1. Symmetric Encryption, Block Ciphers and Stream Ciphers

Learn the fundamentals of symmetric encryption, as well as the differences between block ciphers and stream ciphers, and their respective modes of operation. This lesson will not go too much in depth to keep these lessons simple, so I highly recommend you to explore each concept in your own time.

1 Learn

1.1 Symmetric Encryption

Encrypting and decrypting information **using the same key** for both of these operations is what we call symmetric cryptography.

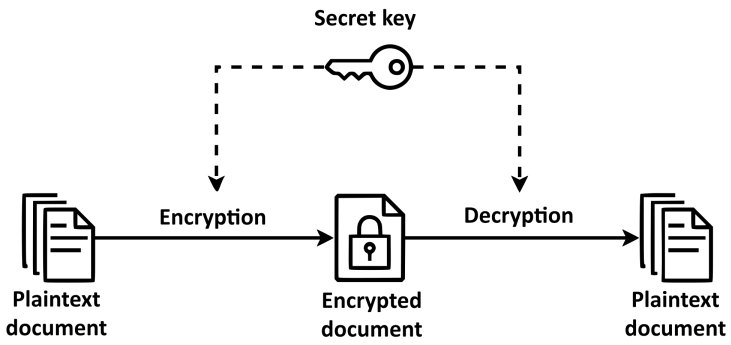

Figure 1: Symmetric encryption process

A plethora of different algorithms have been developed over the years. Most commonly used to this day are AES (also known as Rijndael), ChaCha20, ARIA, Camellia, and a couple of others. You may have also heard about ciphers like RC4, DES and 3DES, however they are considered to be insecure and therefore were deprecated.

1.2 Where is it used?

Whenever we talk about encryption protocols, you can safely assume symmetric encryption is used. For example, TLS secures web access by combining symmetric and asymmetric ciphers, key exchange, authentication, and hashing (in what we call a ciphersuite). Symmetric ciphers are also the standard for encrypting large data volumes. VeraCrypt, a disk encryption utility, uses AES, Camellia, Kuznyechik, where as BitLocker uses AES. SSH used RC4, DES, and 3DES in the past, but now primarily relies on AES and ChaCha20.

1.3 Symmetric vs. Asymmetric

Distinctive differences between symmetric and asymmetric cryptography have been described in the table below.

	Symmetric	Asymmetric
Key aspects	Symmetric cryptography uses **one key** to encrypt and decrypt information.	Asymmetric cryptography uses **two keys** that are mathematically-bound, where one is public and shared with others and the other one is kept private. Public key is used for encrypting messages, and the private key is used to decrypting messages.
Key security	Anyone that has access to the key can decrypt the ciphertext.	You can only decrypt information if you are in possesion of the private key. Having access to the public key does not give the adversary the ability to decrypt information.
Use cases	Encrypting large volumes of data, ie. files, drives, streams, etc.	Encrypting smaller volumes of data (messages, e-mails, keys), creating digital signatures, key exchange
Operation speed	Encryption and decryption is usually very fast and efficient, computational requirements are smaller.	Asymmetric operations are slower due to key sizes, computational overhead mathematical complexity.
Assurances	Symmetric ciphers provide only **Confidentiality**.	Asymmetric ciphers provide **Confidentiality**, as well as **Integrity** and **Non-repudiation**.

You should understand that symmetric cryptography-despite it's security implications and limitations-plays an important part in what we call today hybrid cryptography.

1.4 Block ciphers

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1.5 Stream ciphers

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales

commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

2 Practice

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.