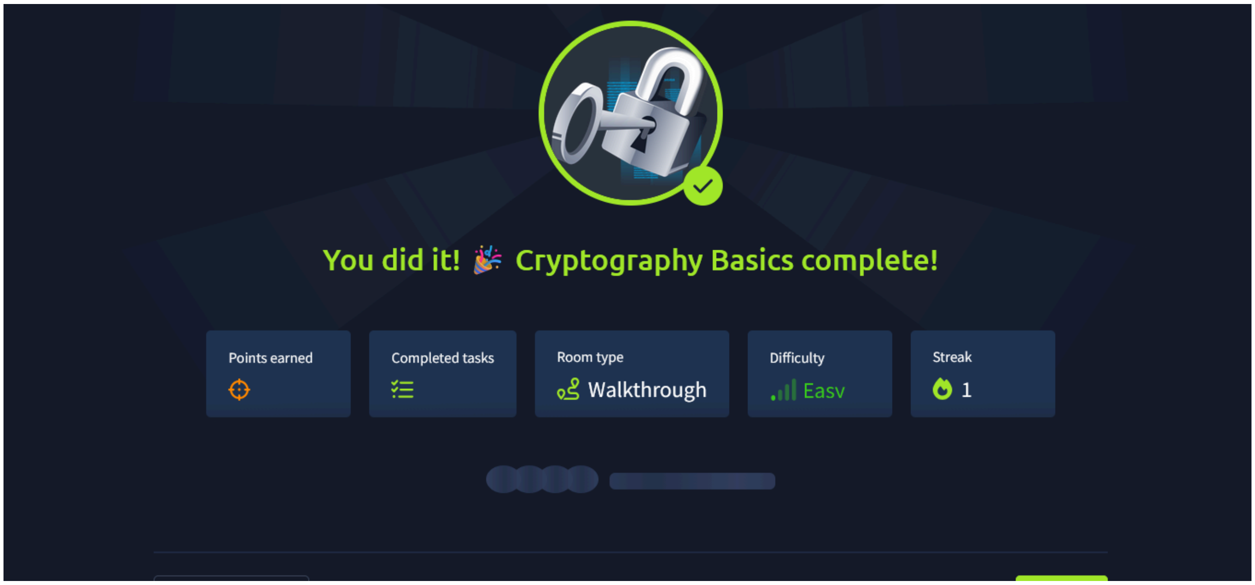
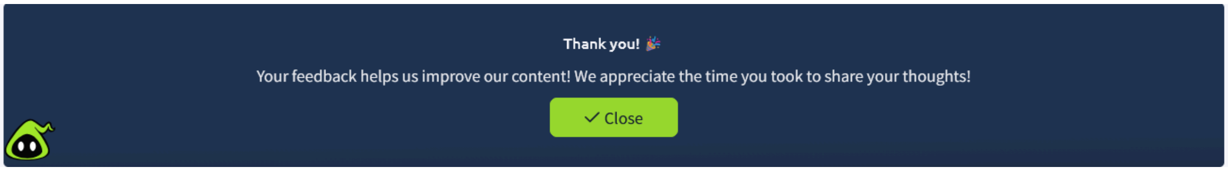
Cryptography basics



