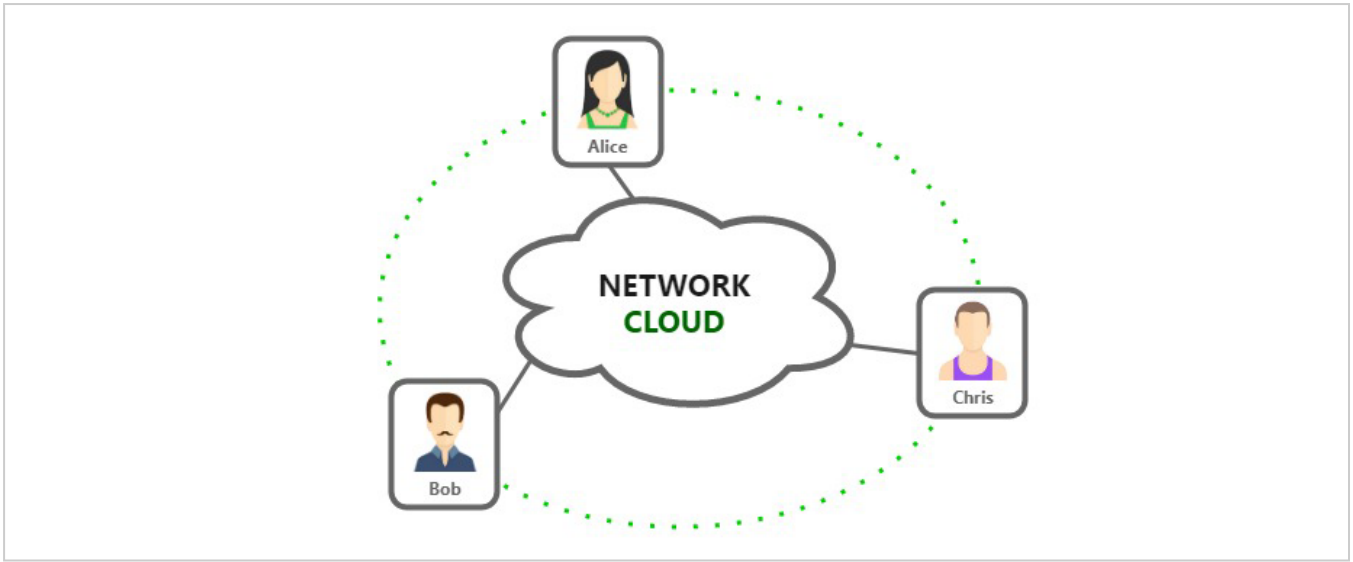
Secure Communication using Public Key Cryptography

In this lesson, we will see how two parties can communicate securely via public key cryptography.

WE'LL COVER THE FOLLOWING

Now that you understand the basic features of asymmetric key pairs, let's see how this is used to ensure that two or more parties can communicate private messages on an open and insecure network.

