IB Computer Science

Public Key Encryption

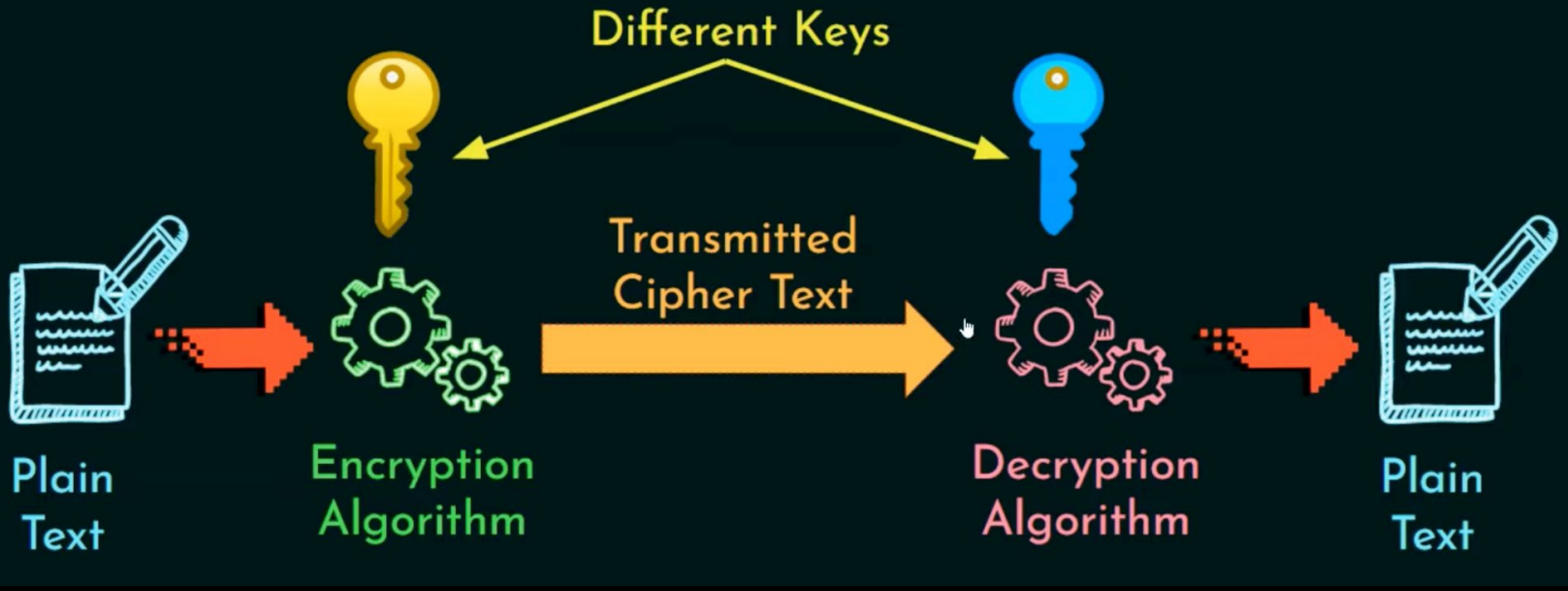
Public Key Encryption

An asymmetric encryption technique which uses *different keys* for encryption and decryption, allowing computers to securely communicate with each other over the internet .

Key

The **key** determines the output of the encryption algorithm; only those who know the key can decrypt the message.

Asymmetric Cryptography



Steps in Public Key Encryption

1. Key Generation
2. Key Exchange
3. Encryption
4. Sending Encrypted Data
5. Decryption

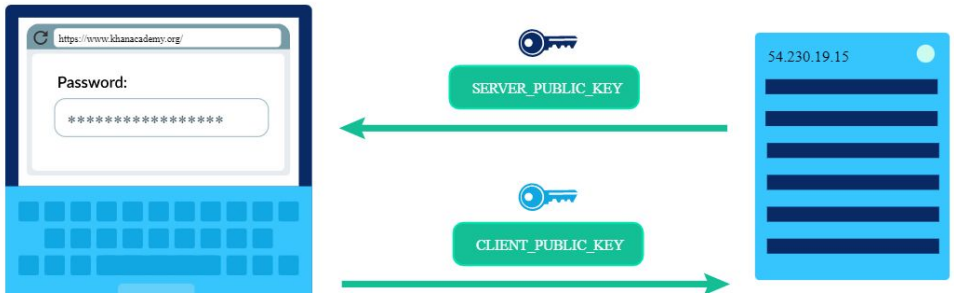
Step 1: Key Generation

Each person (or their computer) generates a pair of keys that identifies them: a **private key** and a **public key**.