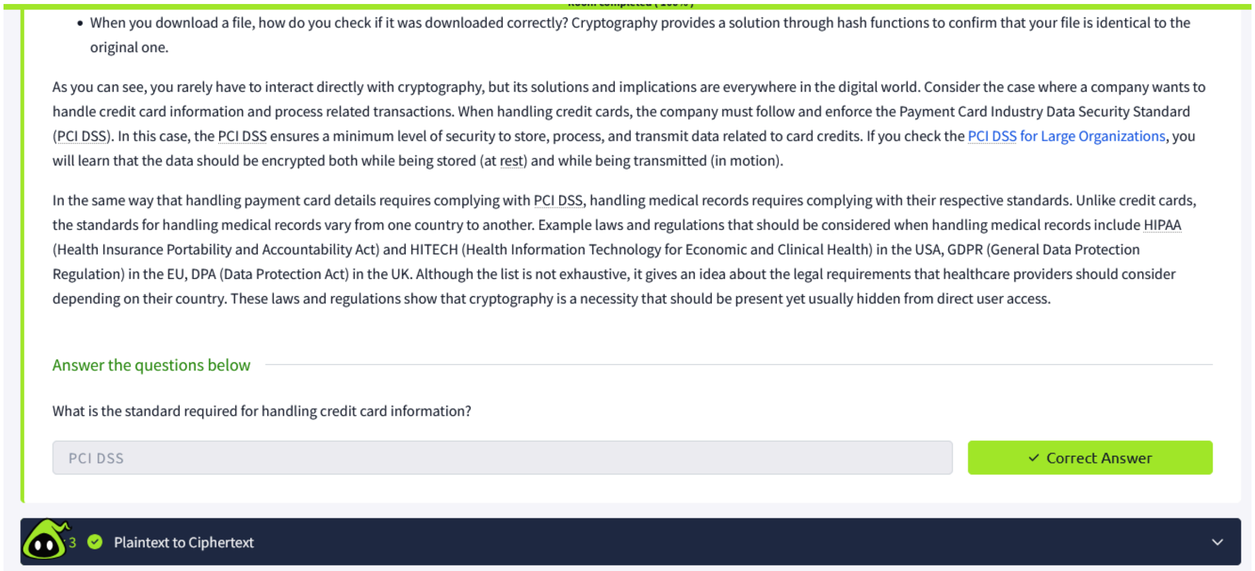
You did it! 🎉 Cryptography Basics complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
		Walkthrough	Easv	1



Thank you! 🎉

Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!



- 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.

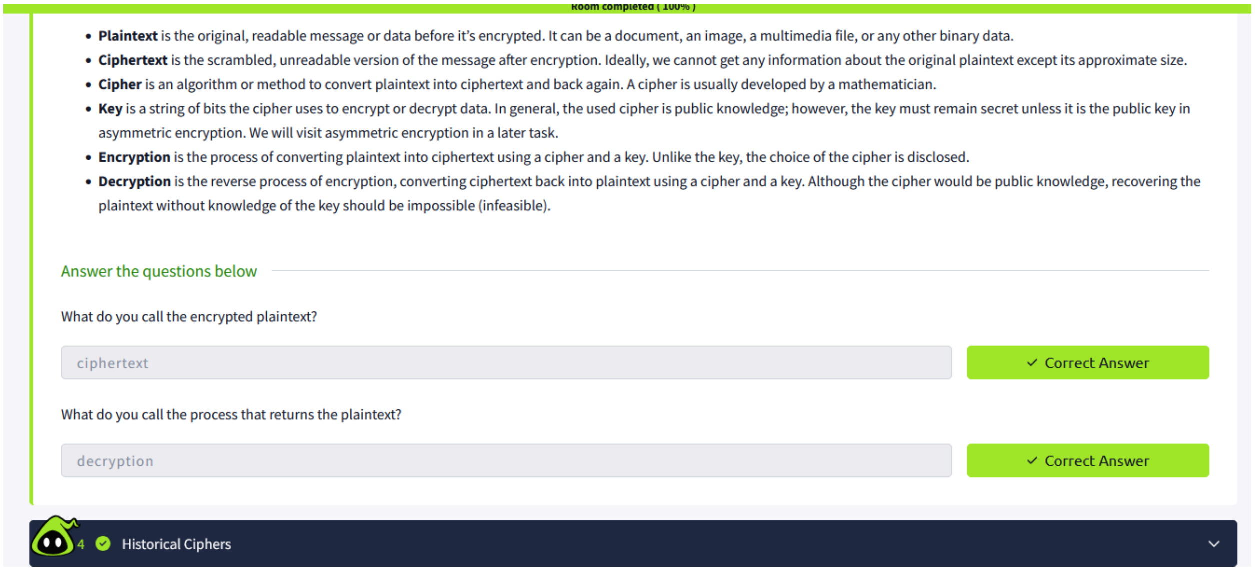
As you can see, you rarely have to interact directly with cryptography, but its solutions and implications are everywhere in the digital world. Consider the case where a company wants to handle credit card information and process related transactions. When handling credit cards, the company must follow and enforce the Payment Card Industry Data Security Standard (PCI DSS). In this case, the PCI DSS ensures a minimum level of security to store, process, and transmit data related to card credits. If you check the PCI DSS for Large Organizations, you will learn that the data should be encrypted both while being stored (at rest) and while being transmitted (in motion).

