UNIVERSIDAD DEL ISTMO

CAMPUS TEHUANTEPEC

MATERIA:

Redes de Computadoras II.

DOCENTE:

I.C Carlos Mijangos Jiménez.

ALUMNO (A):

Karla Guadalupe Cordero Luna.

ACTIVIDAD: INVESTIGACIÓN

SEMESTRE:

7°

PARCIAL:

1°

CARRERA:

Ingeniería En Computación.

FECHA DE ENTREGA: MARTES 15 DE OCTUBRE DE 2025.

1. **RSA (Rivest–Shamir–Adleman)**

   Tipo: Algoritmo de cifrado asimétrico

   Uso principal: Seguridad en la transmisión de datos (por ejemplo, HTTPS, firmas digitales).

   Descripción:

   - Fue creado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977.
   - Usa dos claves diferentes:
     - ✓ Una clave pública (para cifrar).
     - ✓ Una clave privada (para descifrar).
   - Se basa en la dificultad matemática de factorizar números primos grandes.
   - Es muy usado en la comunicación segura por internet, autenticación y certificados digitales.

   Ejemplo de uso:

   Cuando entras a una página con https://, el navegador usa RSA (u otro algoritmo similar) para intercambiar claves de forma segura.

2. **MD5 (Message Digest 5)**

   Tipo: Algoritmo hash (función resumen).

   Uso principal: Verificación de integridad de archivos o contraseñas.

   Descripción:

   - Crea una huella digital de 128 bits (generalmente representada como una cadena de 32 caracteres hexadecimales).
   - Es una función unidireccional: no se puede obtener el texto original a partir del hash.
   - Fue muy popular, pero ya no se considera seguro, porque se pueden crear colisiones (dos entradas diferentes que dan el mismo hash).

   Ejemplo:

   MD5("hola") = 4d186321c1a7f0f354b297e8914ab240

3. **B64 (Base64)**

   Tipo: Método de codificación (no es cifrado).

   Uso principal: Representar datos binarios en formato de texto.

   Descripción:

- Convierte datos binarios (como imágenes, contraseñas cifradas o archivos) a texto legible en ASCII, usando 64 caracteres posibles (A–Z, a–z, 0–9, +, /).
- Se usa mucho en correo electrónico (MIME), autenticación HTTP (Basic Auth) y JSON Web Tokens (JWT).
- No protege los datos, solo los codifica para que puedan transmitirse fácilmente.

Ejemplo:

Base64("hola") = aG9sYQ==