## Symmetrical vs Asymmetrical Encryption

## Symmetrical encryption.

**AES – Group Lab**

Withing each group team will consist from student facing each other in classroom.  
Check is openssl installed, if not install it using apt

Using same file from previous step encrypt file using AES

With your teammate agree on shared key.

Agree of key exchange method.

Each student should encrypt one message with unique content and share between each other.

Transfer files using network.

Decrypt files and see content.

Example of command

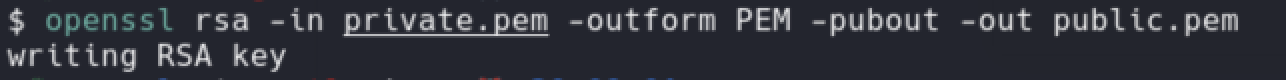
***openssl enc -aes-256-cbc -in file.txt -out file.enc***

## Asymmetric encryption

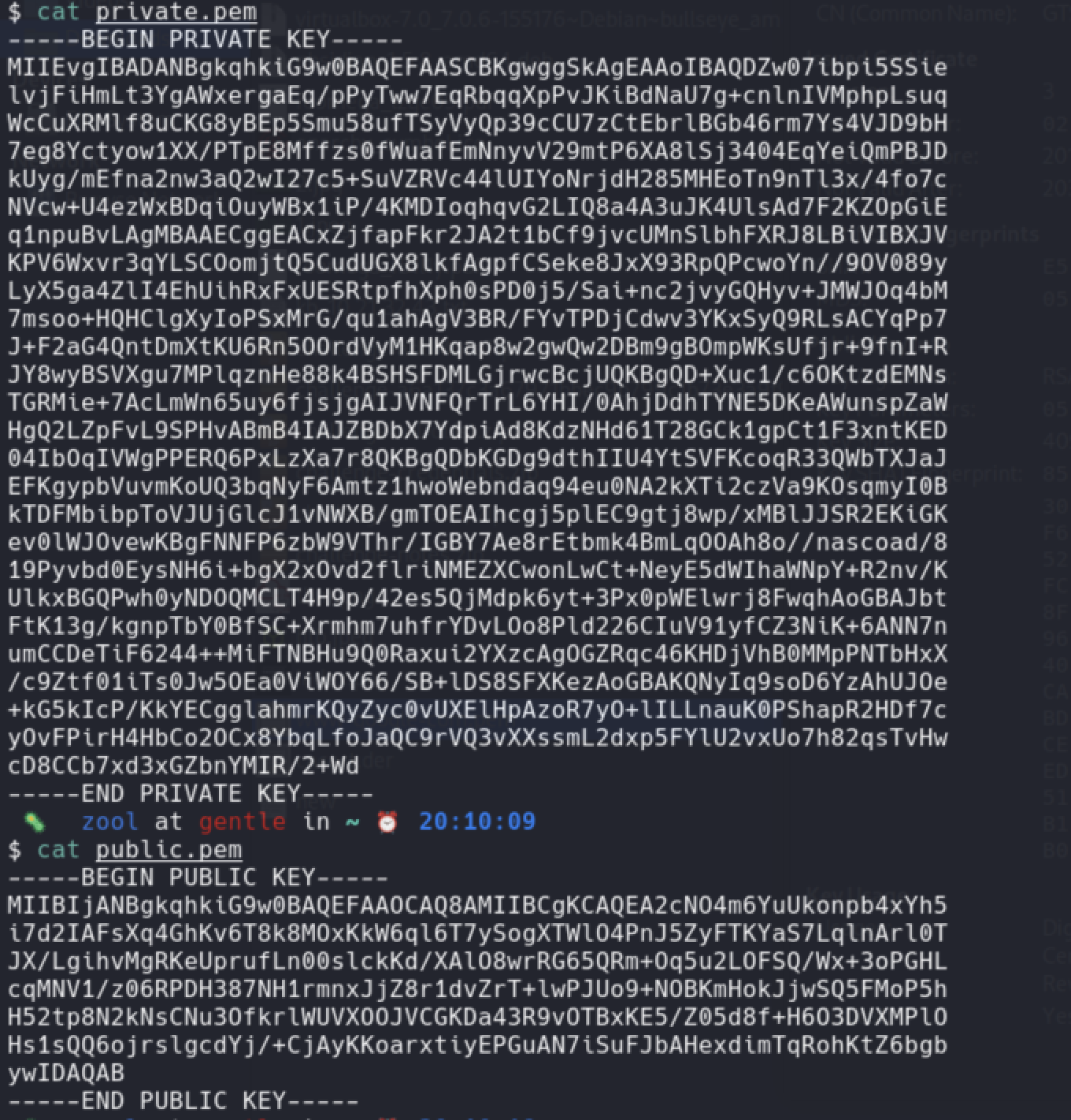
Generate an RSA private key, of size 2048, and output it to a file named priv.pem:

