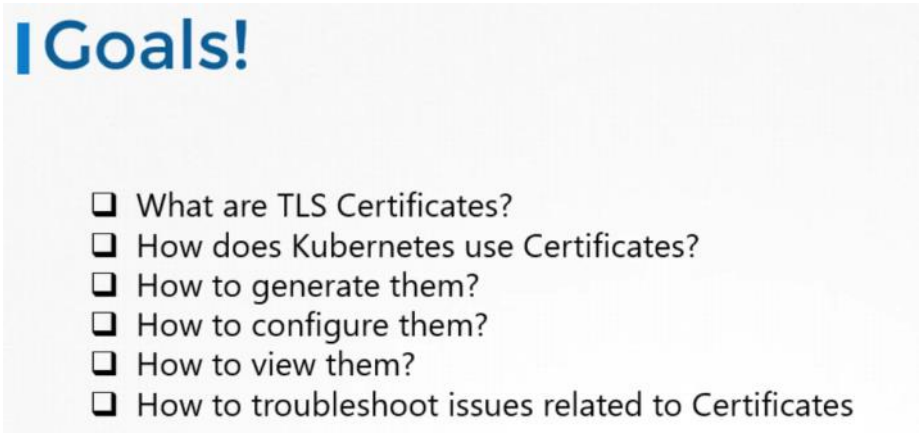
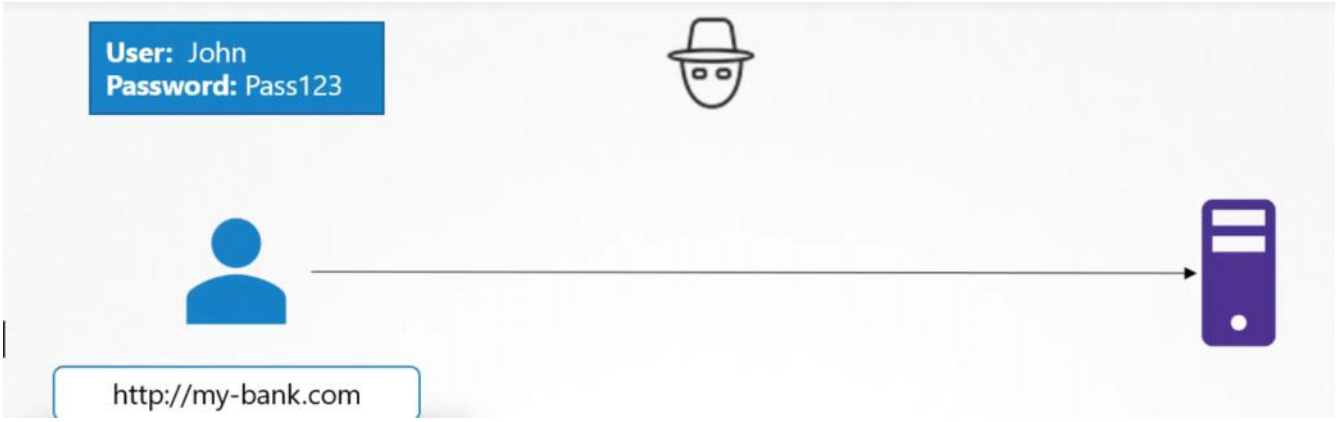
