# CEGEP VANIER COLLEGE
# CENTRE FOR CONTINUING EDUCATION
# Cybersecurity
# 420- 950-VA

**Teacher: Samir Chebbine** **Lab 3** **Feb 05, 2025**

**Lab 3: Introduction to Cryptography & Nmap tool for Network Scanning**

Complete all these following sections as explained in **class.** All *steps* were presented during class time.

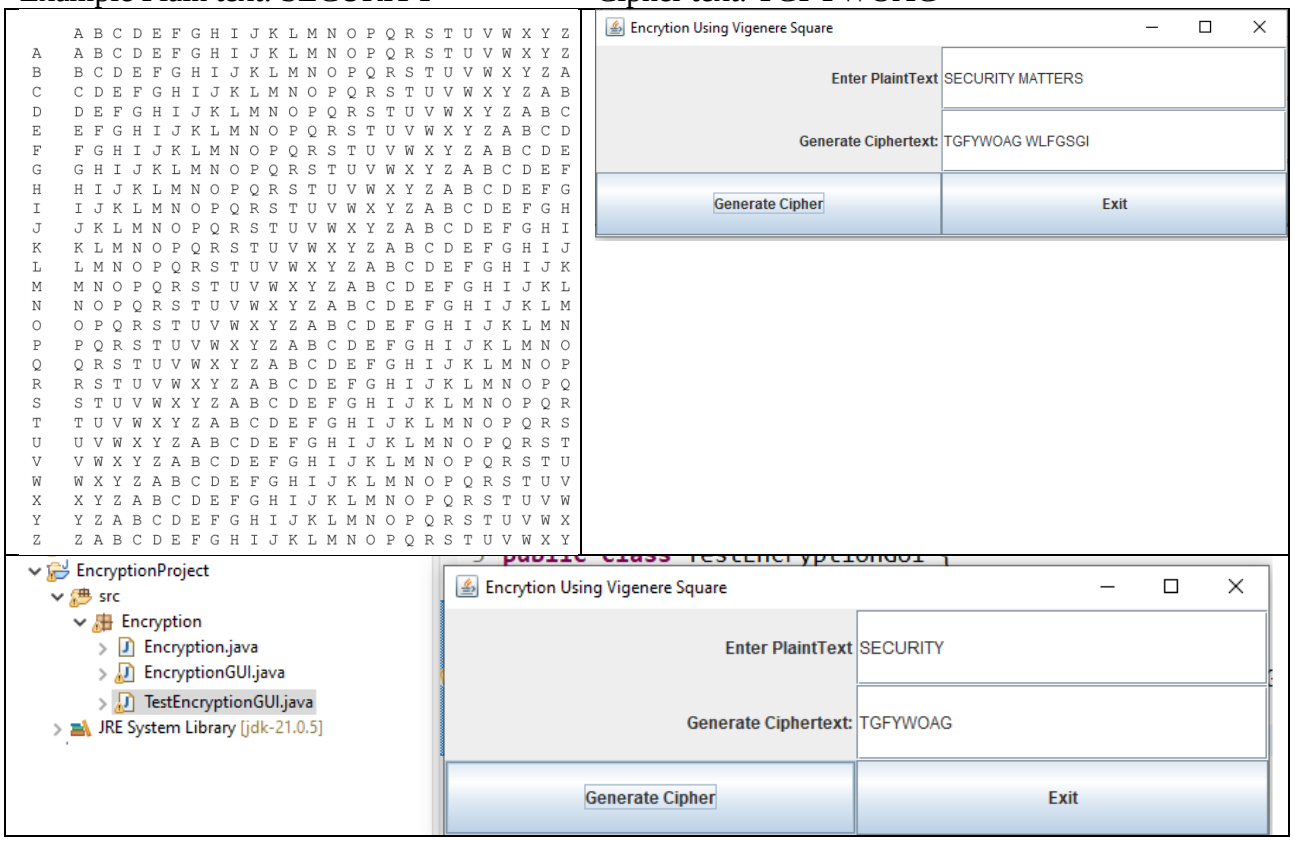
Create and Submit a Word file ***Lab3CybersecurityYourName.doc*** which contains answers of Book Exercises and output screenshots for every project. Submit all packet capture files if any.

