Digital Signatures using Public Key Cryptography

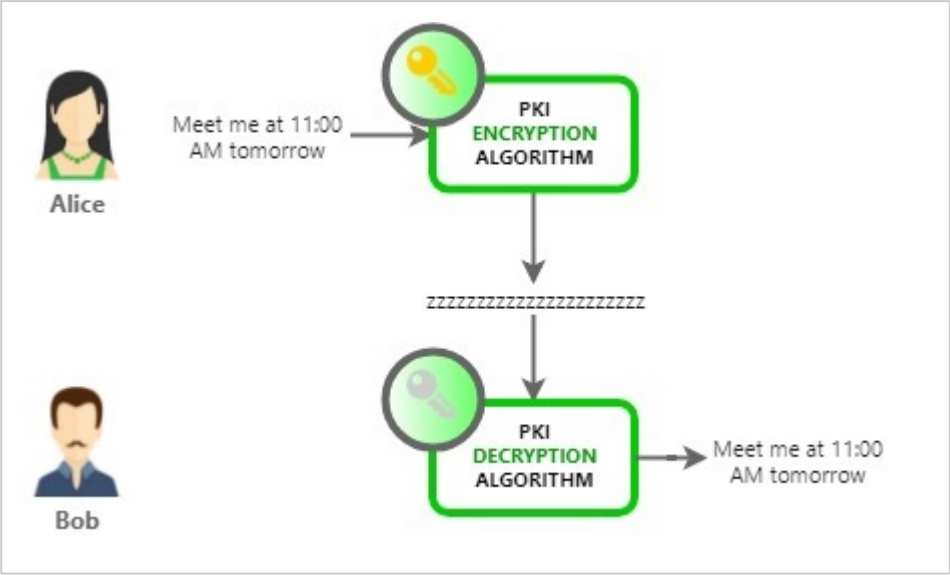
In this lesson, we will see how to ensure the recipient of one's identity using public key cryptography.

WE'LL COVER THE FOLLOWING

Let’s continue with the previous example. Where Bob receives a message, which when he decrypts says “Meet me at 11:00 tomorrow”. How can Bob know for sure that the message was sent by Alice and not Chris?

This can be achieved if the message is “signed” by its sender (Alice). The receiver of the message can then verify the signatures.

We need a way for Alice to “digitally sign” the message so the receiver of the message (Bob) can trust that the message was sent by Alice. Alice can add a digital signature to the message by using her private key to encrypt it. When the message is decrypted by her public key only, Bob can know for sure it came from Alice.

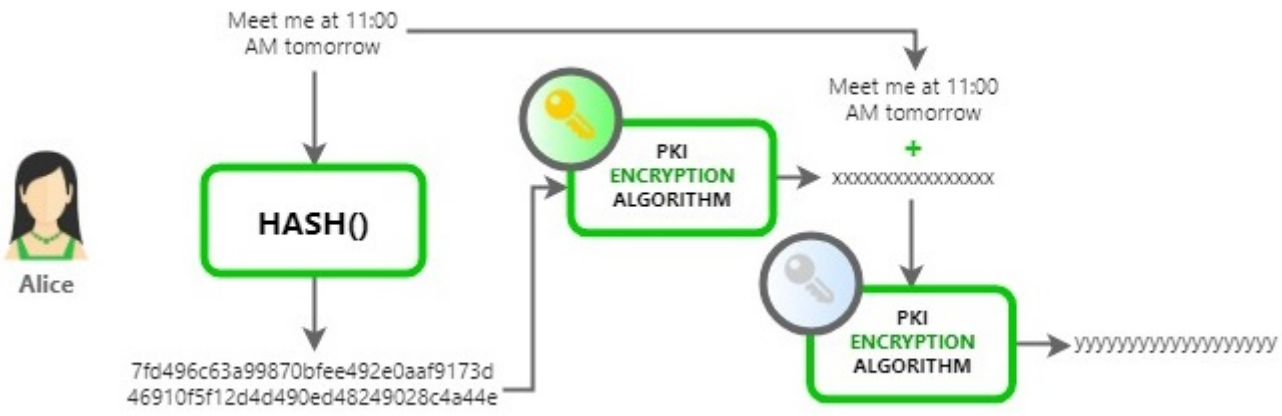


Alice sends digitally signed message to Bob. Bob can verify using Alice's private key

This works, but to make it more efficient, instead of signing the entire lengthy message the sender computes a hash (digest) of message and signs that with his public key instead. The receiver can then re-compute the message hash and compare it with the signed hash to ensure that message was not tampered with.

