**PRACTICAL -10**

**Aim : Implement a digital signature algorithm**.

def euclid(m, n):

if n == 0:

return m

else:

r = m % n

return euclid(n, r)

def exteuclid(a, b):

r1 = a

r2 = b

s1 = int(1)

s2 = int(0)

t1 = int(0)

t2 = int(1)

while r2 > 0:

q = r1//r2

r = r1-q \* r2

r1 = r2

r2 = r

s = s1-q \* s2

s1 = s2

s2 = s

t = t1-q \* t2

t1 = t2

t2 = t

if t1 < 0:

t1 = t1 % a

return (r1, t1)

p = 823

q = 953

n = p \* q

Pn = (p-1)\*(q-1)

key = [ ]

for i in range(2, Pn):

gcd = euclid(Pn, i)

if gcd == 1:

key.append(i)

e = int(313)

r, d = exteuclid(Pn, e)

if r == 1:

d = int(d)

print("decryption key is: ", d)

else:

print("Multiplicative inverse for\

the given encryption key does not \

exist. Choose a different encryption key ")

M = 19070

S = (M\*\*d) % n

M1 = (S\*\*e) % n

if M == M1:

print("As M = M1, Accept the\

message sent by Alice")

else:

print("As M not equal to M1,Do not accept the message sent by Alice ")

**OUTPUT:**

A close-up of a message

Description automatically generated



**PRACTICAL -11**

**Aim : Perform various encryption-decryption techniques with cryptool.**

**Solution:**

Cryptool is a software tool that supports various encryption-decryption techniques, including symmetric key encryption, asymmetric key encryption, and hash functions. Here's a brief overview of each of these techniques:

**Symmetric key encryption:** In symmetric key encryption, the same key is used for both encryption and decryption of the data. Cryptool supports various symmetric key encryption algorithms such as AES, DES, Triple DES, and Blowfish.

**Asymmetric key encryption:** In asymmetric key encryption, two different keys are used for encryption and decryption. The public key is used for encryption, and the private key is used for decryption. Cryptool supports various asymmetric key encryption algorithms such as RSA, ElGamal, and Diffie-Hellman.

**Hash functions:** Cryptool also supports various hash functions such as MD5, SHA-1, SHA-256, and SHA-512. Hash functions are used to create a fixed-size digest of the input data, which is used to verify the integrity of the data.

To use Cryptool, you can download and install it on your computer. Once installed, you can select the encryption-decryption technique you want to use, and then provide the input data to encrypt or decrypt. Cryptool will then generate the output data using the chosen encryption-decryption technique.

Please note that encryption-decryption techniques can be complex and require a thorough understanding of the underlying algorithms and security concepts. It's important to use encryption-decryption techniques responsibly and securely.

**Playfair Cypher using Cryptool**

The Playfair cipher is a polygraphic substitution cipher that encrypts pairs of letters instead of individual letters, making it more difficult to decrypt than a simple substitution cipher. In this cipher, a 5x5 matrix of letters is used to encrypt plaintext. Cryptool is a software tool that can be used to encrypt and decrypt messages using various ciphers, including the Playfair cipher.

Here are the steps to use Cryptool to encrypt and decrypt messages using the Playfair cipher:

Open Cryptool and select "Classic Ciphers" from the list of options.

Click on the "Playfair" cipher option to open the Playfair cipher window.

In the "Key" field, enter a keyword or phrase that will be used to generate the 5x5 matrix of letters. This keyword should contain all the letters of the alphabet except for "J", which is usually replaced with "I".

Enter the plaintext message you want to encrypt in the "Message" field. The plaintext message should only contain letters, and any spaces or punctuation should be removed.

Click on the "Encrypt" button to encrypt the message using the Playfair cipher. The encryptedmessage will be displayed in the "Cipher" field.

To decrypt a message using the Playfair cipher, enter the ciphertext message in the "Cipher" field and click on the "Decrypt" button. The decrypted message will be displayed in the "Message" field.

You can also experiment with different key phrases to see how they affect the encrypted message. Additionally, you can use Cryptool to perform frequency analysis and other techniques to break the Playfair cipher.

The Playfair cipher is a relatively simple cipher to use and understand, but it can be difficult to decrypt without the key phrase. Using Cryptool to encrypt and decrypt messages with the Playfair cipher can help you understand how it works and how it can be used for secure communication



**PRACTICAL -12**

**Aim : Study and use the Wireshark for the various network protocols.**

Wireshark is a powerful network protocol analyzer that allows you to capture and examine network traffic in real time. It supports a wide range of network protocols and can be used to troubleshoot network issues, detect security threats, and analyze network performance. Here are some steps to study and use Wireshark for various network protocols:

**Install Wireshark:** Wireshark is available for download on the official website for Windows, macOS, and Linux. After downloading and installing it, run the application.

**Select an interface**: Select the network interface that you want to capture traffic from. You can do this by going to Capture > Interfaces and selecting the appropriate interface.

**Start capturing:** Click on the "Start" button to start capturing network traffic on the selected interface. You will see a list of captured packets in real time.

**Filter packets:** Wireshark can capture a large amount of network traffic, so it's important to filter out the packets you are interested in. You can use display filters to filter packets by protocol, source or destination IP address, port number, or other criteria.

**Analyze packets:** Once you have captured and filtered the packets, you can analyze them to troubleshoot network issues or detect security threats. You can view detailed information about each packet, including the source and destination addresses, protocol, payload, and more.

**Decode protocols**: Wireshark supports a wide range of network protocols, and can decode the packets so you can see the data being transmitted. For example, if you are analyzing HTTP traffic, you can view the HTTP headers and data in the packet payload.

Save and export packets: You can save the captured packets for later analysis, or export them in various formats, such as pcap or CSV.

Some common protocols that you can study and use Wireshark for include:

**1. TCP/IP:** Wireshark is ideal for analyzing TCP/IP traffic, which is the foundation of the internet and most local area networks.

**2. HTTP:** Wireshark can capture and analyze HTTP traffic, which is used for web browsing and many other applications.

**3. DNS:** Wireshark can capture and decode DNS traffic, which is used to resolve domain names to IP addresses.

**4. FTP:** Wireshark can capture and analyze FTP traffic, which is used to transfer files over the internet.

**5. SMTP:** Wireshark can capture and analyze SMTP traffic, which is used for sending and receiving email.

