWPLhhoGd
m90o+xJx8o33ZKE
air7ffPIE3UZN8mwvw==
=8mc1

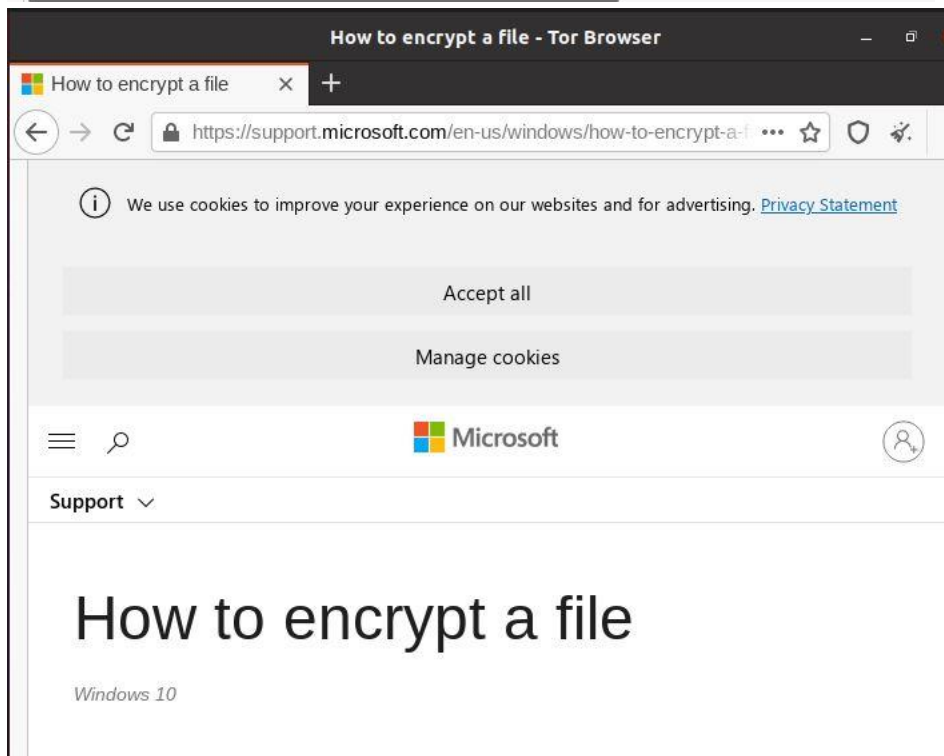
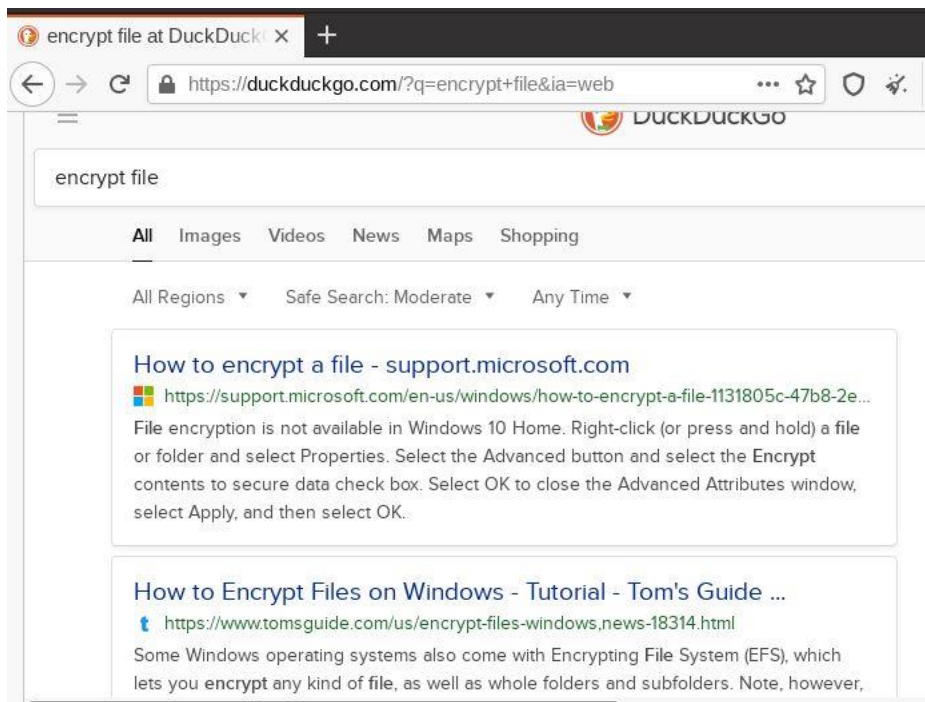
-----END PGP MESSAGE-----





