Cryptography Basics

Importance of Cryptography

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 is used to protect confidentiality, integrity, and authenticity.

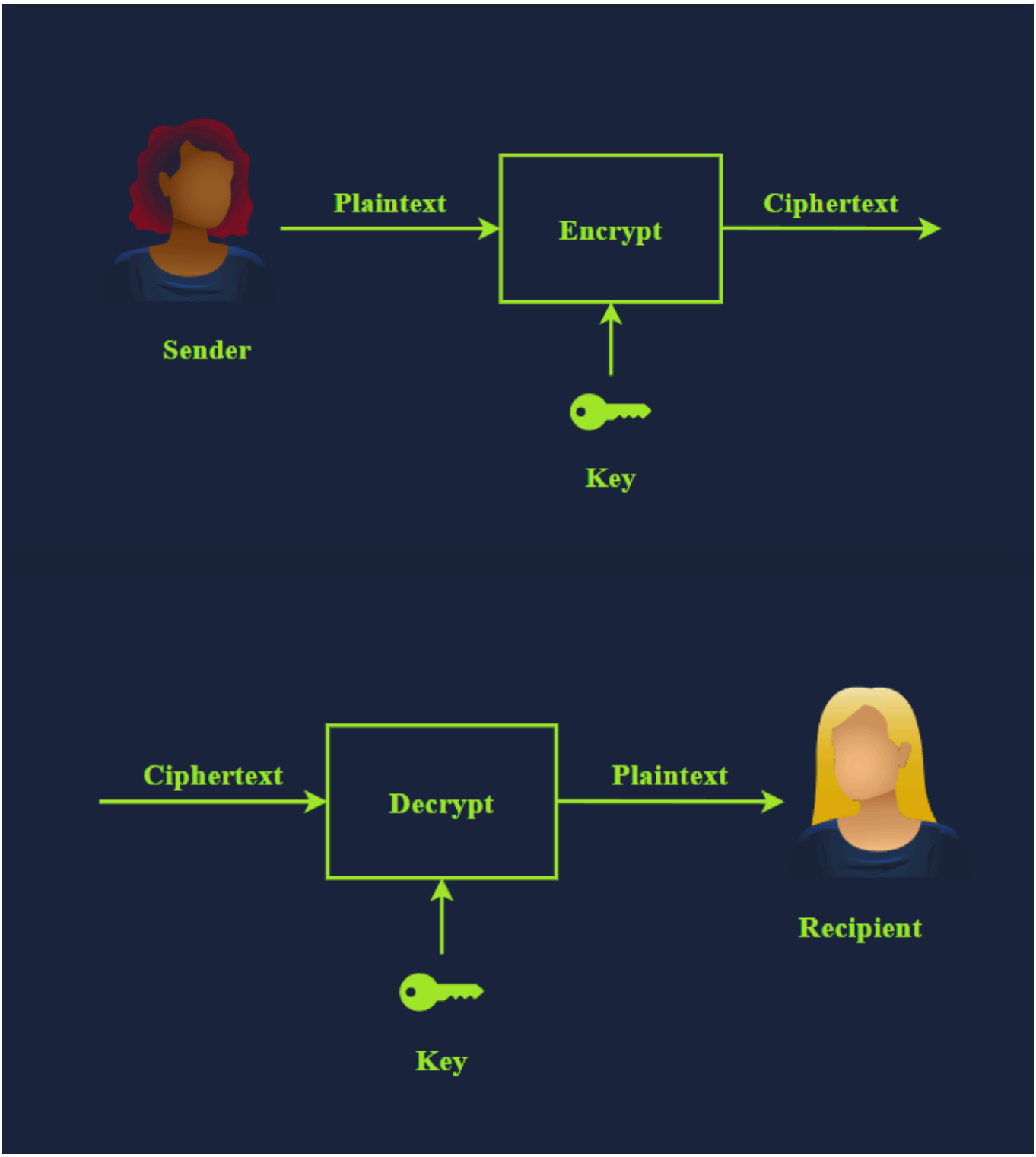
following scenarios where you would use cryptography:

- When you log in to TryHackMe, your credentials are encrypted and sent to the server so that no one can retrieve them by snooping on your connection.
- When you connect over SSH, your SSH client and the server establish an encrypted tunnel so no one can eavesdrop on your session.
- When you conduct online banking, your browser checks the remote server's certificate to confirm that you are communicating with your bank's server and not an attacker's.
- When you download a file, how do you check if it was downloaded correctly? Cryptography provides a solution through hash functions to confirm that your file is identical to the original one.