1. **Cipher Methods:**

a) **Substitution Cipher Using Vigenere Square:** Using Vignere square, write a program to generate the cipher text of a given text using Vigenere square: Example of the following plain text "SECURITY" or "SECURITY MATTERS"

Encryption algorithm: starting in the first row and finding a substitute for the first letter of plaintext one position down, second row and finding a substitute for the second letter of plaintext two positions down and so on.

Example Plain text: SECURITY → Cipher text: TGFYWOAG



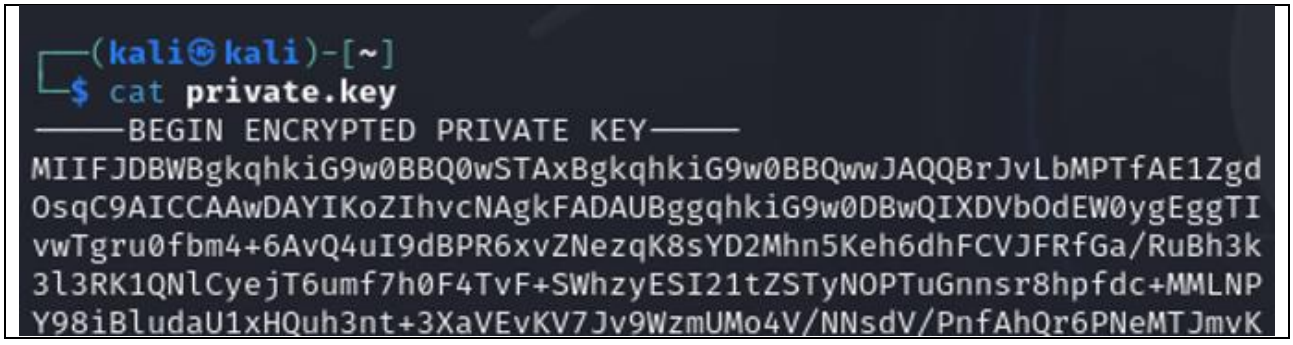

b) **Transposition Cipher:** Using the following transposition key pattern, find the cipher text of the following plain text "SECURITY MATTERS". No need to program this algorithm.
Key pattern: 1 →4, 2→8, 3→1, 4→5, 5→7, 6→2, 7→6, 8→3

2. **Asymmetric Cryptography:**

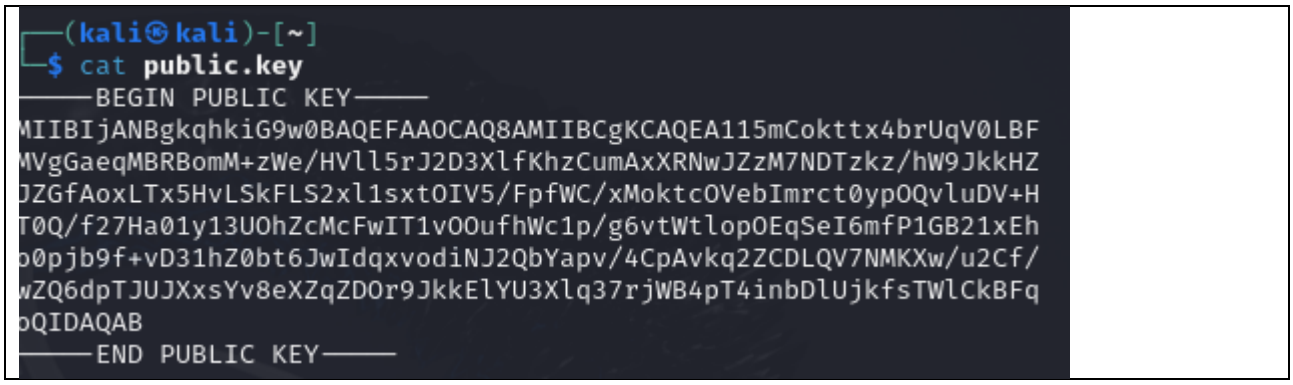
a) **Using RSA encryption and decryption:** Assume a sender would like to send the letter B to receiver. The sender will use the receiver combination public key (e=13, n=77) to encrypt the message. What is the value of ciphertext being sent?