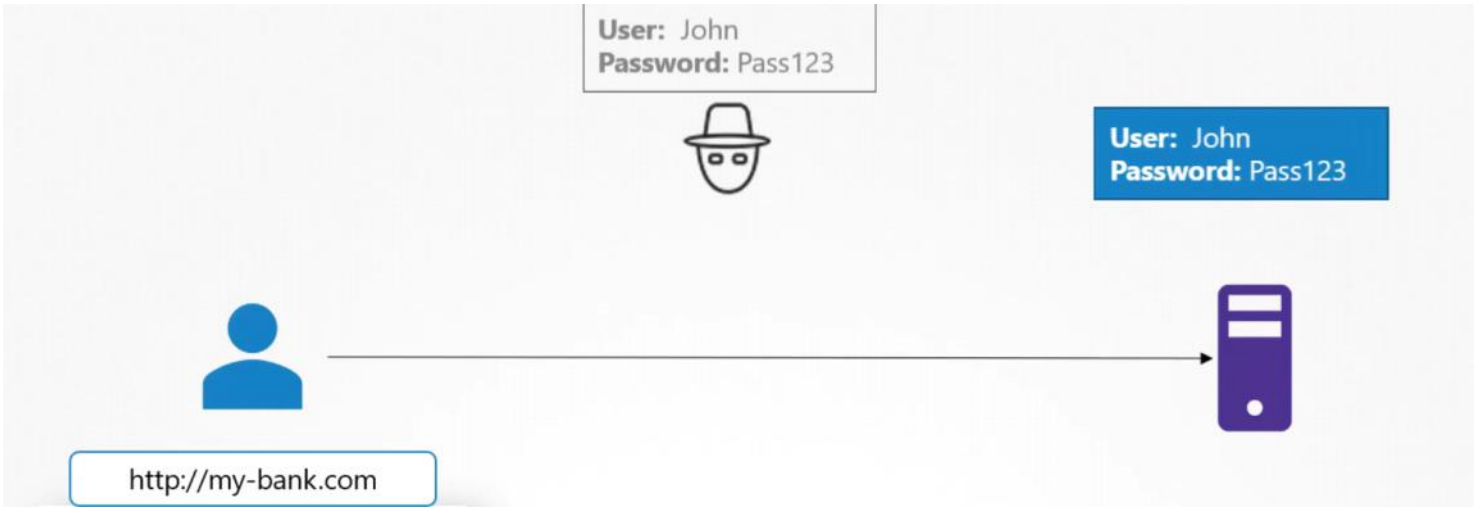
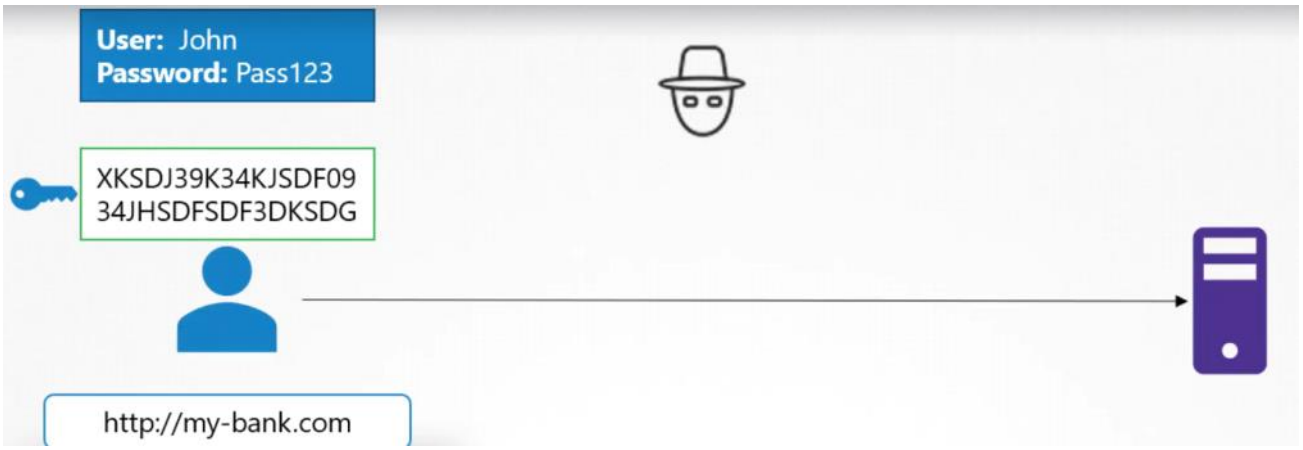


