Topic	Cryptography	
Class Description	**Students will be able to understand about cryptography, techniques used in Cryptography**	
Class	**C-227**	
Class time	**45 mins**	
Goal	● Understand about Cryptography & Cryptanalysis ●	
Resources Required	● Teacher Resources: ○ Laptop with internet connectivity ○ Earphones with mic ○ Notebook and pen ○ Visual Studio Code ● Student Resources: ○ Laptop with internet connectivity ○ Earphones with mic ○ Notebook and pen ○ Visual Studio Code	
Class structure	**Warm-Up** **Teacher - led Activity 1** **Student - led Activity 1** **Wrap-Up**	**10 mins** **10 mins** **20 mins** **5 mins**

WARM UP SESSION - 10mins	
Teacher Action	**Student Action**
Hey <student's name>. How are you? It's great to see you! Are you excited to learn something new today? Okay, so you remember what we did in the last session? Great! Any doubts from last session?	**ESR**: Hi, thanks, yes, I am excited about it!

The teacher clarifies doubts (if any)	
Q&A Session	
Question	**Answer**
Which statement is true about virus? A. Malicious code B. Python code C. Spread from one device to another D. All of the above	**D**
Which one is not a computer virus? A. Worms B. Trojan C. Corona D. None of the above	**C**
TEACHER-LED ACTIVITY - 10mins	
Teacher Initiates Screen Share	
ACTIVITY • **Socket & Client Connection** • **Get screen size** • **Call the function**	
Teacher Action	**Student Action**
Any idea what we will be doing in today's session? So are you enjoying this ethical hacking module? Let's start class with one trick!	**ESR** Yes!

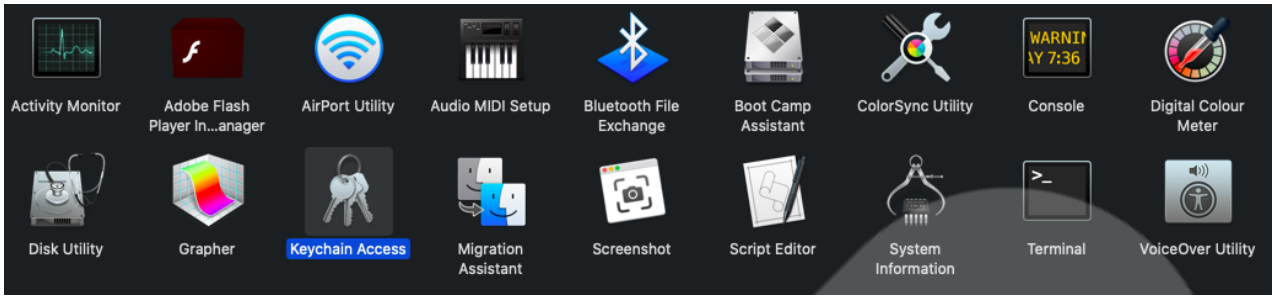
Do you want to learn that trick! What if I tell you the trick to get all the passwords of Wi-Fi? You want to learn how we can do that!	**ESR** Yes! **ESR** Yes!
Open the Terminal/command Prompt Type : ***netsh wlan show profile*** *It will display all the connected Wi-Fi* *Now Select the name of one Wi-Fi and get the password* *netsh wlan show profile name=WifiConnectionName key=clear* *Use Wi-Fi name here*	

```
User profiles
-------------
    All User Profile     : Tamy
    All User Profile     : WR3005N3-757E
    All User Profile     : Galaxy M31D974
    All User Profile     : MyNetwork
    All User Profile     : Palava WIFI
    Current User Profile : cityhomes
```