b) The receiver would like to decrypt the message being sent using the combination private key (d=37, n=77). Demonstrate the decryption process to get the original plaint text message (in this case the letter B)

c) Using openssl tool in Kali Linux distribution, generate a private key in file private.key to be used in digital certificate as shown hereafter.




d) Using openssl tool in Kali Linux distribution, generate a public key in file public.key to be used in digital certificate as shown hereafter.




e) Using openssl tool in Kali Linux distribution, encrypt a text file called secret.txt using the generated public key as shown hereafter.


f) Using openssl tool in Kali Linux distribution, decrypt encrpted.txt file to a text file called plaitntext.txt using the generated private key as shown hereafter.

```
┌──(kali㉿kali)-[~]
└─$ cat plaintext.txt
Hello World
from Vanier College

┌──(kali㉿kali)-[~]
└─$ diff secret.txt plaintext.txt

┌──(kali㉿kali)-[~]
└─$
```

g) Using openssl tool in Kali Linux distribution, generate a digital certificate to be used in secure HTTP communication on port 443 encrypting data transmitted between your website and users' browsers as shown hereafter.

```
Enter pass phrase for private.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:Quebec
Locality Name (eg, city) []:Montreal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Vanier College
Organizational Unit Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:Samir
Email Address []:

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    encrypted.txt  Pictures    Public      samir.crt   Videos
Documents  kali-anonsurf  plaintext.txt  public.key  secret.txt
```

h) Probe any web site ()in this case www.bankofamerica.com) to get information about SSL and TLS protocol connections being used as shown hereafter.

```
  Server Key Exchange Group(s):
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  128 bits  x25519

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  www.bankofamerica.com
Altnames: DNS:www.bankofamerica.com, DNS:mobile.bankofamerica.com, DNS:smallbusinesso
nlinecommunity.bankofamerica.com, DNS:chatui.ml.com, DNS:chatui.merrill.com, DNS:chat
ui.merrilledge.com
Issuer:   Entrust Certification Authority - L1M

Not valid before: Jun 25 14:17:30 2024 GMT
Not valid after:  Jul 25 14:17:29 2025 GMT

┌──(kali㉿kali)-[~]
└─$
```

**3. Nmap tool for Network Scanning: Provide screenshot of every nmap command.**

a) Scan amazon web site to get the list of ports being open as shown hereafter in Figure.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-04 16:50 EST
Nmap scan report for www.amazon.com (54.230.51.91)
Host is up (0.0062s latency).
Other addresses for www.amazon.com (not scanned): 2600:9000:215f:d800:7:49a5:5fd4:b12
1 2600:9000:215f:be00:7:49a5:5fd4:b121 2600:9000:215f:1800:7:49a5:5fd4:b121 2600:9000
:215f:2200:7:49a5:5fd4:b121 2600:9000:215f:a600:7:49a5:5fd4:b121 2600:9000:215f:9a00:
7:49a5:5fd4:b121 2600:9000:215f:c000:7:49a5:5fd4:b121 2600:9000:215f:2e00:7:49a5:5fd4
:b121
rDNS record for 54.230.51.91: server-54-230-51-91.yul62.r.cloudfront.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

b) Save valid IP addresses of computers used in your network within text file called target.txt (at least two IP addresses) and use namp to scan them specifying file name in the command line as shown hereafter.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-04 20:28 EST
Nmap scan report for cloudproxy10117.sucuri.net (192.124.249.117)
Host is up (0.011s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.81.130
Host is up (0.000016s latency).
All 100 scanned ports on 192.168.81.130 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 2 IP addresses (2 hosts up) scanned in 2.00 seconds
```

c) Scan Vanier College web site to get the list of ports 20 to 25 and ports 80 and 443 being used as shown hereafter in Figure.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-04 20:32 EST
Nmap scan report for www.vaniercollege.qc.ca (192.124.249.117)
Host is up (0.0091s latency).
rDNS record for 192.124.249.117: cloudproxy10117.sucuri.net

PORT    STATE    SERVICE
20/tcp  filtered ftp-data
21/tcp  filtered ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
24/tcp  filtered priv-mail
25/tcp  filtered smtp
80/tcp  open     http
443/tcp open     https

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```