A certificate is used to guarantee trust between two parties during a transaction.

TLS certificates ensure that the communication between the user and the server is encrypted.



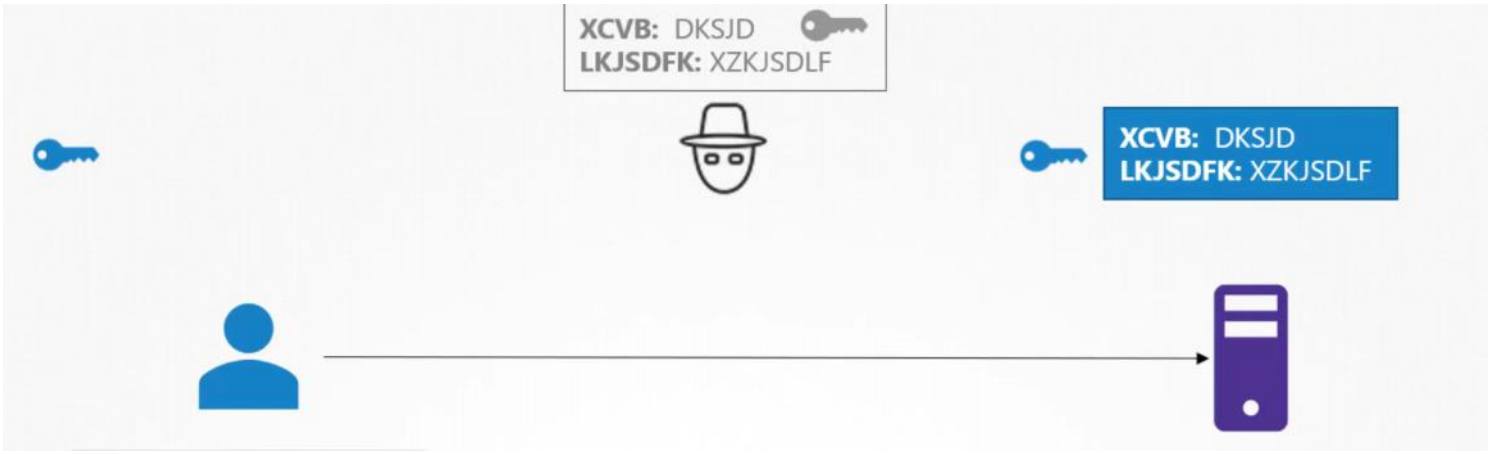

User: John
Password: Pass123
User: John
Password: Pass123
http://my-bank.com

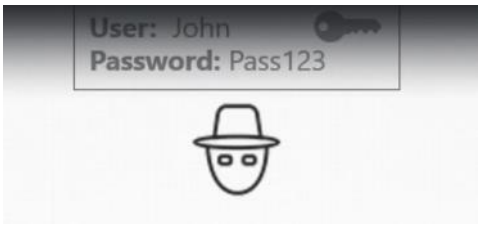

User: John
Password: Pass123
XKSDJ39K34KJSDF09
34JHSDFSDF3DKSDG
http://my-bank.com


User: John
Password: Pass123
XKSDJ39K34KJSDF09
34JHSDFSDF3DKSDG


XCVB: DKSJD
LKJSDFK: XZKJSDLF


XCVB: DKSJD
LKJSDFK: XZKJSDLF





It is a secure way of encryption, but since it uses the same key to encrypt and decrypt the data, and since the key has to be exchanged between the sender and the receiver there is a risk of hacker gaining access to the key and decrypting the data.

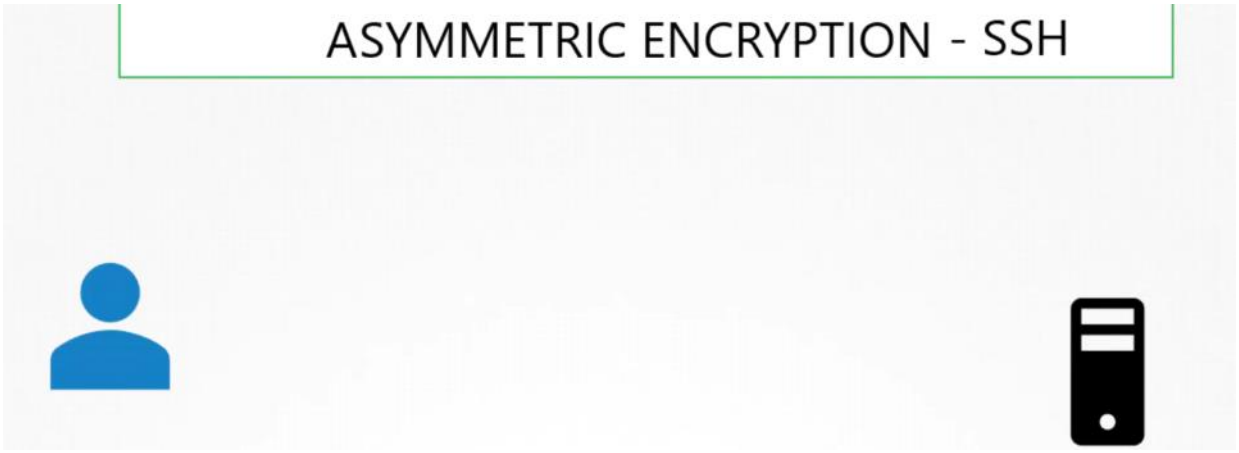
that's where asymmetric encryption comes in.

Instead of using a single key to encrypt and decrypt data,

asymmetric encryption uses a pair of keys,

Private Key Public Key

a private key and a public key.

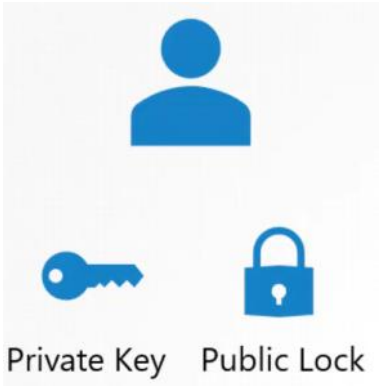


You don't want to use passwords as they're too risky

so you decide to use key pairs.