5. Install and configure TOR (includes performing a search)





6. Perform a basic steganography encryption

```
ubuntu@ubuntu2004:~/Downloads$ outguess -k "secret key" -d examplefile.txt image-output.jpg output.jpg
Reading image-output.jpg...
JPEG compression quality set to 75
Extracting usable bits: 94581 bits
Correctable message size: 47731 bits, 50.47%
Can not open examplefile.txt
ubuntu@ubuntu2004:~/Downloads$ outguess -k "secret key" -d examplefile image-output.jpg output.jpg
Reading image-output.jpg...
JPEG compression quality set to 75
Extracting usable bits: 94581 bits
Correctable message size: 47731 bits, 50.47%
Encoded 'examplefile': 120 bits, 15 bytes
Finding best embedding...
  0: 92(60.5%)[76.7%], bias 76(0.83), saved: -4, total: 0.10%
  1: 69(45.7%)[57.5%], bias 57(0.83), saved: -1, total: 0.07%
 43: 68(44.7%)[56.7%], bias 56(0.82), saved: -1, total: 0.07%
 59: 67(44.4%)[55.8%], bias 54(0.81), saved: 0, total: 0.07%
 78: 70(46.1%)[58.3%], bias 49(0.70), saved: -1, total: 0.07%
105: 62(40.8%)[51.7%], bias 51(0.82), saved: 0, total: 0.07%
105, 113: Embedding data: 120 in 94581
Bits embedded: 152, changed: 62(40.8%)[51.7%], bias: 51, tot: 95502, skip: 95350
Foiling statistics: corrections: 38, failed: 0, offset: 22.200000 +- 37.976308
Total bits changed: 113 (change 62 + bias 51)
Storing bitmap into data...
Writing output.jpg...
```

```
ubuntu@ubuntu2004:~/Downloads$ outguess -k "secret key" -r output.jpg examplefile
Reading output.jpg...
Extracting usable bits: 94581 bits
Steg retrieve: seed: 105, len: 15
ubuntu@ubuntu2004:~/Downloads$ cat examplefile
secret message
ubuntu@ubuntu2004:~/Downloads$
```

7. Provide 2 paragraphs (minimum 4 sentence per paragraph) on the weaknesses and strengths of cryptography

The biggest strength of Cryptography is, Data Encryption. It ensures no data breaches and Encryption is on the data. It also ensures confidentiality of the data. That also means, your data is highly secured between the sender and the recipient. Security is also included no matter where your data is. Another strength is, that it maintains your data in very secured way. Although key management can be difficult and to protect from data breach is also very important.

The biggest weakness of Cryptography is, they key management between the sender and the receiver. If the key is lost, then their data cannot be secured. It is also expensive. The system should be upgraded and up-to-date to perform such encryption. So, it can cost a lot. Also, the compatibility matters in the Data encryption. If the devices aren't compatible the encryption cannot be performed. Another weakness is, if the data is loss during encryption and decryption there is no guarantee to store the data.