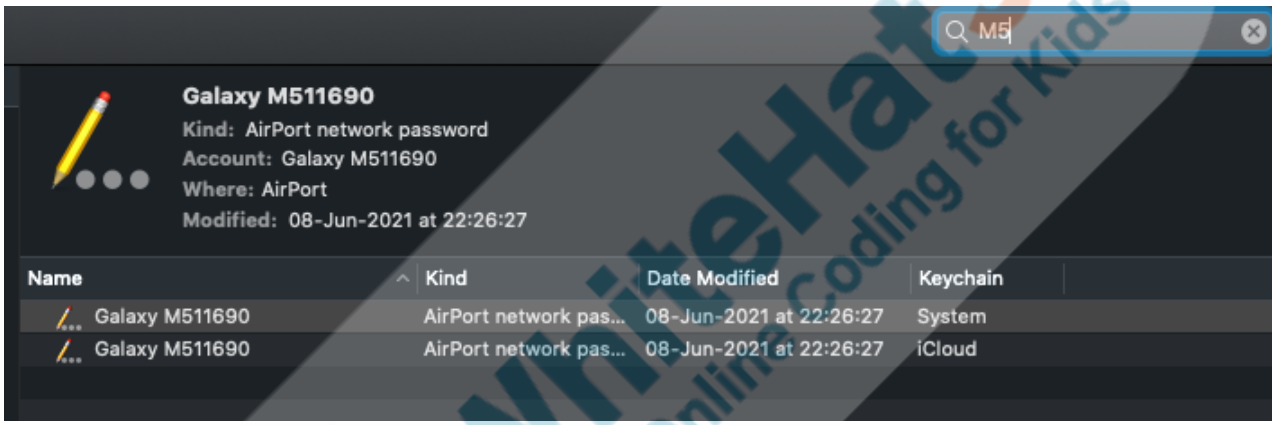
```
C:\Users\User>netsh wlan show profile name=WR3005N3-757E key=clear

Profile WR3005N3-757E on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                 : 1
    Type                    : Wireless LAN
    Name                    : WR3005N3-757E
    Control options         :
        Connection mode     : Connect automatically
        Network broadcast   : Connect only if this network is broadcasting
        AutoSwitch          : Do not switch to other networks
        MAC Randomization   : Disabled

Connectivity settings
---------------------
    Number of SSIDs         : 1
    SSID name               : "WR3005N3-757E"
    Network type            : Infrastructure
    Radio type              : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication          : WPA2-Personal
    Cipher                  : CCMP
    Authentication          : WPA2-Personal
    Cipher                  : GCMP
    Security key            : Present
    Key Content             : 70029949
```

To access saved WiFi passwords on Mac:

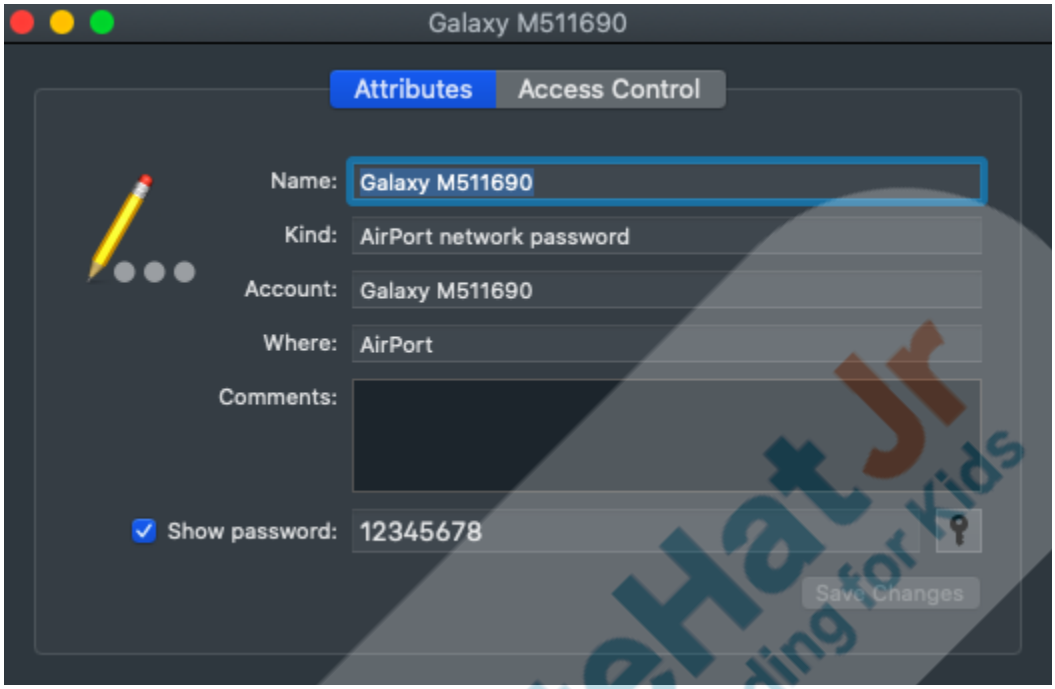
- Go to Applications>Utilities folder>Keychain Access app



