8. Symmetric v/s Assymmetric Encryption: Pros/Cons.

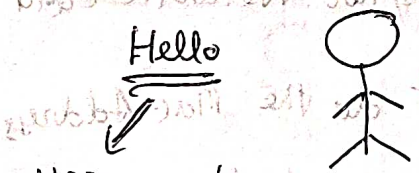
Same as Real life Example-

You have a safe box, and you have a key, you can open the safe box only with the same key.

[Symmetric Encryption Networking] (AES)

(Step1)

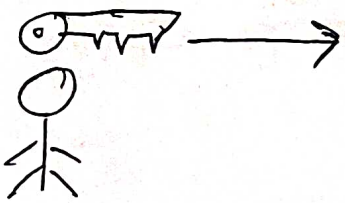
user1



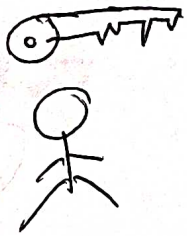
User2 wants to send Hello to user1.

user2

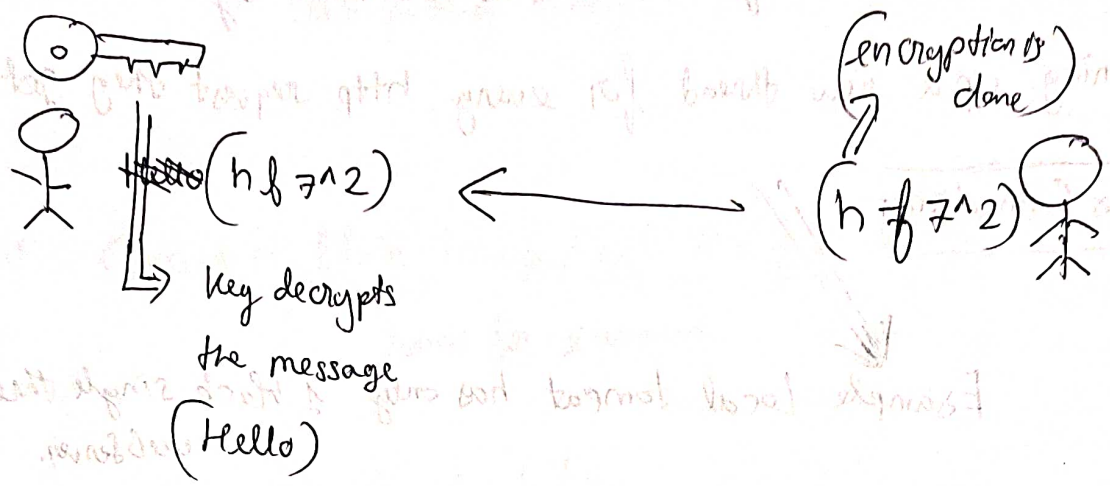
(Step2)



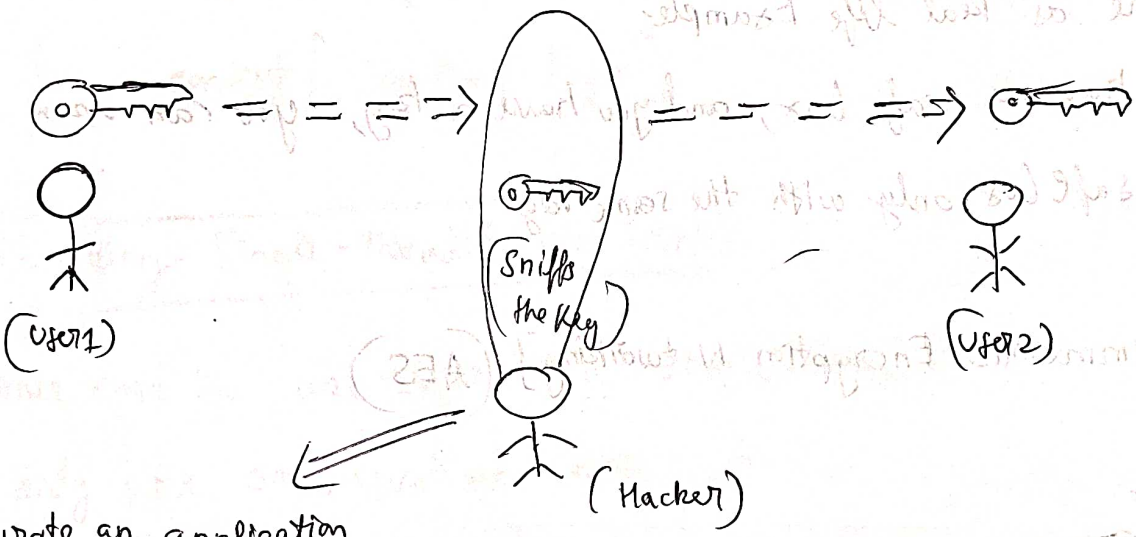
user1 sends the key over to user2.



