A digital signature is a data structure that provides proof of a origin, i.e., Authentication and integrity, and depending on how it is used, it can also provide non-repudiation Figure 13.14 illustrates how a digital signature is used.

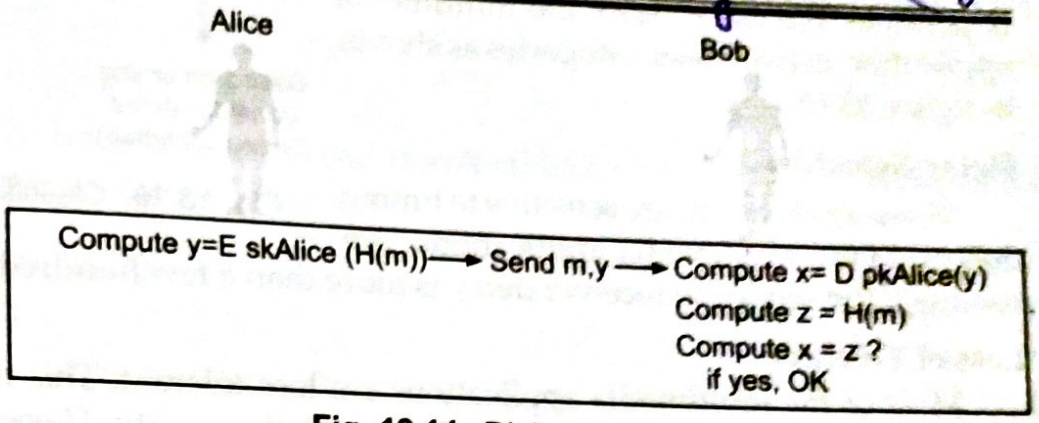

Fig. 13.14. Digital signature

Alice wants to send a message to Bob, however she doesn't want it to be modified during transmission and Bob wants to be sure that the message really came from Alice. What Alice does is that she computes a hash digest (Digest H(m) is finger print of large message like CRCs) of the message which she encrypts with her private key **skAlice.** She then sends both the message and the encrypted digest which is here signature. Bob can then verify the signature by computing the hash digest of the message he received and comparing it with the digest he gets when decryption the signature using Alice's public key **pkAlike**. If the digest are equal, Bob knows that Alice sent the message and that it has not been modified since she signed it. (E-encryption, D-decryption).

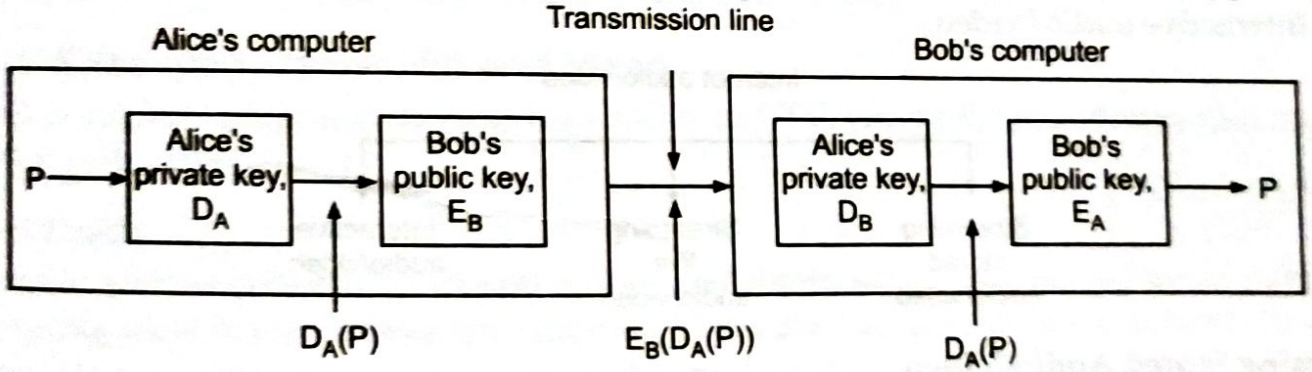

Fig. 13.15. Alice signes and only Bob gets it

In figure 13.15, signature by Alice is ensured, but anybody can decrypt using Alice public key which is available to every body. Figure 13.15, (P=m=message=plaintext), not only ensures signature by Alice but also decryption by Bob since document also encrypted by Bob's public key. One more thing, we would like to reveal that in former figure that, not whole document.