CRYPTOGRAPHY

PART III

Overview

- A quick revision on Asymmetric cryptography
- **RSA** encryption algorithm
- How do go on now?

Asymmetric cryptography

- Different keys for encryption (“public key”) and decryption (“private key”)
- Can be used over insecure channels
- Schemes rely on cool math
- S L O W

RSA

It stands for **R**ivest-**S**hamir-**A**dleman, surnames of it's creators.

Asymmetric cryptography

RSA

- p, q: Large random primes
- n: modulus, p*q
- e: public key exponent (coprime to phi)
- phi: Totient function of n
- d: private key exponent, the modulo inverse of e over the base phi

RSA

- m: The number form of plaintext
- c: The number form of ciphertext
- **Public key**: (n, e)
- **Private key**: d

Key Generation

- Generate two distinct primes p and q
- Multiply n = p*q
- Compute Totient function λ(n)
  = lcm(λ(p), λ(q))
  Since p and q are prime, λ(p) = p - 1
  Hence, λ(n) = lcm(p-1, q-1)

Key Generation

- Choose an integer e such that it is coprime $\lambda(n)$, $1 < e < \lambda(n)$, generally $e = 65537$
- Compute $d \equiv e^{-1} (\mod \lambda(n))$

Key Generation

- The public key tuple is (n,e)
- The integer d is the private key.

Encryption/Decryption

Encryption:

- We convert the message to integer form, m
- Then compute c by:

