Algoritmos para encriptamiento:

RSA (Rivest-Shamir-Adleman)

RSA (Rivest-Shamir-Adleman)

Es un algoritmo de cifrado asimétrico usado para enviar información de forma segura.

¿Para qué sirve? Para cifrar datos (asegurar que solo el destinatario pueda leerlos) y para crear firmas digitales (asegurar que un mensaje proviene de quien dice ser). Es la base de las conexiones seguras en internet (HTTPS), las transacciones bancarias y la comunicación segura.

¿Cómo funciona? La clave de RSA es que utiliza un par de llaves matemáticamente vinculadas:

1. Llave Pública: Se puede compartir con cualquiera. Sirve para "cerrar la caja" (cifrar el mensaje).
2. Llave Privada: Es secreta y solo el dueño la conoce. Sirve para "abrir la caja" (descifrar el mensaje).

El proceso se basa en la dificultad matemática de factorizar números muy grandes. Es muy fácil tomar dos números primos gigantes y multiplicarlos para obtener un número público. Sin embargo, es prácticamente imposible tomar ese número público y adivinar cuáles fueron los dos primos originales que lo crearon. Esa es la "función trampa"

que le da su seguridad.

Analogía simple: Imagina que repartes candados abiertos (tu llave pública) a todos tus amigos. Cualquiera puede tomar uno de tus candados, meter un mensaje en una caja y cerrarlo. Pero la única persona en el mundo que tiene la llave para abrir ese candado (tu llave privada) eres tú.

Punto Clave: Lo que se cifra con la llave pública, solo se puede descifrar con la llave privada correspondiente, y viceversa.

MD5 (Message Digest 5)

Es un algoritmo de hash(o de resumen), lo que significa que crea una "huella digital" única de un dato o archivo.

¿Para qué sirve? Su propósito principal es verificar la integridad de los datos. Se usa para comprobar que un archivo que descargaste de internet no ha sido alterado o corrompido. No sirve para ocultar información.

¿Cómo funciona? MD5 toma una entrada (un archivo, un texto, cualquier dato) de cualquier tamaño y, a través de una serie de operaciones matemáticas, produce una salida de tamaño fijo: una cadena de 32 caracteres hexadecimales (128 bits).

Es un proceso de una sola vía. No puedes tomar el hash

MD5 y reconstruir el archivo original.

Cualquier cambio, por mínimo que sea, en el archivo de entrada (como cambiar una sola letra) producirá un hash MD5 completamente diferente.

Analogía simple: Piensa en MD5 como unalicuadora de datos. Metes cualquier ingrediente (tu archivo) y la licuadora siempre te dará un batido del mismo tamaño. Puedes hacer el batido cuantas veces quieras con los mismos ingredientes y siempre saldrá idéntico. Pero es imposible tomar el batido y separar los ingredientes originales.

Punto Clave: MD5 no es cifrado, es un resumen. Importante: Hoy en día, MD5 se considera criptográficamente roto e inseguro para fines de seguridad (como almacenar contraseñas), porque se han descubierto "colisiones" (dos archivos diferentes que pueden generar el mismo hash). Sin embargo, todavía se usa comúnmente para verificar la integridad de archivos.

Base64

Es un algoritmo de codificación, no de cifrado. Su única función es transformar datos binarios en texto plano.

¿Para qué sirve? Para enviar datos binarios (como imágenes, PDFs, o archivos ejecutables) a través de medios que solo están diseñados para manejar texto simple (ASCII). El caso

de uso más famoso es adjuntar archivos a un correo electrónico.

¿Cómo funciona? Los sistemas de texto pueden corromperse si encuentran caracteres binarios "extraños". Base64 resuelve esto traduciendo los datos binarios a un alfabeto seguro de 64 caracteres que incluye `A-Z`, `a-z`, `0-9`, `+` y `/`.

1. Toma los datos binarios en bloques de 3 bytes (24 bits).
2. Divide esos 24 bits en cuatro bloques de 6 bits cada uno.
3. Cada bloque de 6 bits corresponde a uno de los 64 caracteres del alfabeto Base64.
4. El resultado es una larga cadena de texto que se puede enviar de forma segura sin que se corrompa. El receptor simplemente revierte el proceso para obtener el archivo original.

Analogía simple: Es como un traductor para un viajero. Tienes un objeto (tus datos binarios) que no puedes llevar en el avión. Lo describes detalladamente en una carta usando un lenguaje universal (el alfabeto Base64). Envías la carta, y la persona que la recibe usa esa descripción para reconstruir el objeto idéntico.

Punto Clave: Base64 no ofrece ninguna seguridad. Es una codificación totalmente reversible y su propósito es la compatibilidad de transporte, no la confidencialidad.