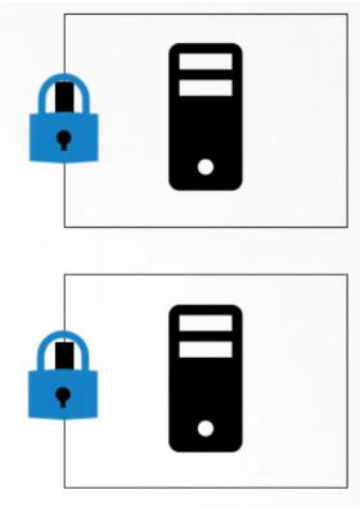
You generate a public and private key pair.

```
ssh-keygen
id_rsa  id_rsa.pub
```

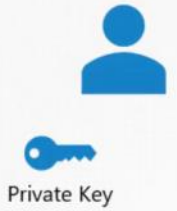


```
cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc…KhtUBfoTzlBqR
V1NThvOo4opzEwRQo1mWx user1
```

```
ssh -i id_rsa user1@server1
Successfully Logged In!
```



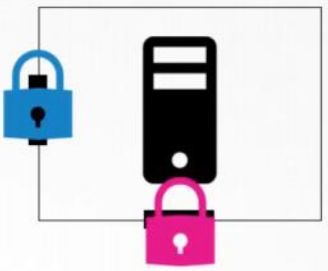
ASYMMETRIC ENCRYPTION - SSH

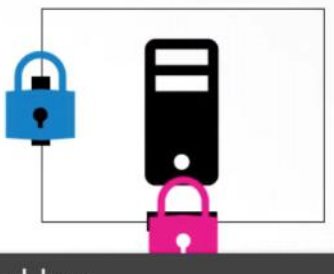


Private Key