Plaintext to Ciphertext

The plaintext is the readable data

he plaintext is passed through the encryption function along with a proper key; the encryption function returns a ciphertext

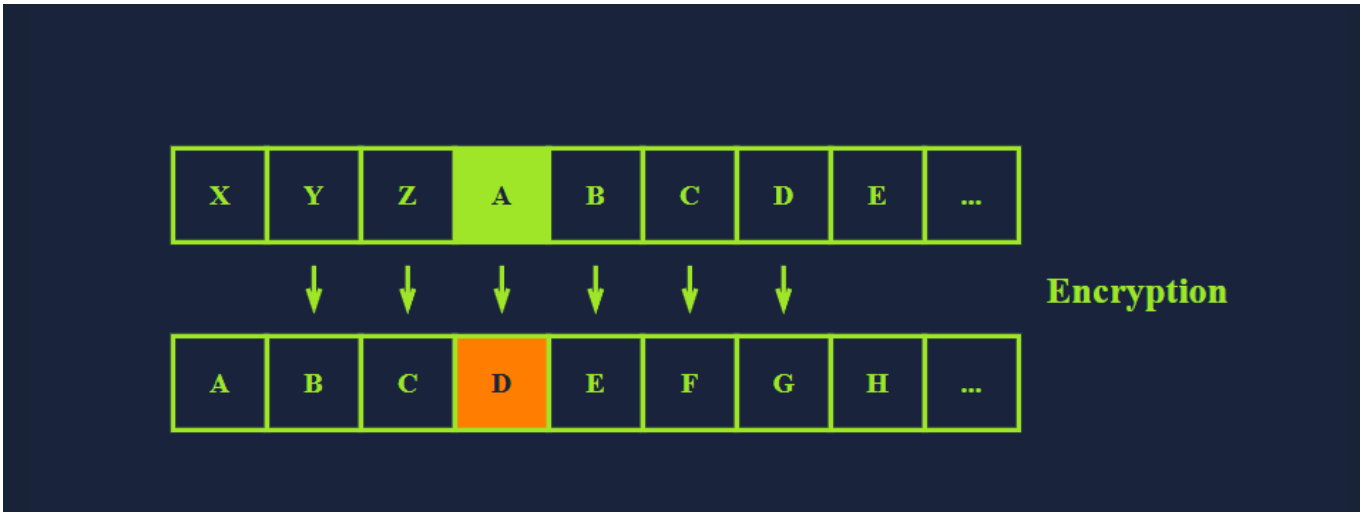


Plaintext is the original, readable message
Ciphertext is the scrambled, unreadable version
Cipher is an algorithm or method to convert plaintext into ciphertext and back again.
Key is a string of bits the cipher uses to encrypt or decrypt data
Encryption is the process of converting plaintext into ciphertext using a cipher and a key.
Decryption is the reverse process of encryption, converting ciphertext back into plaintext using a cipher and a key.