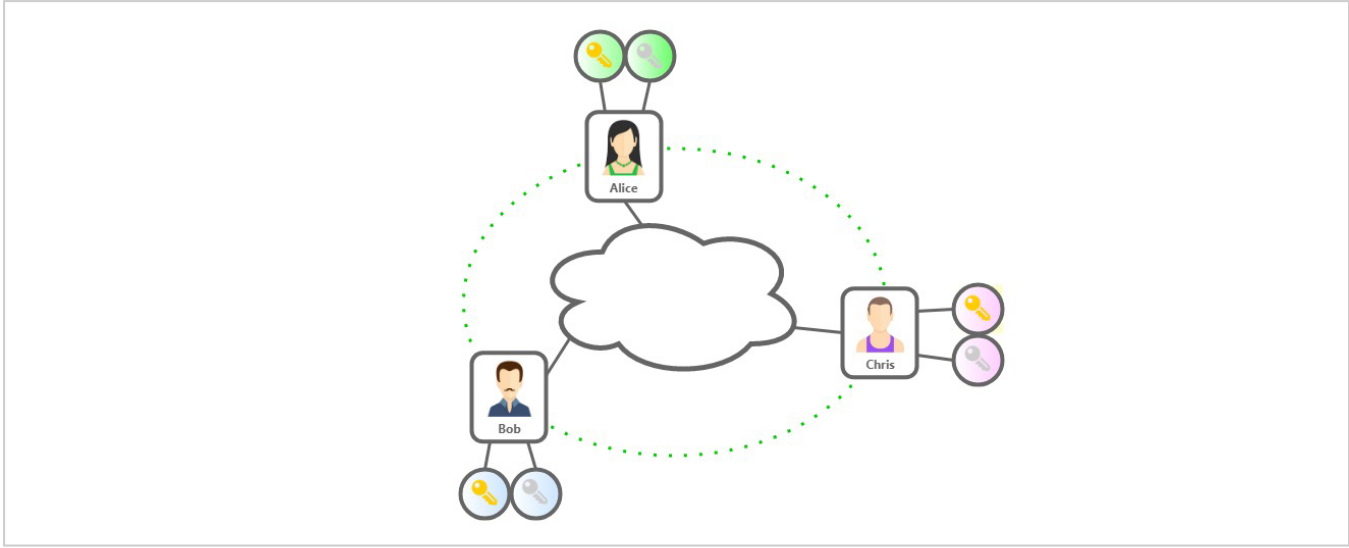
Lets say Alice, Bob and Chris are connected through a network on which everyone can read data being transferred. If Alice was to send a secret message to Bob only, it would not be possible as Chris gets to read everything transmitted through the network.



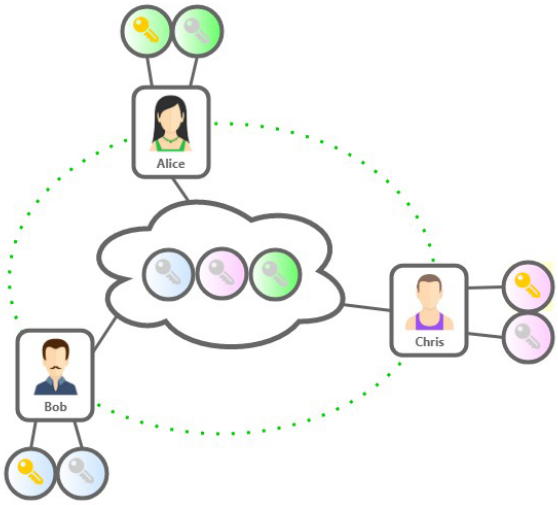
Insecure network

How can we transmit a secret message using PKC?

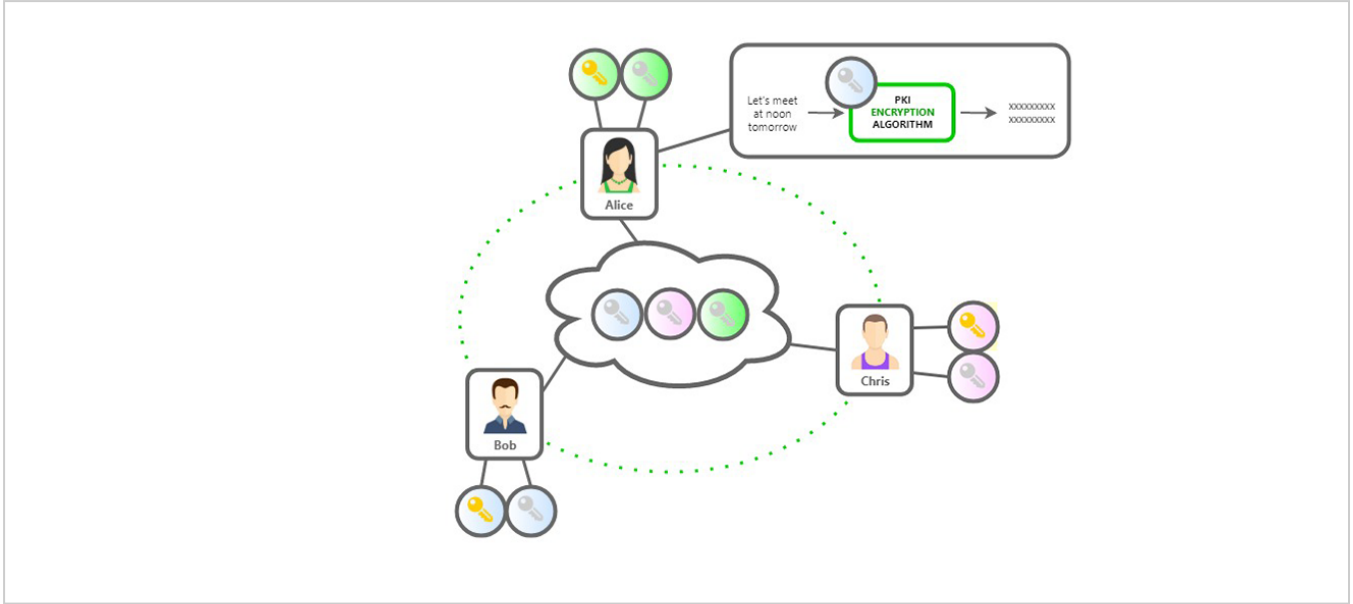
1. Each participant generates their own key pairs.