In the same way that handling payment card details requires complying with PCI DSS, handling medical records requires complying with their respective standards. Unlike credit cards, the standards for handling medical records vary from one country to another. Example laws and regulations that should be considered when handling medical records include HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health) in the USA, GDPR (General Data Protection Regulation) in the EU, DPA (Data Protection Act) in the UK. Although the list is not exhaustive, it gives an idea about the legal requirements that healthcare providers should consider depending on their country. These laws and regulations show that cryptography is a necessity that should be present yet usually hidden from direct user access.

Answer the questions below

What is the standard required for handling credit card information?

PCI DSS



Room completed (100%)

- **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).

Answer the questions below

What do you call the encrypted plaintext?

ciphertext

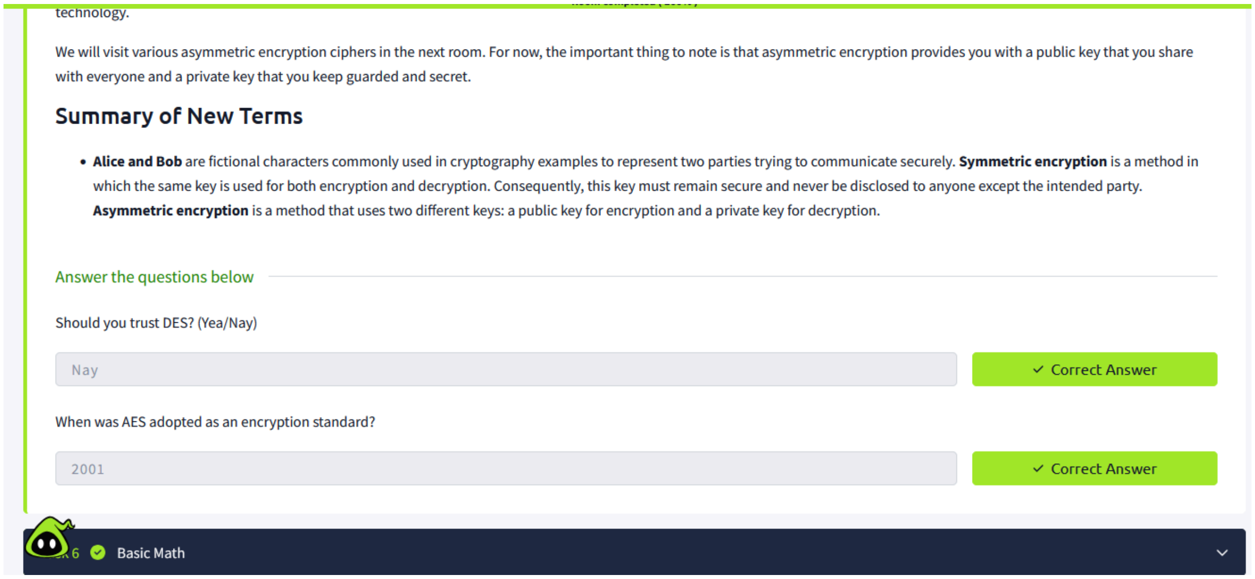
✓ Correct Answer

What do you call the process that returns the plaintext?

decryption

✓ Correct Answer

4 ✓ Historical Ciphers



technology.

We will visit various asymmetric encryption ciphers in the next room. For now, the important thing to note is that asymmetric encryption provides you with a public key that you share with everyone and a private key that you keep guarded and secret.

Summary of New Terms

- **Alice and Bob** are fictional characters commonly used in cryptography examples to represent two parties trying to communicate securely. **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.

Answer the questions below

Should you trust DES? (Yea/Nay)