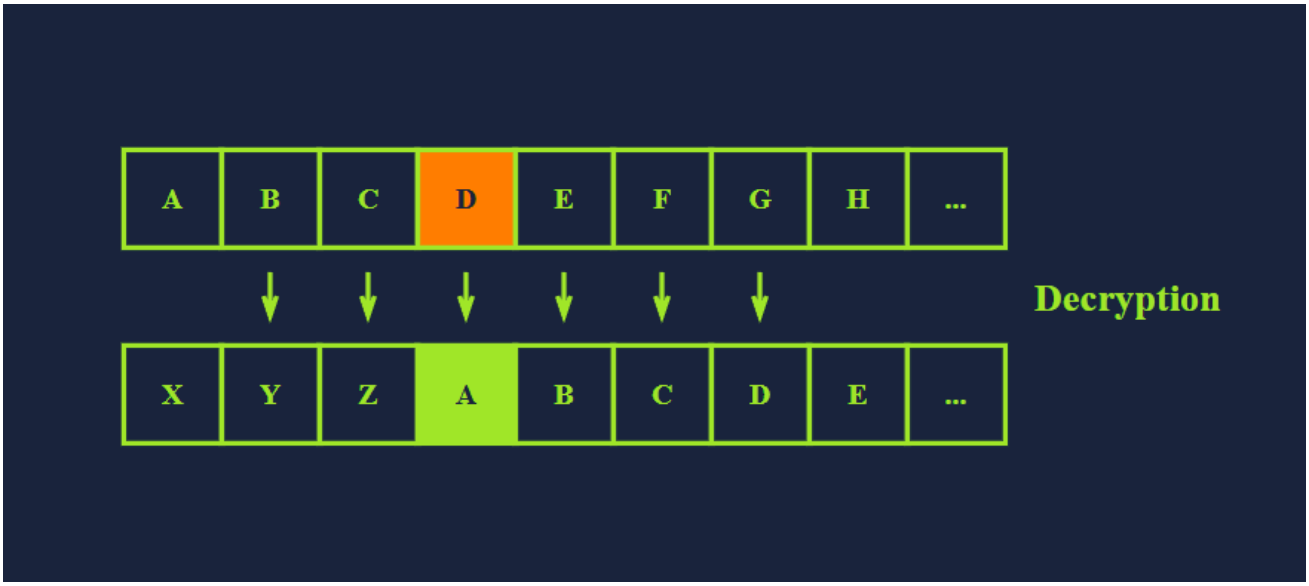
Historical Ciphers

Consider the following example:

- Plaintext: `TRYHACKME`
- Key: 3 (Assume it is a right shift of 3.)
- Cipher: Caesar Cipher
  the cipher text shifts the alphabet
  Cipher text = `WUBKDFNPH`



- Ciphertext: `WUBKDFNPH`
- Key: 3 (since we encrypted with a right shift we decrypt with a left shift of 3)
- Cipher: Caesar Cipher
  Plain text = `TRYHACKME`



Caesar Cipher is considered insecure.