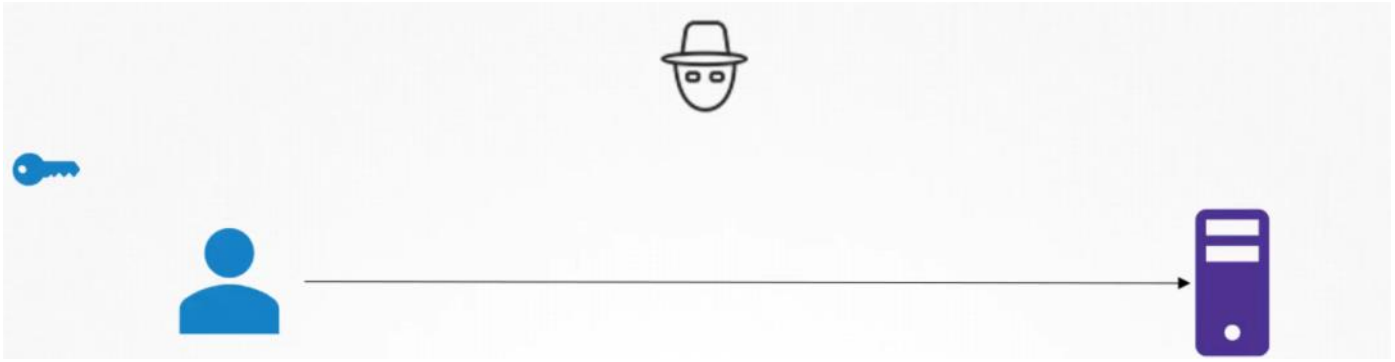
Private Key

Public Lock



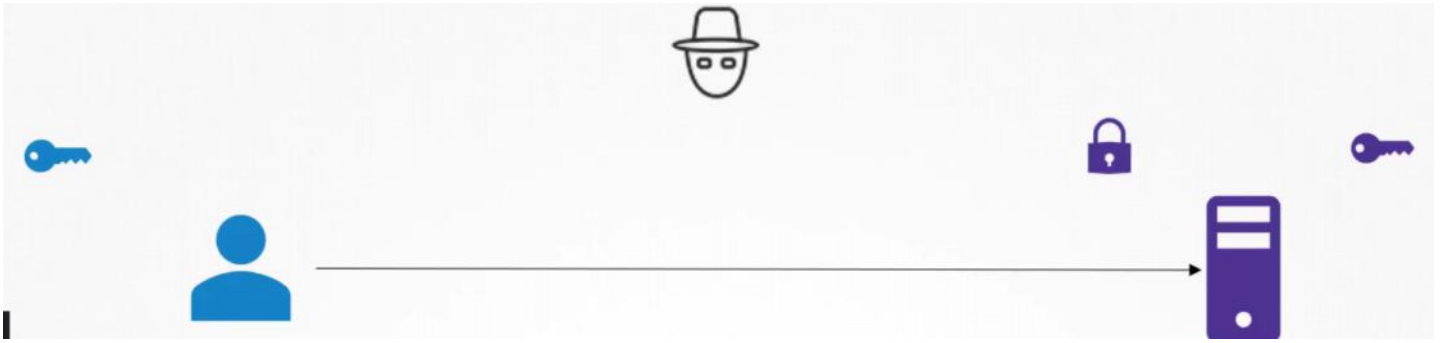


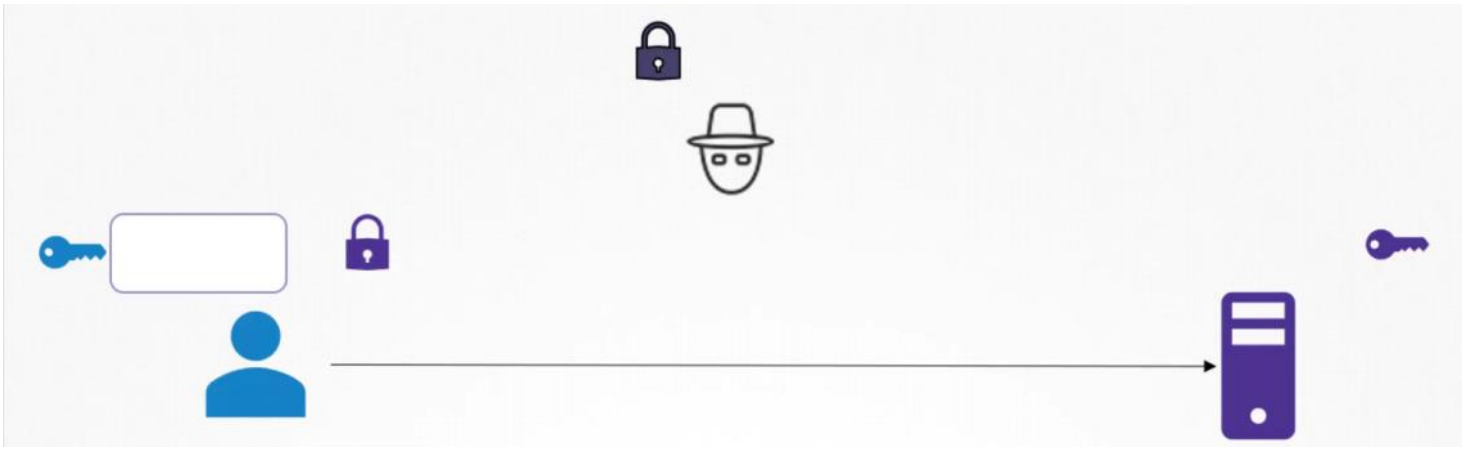
```
cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc…KhtUBfoTzlBqRV1NThvOo4opzEwRQo1mWx user1
ssh-rsa AAAXCVJSDFDF…SLKJSDLKFw23423xckjSDFDFLKJLSDFKJLx user2
```

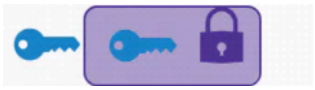


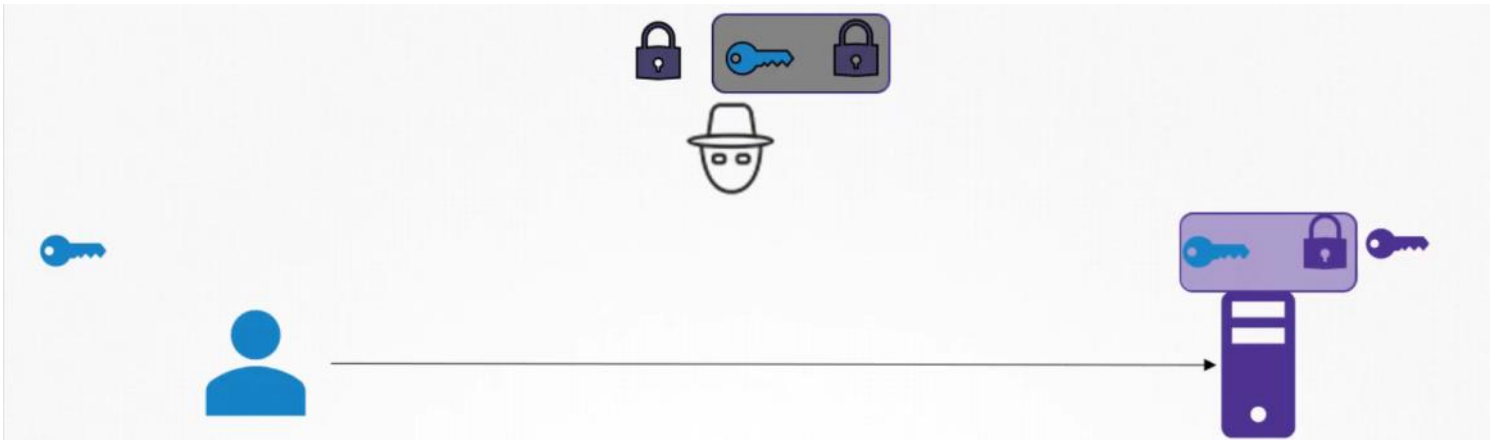
```
openssl genrsa -out my-bank.key 1024
my-bank.key
```