Nay

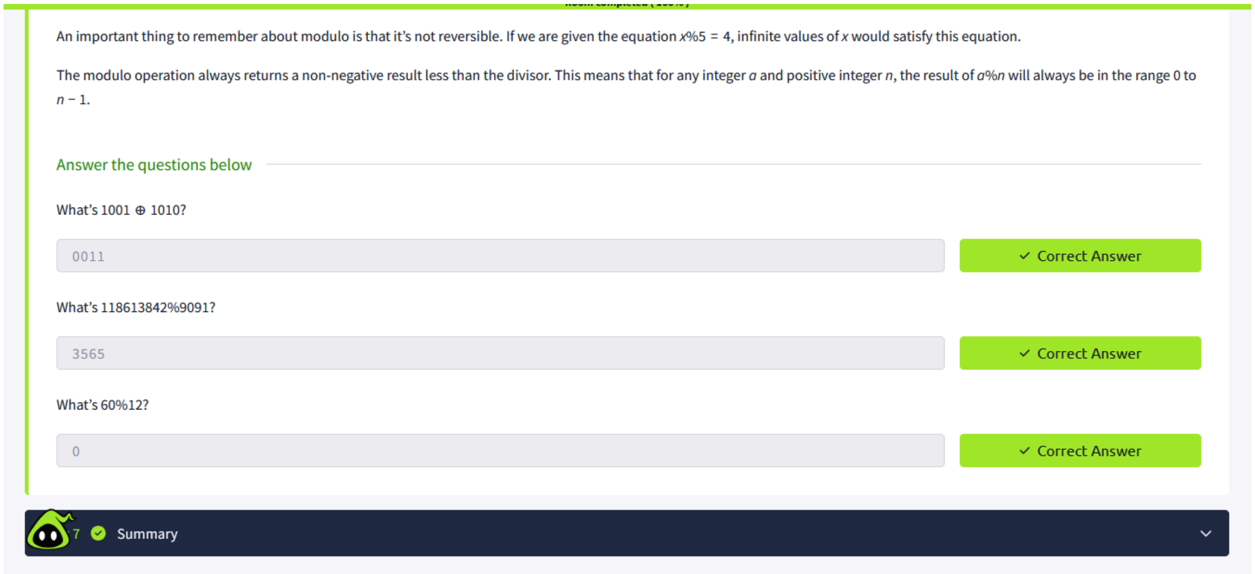
✓ Correct Answer

When was AES adopted as an encryption standard?

2001

✓ Correct Answer

sk 6 ✓ Basic Math



An important thing to remember about modulo is that it’s not reversible. If we are given the equation $x\%5 = 4$, infinite values of x would satisfy this equation.

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 $n-1$.

Answer the questions below

What’s 1001 ⊕ 1010?

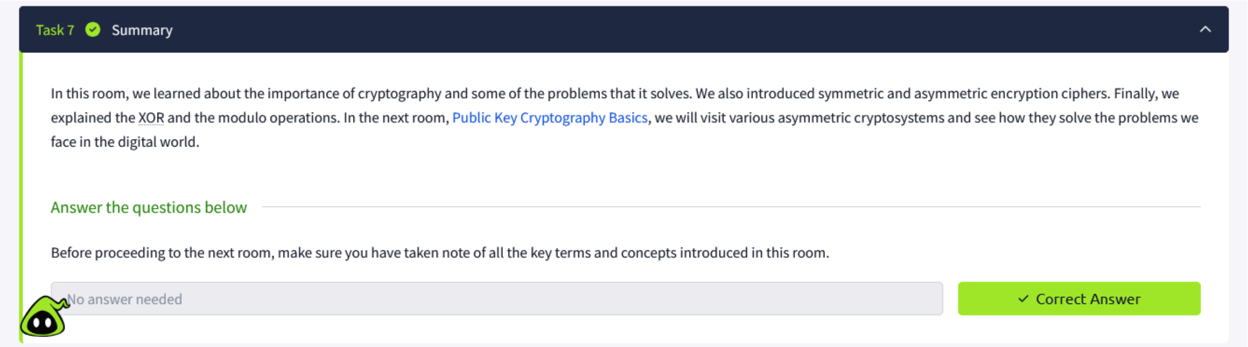
0011 | ✓ Correct Answer

What’s 118613842%9091?

3565 | ✓ Correct Answer

What’s 60%12?

0 | ✓ Correct Answer



In this room, we learned about the importance of cryptography and some of the problems that it solves. We also introduced symmetric and asymmetric encryption ciphers. Finally, we explained the XOR and the modulo operations. In the next room, Public Key Cryptography Basics, we will visit various asymmetric cryptosystems and see how they solve the problems we face in the digital world.

Answer the questions below

Before proceeding to the next room, make sure you have taken note of all the key terms and concepts introduced in this room.

No answer needed | ✓ Correct Answer