# Information Security

Momina Atif Dar P18-0030

Section A

According to the scenario stated in the question, let's suppose A and B are two offices that wish to exchange confidential data with each other, or A office has some employees who are authorized to see the data, but the rest are not.

*Assumption: A and B both have their Public and Private key pair generated using RSA.*

**Encryption side: (A's side)**

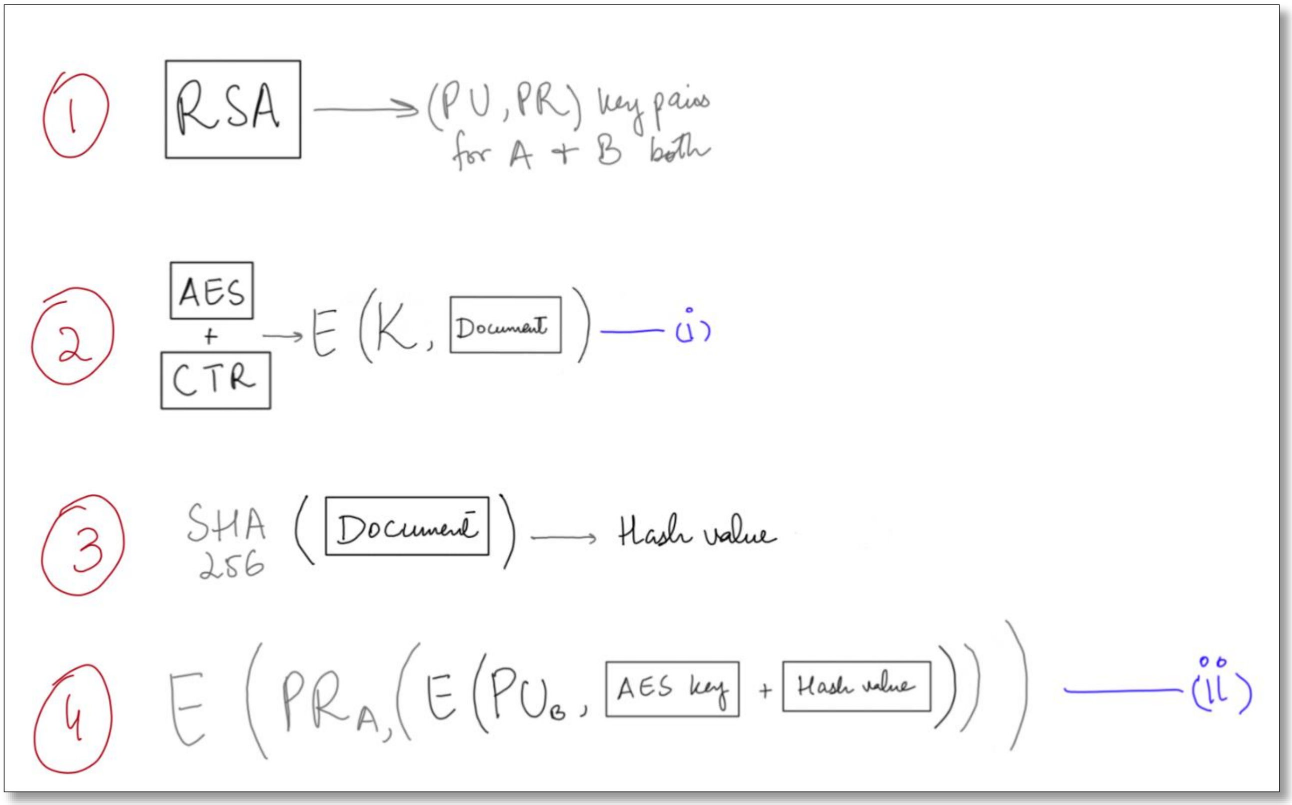
I suggest encrypting confidential data with the AES encryption algorithm because it's a safe option and is prone to many attacks. Before encryption, A office should calculate the Hash value of each document using SHA256 to ensure that nobody alters the contents of documents. With AES, I choose Counter Mode Operation (CTR) to enhance the effectiveness of encryption. CTR is considered for its hardware and software efficiency and the counters can run in parallel which makes it fast, and any counter can be accessed separately. After this, A should encrypt the AES key used to encrypt data and Hash value using A's private key and then using B's public key. Encryption with A's private key will ensure Digital Signature (authenticity) and B's public key will ensure information security (confidentiality). Now, A is sending two types of encrypted data; private documents encrypted with AES and a [key + hash value] encrypted with public-private keys.

*Assumption: B already knows the Hash function and already has the public key of A.*

**Decryption side: (B's side)**

B received the data and decrypts the [key + hash value] data using A's public key first and then using its own private key – confidentiality and authentication are ensured. Now, B has AES secret key and hash function. Using that AES secret key B decrypts the documents.

*P.S. Diagram on next page*



1 $\boxed{\text{RSA}} \longrightarrow (PU, PR)$ key pairs for A + B both

2 $\boxed{\text{AES}} + \boxed{\text{CTR}} \longrightarrow E\left(K, \boxed{\text{Document}}\right)$ — (i)

3 SHA 256 $\left(\boxed{\text{Document}}\right) \longrightarrow$ Hash value

4 $E\left(PR_{A}, \left(E\left(PU_{B}, \boxed{\text{AES key}} + \boxed{\text{Hash value}}\right)\right)\right)$ — (ii)

*(i) And (ii) are communicated to B (receiver)*