Public and private keys.

1. Used to send secret information through a public network.
2. Digital signature: all about identification, how can you verify that i sent that message?
3. Each wallet is based on a public and private key pair
4. Generates a random number and that is the private key, through a special formula the private key creates a public key. The public key is dervied from the private key. Public key can be shared anywhere, but private must be kept for yourself. No way to take the public key and derive it into the private key (hash function).
5. To send a private messsage, one encrypts a message with another persons public key, and then the private key of that person can decrypt it so they can read it.
6. Digital signatures is what this type of encrypton is used for in the blockchain, because youk can verify who sent the message because the private key can sign the message, creates a signatur eon the message and the other persons knows that the message was signed by the persons private key that created the public key through mathematics.
7. This is used to sign your transactions so the nodes that confirm the transactions knows who it is from and if that person have the founds to legitimate that transaction.

Homework:

1. The concept of a public and a private key pair is that it creates a digital footprint and you can encrypt messages and information you want to send on a public networkk. The digital footprint can be created on for example a transaction when your private key signs the transaction and the blockchain system for example knows that you sent the transaction through mathematics because your public key is linked to your private key.
2. The 2 usecases of public key cryptography is encrypting messages meant for a specific person, and create digital footprints (identification).