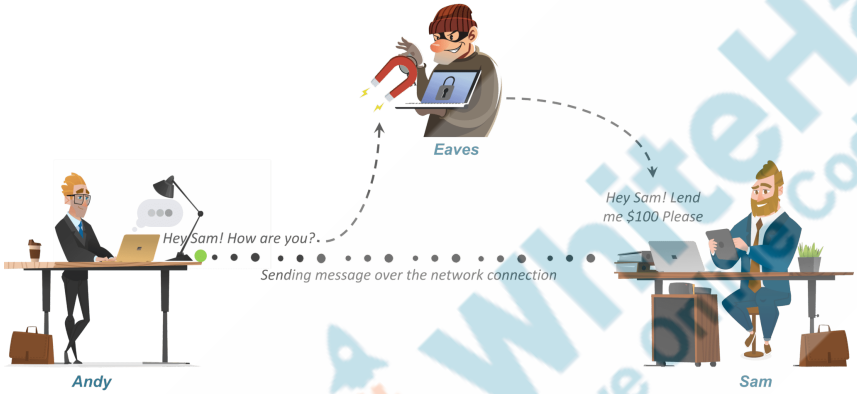
- Search for the WiFi name



Double click on it and check the show password box below

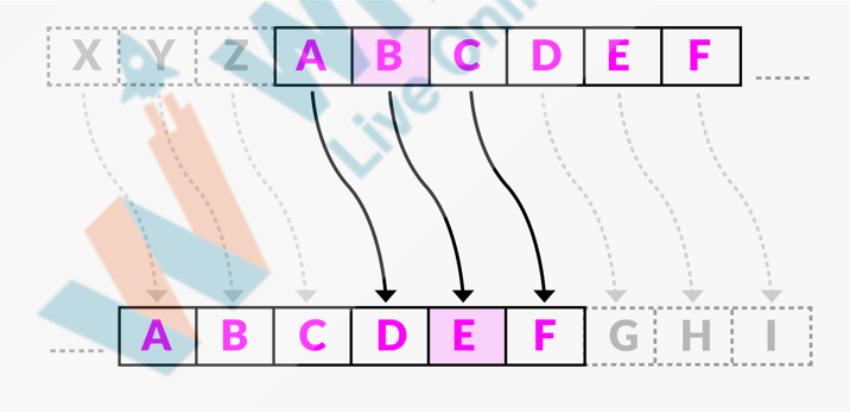


So, how it's easy to get the passwords Don't you think it should be in an unreadable format so no one will be able to read it! Ok,let's try to get solution for the same	**ESR** Yes!
Do you have any secrets? With whom you share your secrets? You know, I have lot of secrets and i do share my secret everyone Now you must be wondering how it would be secret if i am sharing with everyone Right !	**ESR:** Varied! **ESR:** Varied! **ESR**

Actually, I usually speak in secret codes. If somebody has the same secret code, then they can understand my secrets; otherwise, they can't! Isn't fun! Let's understand with this one example Let's say there's a person named ***Tammy***. Now suppose ***Tammy*** sends a message to his friend ***Sana*** who is on the other side of the world. It's clear that she wants this message to be private, and no one else should be able to see it. Usually, she uses WhatsApp for sending this message. The main goal is to secure this communication.  Let's say there is a smart guy called ***Diana*** who secretly got access to your communication channel. Since this guy has access to your communication, for example, he can try to change the message. Now, this is just a small example. What if *Diana* gets access to your private information? The result could be dangerous So how can ***Tammy*** be sure that nobody in the middle could access the message sent to *sana*? That's where *r* ***Cryptography*** comes in. Let me tell you " What is **Cryptography"**? Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.	**Varied!** **ESR** Varied! **ESR** Varied!