Adding a Digital Signature

1. Alice computes a message digest by hashing the message she is about to send. SHA256(“Meet me at 11:00 tomorrow”).
2. Alice calculates the message digest = HASH(message);
3. Alice signs the message digest by encrypting it with her private key.
4. Alice appends the signed digest with message and encrypts with Bob’s public key Alice sends it over to Bob

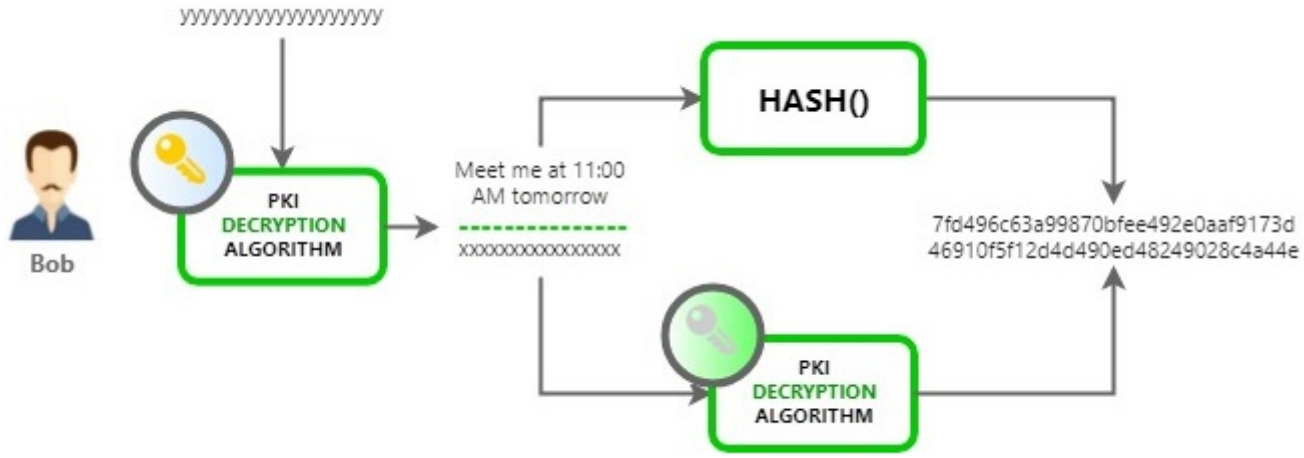


Alice sending digitally singed and encrypted message to Bob

Verifying a Digital Signature

1. Bob decrypts the message using his private key
2. Bob decrypts the digest using Alice's' public key
3. Bob computes digest of the message. If it matches the digest he received as signatures it confirms him that:

- Message is not tampered with
- Message has been sent by Alice only - Since only Alice's public key could decrypt the hash



Bob verifying the message he received from Alice

So far...

We have seen how awesome public key cryptography is and how, when combined with hash functions, it provides us with the capability to digitally sign any data.

- It helps us communicate securely on insecure channel (open internet), ensuring only the intended receiver of a message can read the message
- Ensuring the receiver can trust that the message is coming from a specific sender
- Ensuring the message is not tampered with during transmission

For all of this to work Bob needs Alice's public key. However, can he trust the public key he received indeed belongs to Alice? He received the key over the same untrusted network.

1 Which of the following is ensured by using the above method to send messages securely?

COMPLETED 0%

1 of 2

To answer the questions raised in this lesson, we need to understand the concept of PKI. Lets move on to next lesson for that.