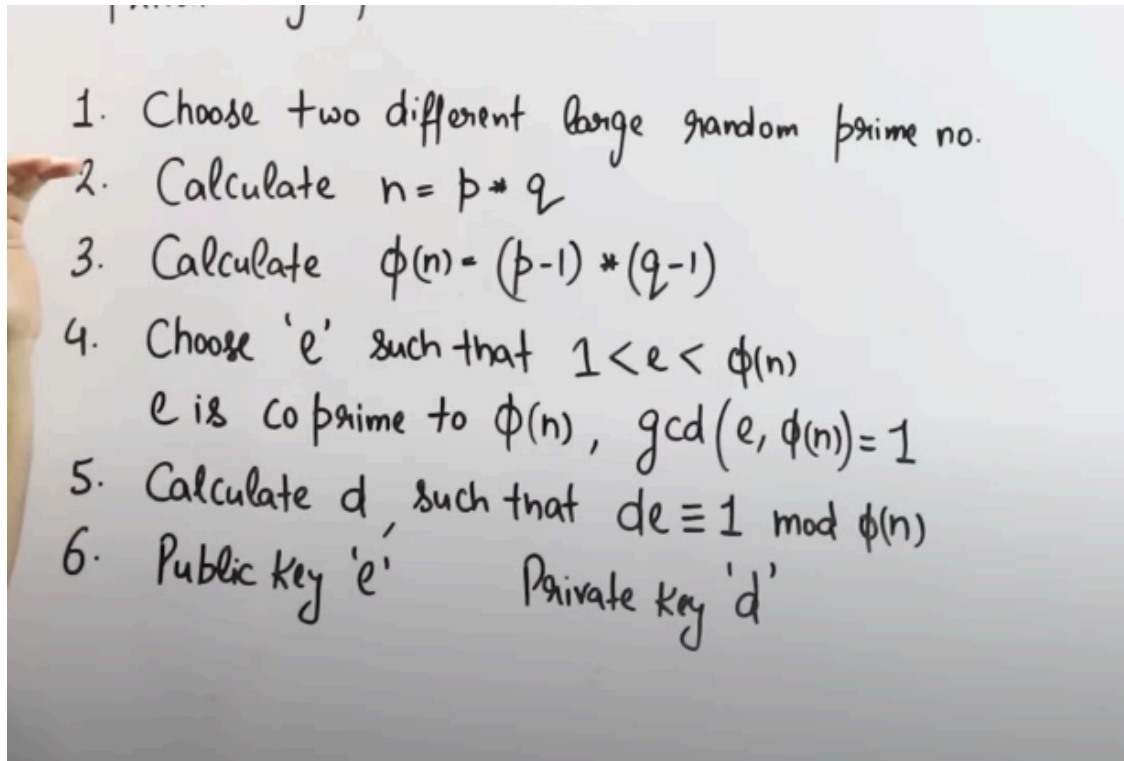# 1

September 9, 2025

[ ]:

plain text encrypt to cipher text

there wont be a secure line bw every src and des
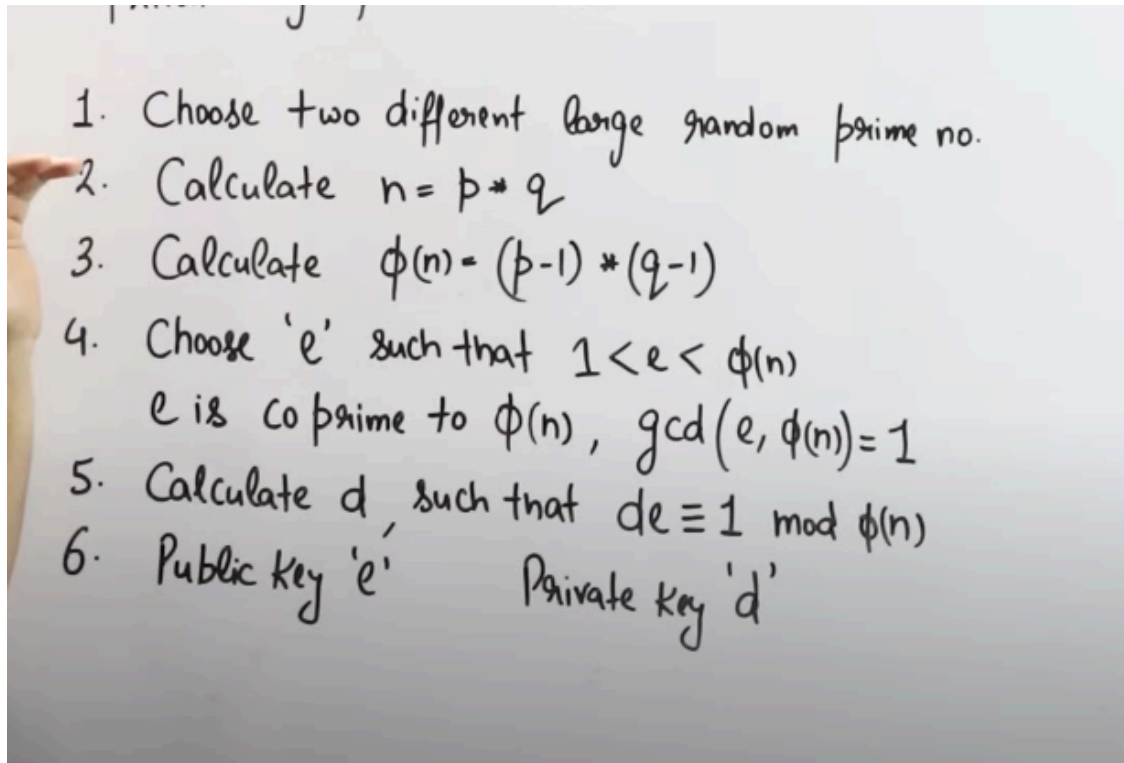
1 Symmetric key cryp

1. Choose two different large random prime no.
2. Calculate $n = p * q$
3. Calculate $\phi(n) = (p-1) * (q-1)$
4. Choose 'e' such that $1 < e < \phi(n)$
   e is co prime to $\phi(n)$, $\gcd(e, \phi(n)) = 1$
5. Calculate d, such that $de \equiv 1 \mod \phi(n)$
6. Public key 'e'   Private key 'd'

1. Choose two different large random prime no.
2. Calculate $n = p * q$
3. Calculate $\phi(n) = (p-1) * (q-1)$
4. Choose 'e' such that $1 < e < \phi(n)$
   e is co prime to $\phi(n)$, $gcd(e, \phi(n)) = 1$
5. Calculate d, such that $de \equiv 1 \mod \phi(n)$
6. Public key 'e'   Private key 'd'

2 RSA

it is the real life implemenetation of the above

we generate the keys using prime numbers

1. Choose two different large random prime no.
2. Calculate $n = p * q$
3. Calculate $\phi(n) = (p-1) * (q-1)$
4. Choose 'e' such that $1 < e < \phi(n)$
   e is co prime to $\phi(n)$, $\gcd(e, \phi(n)) = 1$
5. Calculate d, such that $de \equiv 1 \mod \phi(n)$
6. Public key 'e'   Private key 'd'