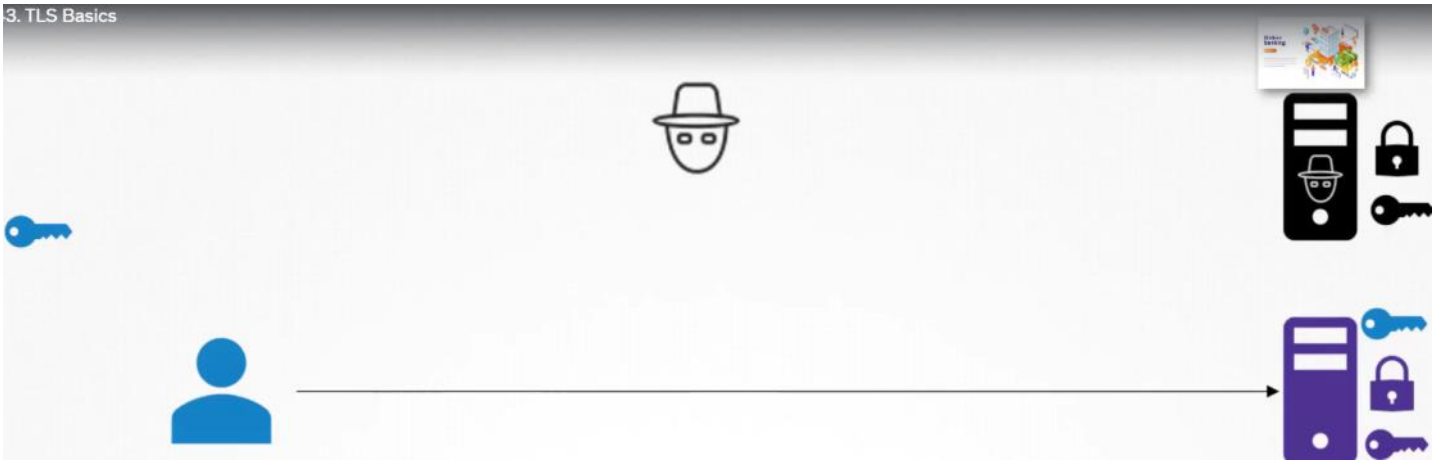
```
openssl rsa -in my-bank.key -pubout > mybank.pem
my-bank.key  mybank.pem
```

