Encryption Algorithms

Process of Converting Plain Text to Cipher Text

Data Encryption

- Data encryption is a common and effective security method—a sound choice for protecting an organization's information

Why Encryption

- Authentication. Public key encryption proves that a website's origin server owns the private key and thus was legitimately assigned an SSL certificate.
- Privacy. Encryption guarantees that no one can read messages or access data except the legitimate recipient or data owner.
  - This measure prevents cybercriminals, hackers, internet service providers, spammers, and even government institutions from accessing and reading personal data.
- Regulatory Compliance. Many industries and government departments have rules in place that require organizations that work with users' personal information to keep that data encrypted.
- Security. Encryption helps protect information from data breaches, whether the data is at rest or in transit.

DES (Data Encryption Standard)

- The DES algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST).
- The algorithm takes plain text in 64-bit blocks and converts them into cipher text using 48-bit keys.
- Since it's a symmetric-key algorithm, it employs the same key in both encrypting and decrypting the data.
- DES is based on the Feistel block cipher, called LUCIFER, developed in 1971 by IBM cryptography researcher Horst Feistel.

AES

- The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government, as well as other organizations.
- Although extremely efficient in the 128-bit form, AES also uses 192- and 256-bit keys for very demanding encryption purposes.
- AES is widely considered invulnerable to all attacks except for brute force.
- Regardless, many internet security experts believe AES will eventually be regarded as the go-to standard for encrypting data in the private sector.

Triple DES

- Triple DES is the successor to the original Data Encryption Standard (DES) algorithm, created in response to hackers who figured out how to breach DES.
- It's a symmetric encryption that was once the most widely used symmetric algorithm in the industry, though it's being gradually phased out.
- Triple DES applies the DES algorithm three times to every data block and is commonly used to encrypt UNIX passwords and ATM PINs.

Rivest-Shamir-Adleman (RSA)

- Rivest-Shamir-Adleman is an asymmetric encryption algorithm that works off the factorization of the product of two large prime numbers. Only a user with knowledge of these two numbers can decode the message successfully. Digital signatures commonly use RSA, but the algorithm slows down when it encrypts large volumes of data.

RSA

- RSA is a public-key encryption asymmetric algorithm and the standard for encrypting information transmitted via the internet.
- RSA encryption is robust and reliable because it creates a massive bunch of garbage that frustrates would-be hackers, causing them to expend a lot of time and energy to crack into systems.

Blowfish

- Blowfish is another algorithm that was designed to replace DES.
- This symmetric tool breaks messages into 64-bit blocks and encrypts them individually.
- Blowfish has established a reputation for speed, flexibility, and being unbreakable.
- It's in the public domain, so that makes it free, adding even more to its appeal.
- Blowfish is commonly found on e-commerce platforms, securing payments, and in password management tools.

Twofish

- Twofish is Blowfish's successor.
- It's a license-free, symmetric encryption that deciphers 128-bit data blocks.
- Additionally, Twofish always encrypts data in 16 rounds, no matter what the key size.
- Twofish is perfect for both software and hardware environments and is considered one of the fastest of its type.
- Many of today's file and folder encryption software solutions use this method.

Query Session

WKDQN BRK