TLS

ENCRIPTACIÓN

AES

PROTEGER DATOS SENSIBLES (COMO CONTRASEÑAS Y DATOS BANCARIOS), ASEGURAR COMUNICACIONES (TLS, IPSEC), CIFRAR ALMACENAMIENTO (DISCOS), EN DISPOSITIVOS IOT DE BAJO CONSUMO Y EN AUTENTICACIÓN Y FIRMAS DIGITALES.

FUNCION AES_CIFRADO(CLAVE, BLOQUE):
1. EXPANSIÓN DE CLAVE: GENERAR SUBCLAVES.
2. INICIALIZAR ESTADO: COPIAR BLOQUE.
3. AÑADIR CLAVE: XOR ESTADO CON SUBCLAVE.

PARA CADA RONDA:
4. SUSTITUCIÓN DE BYTES.
5. DESPLAZAMIENTO DE FILAS.
6. MEZCLA DE COLUMNAS.
7. AÑADIR CLAVE: XOR ESTADO CON SUBCLAVE.

8. ÚLTIMA RONDA (SIN MEZCLA DE COLUMNAS).
9. RETORNAR BLOQUE CIFRADO.

RC4

RC4 SE USA EN COMUNICACIONES SEGURAS (WEP, WPA), CIFRADO DE DATOS EN ARCHIVOS, SESIONES SSL/TLS, Y EN ALGUNAS APLICACIONES DE VPN.

FUNCION RC4(CLAVE, TEXTO):
1. INICIALIZAR VECTOR S CON VALORES 0 A 255.
2. CREAR VECTOR K DE LA MISMA LONGITUD QUE LA CLAVE.
3. MEZCLAR VECTOR S USANDO LA CLAVE.

PARA CADA BYTE EN EL TEXTO:
4. CALCULAR UN ÍNDICE CON S.
5. GENERAR EL BYTE DE CIFRADO CON S.
6. XOR EL BYTE DE TEXTO CON EL BYTE DE CIFRADO.

7. RETORNAR TEXTO CIFRADO.

AUTENTICACIÓN

MAC

MAC SE UTILIZA EN APLICACIONES QUE REQUIEREN AUTENTICACIÓN DE MENSAJES, COMO EN PROTOCOLOS DE COMUNICACIÓN SEGURA (TLS, IPSEC), ALMACENAMIENTO SEGURO Y TRANSACCIONES FINANCIERAS, PARA ASEGURAR QUE LOS DATOS NO HAYAN SIDO ALTERADOS Y PROVENGAN DE UNA FUENTE LEGÍTIMA.

FUNCION MAC(CLAVE, MENSAJE):
1. CONCATENAR CLAVE Y MENSAJE.
2. APLICAR UNA FUNCIÓN HASH (EJ. SHA-256) AL VALOR CONCATENADO.
3. RETORNAR EL HASH COMO MAC.

SHA-1 / SHA-2

SHA-1 Y SHA-2 (CON HMAC) SE UTILIZAN EN PROTOCOLOS DE AUTENTICACIÓN Y FIRMA DIGITAL (COMO EN TLS/SSL, IPSEC), VERIFICACIÓN DE INTEGRIDAD DE DATOS Y AUTENTICACIÓN DE MENSAJES, GARANTIZANDO QUE LOS DATOS NO HAYAN SIDO ALTERADOS Y PROVENGAN DE UNA FUENTE LEGÍTIMA, CON SHA-2 SIENDO MÁS SEGURO QUE SHA-1.

FUNCION HMAC_SHA(CLAVE, MENSAJE, HASH_FUNC):
1. SI LA CLAVE ES CORTA, EXTENDERLA CON CEROS.
2. SI LA CLAVE ES LARGA, APLICAR HASH_FUNC A LA CLAVE.
3. K_IPAD = CLAVE XOR 0X36 (64 BYTES)
4. K_OPAD = CLAVE XOR 0X5C (64 BYTES)
5. PASO1 = HASH_FUNC(K_IPAD || MENSAJE)
6. HMAC = HASH_FUNC(K_OPAD || PASO1)
7. RETORNAR HMAC

INTEGRIDAD

CRC

CRC SE USA PARA DETECTAR ERRORES EN TRANSMISIÓN DE DATOS, COMO EN PROTOCOLOS DE RED (ETHERNET, HDLC), ALMACENAMIENTO DE DATOS (DISCOS, CD/DVD), Y SISTEMAS DE COMUNICACIÓN DE ALTA CONFIABILIDAD.

FUNCION CRC(MENSAJE, POLINOMIO):
1. INICIALIZAR CRC = 0.
2. PARA CADA BYTE DEL MENSAJE:
   A. REALIZAR XOR ENTRE CRC Y BYTE.
   B. DESPLAZAR CRC Y APLICAR POLINOMIO.
3. RETORNAR CRC.

MD5

MD5 SE USA PARA VERIFICAR LA INTEGRIDAD DE ARCHIVOS, CONTRASEÑAS, FIRMAS DIGITALES Y SUMAS DE VERIFICACIÓN EN PROTOCOLOS COMO SSL/TLS, PERO NO ES SEGURO PARA APLICACIONES CRÍTICAS DEBIDO A VULNERABILIDADES.

FUNCION MD5(MENSAJE):
1. INICIALIZAR LOS REGISTROS A, B, C, D.
2. DIVIDIR EL MENSAJE EN BLOQUES DE 512 BITS.
3. PARA CADA BLOQUE:
   A. REALIZAR OPERACIONES DE MEZCLA CON A, B, C, D.
4. CONCATENAR A, B, C, D PARA OBTENER EL RESUMEN MD5.
5. RETORNAR MD5.