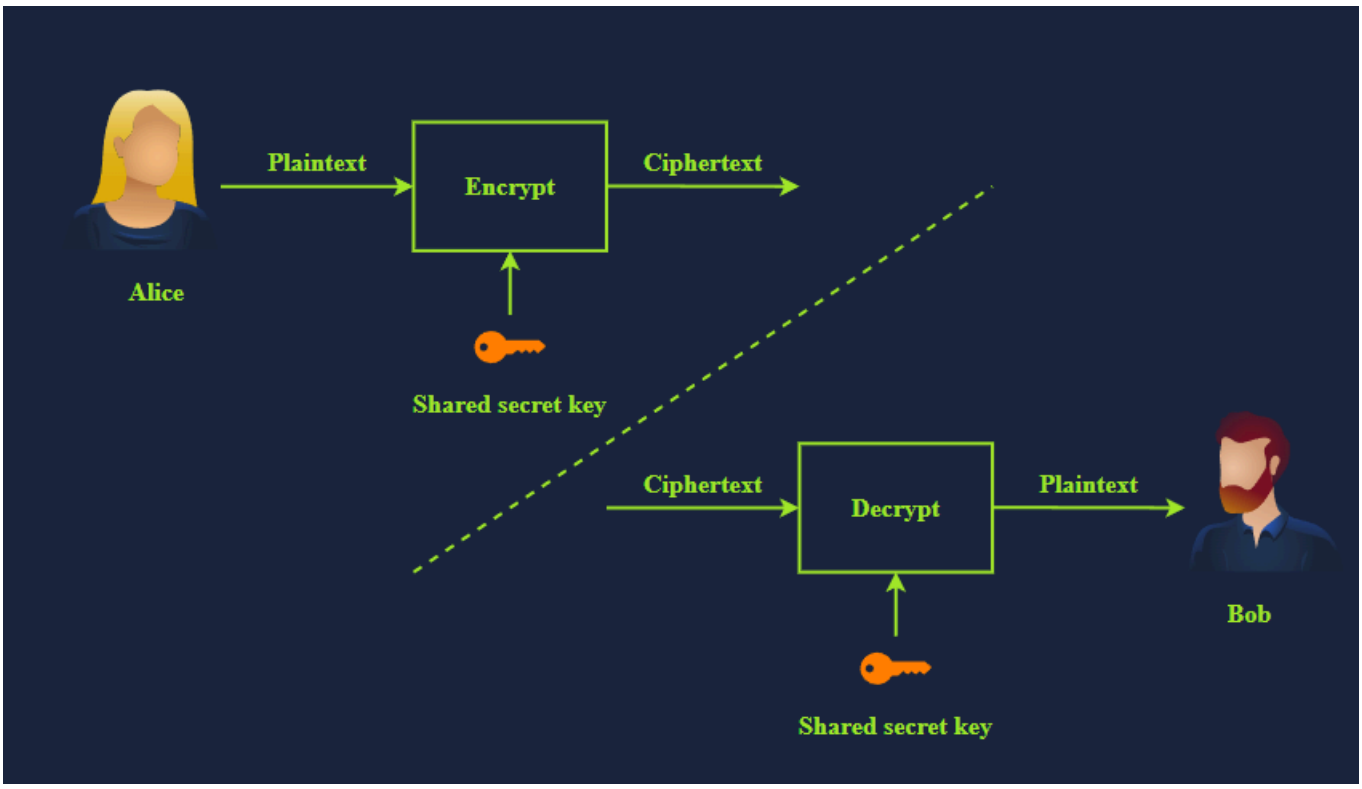
other ciphers:

- The Vigenère cipher from the 16th century
- The Enigma machine from World War II
- The one-time pad from the Cold War

Types of Encryption

Symmetric Encryption

uses the same key to encrypt and decrypt the data
Keeping the key secret is a must; it is also called **private key cryptography**