So, to protect her message, ***Tammy*** first converts her readable message to unreadable form. Here, she converts the message to some random numbers, symbols,and maybe letters. **Encryption** is the process of converting information into a form that is not readable by humans.The encrypted information is known as a **ciphertext** **Tammy** sends this ***ciphertext*** or **encrypted message** over the communication channel, she won't have to worry about somebody in the middle of discovering her private messages. Suppose, ***Diana*** here discovers the message and she somehow manages to alter it before it reaches *Sam*. Now, ***Sana*** would need a key to ***decrypt*** the message to recover the original plaintext. In order to convert the ***ciphertext*** into ***plain text,*** *Sana* would need to use the decryption key. Using the key she would convert the ciphertext or the numerical value to the corresponding plain text. **Decryption** is done using a secret key, which is only known to the recipients of the information. A key is required to decrypt the hidden messages. By doing so, even if a hacker obtains the information, it will no longer make sense to them. Now, for encryption and decryption we have different techniques. **Symmetric key algorithms (Private key cryptography):** A symmetric encryption is one that uses the same key to encrypt and decrypt data. One example of this is the Caesar Cipher. **Asymmetric key algorithms (Public key cryptography)**	**ESR** Varied!

Each party has a private key (kept secret) and a public key (known to all). These are used in the following way: ● Public keys are used for encrypting, Private keys are used for decrypting. **For example**: to send something encrypted to a party A, use its public key and send the encrypted data. Since only that party B has the corresponding private key, only that party can decrypt it. This type of cryptography is used in ***whatsapp, facebook, zoom etc.***	
Open the Teacher Activity 1	*Student opens the Student Activity 1*
Today we are going to learn one of the encryption technique ie ***"Caesar cipher"*** or **"shift cipher"** But Before that we must know about "***ASCII"*** Codes Can you tell me what "***ASCII"*** *codes are?* ***The American Standard Code for Information Interchange (ASCII)*** is a character encoding standard for text files in computers and other devices. The ***ASCII*** character set consists of 128 symbols and is a subset of Unicode. The symbols consist of letters (both uppercase and lowercase), numbers, punctuation marks, special characters, and control characters. In the character set, each symbol can be represented by a Decimal value ranging from 0 to 127, as well as equivalent Hexadecimal and Octal values. Means letter A has some ***ASCII*** value and small letter a has different ***ASCII*** value an space has some other value	***ESR*** *Varied!*
Open the Teacher Activity 2	*Student opens the Student Activity 2*

Now i will ask the ascii codes, you need to tell me the the decimal number for the same and then later on we will work convert this decimal into binary	
Now we know about ASCII codes **Let's learn how this *caesar cipher technique works*** In Caesar, each letter of each text is replaced by a letter with a fixed number of alphabetical positions down. For example with a shift of 1, A would be replaced by B, B would become C, and so on Thus to cipher a given text we need an integer value, known as shift which indicates the number of positions each letter of the text has been moved down. When all this is done, we need to convert all characters into ASCII first and then vice versa	
	
Now lets Create one function ***main()*** which will ask for user input which function want to perform encryption , decryption ● Print ("Choose one option) ● Initialize variable ***choice*** which will ask for input	

encryption decryption

- If choice = =1 , perform ***encryption***
- If choice ==2 perform ***decryption***
- Else print(**“wrong choice”**)

```
def main():
    print()
    print("Choose one option")
    choice = int(input("1. Encryption\n2. Decryption\nChoose(1,2): "))
    if choice == 1:
        encryption()
    elif choice == 2:
        decryption()
    else:
        print("Wrong Choice")
```

Teacher Stops Screen Share

STUDENT-LED ACTIVITY - 20 mins

- **Ask the student to press the ESC key to come back to the panel.**
- **Guide the student to start Screen Share.**
- **The teacher gets into Full Screen.**

ACTIVITY

- **Student will perform the symmetric Algorithm**
- **Student will perform the asymmetric Algorithm**

Teacher Action	Student Action
Guide the student to get the boilerplate code from Student Activity 2	*Student clones the code from Student Activity2*
As a next step, we will take the input messages from the user and then use the ***ord()*** function to convert the characters into ASCII codes. Total ***ASCII*** value characters is 126 , it will convert every character into ***ASCII*** value	

ShowASCII table to student in *student activity 2* Create function name **encryption()** ● Print ***("encryption")*** ● Variable ***msg*** which will save input from user ● Variable ***key*** will save required shift range from (1-94) from user ● Use for loop and check the length of the ***"msg"*** ● Create variable temp , which will storeASCII value of character. ***ord()*** function returns the Unicode code from a given character. This function accepts a string of unit length as an argument and returns the Unicode equivalence of the passed argument. ● If temp is greater than 126, 126 are total no of ***ASCII*** characters then check the user input number which is store in temp subtract 127 and add 32 shift ● Create variable ***encrypted_text*** which will store temp value after converting into character again The ***chr()*** method returns a string representing a character whose Unicode code point is an integer ● print ***("encrypted text")*** ● Call the main function	

```python
def encryption():
    print("Encryption")
    msg = input("Enter your message: ")
    key = int(input("Enter key(1-94): "))  # based on 26 letters of alphabet

    encrypted_text = ""

    for i in range(len(msg)):
        temp = (ord(msg[i]) + key)
        if(temp > 126):
            temp = temp - 127 + 32

        encrypted_text += chr(temp)

    print("Encrypted: " + encrypted_text)

    main()
```