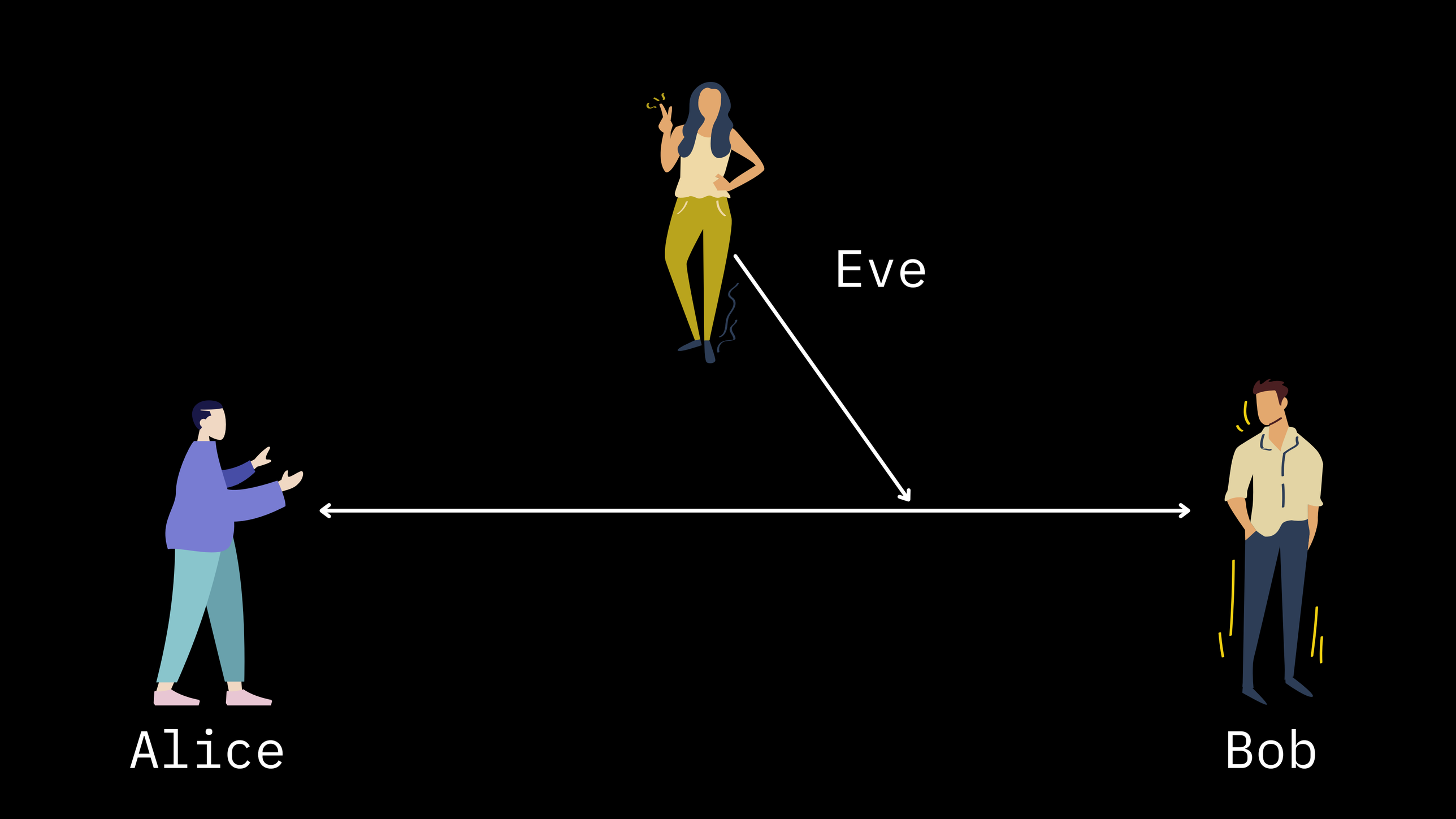
$$m^e \equiv c \pmod{n}$$

