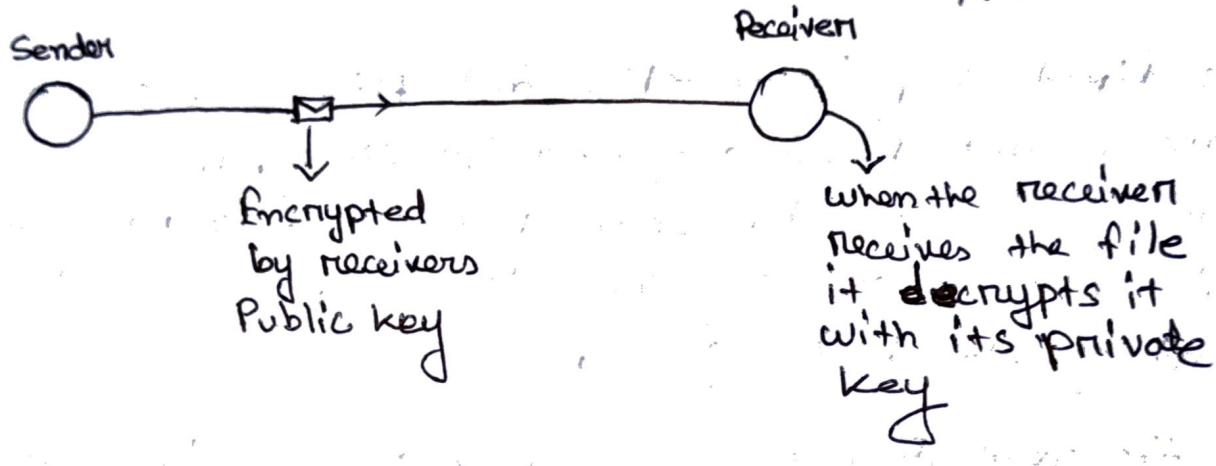
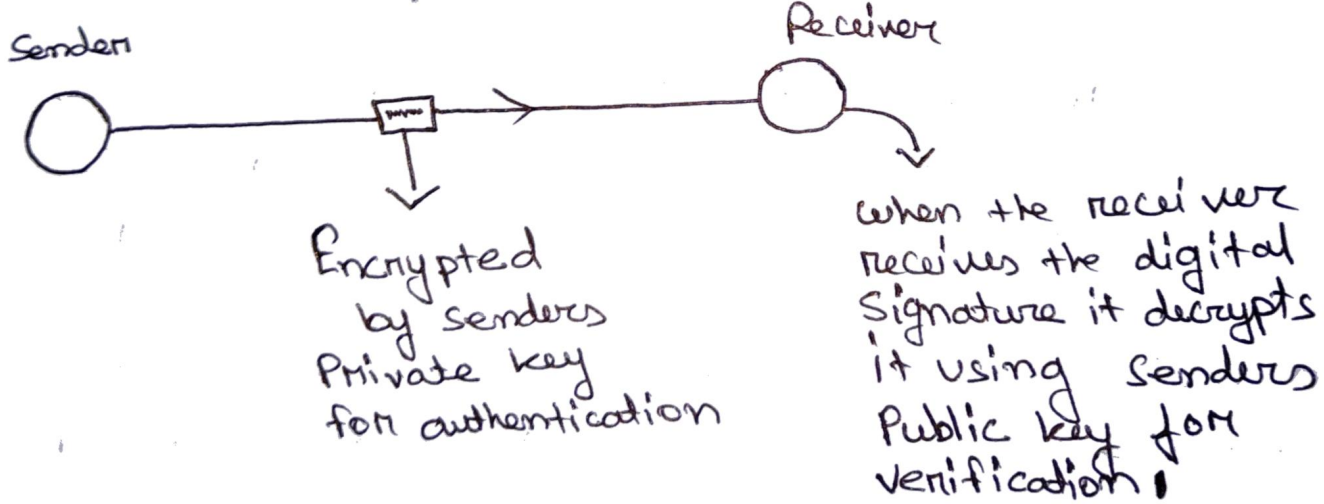
Week 1
Part 3

What type of key is applied when we encrypt something?

In asymmetric encryption, when we encrypt something we encrypt it with the recipient's public key.



In asymmetric digital signature, when we sign something we sign it with the sender's private key.



Diffie-Hellman is a key exchanging algorithm

Example,

Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure.

The first step is ~~to~~ Bob and Alice will choose a large prime number P and a nonzero integer g. The value of P and g is same for both Bob and Alice. P and g are Public values. Let's say for this example the value of P and g are P=7, g=2.

In the next step Alice will pick a secret integer a and does not reveal to anyone, ~~not even Bob~~. Bob also does the same picking a secret number b and does not reveal to anyone. Let's say a=4 and b=5.

1. Compute the Public key of Alice.
2. Compute the Public key of Bob.
3. Compute the secret symmetric key.

For finding the Public key of Alice, we need to use a formula which is used to find Public keys.

$$A = g^a \pmod P$$

- A: Public key of Alice
- g: non-zero integer, g = 2
- a: Secret integer that Alice Picked, a = 4
- mod: modulus
- P: Large Prime number P = 7

Calculation,

$$A = g^a \pmod{P}$$

$$A = 2^4 \pmod{7}$$

$$A = 16 \pmod{7}$$

$$\boxed{A = 2} \rightarrow \text{Public key of Alice}$$

for finding the Public key of Bob, we need to follow similar approach.

Calculation,

$$B = g^b \pmod{P}$$

$$B = 2^5 \pmod{7}$$

$$B = 32 \pmod{7}$$

$$\boxed{B = 4} \rightarrow \text{Public key of Bob}$$

Now, Alice and Bob will exchange these numbers. Alice will send A to Bob and Bob will send B to Alice. Then, finally Alice and Bob will use their secret integers to find the secret symmetric keys using the same formula but this time there will be a little change.

~~Calculation~~

Calculation for Alice,

$$A' = B^a \pmod{P}$$

↳ Bob's Public key

$$A' = 4^4 \pmod{7}$$

$$\boxed{A' = 4} \rightarrow \text{Symmetric key of Alice}$$

Similarly, for Bob,

Calculation,

$$B' = A^b \pmod{P}$$

↳ Public key of Alice

$$B' = 2^5 \pmod{7}$$

$$\boxed{B' = 4}$$ → Symmetric key of Bob.

We can see that both Alice and Bob ~~ge~~ independently generated the ~~secret~~ Symmetric key 4. This 4 is now going to be used for secret key communication.