Examen Tema 5

Created	@11 de enero de 2025 17:42
Tags	

Preguntas Autoevaluación Teoría

Tema 5: Criptografía

Criptografía que emplean una única clave, utilizada y compartida en secreto por emisor y receptor. Pueden usar cifrado de bloque (dentro de un modo de operación) o de flujo.

Critografía simétrica

Criptografía donde cada usuario genera un par de claves, la pública (conocida por todos) y la privada (conocida por sólo él mismo).

Criptografía asimétrica

Clave solo conocida por el usuario.

Clave privada

Clave conocida por todos.

Clave pública

Mensaje encriptado.

Criptograma

Se puede definir con una quíntupla (M, C, K, E, D).

Criptosistema

Ocultación en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no).

Esteganografía

Garantiza la autenticación.

Firma digital

Función que se utiliza principalmente para garantizar la autenticidad de la información.

Hash

Conjunto de técnicas empleadas para la ruptura de los códigos criptográficos.

Criptoanálisis

Se emplea para agrupar tanto a la Criptografía como al Criptoanálisis.

Criptología

Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Criptografía

Imposibilidad computacional (tiempo de cálculo en años que excede cualquier valor razonable) de romper el cifrado o encontrarla clave secreta a partir de otros datos de carácter público.

Fortaleza

$p(C, M, K) = p(C, M', K')$

Criptosistema con secreto perfecto

Sólo se usa durante la conexión que se establece entre dos sistemas a comunicar. Cada clave sólo se usa una vez.

Clave de sesión

Cada agente tiene una y la comparte con el servidor para distribuir las claves de sesión.

Clave permanente

Se cifra carácter a carácter según un flujo continuo de claves.

Cifrado en flujo

El cifrado/descifrado consiste en realizar la función XOR. La clave permitía obtener una secuencia binaria y aleatoria S que se almacenaba en una cinta que alimentaba un teletipo. Esa clave era igual de larga que el mensaje y sólo se usaba una vez (one time pads).

Cifrado Vernam

Operan sobre cadenas de un tamaño fijo (bloques). Cada bloque se cifra con la misma clave. Se integran en un modo de operación.

Cifrado en bloques

Cambiar un carácter por otro según una regla.

Sustitución

Sustitución simple que usa un alfabeto rotado p posiciones hacia delante.

ROT

Tratan de «aplanar» la distribución de probabilidad. A cada carácter pueden corresponderle varios caracteres, según su frecuencia en el lenguaje.

Homofónicas

Generalización del método César. La clave consiste en N claves de cifrado por sustitución simple, que se usan consecutivamente y de manera cíclica para todo el mensaje.

Vigénere

Se cifra por digramas (bloques de dos caracteres). Una de las reglas es: si M1M2 están en la misma fila, C1C2 son los dos caracteres de la derecha.

Playfair

También denominado permutación. Consiste en reordenar los caracteres del mensaje. Por columnas, filas, patrones geométricos...

Transposición

Algoritmo de cifrado en bloque desarrollado por el gobierno de los EEUU como un intento de crear un estándar para las comunicaciones.

DES

A diferencia de DES, el proceso de selección, revisión y estudio fue abierto a todo el mundo. Es software libre.

AES

Es uno de los más difundidos, y es considerado como un estándar en la criptografía de clave pública.

RSA

Transport Layer Security y su predecesor Secure Socket Layer son protocolos de la capa de aplicación en el modelo TCP/IP.

TLS y SSL

Protocolo de la capa de Internet. Ofrece servicios de seguridad a un nivel bajo.

IPsec

Protocolo de la capa de aplicación que permite crear una conexión remota con la consola de administración de una máquina.

SSH

Datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los datos, así como protegerlos contra falsificaciones.

Firma electrónica

Documento electrónico que permite vincular una clave pública con la identidad real de su creador.

Certificado digital

¿Cuál de los siguientes no es un modo de operación de cifrado?

