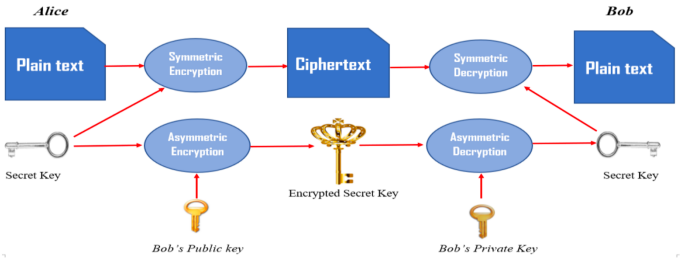
NOTE: How Hybrid cryptography works?

From slide 4, lectorial 7

Hybrid encryption

- How does it work?



Reference: Lai, J.-F. & Heng, S.-H., 2022. Secure file storage on cloud using hybrid cryptography. *Journal of Informatics and Web Engineering*, 1(2), pp.1-18. Available at: https://doi.org/10.33093/jiwe.2022.1.2.1 [Accessed 5 Sep. 2024].

- Key Generation (Asymmetric):
  - Each participant generates a pair of keys for asymmetric encryption: a public key, which can be shared with anyone, and a private key, which is kept secret.
- Encryption of Data (Symmetric):
  - The sender generates a random symmetric key, which is used only for the duration of the session.
  - The sender encrypts the data using this symmetric key with a symmetric encryption algorithm (like AES), which is fast and efficient for large am ounts of data.
- Encryption of Symmetric Key (Asymmetric):
  - The sender encrypts the symmetric key using the recipient's public key. Since only the recipient's private key can decrypt this, the symmetric key is securely transmitted.
- Transmission of Encrypted Data:
  - Both the encrypted data and the encrypted symmetric key are sent to the recipient.
- Decryption of Symmetric Key (Asymmetric):
  - The recipient uses their private key to decrypt the symmetric key.

- Decryption of Data (Symmetric):
    - The recipient uses the decrypted symmetric key to decrypt the data encrypted in step 2.
- (Optional) Verification:
    - If integrity and authenticity need to be ensured, digital signatures and hash functions may be used in addition to encryption. The sender can sign the message or its hash using their private key, which the recipient can verify using the sender's public key.