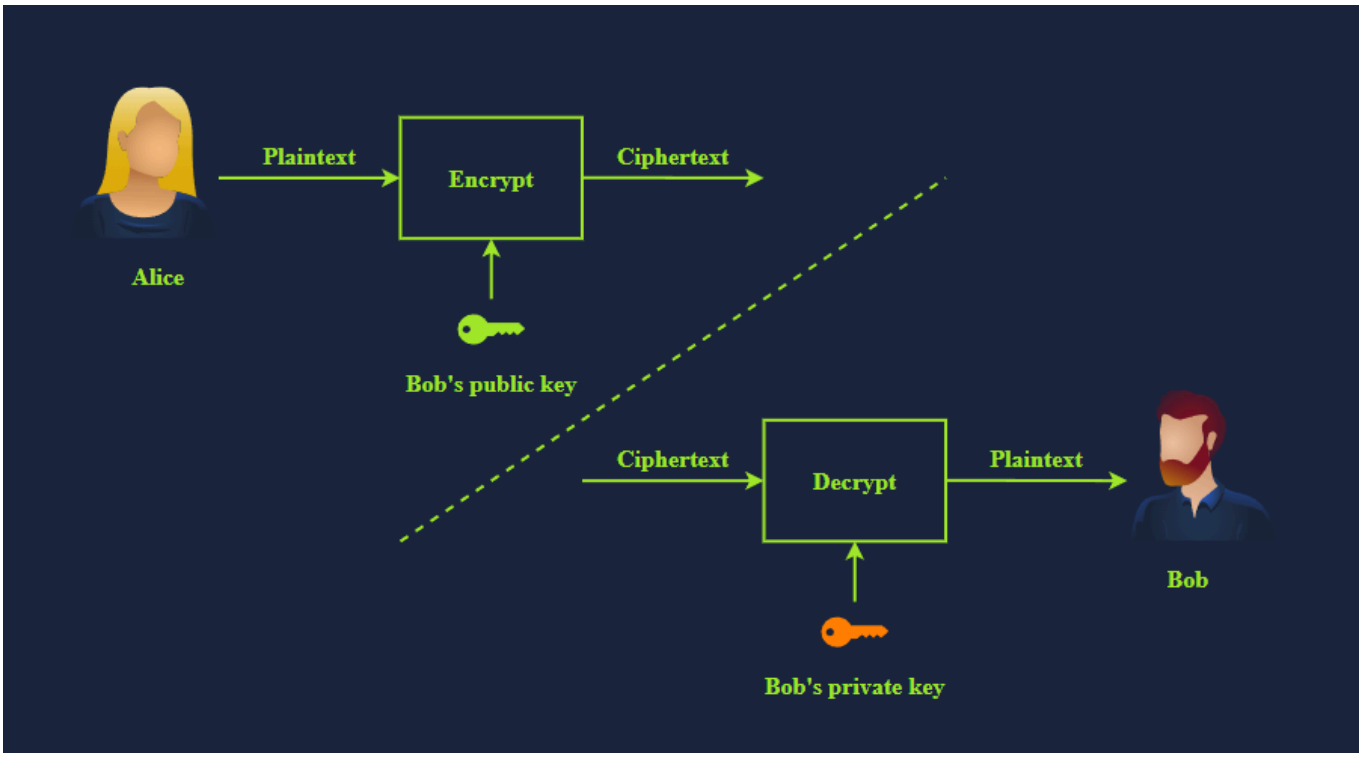
Maintaining the secrecy of the key can be a significant challenge, especially if there are many recipients

examples of symmetric encryption are DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advanced Encryption Standard).

- **DES** was adopted as a standard in 1977 and uses a 56-bit key. With the advancement in computing power, in 1999, a DES key was successfully broken in less than 24 hours, motivating the shift to 3DES.
- **3DES** is DES applied three times; consequently, the key size is 168 bits, though the effective security is 112 bits. 3DES was more of an ad-hoc solution when DES was no longer considered secure. 3DES was deprecated in 2019 and should be replaced by AES; however, it may still be found in some legacy systems.
- **AES** was adopted as a standard in 2001. Its key size can be 128, 192, or 256 bits.

Asymmetric Encryption

uses a pair of keys, one to encrypt and the other to decrypt
To protect confidentiality, asymmetric encryption or **asymmetric cryptography** encrypts the data using the public key



Examples are RSA, Diffie-Hellman, and Elliptic Curve cryptography (ECC). The two keys involved in the process are referred to as a **public key** and a **private key**. Data encrypted with the public key can be decrypted with the private key. Your private key needs to be kept private,

Basic Math

The building blocks of modern cryptography lie in mathematics. To demonstrate some basic algorithms, we will cover two mathematical operations that are used in various algorithms:

- XOR Operation
- Modulo Operation

XOR Operation

XOR compares two bits and returns 1 if the bits are different and 0 if they are the same
This operation is often represented by the symbol $\oplus$ or ^.

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

Modulo Operation

modulo operator, commonly written as % or as mod

he modulo operator, $X\%Y$, is the **remainder** when X is divided by Y

Let's consider a few examples.

- 25%5 = 0 because 25 divided by 5 is 5, with a remainder of 0, i.e., 25 = 5 × 5 + 0
- 23%6 = 5 because 23 divided by 6 is 3, with a remainder of 5, i.e., 23 = 3 × 6 + 5
- 23%7 = 2 because 23 divided by 7 is 3 with a remainder of 2, i.e., 23 = 3 × 7 + 2

The modulo operation always returns a non-negative result less than the divisor. This means that for any integer a and positive integer n, the result of $a\%n$ will always be in the range 0 to $n - 1$.

https://www.wolframalpha.com/