As a next step, we will take the input messages from the user and then use the ***ord()*** function to convert the characters intoASCII codes. TotalASCII ***value characters*** is 126 , it will convert every character intoASCII value

ShowASCII table to student in student activity 2

Create function name **decryption()**

- Print ***("decryption")***
- Variable encryp_***msg*** which will save encrypted value which user want to decrypt
- Variable ***decryp_key*** will save required shift range from (1-94) from user
- Use for loop and check the length of the ***"encryp _msg"***
- Create variable temp , which will storeASCII value of character. ***ord()*** function returns the Unicode code from a given character and then subtract the same shift value i.e decrypt_key
- If temp is less than 32, check the user input number

which is store in temp add 127 and subtract 32 shift

- Create variable ***decrypted_text*** which will store temp value after converting into character again
  The ***chr()*** method returns a string representing a character whose Unicode code point is an integer.

- print ***("decrypt text")***

```
def decryption():

    print("Decryption")

    print("Message can only be Lower or Uppercase alphabet")
    encrp_msg = input("Enter encrypted Text: ")
    decrp_key = int(input("Enter key(1-94): "))

    decrypted_text = ""

    for i in range(len(encrp_msg)):
        temp = (ord(encrp_msg[i]) - decrp_key)
        if(temp < 32):
            temp = temp + 127 - 32

        decrypted_text += chr(temp)

    print("Decrypted Text: " + decrypted_text)
```

Call the main loop

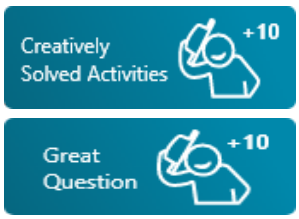
```
if __name__ == "__main__":
    main()
```

Teacher Guides Student to Stop Screen Share

WRAP UP SESSION - 5 Mins

Quiz time - Click on in-class quiz

Question	Answer
What is cryptography?	**D**

A. Technique to protect information B. Technique of securing information and communications C. Data Privacy D. All of the above	
What is the use of **ord()**? A. converts a character into its Unicode code value B. Act as a intilizarer C. Act as a constructor D. None of the above	**A**
What is the use of **chr()**? A. Act as a constructor B. converts a Unicode into its character value C. Act as a intilizarer D. All of the above	**B**
End the quiz panel	
FEEDBACK • **Appreciate the students for their efforts in the class.** • **Ask the student to make notes for the reflection journal along with the code they wrote in today's class.**	
Teacher Action	**Student Action**
You get Hats off for your excellent work! In the next class	*Make sure you have given at least 2 Hats Off during the class for:* 

	Strong Concentration +10
Project Discussion Jeff needs to go outside in order to accomplish some important tasks. There are some folders on his computer that he does not want to share with anyone except her mother. So he wants to lock the particular folder with some message. He wants to convert that message into encrypted form before going outside with a key so that no one can open them. In case of emergency, her mother can decrypt it by using the same key that he will share with her before going outside.	
Teacher Clicks	✖ End Class
ADDITIONAL ACTIVITIES	
Additional Activities	*The student uses the markdown editor to write her/his reflections in the reflection journal.*

ACTIVITY LINKS		
Activity Name	**Description**	**Link**
Teacher Activity1	Caesar Cypher	https://en.wikipedia.org/wiki/Caesar_cipher

Teacher Activity 2	Ascii code	https://www.techonthenet.com/ascii/chart.php
Teacher Activity 3	Reference Code	https://github.com/pro-whitehatjr/Pro-C227-ReferenceCode
Student Activity 1	Caesar Cypher	https://en.wikipedia.org/wiki/Caesar_cipher
Student Activity 2	Ascii Code	https://www.techonthenet.com/ascii/chart.php
Student Activity 3	Boilerplate Code	https://github.com/pro-whitehatjr/Pro-C227-StudentBoilerCode