LEMUEL OKECHUKWU

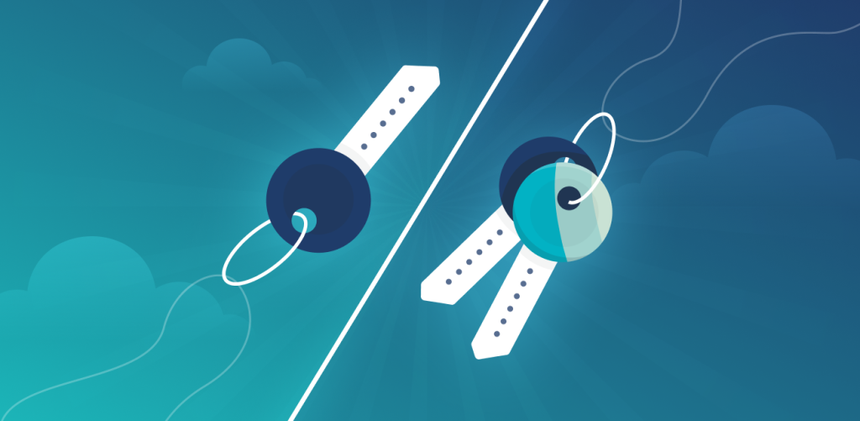
VEPH/20B/CY082

TASK 23A

**ENCRYPTION KEYS’ AND ITS ROLES**

**TASK 22A:**

* **Describe how symmetric and asymmetric encryption differ in terms of key management. Explain how encryption ensures confidentiality and what risks exist if key compromise occurs.**
* **What role does the public and private key play in secure data exchange? Explain the terms digital signature and digital certificate?**

[](https://surfshark.com/blog/symmetric-asymmetric-encryption)

Encryption as we all can infer is a way of hiding readable data in unreadable formats so only the receiver can decipher it. These could be done in lettering or picturesque form or mathematical formats that everyone and anyone cannot understand.

Also, we can understand that digital signature is a form of watermark used for authentication while a digital certificate is a file that verifies the identity of a holder.

**Symmetric Encryption** uses mathematical permutations to encrypt a plain text message. It also uses the same mathematical permutation, known as a key, to decrypt messages.

Importantly, the same plain text letter does not always come out the same in the encrypted message (e.g. “SSS” would not encrypt to three of the same characters), which makes it difficult to decode the encrypted message without the key.

Even though it’s difficult to decrypt messages without the key, the fact that this approach uses the same key for both encryption and decryption creates risk. Specifically, people (or technology) who want to correspond via symmetric encryption must share the key to do so, and if the channel used to share the key gets compromised, so does the entire system for sharing secure messages since anyone with the key can encrypt or decrypt those communications.

By today’s standards, symmetric encryption is a relatively simple cryptographic algorithm, however it was once considered state of the art and used by the German army in World War II.

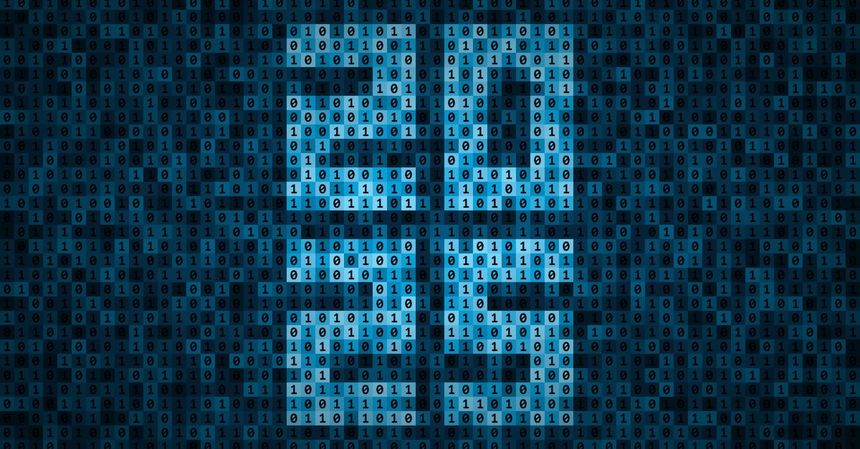
**Asymmetric Encryption** also uses mathematical permutations to encrypt a plain text message, but it uses two different permutations, still known as keys, to encrypt and decrypt messages. With asymmetric cryptography, a public key that can be shared with anyone gets used to encrypt messages while a private key that’s known only by the recipient gets used to decrypt messages.  How exactly does this all work? Let’s say Alice wants to send a private message to Bob. Bob can share his public key with Alice, which she then uses to encrypt her message. Once the message gets encrypted, only Bob’s private key can decrypt it. This means that as long as Bob ensures no one else has his private key, then no one can read the encrypted message.

