ASSIGNMENT 3 : INFORMATION SECURITY
Cyber Laws of Pakistan

SYED ASAD ZAMAN
p180034@nu.edu.pk

When it come to the security of information three key aspects are considered:

- Data Integrity
- Data Confidentiality
- Authentication

In the scenario given these three aspects of security can be implemented as the data is confidential and it can only be seen & verified by the intended users only.

1 PUBLIC & PRIVATE KEY CRYPTOGRAPHY

In order to acheive the data confidentiality public key cryptography will be used. As the information in this scenario can only be read by the specific users only so in that case the public cryptography is handy to used. Another challenge in the scenario given is to insure the information exchange in between the two parties doesn't lose its integrity. Here the concept of digital signature came into play. In this concept when sender send a message it signed it with its digital signature which is the verified by the receiver. If the information is tampered in between the communication the digital signature will also be change and hence the data can be verified that whether it is from the intended sender or not

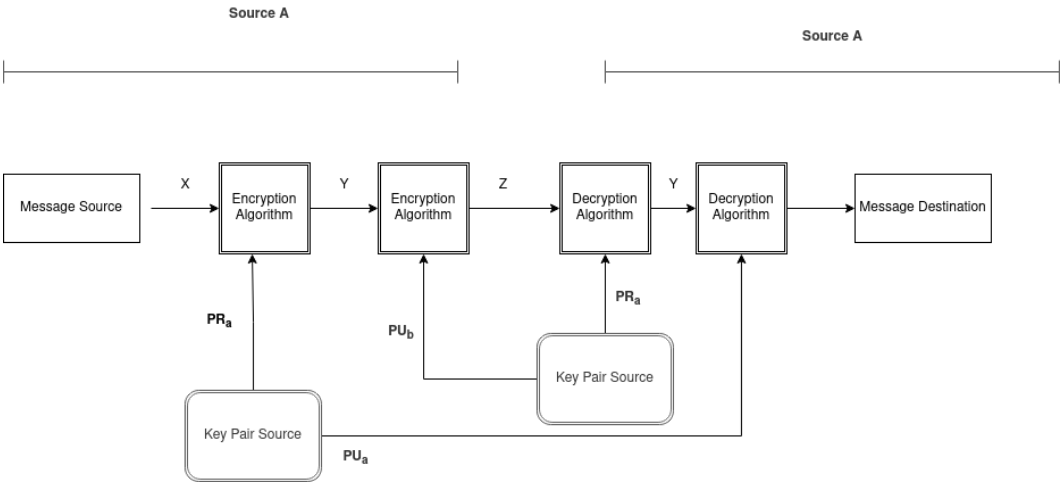

Figure 1: Diagrammatic Illustartion of Public & Private Key Cryptography

2 ENCRYPTION ALGORITHM

So for the encryption algorithm AES will be used the basic reason behind using the AES for encryption is that it is secure and relatively fast than other encryption algorithms like RSA etc. Besides, the AES is compartively more resistant to cryptanalytic attacks than other encryption algorithms.

3 HASHING

To ensure the data integrity hashing will be used. One main use of hashing is to compare two files for equality. Without opening two document files to compare them word-for-word, the calculated hash values of these files will allow the owner to know immediately if they are different. The hashing algorithm for this purpose which will be used is SHA-256