References: -

<https://www.iosrjournals.org/iosr-jece/papers/NCNS/76-81.pdf>

8. Provide 1 paragraph on Type 1 Cryptographic Products and 1 paragraph on Type 3 Cryptographic Products

It is also referred to as Type 1 Encryption. It is NSA (National Security Agency) classified information. Example: AES (Advanced Encryption Standard) Encryption (256-bit keys only – Block Cipher). It has many encryption types but the most important one is Accordian which is R21-TECH-13-00, "ACCORDIAN 3.0 Specification" (August 2000).

It is also referred to as Type 3 Encryption. A Type 3 Algorithm refers to NIST (National Institute of Standards and Technology) endorsed algorithms, registered and FIPS (Federal Information Processing Standards) published, for sensitive but unclassified U.S. government and commercial information. Example: - AES Encryption (FIPS 197).

References: -

https://en.wikipedia.org/wiki/NSA_product_types

9. What is FIPS 140-2 security levels and provide an overview of each level (Provide 2 paragraphs)

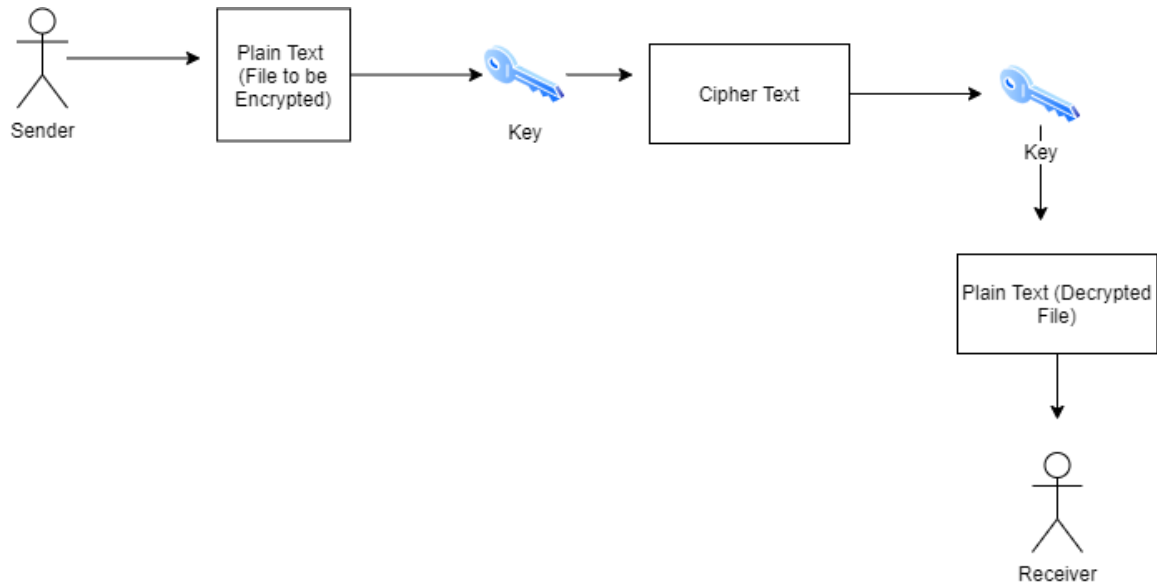
The Federal Information Processing Standard Publication 140-2, (FIPS PUB 140-2) security levels used to approve cryptography algorithms and standards. FIPS 140-2 refers four levels to identify which level is used by the cryptography encryption.

Level 1, it is the lowest level of security. It should approve at least one basic cryptography algorithm. Example of Level 1 is the basic PC encryption board. Level 2, it is better than Level 1 more secured than it. Focuses on physical security mechanisms. Level 3, attempts to prevent intruder suspecting your systems. Level 4, highest level of the security prevents unnecessary data breaches. It protects with the highest cryptographic module.