 The question that comes to mind will be which of this approach is best suited for today’s world? That answer is that but both are still in use today — and many times they get used in tandem as the big trade-off that exist between them are security and speed.

While symmetric encryption boost of speed because the keys used are much shorter than they are in asymmetric encryption. Here only one key is used for encryption and decryption as against asymmetric encryption where the process of sharing messages is far less efficient, and it can also create performance issues as network processes get bogged down trying to encrypt and/or decrypt messages. This can result in slow processes, issues with memory capacity and fast drainage on batteries.

Second, we have security, where asymmetric encryption presents an advantage over symmetric encryption. Symmetric encryption carries a high risk around key transmission, as the same key used to encrypt messages must be shared with anyone who needs to decrypt those messages. Every time the key gets shared, the risk of interception by an unintended third party exists.

Asymmetric encryption offers better security because it uses two different keys — a public key which only gets used to encrypt messages, making it safe for anyone to have, and a private key to decrypt messages that never needs to be shared. Since the private key never needs to be shared, it helps ensure only the intended recipient can decrypt encoded messages and creates a tamper-proof digital signature.

[](https://www.globalsign.com/en/blog/certificate-authority-101-a-glossary-of-key-terms)

We delve into the space of digital signatures and certificates, where the former authenticates and the latter verifies the said data. They are forms of encryption tools used in bolstering the confidentiality outlook as they are Public Key Infrastructure.

**The private key** is used to digitally sign your Certificate Signing Request (CSR), and later to secure and verify connections to your server.

Your private key should be closely guarded, since anyone with access to it can readily break your encryption. (Note again that the private key is just a text file – however, it’s a really important text file and should be protected accordingly.)

If you lose your private key, or believe it was compromised in any way, SSL.com recommends “re-keying” your certificate. To rekey, you’ll create and submit a new CSR, and SSL.com will reissue your certificate using your new key pair

**The public key**, by contrast, is distributed as widely as possible – it’s included as part of your SSL certificate, and works together with your private key to make sure that your data is encrypted, verified and not tampered with during transport.

Anyone with access to your public key can verify that your message is authentic without having to know your secret private key. The SSL/TLS protocol uses a pair of keys – one private, one public – to authenticate, secure and manage secure connections. These keys are a linked pair of text files and are created together as a pair when you create your Certificate Signing Request (CSR).

Digital Certificates are electronic documents that are used to verify the identity of a person, organization, or device in online communication. Digital Certificates serve as digital identities, providing proof of identity to enable secure communication and data exchange. They are used to enable secure communication and data exchange in a variety of online applications, including e-commerce, online banking, and secure email communication.

The use of PKI and Digital Certificates is essential for secure online communication and data exchange, protecting against online threats such as phishing and man-in-the-middle attacks, and ensuring the integrity of online transactions.

[Certificate Type](https://www.ssl.com/category/certificate-type/), [S/MIME, Client, and Document Signing](https://www.ssl.com/category/certificate-type/s-mime-client-and-document-signing/), [SSL/TLS](https://www.ssl.com/category/certificate-type/ssl-tls/)

[SSL and Digital Certificates](https://www.ssl.com/tag/ssl/), [SSL/TLS](https://www.ssl.com/tag/ssltls/)