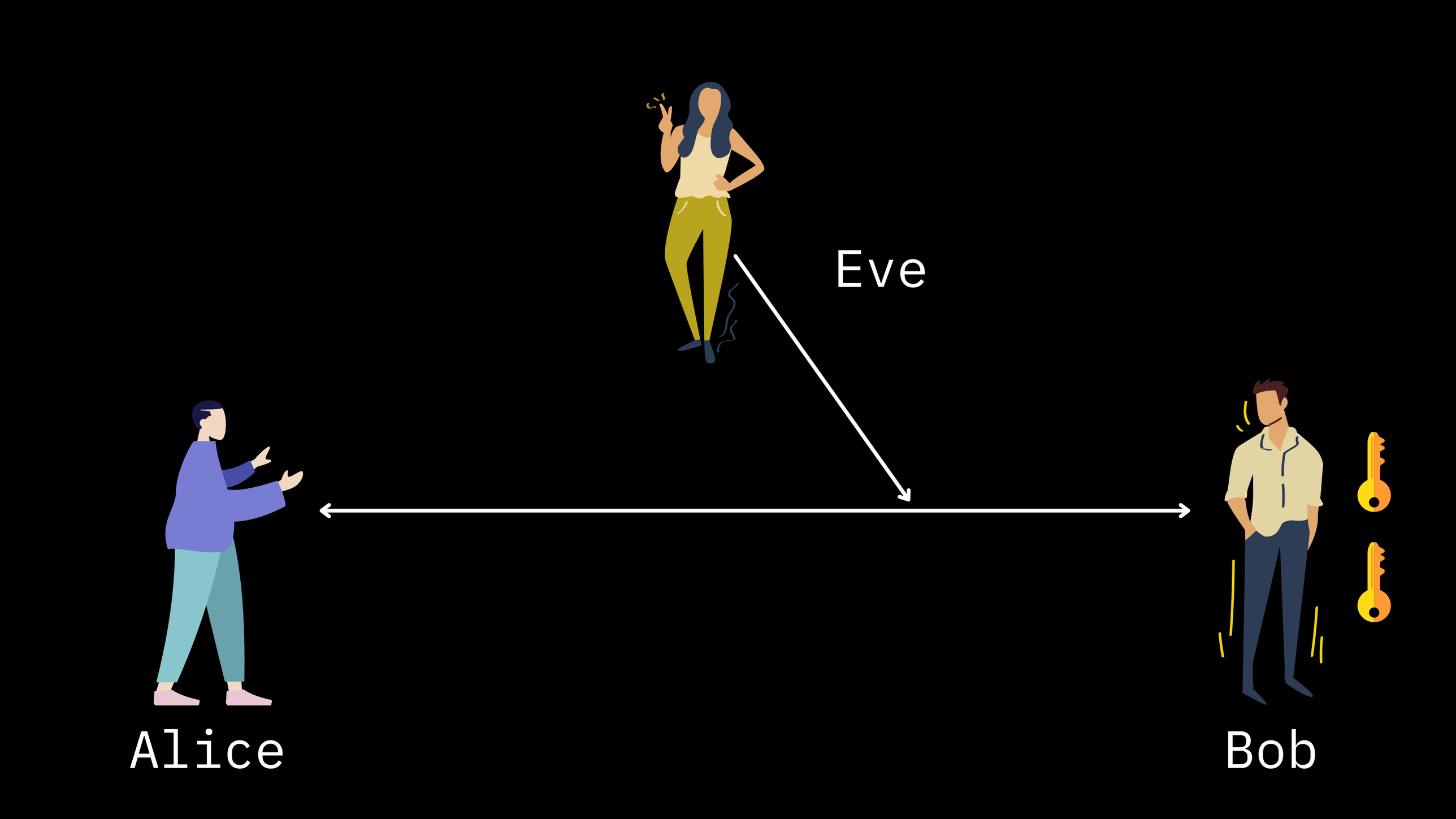
Decryption:

