Red Hat
Enterprise Linux

Cryptography - Data Obfuscation Techniques

Operate First Data Science Community Meetup

Surya Prakash Pathak
Data Scientist
Open Services team

Red Hat

Contents

- Intro to Cryptography
- Types of Cryptography
- Cryptographic hash function
- Demo

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. It is a science of providing security and protection of information.

Useful for **Data Scientist, Developers, Software Engineers**. Has a huge application in cyber security.

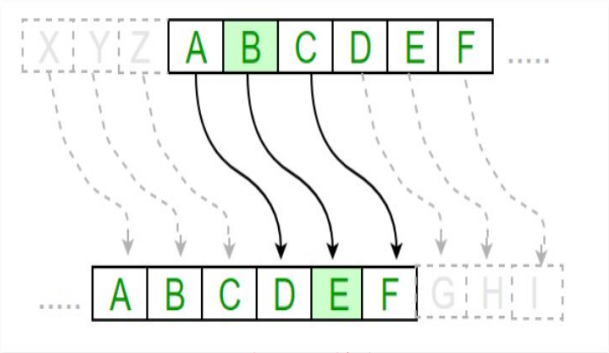
Crypto + Graphy → Secret Writing

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

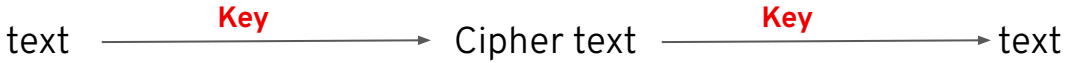


Caesar Cipher

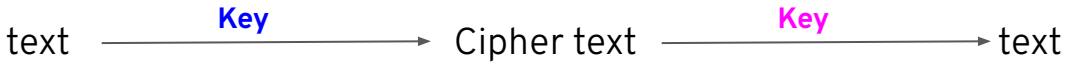
Purpose of Cryptography

- **Authentication :** Process of proving one's identity.
- **Privacy :** Ensuring that no one can read the message except the intended receiver.
- **Integrity :** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non- repudiation :** A mechanism to prove that the sender really sent this message.

Types of Cryptographic Algorithms



1) **Secret key (symmetric) cryptography:** It uses a single key for both encryption and decryption.



2) **Public key (Asymmetric) cryptography:** It uses two keys, one for encryption and other for decryption

3) **Hash Functions (one-way cryptography):** It has no key, since the plain text is not recoverable from the cipher text.

Hash Function

A hash function is any function that can be used to map data to arbitrary size to fixed sized values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

Message or data block (M)

Hash value (h)

#

h = #(M)

Properties of Cryptographic Hash

- **Pre-Image Resistance:** For essentially all pre-specified outputs, it is computationally infeasible to find any input which hashes to that output. This means that a hash can be computed relatively easily for a given string(s), but inverting the output to find the original string(s) is difficult.

- **Second Pre-Image Resistance:** It is computationally infeasible to find any second input which has the same output as any specified input. This means given a certain string input, it should be difficult to find another input that produces the same hash. Also known as Weak Collision Resistance.

- **Collision Resistance:** It is computationally infeasible to find any two distinct inputs which hash to the same output. This means it should be difficult to find two different strings that create the same hash.


AND NOW
TIME FOR A LIVE DEMO

Tips for secure Passwords

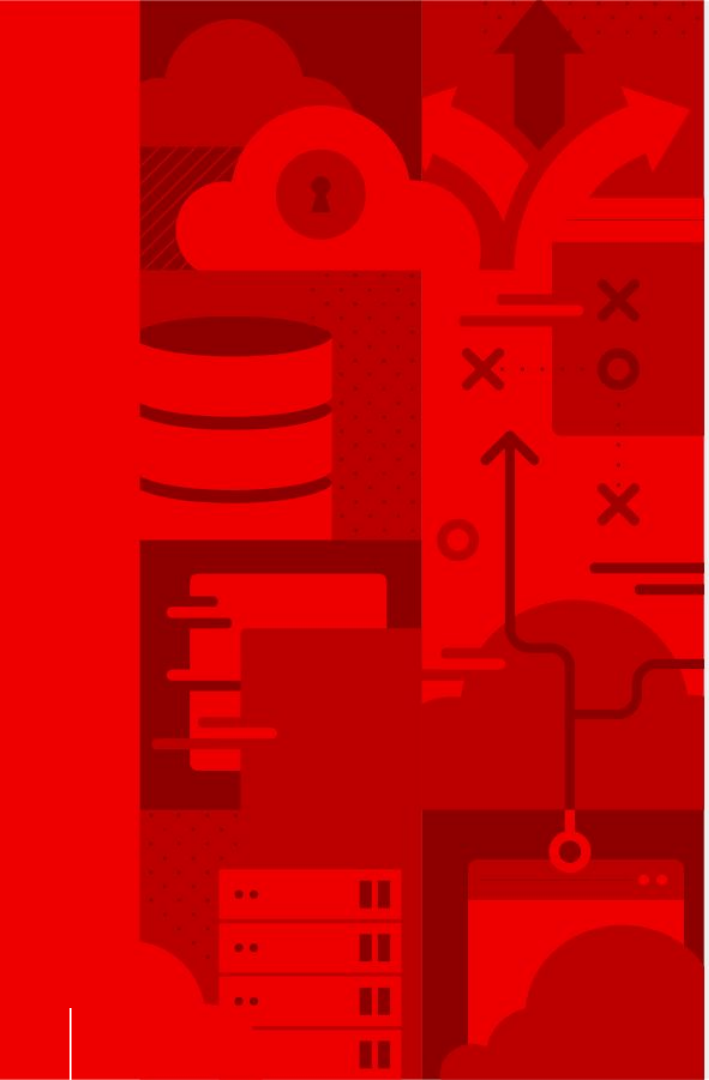
- Use a Password generator.
- Go over all your accounts and delete the ones you no longer use.
- Use two-factor authentication, whenever possible.
- Regularly check each of your accounts.

Fun facts about Passwords

The top 10 most common passwords list:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Source: Link



Thank you!

For queries,

Email :supathak@redhat.com

Github

Linkedin

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat