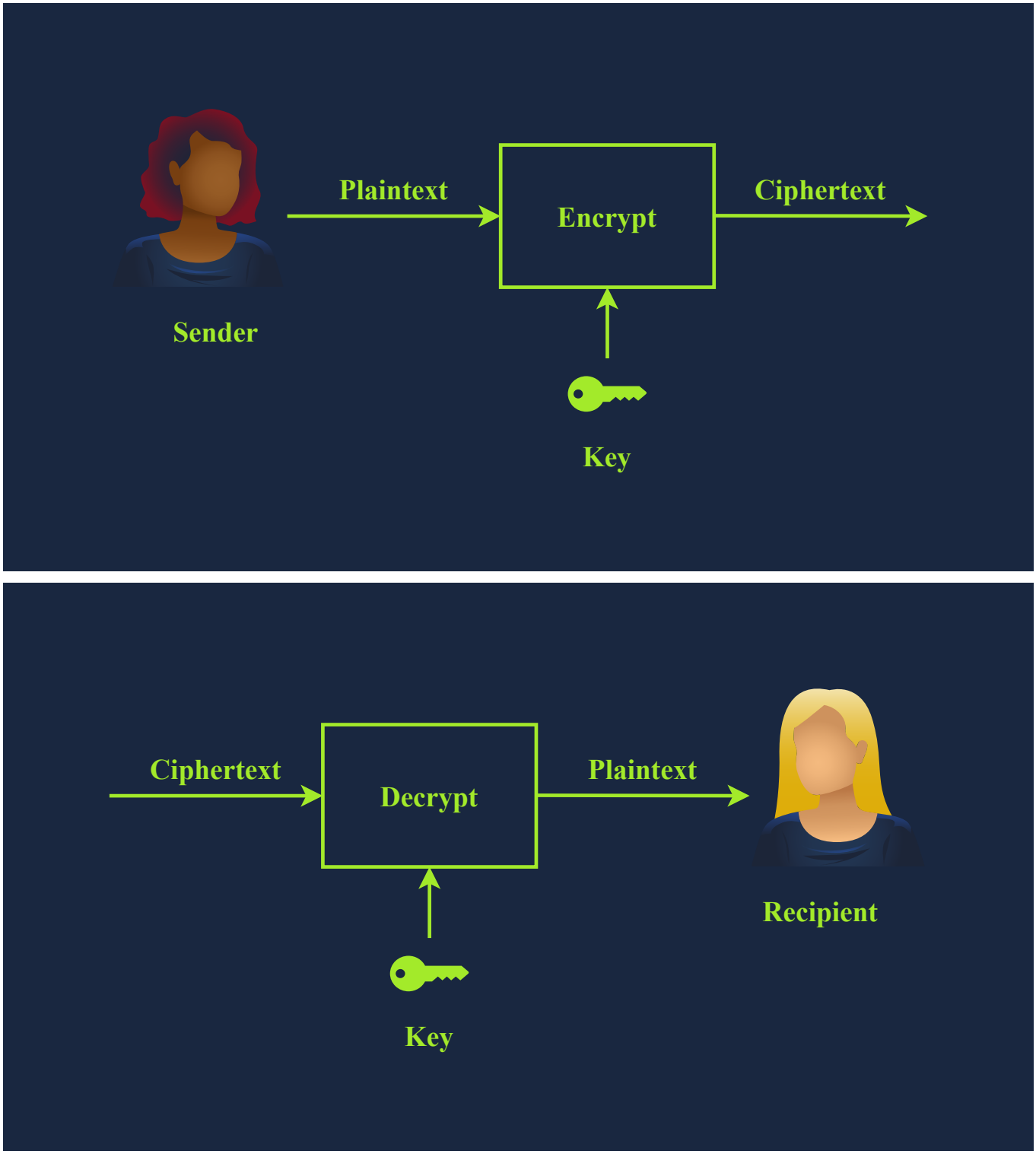
# Cryptography
## Day 25/365

Cryptography's ultimate purpose is to ensure *secure communication in the presence of adversaries*. The term secure includes confidentiality and integrity of the communicated data. Cryptography can be defined as the practice and study of techniques for secure communication and data protection where we expect the presence of adversaries and third parties. In other words, these adversaries should not be able to disclose or alter the contents of the messages.




- **Plaintext** is the original, readable message or data before it's encrypted. It can be a document, an image, a multimedia file, or any other binary data.
- **Ciphertext** is the scrambled, unreadable version of the message after encryption. Ideally, we cannot get any information about the original plaintext except its approximate size.
- **Cipher** is an algorithm or method to convert plaintext into ciphertext and back again. A cipher is usually developed by a mathematician.
- **Key** is a string of bits the cipher uses to encrypt or decrypt data. In general, the used cipher is public knowledge; however, the key must remain secret unless it is the public key in asymmetric

encryption. We will visit asymmetric encryption in a later task.