- Simply compute:

$$c^d \equiv m \pmod{n}$$

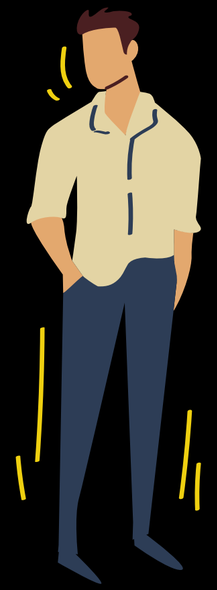
- And recover message from m.


Eve
Alice
Bob


Eve
Alice
Bob

Encrypts
with
public key

Eve

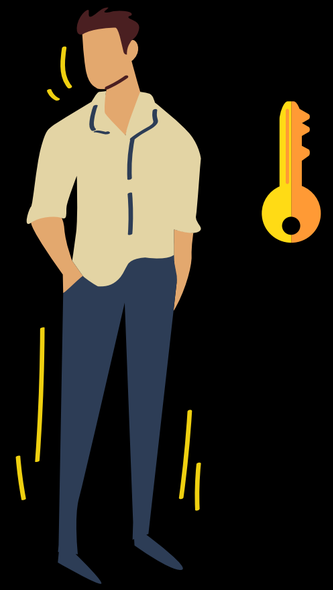


Alice

Bob

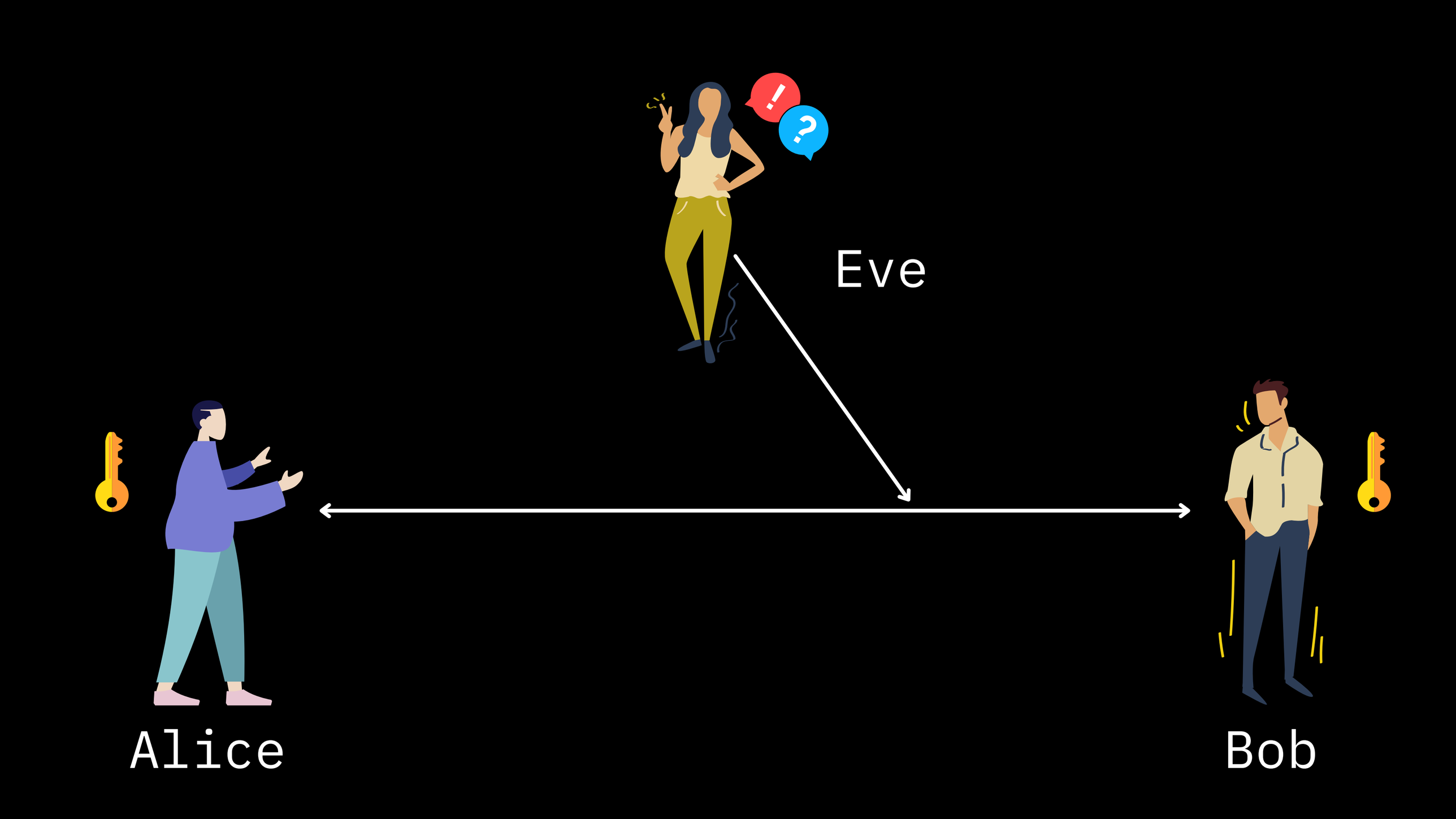
Eve

Decrypts with private key



Alice

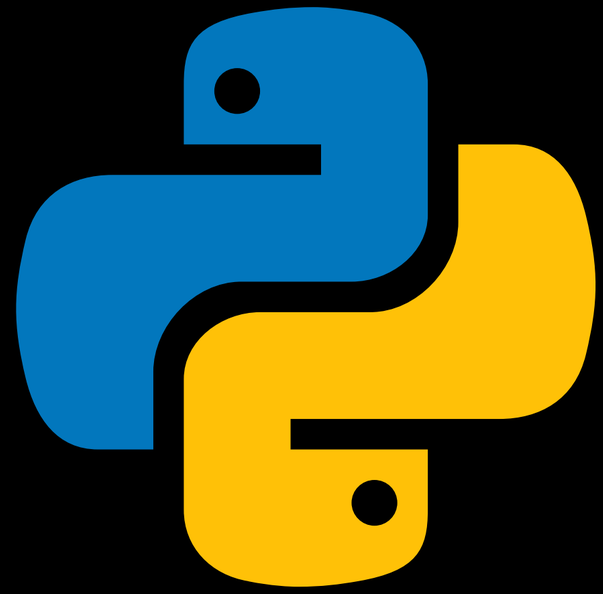
Bob


Eve
Alice
Bob

RSA

Let's see it in python !!

```
pip install pycryptodome
```



RSA attacks

- n too small - just factor it! (gets unfeasible once n is larger than ~512 bits)
- d too small → Wiener's attack
- e too small / partial key known → Coppersmith's attack
- multiple moduli → Batch GCD
- faulty prime generation
- Something else → Google!

What next ?

This is just a tip of the iceberg !!

What next ?

Practice these ciphers at:
 Cryptohack (https://cryptohack.org/)
 Cryptopals (https://cryptopals.com/)
And LEARN new ones !!

THANK YOU

CONTACT US

@nitdgplug

/nitdgplug

@lugnitdgp

@nitdgplug

GNU/Linux Users' Group NIT-Dgp

nitdlug@gmail.com

GNU/Linux Users' Group NIT-Dgp