Cryptography

Cryptography is the science and practice of securing communication and information from adversaries or unauthorized third parties. It involves techniques for encoding messages or data in such a way that only authorized parties can access and understand them. The primary goals of cryptography are confidentiality, integrity, authentication, and non-repudiation.

There are several fundamental concepts and techniques in cryptography:

Encryption: This involves transforming plaintext (readable data) into ciphertext (unreadable data) using an encryption algorithm and a cryptographic key. The ciphertext can then be transmitted securely and decrypted back into plaintext by the intended recipient using the corresponding decryption algorithm and key.

Decryption: The process of converting ciphertext back into plaintext using a decryption algorithm and the appropriate key.

Cryptographic Keys: These are values used by encryption and decryption algorithms to transform data. Keys can be symmetric (the same key is used for both encryption and decryption) or asymmetric (different keys are used for encryption and decryption).

Symmetric Encryption: In symmetric encryption, the same key is used for both encryption and decryption. Popular symmetric encryption algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

Asymmetric Encryption: Also known as public-key cryptography, asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. The most common asymmetric encryption algorithms are RSA and ECC (Elliptic Curve Cryptography).

Hash Functions: Hash functions take an input (or 'message') and return a fixed-size string of bytes. They are used to ensure data integrity and to create digital signatures. Common hash functions include SHA-256 and MD5.

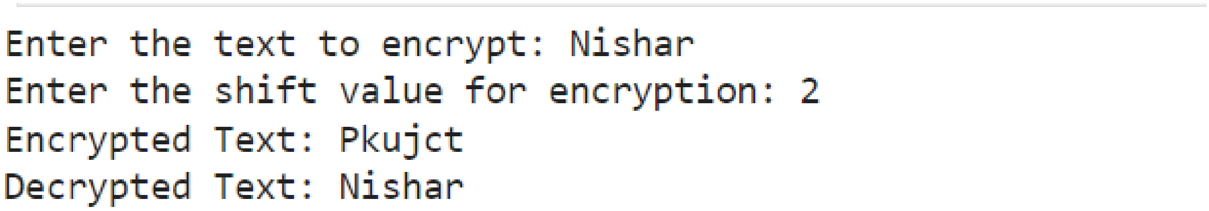
Digital Signatures: A digital signature is a cryptographic mechanism used to verify the authenticity and integrity of a message or document. It involves generating a unique digital signature using a private key that can be verified by anyone with access to the corresponding public key.

Cryptographic Protocols: These are sets of rules and procedures used to secure communication over a network. Examples include SSL/TLS (Secure Sockets Layer/Transport Layer Security) for secure web browsing and SSH (Secure Shell) for secure remote access.

Encryption/Decryption Python Program

```
def encrypt(text, shift):
    encrypted_text = ""
    for char in text:
        if char.isalpha():
            is_upper = char.isupper()
            char = chr(((ord(char) - ord('A' if is_upper else 'a') + shift) %
26) + ord('A' if is_upper else 'a'))
        encrypted_text += char
    return encrypted_text

def decrypt(encrypted_text, shift):
    return encrypt(encrypted_text, -shift)

def main():
    text = input("Enter the text to encrypt: ")
    shift = int(input("Enter the shift value for encryption: "))

    encrypted_text = encrypt(text, shift)
    decrypted_text = decrypt(encrypted_text, shift)

    print("Encrypted Text:", encrypted_text)
    print("Decrypted Text:", decrypted_text)

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

Output:



```
Enter the text to encrypt: Nishar
Enter the shift value for encryption: 2
Encrypted Text: Pkujct
Decrypted Text: Nishar
```