@satheeshkv

Encryption & Hashing

#DigitalSecurity

SWIPE

- **Encryption** is the process of converting plaintext data into ciphertext to protect its confidentiality.
- **Use cases:** Encryption is used to protect sensitive information such as passwords, credit card numbers, and other personal information from unauthorized access.
- **Types:** Encryption can be classified into two types: symmetric encryption, where the same key is used for both encryption and decryption, and asymmetric encryption, where two different keys are used.
- **Algorithms:** Encryption algorithms include AES, DES, RSA, and Blowfish, among others.

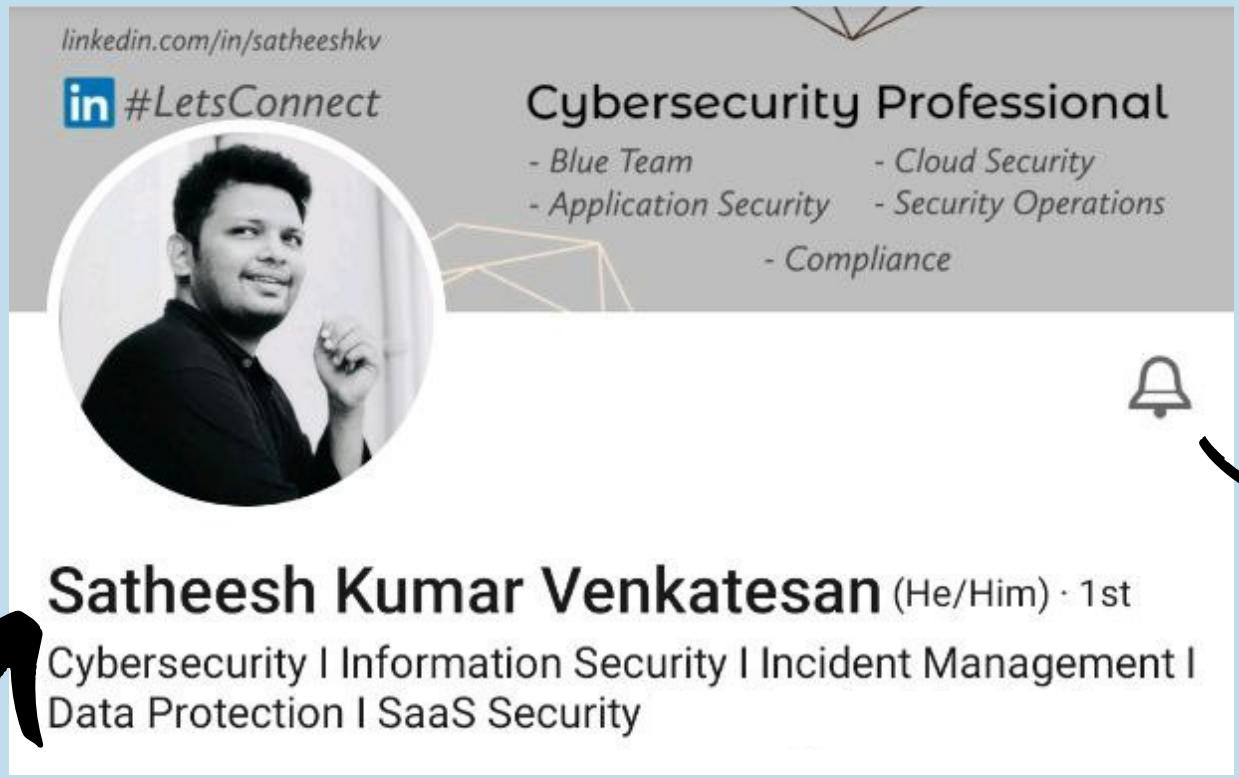
- **Symmetric encryption** uses a single key to encrypt and decrypt data.
- **Use cases:** Symmetric encryption is commonly used to encrypt data that is stored locally or transmitted over a secure network.
- **Algorithms:** Symmetric encryption algorithms include AES, DES, and Blowfish, among others.
- **Key management:** Symmetric encryption requires careful management of the encryption key to ensure its confidentiality and integrity.

- **Symmetric encryption** uses a single key to encrypt and decrypt data.
- **Use cases:** Symmetric encryption is commonly used to encrypt data that is stored locally or transmitted over a secure network.
- **Algorithms:** Symmetric encryption algorithms include AES, DES, and Blowfish, among others.
- **Key management:** Symmetric encryption requires careful management of the encryption key to ensure its confidentiality and integrity.

- **Asymmetric encryption** uses a pair of keys, one public and one private, to encrypt and decrypt data.
- **Use cases:** Asymmetric encryption is commonly used to establish secure communication channels between parties that have not previously communicated with each other.
- **Algorithms**: Asymmetric encryption algorithms include RSA, DSA, and ECC, among others.
- **Key management:** Asymmetric encryption requires careful management of the public and private keys to ensure their confidentiality and integrity.

- **Hashing** is the process of converting data of any size into a fixed-size output called a hash.
- **Use cases:** Hashing is used to verify the integrity of data and ensure that it has not been tampered with.
- **Types:** Hashing can be classified into two types: Cryptographic hashing, which is used for security purposes, and Non-cryptographic hashing, which is used for indexing and searching.
- **Algorithms:** Hashing algorithms include SHA-256, SHA-512, MD5, and CRC32, among others.

- Overall, Encryption is two-way, the data can be decrypted so it is readable again. Hashing, on the other hand, is one-way, meaning the plaintext is scrambled into a unique digest, through the use of a salt, that cannot be decrypted.



Set **All** to get
Daily Cybersecurity
Info

Follow & **Connect**

Let's be a part in my Professional Journey