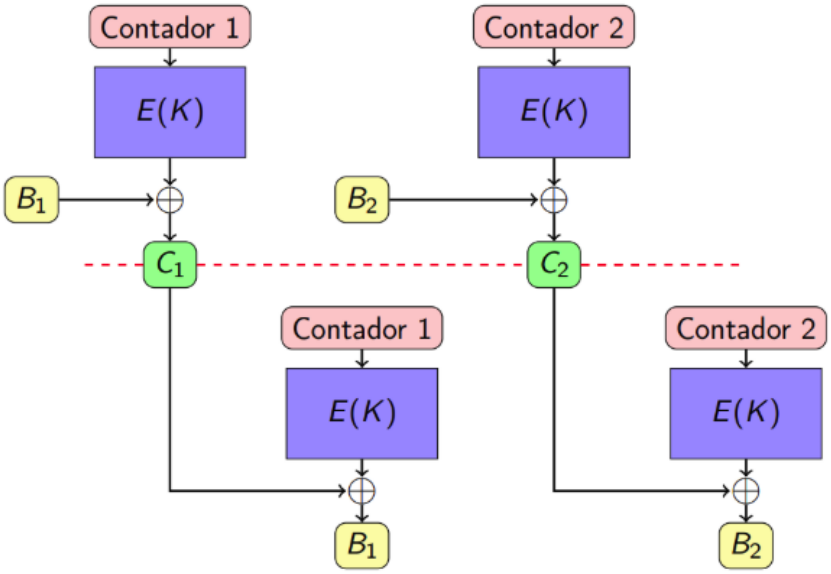
Cipher Flow Chainging (CFC)

Si solo queremos asegurar la autenticidad de un mensaje transmitido por la red empleando cifrado asimétrico, deberá cifrarse el mensaje con:

Clave privada

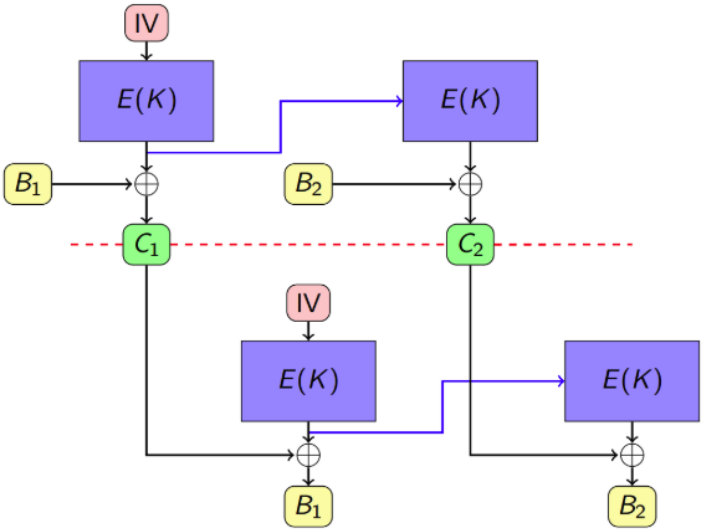
Responde a las siguientes imágenes

1.COUNTER (CTR)