(Step3)



Problem with this?



wrote an application where his/her Network Card does not do the Mac Address Verification of the packet.

(Now the Hacker can decrypt the encrypted messages and see through)

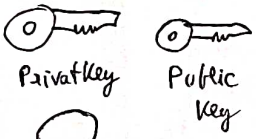
[Asymmetric Encryption]

Principle:

Public Key: You can encrypt with Public Key. But you cannot decrypt using this.

Private Key: Used for decryption.

Step1

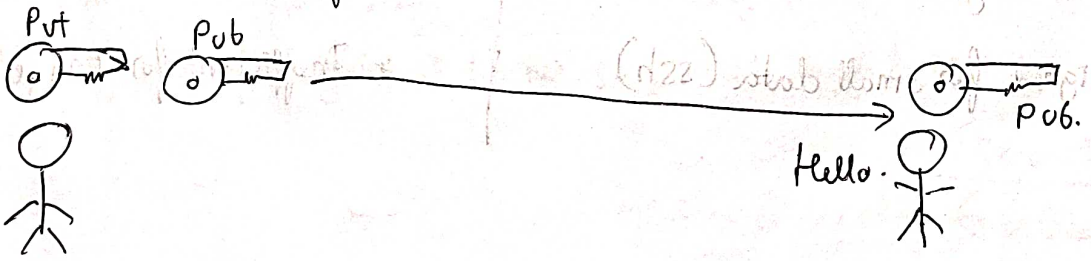


User1

(User2 wants to say Hello)

User2

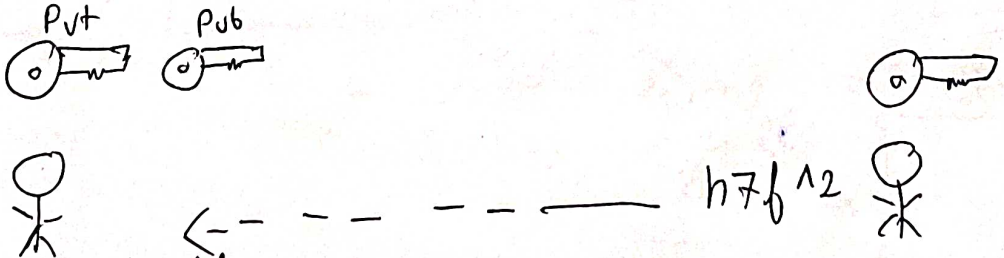
Step2 Send publicKey from user1 to user2.



User1

User2.

Step3



Assymetric Encryption has a huge computation time, It has higher latency.

* RSA → (Rivest - Shamir - Adleman)
* Diffie - Hellman

Symmetric Encryption Pros & Cons.

Pros	Cons
* Fast	* Hard to transport shared key.
* Efficient for Large Data	

[Assymmetric Encryption Pros & Cons]

Pros	Cons.
* Public key can be shared	* Slow
* Designed for small data (ssh)	* Inefficient for Large Data