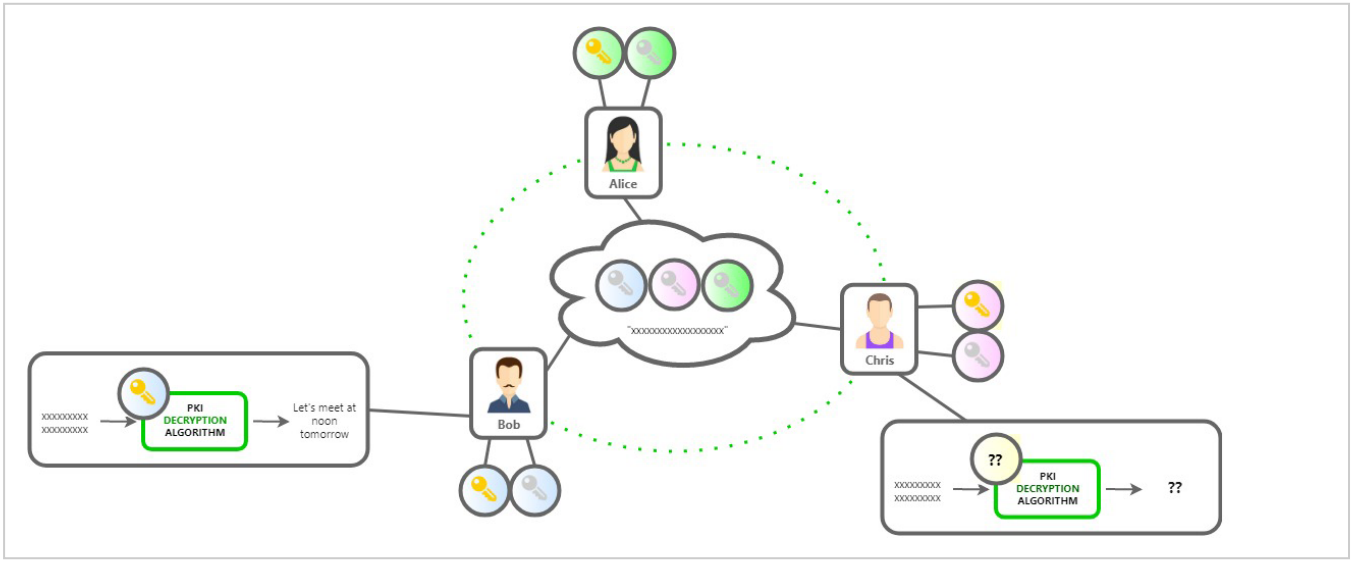
2. Each party **guards their private key** and **broadcasts the public key** on the network.



3. Now let's say Alice wants to send a message to Bob saying "Let's meet at noon tomorrow" but she does not want Chris to know about it. Alice will encrypt the message with Bob's public key and share through the network.



4. Since the corresponding private key is only known to Bob, only Bob can decrypt it. Chris cannot make any sense of the encrypted message.



No Image selected

1 The above example works on what principle of public key cryptography?

In the next lesson, we will see how to add digital signatures using public key cryptography.