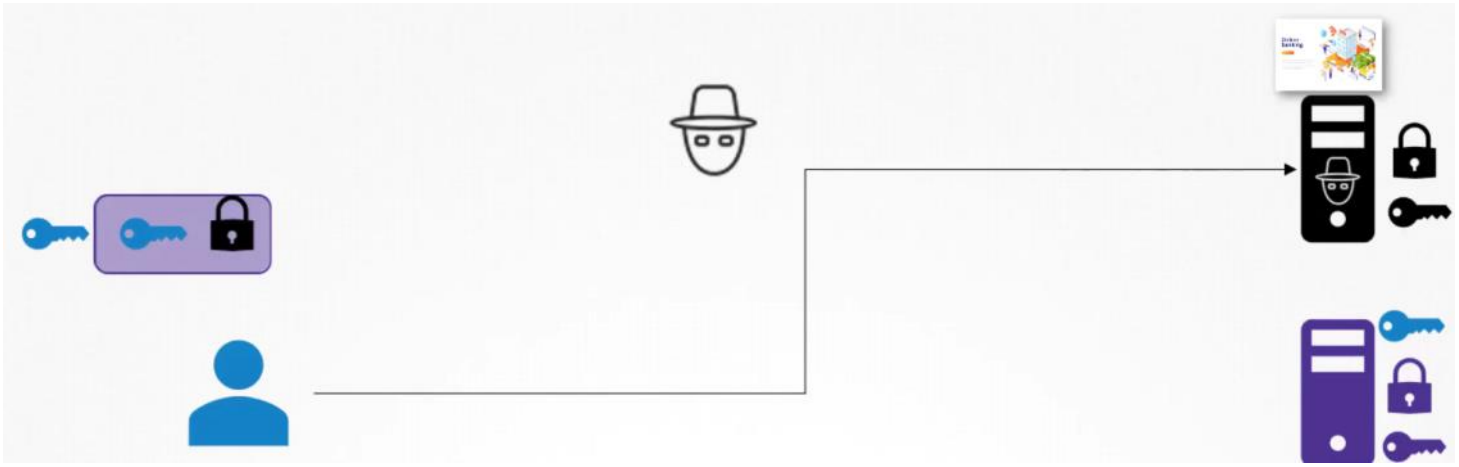






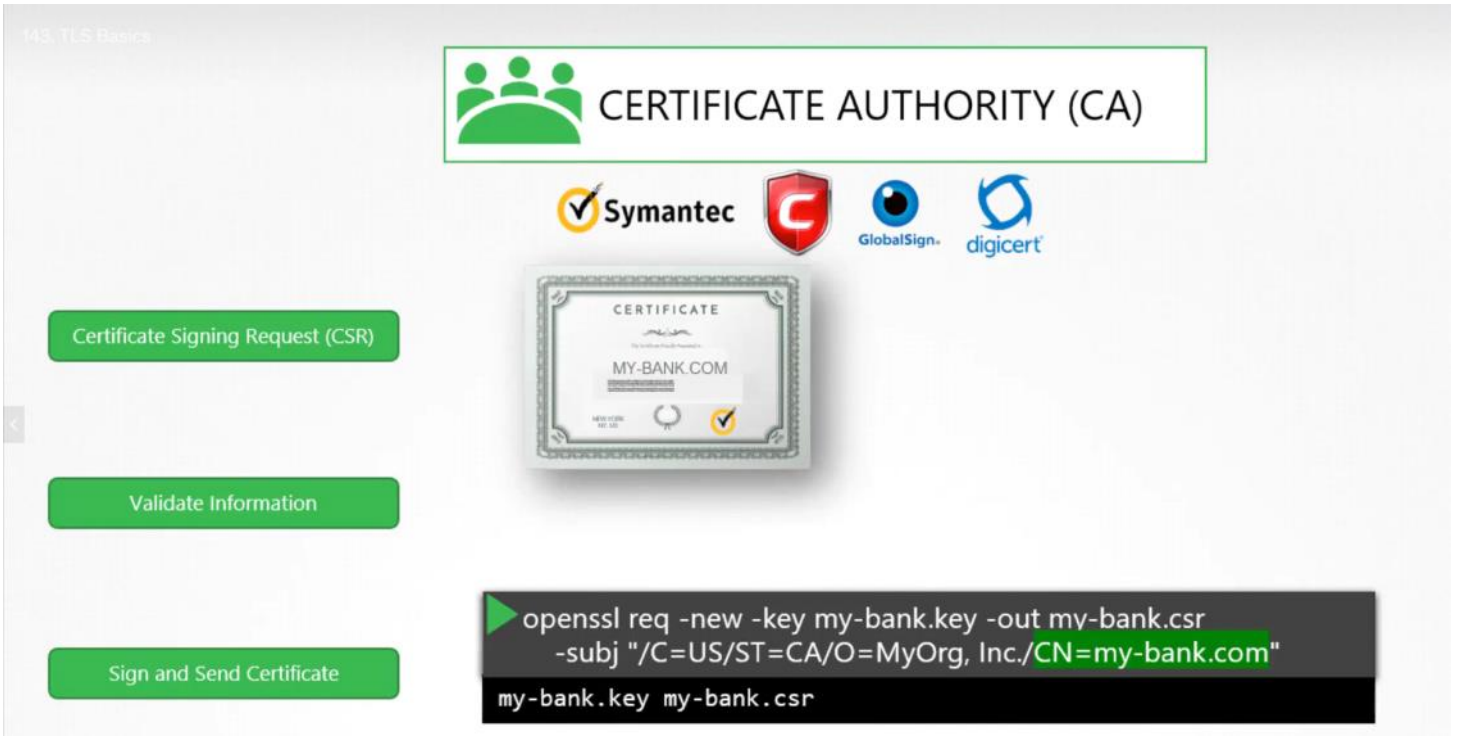



3. TLS Basics




CERTIFICATE AUTHORITY (CA)
Symantec
GlobalSign
digicert

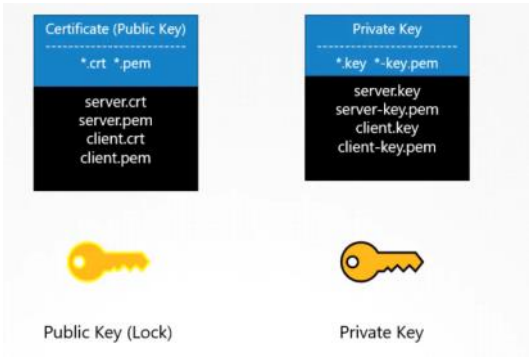

CERTIFICATE AUTHORITY (CA)
Symantec
GlobalSign
digicert
Certificate Signing Request (CSR)
CERTIFICATE
MY-BANK.COM
openssl req -new -key my-bank.key -out my-bank.csr
-subj "/C=US/ST=CA/O=MyOrg, Inc./CN=my-bank.com"
my-bank.key my-bank.csr