- **Encryption** is the process of converting plaintext into ciphertext using a cipher and a key. Unlike the key, the choice of the cipher is disclosed.
- **Decryption** is the reverse process of encryption, converting ciphertext back into plaintext using a cipher and a key. Although the cipher would be public knowledge, recovering the plaintext without knowledge of the key should be impossible (infeasible).

**Symmetric encryption** is a method in which the same key is used for both encryption and decryption. Consequently, this key must remain secure and never be disclosed to anyone except the intended party. **Asymmetric encryption** is a method that uses two different keys: a public key for encryption and a private key for decryption.

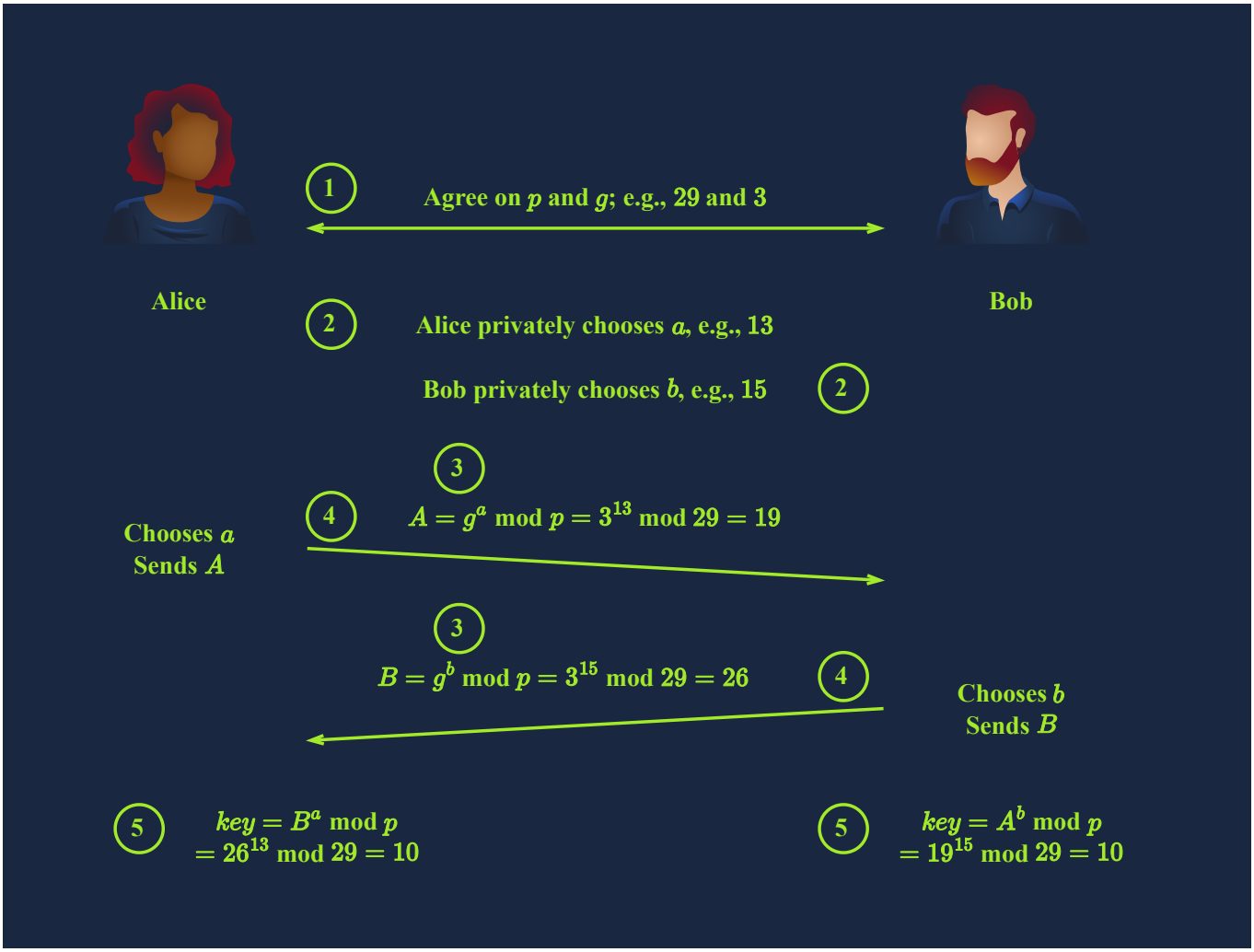
---

## Cryptography provides solutions to:

- **Authentication**: You want to be sure you communicate with the right person, not someone else pretending.
- **Authenticity**: You can verify that the information comes from the claimed source.
- **Integrity**: You must ensure that no one changes the data you exchange.
- **Confidentiality**: You want to prevent an unauthorised party from eavesdropping on your conversations.

---

## Diffie-Hellman key exchange




---

Digital signature = signing a document using a private key or a certificate