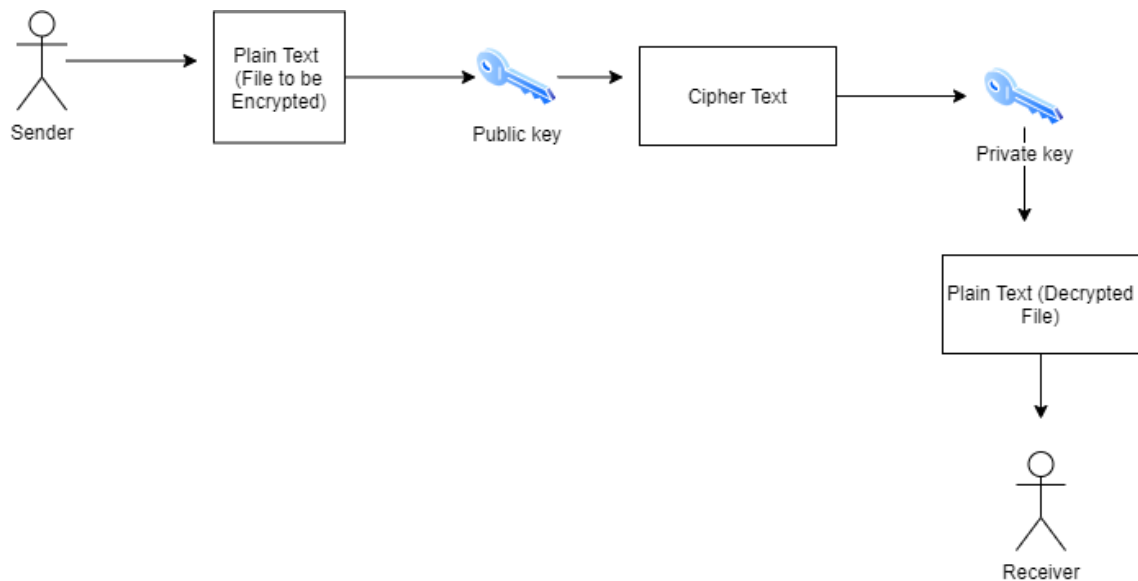
References: -

https://en.wikipedia.org/wiki/FIPS_140-2

10. Discuss the differences between asymmetric and symmetric encryption. Use diagrams to explain the process. Use Diagram or Visio and place .png, .jpeg, or .etc in the document (Provide 2 paragraphs)



In Symmetric Encryption, the operation uses a single key to encrypt and decrypt the data. Above diagram represents symmetric encryption where, sender sends the plain text the file to be encrypted and generates a key (shared) with that file. Then the same key is used to decrypt the file and sends to the receiver. It makes it easy to use but it is sometimes less secure than asymmetric operation.



In Asymmetric Encryption, the operation uses a public key and a private key to encrypt and decrypt the data. Above diagram represents asymmetric encryption where, sender sends the plain text that is the file to be encrypted and generates a key (public) with that file. The public key is used to encrypt the data while private key is used to decrypt the file and sends to the receiver. It is more secured than symmetric operation.

11. What is the importance of a Key Management Plan (KMP)? Provide 2 paragraphs and include associated roles in key management

Strongest and the most secured Data Encryption requires Key Management Plan. Key management ensures data security if handled crucially. To secure your data, it is very important to manage your key you're sharing with the receiver.

Key Management Plan includes many roles, they are: - System Authority, who manages the level as the Chief Information Officer and manages overall security operation. Cryptographic Officer, manages overall cryptography modules. Key Custodian, uses designated keys to manage cryptographic modules.

References: -

<https://dis-blog.thalesgroup.com/security/2018/09/26/the-importance-of-key-management-when-implementing-a-secure-information-gateway/#:~:text=Strong%20data%20encryption%20requires%20encryption,risks%20posed%20by%20privileged%20users.>

<https://www.cryptomathic.com/news-events/blog/assignment-and-configuration-of-roles-in-a-crypto-key-management-system>