# Cryptography Tools In OpenSSL

**By: Nadia Karichev and Jesus Ramirez**

# What is OpenSSL?

OpenSSL is an open-source software library used for secure communication over computer networks. It implements the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols, providing essential cryptographic functions and various utility commands for managing SSL/TLS certificates.

Encryption & Decryption


Hashing


Saltin g

# When and Why Encrypt?

**Importance of Encryption:** Encryption is crucial for protecting sensitive data from unauthorized access. It ensures privacy, data integrity, and secure communication, preventing data breaches and cyber attacks

**When to Encrypt:** Encryption is necessary when handling personal, financial, or confidential information, such as during online transactions, storing sensitive data, and communicating over unsecured networks

**2022-2024 Statistics**

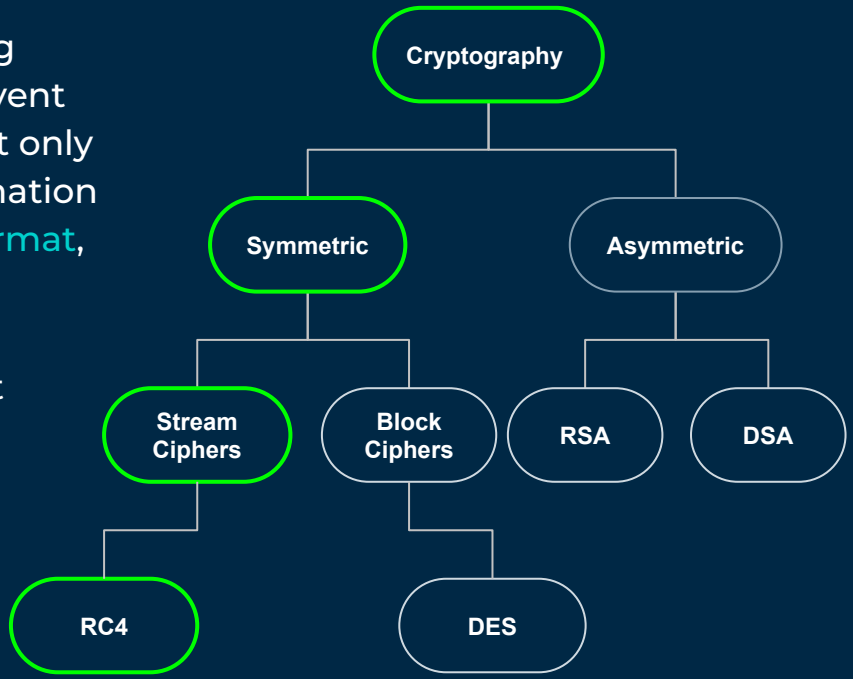
- Seven million unencrypted data records are compromised every day[1].
- Over 80% of data breaches involve data stored in the cloud, with many breaches attributed to unencrypted data[2].
- Only 45% of sensitive data stored in the cloud is currently encrypted[3].


1. Craig McCart, comparitech.com, (March 29, 2022)
2. Beth Stackpole, mitsloan.mit.edu, (April 30, 2024)
3. Daniel Todd, itpro.com, (July 5, 2023)

# Encryption & Decryption

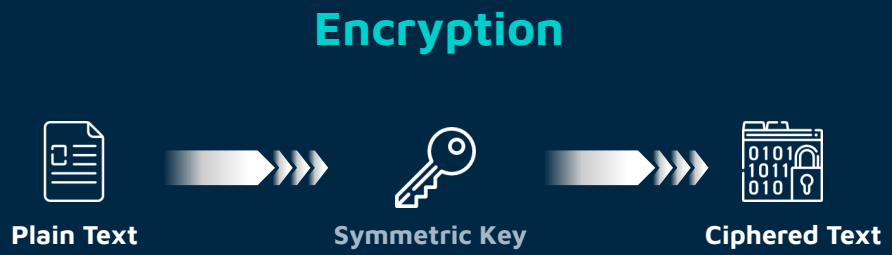
Encryption is the process of converting information or data into a code to prevent unauthorized access. This ensures that only authorized parties can read the information by converting it into an unreadable format, known as ciphertext.

**RC4** is a symmetric stream cipher that encrypts data by generating a pseudorandom stream of bits and combining it with the plaintext using bitwise exclusive OR (XOR).



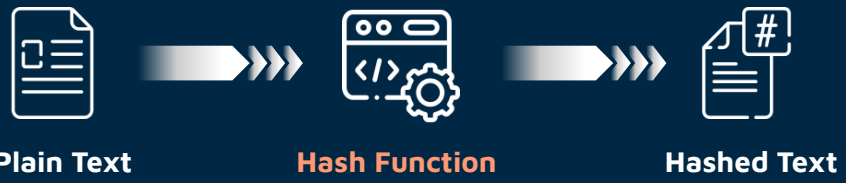
# Symmetric Encryption

Symmetric encryption is a method of encryption where the same key is used to both encrypt and decrypt data. This approach is efficient and straightforward, making it suitable for securing large volumes of data.

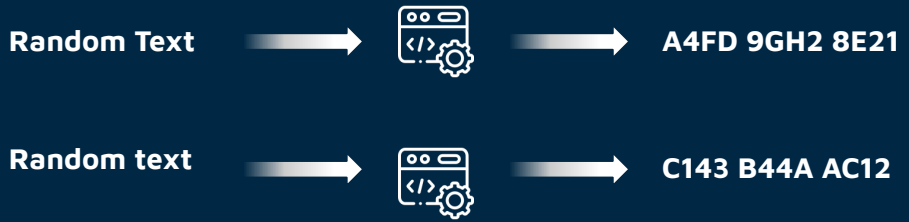


# Hashing

Hashing is the process of converting data into a fixed-size string of characters, which appears random. This method creates a unique identifier, or "fingerprint," for the data, facilitating efficient data retrieval and verification without storing the original data.




- Fast Data Access
- Efficient Storage
- Unique Identifiers
- Ensuring Data Integrity



# Salting

Salting is the process of adding a unique, random value to data before hashing it. This ensures that even identical data entries produce different hash values, enhancing security by protecting against precomputed attacks like rainbow tables.

# If you get Stuck

As you work through the exercises, you'll encounter steps or commands that require you to problem-solve. If you get stuck, there's an Employee_Handbook file for each section (encryption, decryption, hashing, and salting). Each file contains the full commands related to that section. Use cat [section]_Employee_Handbook.txt in the terminal to view the guidance if needed. If you're still unsure after consulting the file, feel free to call one of us over for help.

- Changing Directories
- View Contents of File
- List Items in Directory

# Basic Linux Commands

| | |
|---|---|
| Go to root directory | cd |
| Go back one directory | cd.. |
| Go to specific directory | cd /home/kali/[directory_name] |
| Print working directory | pwd |
| View items in directory | ls |
| View contents of file | cat [file_name] |
| Open text editor to edit file | nano [file_name] |
| Move item to new location | mv [file_name]  /home/kali[new_location] |
| Rename file or directory | mv [old_name]  [new_name] |
| Remove file or directory | rm [file_or_directory_name] |

# Sign In Form