***openssl genrsa -out private.pem 2048***  
  
Extract the public key

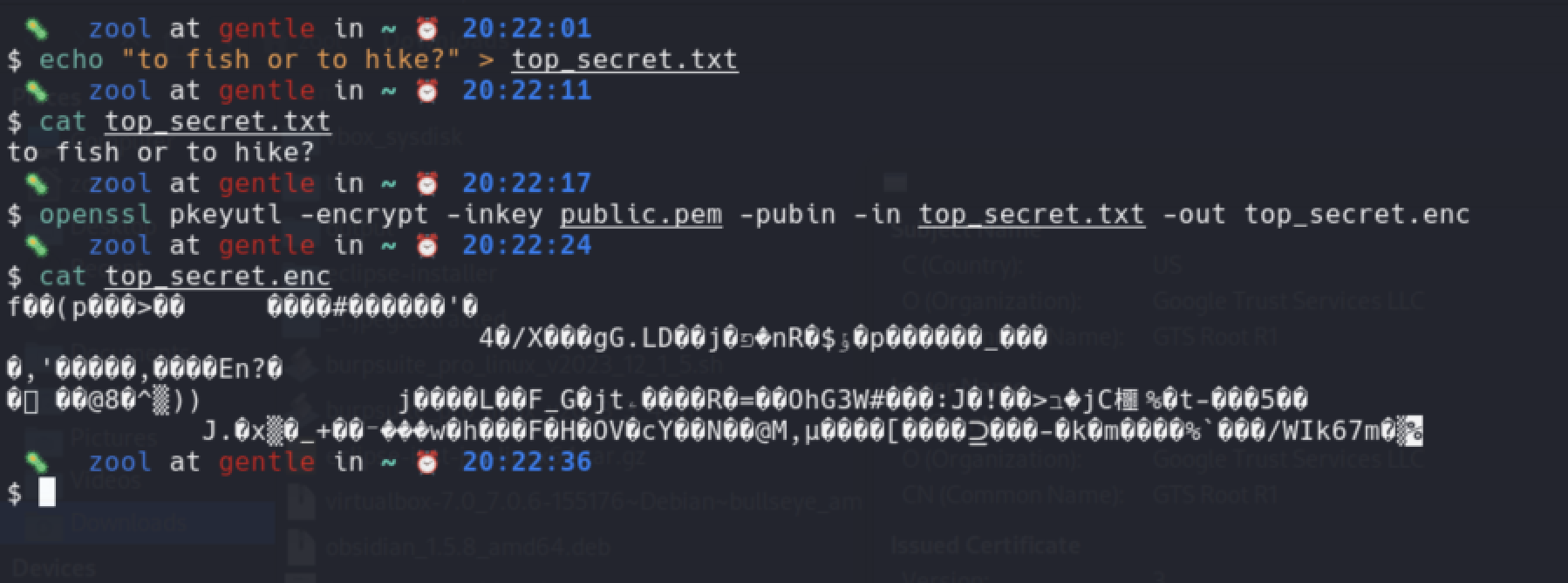
***openssl rsa -in private.pem -outform PEM -pubout -out public.pem***



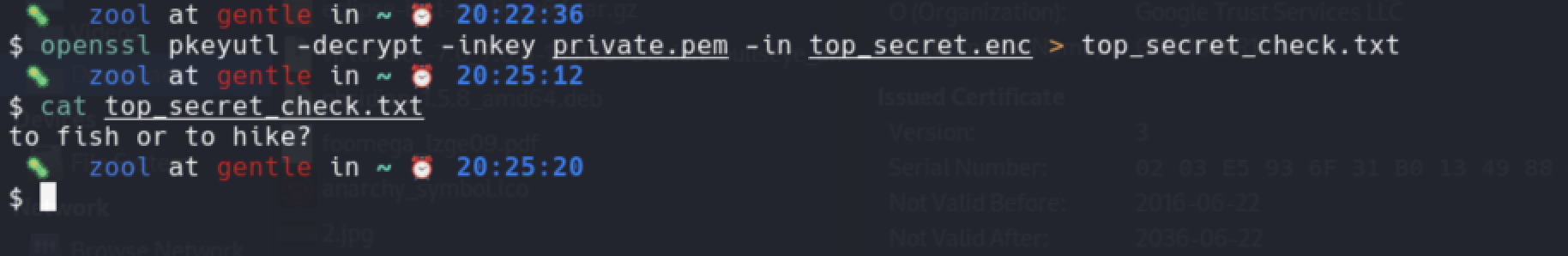
Let’s compare size of those keys.



## Encrypt data using private key:



Decrypt data using private key



## Group Task:

1. Generate RSA key pair and name them your\_name\_private and your\_name\_public
2. Exchange public keys with teammates
3. Encrypt message/file. using public key of 2 teammates
4. Exchange message/file.
5. Decrypt using private key.
6. Try to decrypt file you have encrypted with someone's public key with you r private key.