LEMUEL OKECHUKWU

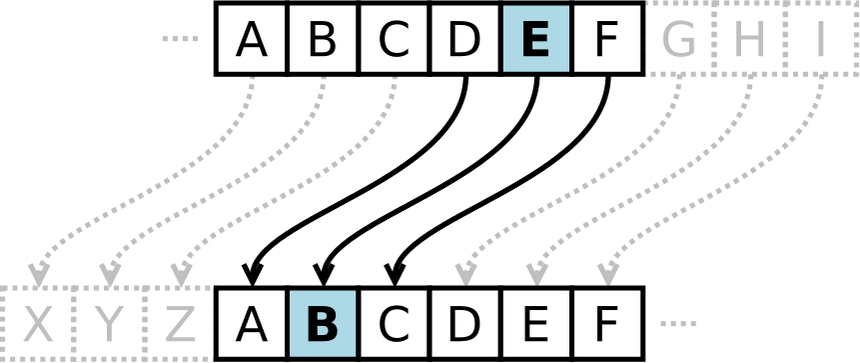
VEPH/20B/CY082

TASK 24A

CRYPTOGRAPHY DEMYSTIFIED AND PROTECTING YOUR DIDGITAL PRIVACY

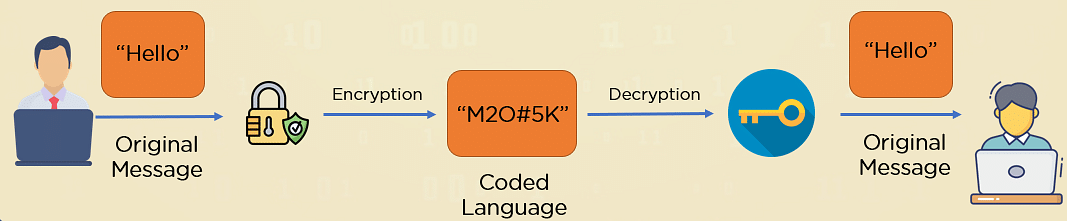
**TASK 24A:**

* **Describe the core functions of cryptography**
* **What role does the public and private key play in secure data exchanged. Explain the terms digital signature and digital certificate?**

[](https://en.wikipedia.org/wiki/Cryptography)

Today’s digital space has become flooded with doubts regarding the safety of personal information and privacy, in general. Some of these concerns have been taken care of, thanks to the adoption of cryptography and encryption. Cryptography is the science of encrypting or decrypting information to prevent unauthorized access. In cryptography, you transform data and personal information to make sure only the correct recipient can decrypt the message.

Digital signatures and digital certificates are security solutions that can secure your data from these cyber thieves. Information can be exchanged on an insecure network, such as the internet, securely and privately using PKI. To achieve this, PKI uses two key technologies: digital signatures and [digital certificates](https://www.encryptionconsulting.com/education-center/what-are-digital-certificates/) which are the key components in the [certificate authority](https://www.encryptionconsulting.com/education-center/what-is-a-certificate-authority/) trust model.



For want of time, we will delve into the world of cryptography where it deals with [Encryption](https://www.simplilearn.com/data-encryption-methods-article) which is a process of scrambling the information, to avoid third parties from comprehending the message even if it is intercepted. This scrambling is done using specific mathematical calculations and steps, often collectively known as ciphers. Along with the cipher, it uses an encryption key to encrypt the message. And also, the Decryption key, a process of reversing the work done by encryption. It converts the scrambled information into its original form so that the data is readable again. Usually, the encryption key which is used to scramble the data can decrypt the data, but that varies depending on the type of cryptography used.

The aim of modern cryptography is to provide specific security features that enable secure communications via an unsecured channel to prevent a third party from:

* eavesdropping,
* modifying the message content,
* or even usurping the identity of one of the two communicating entities.

Therefore, the 3 main purposes of modern cryptography are:

**Confidentiality**: The message must be comprehensible only to the recipient. If the content is intercepted, it must remain **unintelligible to any third party** who does not have the key to decipher it.

**Integrity**: The message must be protected against any attempt at modification by a third party. The recipient must be able to verify that the message **has not been altered** during transfer.

**Authenticity**: The recipient must be able to verify the **origin of the message**, in other words, be sure that the message actually comes from the person with whom they have established a communication channel, and not from a third party.

In secure data exchange, the public and private keys play crucial roles. The public key is used for encryption and verifying digital signatures, while the private key is used for decryption and creating digital signatures. This ensures that only the intended recipient can decrypt the data, and the authenticity of the sender can be verified.



Digital signatures and digital certificates are security solutions that can secure your data from these cyber thieves**.** Though these words are a bit similar, their synonyms and functions are completely different. Using cryptographic key technology, a digital signature is simply attached to an email or document. The same [hash algorithm](https://www.encryptionconsulting.com/education-center/encryption-vs-hashing/) is used by the signature to decrypt the message when it is received by the recipient.

The difference between a digital signature and a digital certificate can be judged from the below-mentioned factors.

#1. Basic Function:

* Digital signatures confirm the integrity of data and verify the authenticity of the document.
* Digital certificates verify the owner’s identity and enhance site trustworthiness.

#2. Process:

* The document on which the digital signature is done is encrypted by the sender and decrypted by the receiver, respectively. The same is done with the help of asymmetric keys.
* In the case of digital certificates, the [reliable Certificate Authority](https://www.clickssl.net/ssl-certificate-authorities) carries the entire procedure of verification, key generation, and issuance once the request for the same is received.

#3. Motto:

* Digital Signatures assure document authentication, data integrity, and non-repudiation.
* Digital certificates assure authentication, data confidentiality, and data integrity apart from site security.

#4. Issuance:

* Digital signatures are issued to specific individuals by authorized agencies.
* CAs issue digital certificates after verification of owner identity and business.

#5. Ensure:

* These signatures ensure that the signer can’t repudiate the document on which they have signed.
* These certificates ensure that the client and the browser communication stays secured with [encryption](https://www.clickssl.net/blog/what-is-encryption).

#6. Work On:

* The working of Digital signatures is based on Digital Signature Standard (DSS).
* The working of digital certificates is based on cryptographic keys and encryption securities.

Cybersecurity and encryption are tasks that require research, time, and effort in order to be effective.  Evolving from ancient ciphers to complex algorithms, it safeguards data in transit and at rest. The advent of tailored encryption services underscores the growing importance of robust cryptographic solutions in safeguarding sensitive information. Digital signatures and digital certificates are essential since one identifies the owner of the document, whereas one identifies the organization’s identity respectively. It does not matter whether SHA-1/SHA-2 algorithms are used or RSA is used; both these certificates’ tasks are commendable in the digital market.