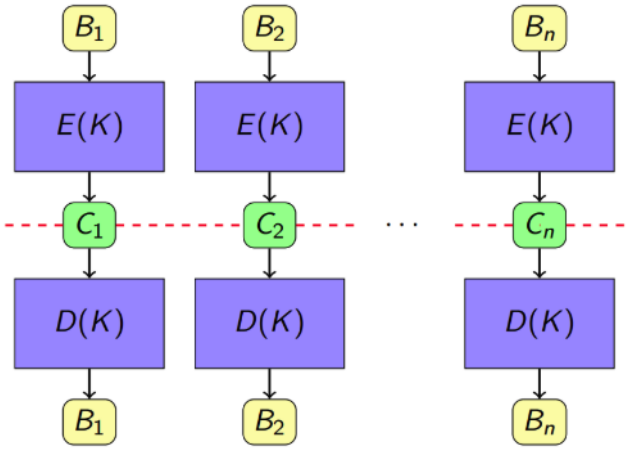


2.ESCÍTALA

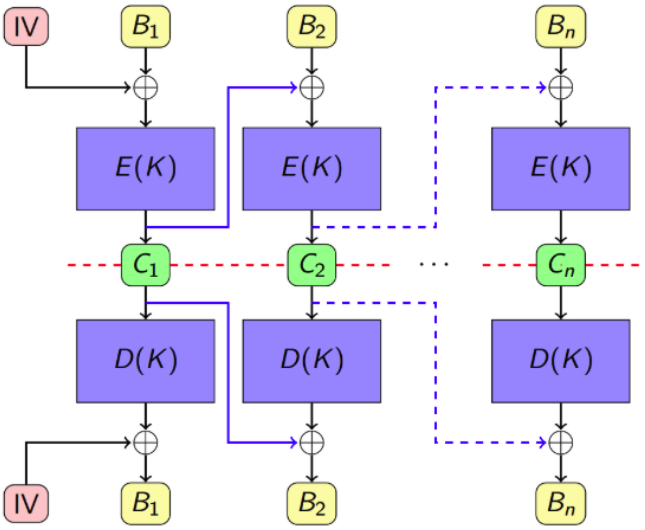
3.OUTPUT FEEBACK (OFB)



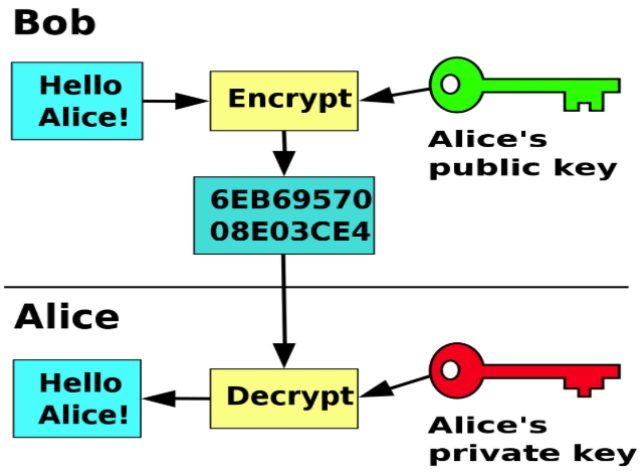
4.ELECTRONIC CODEBOOK (ECB)



5.CIPHER BLOCK CHAINGING (CBC)



6.CIFRADO ASIMÉTICO



Ejercicios de criptografía

Playfair

A	B	C	D	E
F	G	H	**I**/J	K
L	M	**N**/Ñ	O	P
Q	R	S	T	U
V	W	X	Y	Z

Vigénere y transposición por columnas

Letra	a	b	c	d	e	f	g	h	i	j	k	l	m
Número	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
Número	13	14	15	16	17	18	19	20	21	22	23	24	25	26

1. Si partimos de la primera matriz, y usamos **MONEDA** como clave, ¿qué se obtiene al cifrar **MINANDO CRIPTOMONEDAS** con el método **Playfair**? Cuando se plantee la opción, escoja **I** y **N** en vez de J y Ñ.

   OH MC EM NB WR LU NO NE DME CQ

2. Si estamos empleando un sistema de cifrado **RSA** con clave pública (17,187), ¿cuál sería la codificación del bloque 51 que queremos transmitir?

   17

3. ¿Cómo se cifraría el mensaje **EL SISTEMA SE REINICIARA SI EL LADRON ENTRA** si empleamos el método de transposición por columnas, usando **SEGURIDAD** como clave? Usa la segunda tabla.

   MIEEX ENINX LSILT SEAAR TISOX SEARX EACLN IRRDA

4. ¿Qué se obtiene al cifrar M=**CLAVE SEGURA** con el cifrado de Vernam, teniendo en cuenta la siguiente secuencia aleatoria: **10 80 52 95 15 43 12 56 14 52 30**?

   MKYJSIPIIPD

5. ¿Cómo se cifraría el mensaje **EXAMEN DE CRIPTOGRAFIA** si empleamos el método de Vigénere, usando **TECLADO** como clave? Usa la segunda tabla.