The keys are generated by multiplying together two incredibly large primes. The algorithm repeatedly generates random large numbers and checks if they're prime, until it finally finds two random large primes.

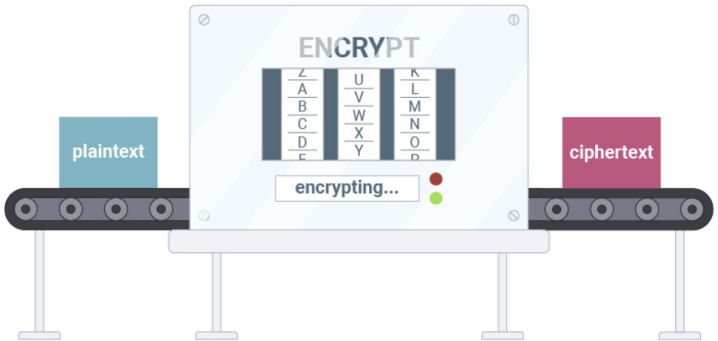
Step 2: Key Exchange

The sending and receiving computers exchange *public keys* with each other via a reliable channel, like TCP/IP. The private keys are *never* exchanged.



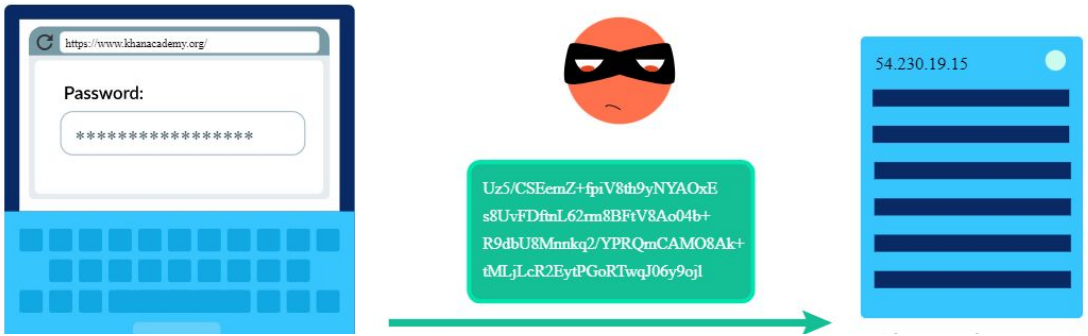
Step 3: Encryption

The sending computer encrypts the secret data using the receiving computer's *public* key and a mathematical operation.



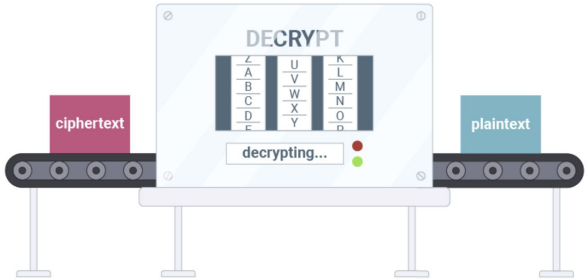
Step 4: Sending Encrypted Data

The sender can now safely transmit the encrypted data over the Internet without worry of onlookers.



Step 5: Decryption

Now the receiver can decrypt the message, using their *private key*. That's the only key that can be used to decrypt the message.



How does it work?

Public key encryption uses a mathematical operation– a "one-way function", that relies on prime numbers, the difficulty of factoring large primes, and modular arithmetic.

The operation of the one-way function is incredibly difficult for a computer to reverse and discover the original data. Even the public key cannot be used to decrypt the data.