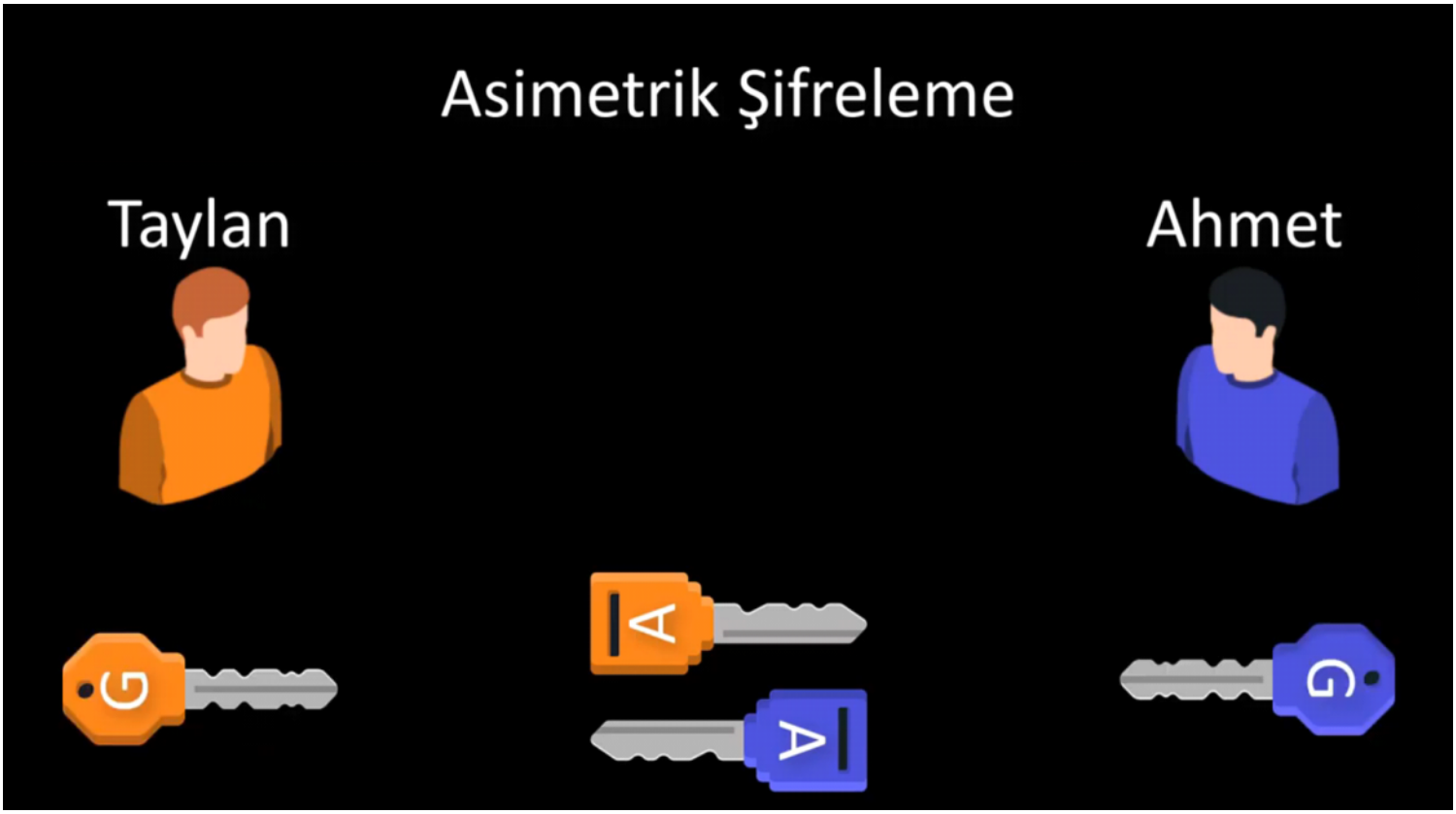

143. TLS Basics
CERTIFICATE AUTHORITY (CA)
Symantec
GlobalSign
digicert
CERTIFICATE
MY-BANK.COM
Certificate Signing Request (CSR)
Validate Information
Sign and Send Certificate
openssl req -new -key my-bank.key -out my-bank.csr
-subj "/C=US/ST=CA/O=MyOrg, Inc./CN=my-bank.com"
my-bank.key my-bank.csr


CERTIFICATE AUTHORITY (CA)
Symantec
GlobalSign
digicert


https://my-bank.com


Symantec
Private CA
https://my-bank.c


Certificate (Public Key)
*.crt *.pem
server.crt
server.pem
client.crt
client.pem
Private Key
*.key *-key.pem
server.key
server-key.pem
client.key
client-key.pem
Public Key (Lock)
Private Key


Asimetrik Şifreleme
Taylan
Ahmet
G
A
A
G