   XBCWEPRXGTSPWDZVCPID

Preguntas Autoevaluación Prácticas

Práctica 6: Explotación de aplicaciones web y bases de datos

Sentencia siempre verdadera: TAUTOLOGÍA

Comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones APIs (Application Programming Interfaces) en las que se puedan confiar: OWASP

Número de vulnerabilidades catalogadas por OWASP como las más comunes: DIEZ

Herramienta que nos permite parar las peticiones HTTP/HTTPS realizadas por el navegador con el propósito de analizarlas, manipularlas e incluso enviarlas al servidor: PROXY

Tipo de ataque donde se realiza una consulta a una base de datos pero especificando parámetros que realmente es un código malicioso para obtener información sensible o realizar actos maliciosos sobre la propia base de datos: INYECCIÓN

Ejemplo de aplicación que podemos usar como proxy web: BURP

Según el OWASP Top Ten de 2021, la segunda vulnerabilidad más común es CRYPTOGRAPHIC Failures.

Entorno de entrenamiento que permite desplegar una máquina virtual y, además, proporciona herramientas, objetivos y documentación para aprender sobre securidad en aplicaciones web: TRYHACKME

Término que se utiliza para practicar la explotación de vulnerabilidades porque es una aplicación web mal programada dónde quienes la programaron se dejaron muchos fallos. OWASP JUICE SHOP

Vulnerabilidad muy común, y tercera en el ranking, de acuerdo a OWASP 2021: INYECCIÓN

Extensión del navegador que facilita la configuración del proxy web: FOXYPROXY

Función de burp más adecuada que permite replicar paquetes para realizar ataques como el de fuerza bruta: INTRUDER

Práctica 7: Escalada de privilegios

¿Cuál es un componente fundamental presente en todos los sistemas actuales, que permite determinar quien puede editar un archivo determinado o ejecutar determinadas acciones?

PRIVILEGIOS

¿A qué elemento se corresponde la siguiente cadena de permisos: drwxr-xr-x?

DIRECTORIO

¿A qué elemento se corresponde la siguiente cadena de permisos -rw-r--r--?

FICHERO

¿Qué permiso le falta al propietario del fichero cuya cadena de permisos es la siguiente: -r-xr-----?

ESCRITURA

¿Cuál es el usuario que genera un fichero dentro de un directorio donde este tiene permisos?

PROPIERTARIO

En la orden chmod, ¿a qué se corresponde la letra g ?

GRUPO

¿A qué permiso se corresponde la letra x ?

EJECUCIÓN

Formato numérico de permisos en el que se dividen en 3 campos de 3 bits.

OCTAL

¿Quién tendría más permisos sobre el fichero ejemplo.txt si se ejecuta la siguiente orden? chmod 752 ejemplo.txt

PROPIETARIO

Permisos de Windows que se aplican a todos los ficheros y carpetas almacenados en un volumen determinado.

NTFS

¿Qué decimos que hacemos con los privilegios cuando un atacante obtiene más permisos de los que debería?

ESCALAR

**Tipo de escalada de privilegios donde el usuario mantiene sus privilegios pero obtiene acceso a datos y funcionalidades que no debería
tener disponibles.**

HORIZONTAL

Tipo de escalada de privilegios donde el atacante comienza con una cuenta de usuario con pocos privilegios y pasa a tener un mayor número de estos.

VERTICAL

Permiso sobre un fichero que indica que quien lo ejecute tendrá los mismos permisos que su creador.

BIT SUID

Herramienta de Linux que permite ejecutar automáticamente una orden en un momento de tiempo determinado.

CRONTAB

Cuando asignamos un permiso especial en el cual los elementos solo pueden ser renombrados o borrados por su propietario o el usuario root, nos referimos a:

Sticky bit

Usuario que tiene acceso administrativo al sistema.

SUPERUSUARIO

∗/2∗ ∗ ∗ ∗ root /tmp/cleanup.pycrontab ejecutará la orden anterior cada dos

MINUTOS