0291823 Enrique Ulises Baez Garcia Tejeda

1er parcial criptografía

1)

- Cifrado: convertir info en algún formato no legible para mantenerla segura.
  Necesitas una llave/clave para descifrarlo. Y verlo de forma correcta.
  Tipo los lenguajes clave de comunicación

- Codificado: Transformar info a cualquier formato para transferirlo o guardarlo más fácil.
  Tipo la vectorización o las imagenes en base 64.

ISO 7498-1
Estructura del modelo OSI (7 capas)

- Física
- Enlace de datos
- Red
- Transporte
- Sesión
- Presentación
- Aplicación

Interoperabilidad, básicamente así funcionan las redes de datos, protocolos de red

ISO 7498-2

Arquitectura de Seguridad

Expande la autor porque añade seguridad, autenticación, integridad de datos, control de acceso

Seguridad en las capas del modelo OSI para proteger los datos que pasan por la red.

0241823 Enrique Ulises Baez Gomez Tayde

2) Metodos de cifrado

Enrique Ulises Baez Gomez Tayde

Cesar:

Por sustitución, desplaza el alfabeto X posiciones.

Hqultxh xoluhv Edhc Jrphc Wdjoh

Monosustitución:

Por sustitución, reemplazas una letra con otra sin que sea secuencial (obligatoria). Se usa la tabla de sustitución

Nmirjfv Forhuh Yzva Tlnva Gztou

Vigenère:

Por sustitución polialfabética, muchos alfabetos para cifrar un mensaje. Se usa una palabra clave y se desplaza de acuerdo a eso.

Wugwdcg Msxgra Dslo Ubugr Apoym

Playfair:

Sustitución de ~~digrafos~~ digrafos. Matriz 5x5 para cifrar las letras. Quitas las repetidas.

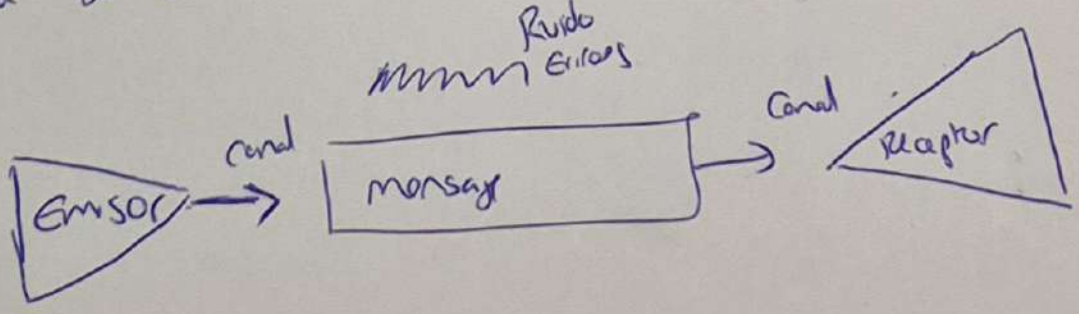
LSMARMLMEDIMOIIGXLSTLVRBKEGV

Hill:

Poligráfico. Matrices para cifrar bloques de letras. Cada letra es un número, y cada letra se agrupa en bloque tamaño fijo. Usas multiplicación de matrices

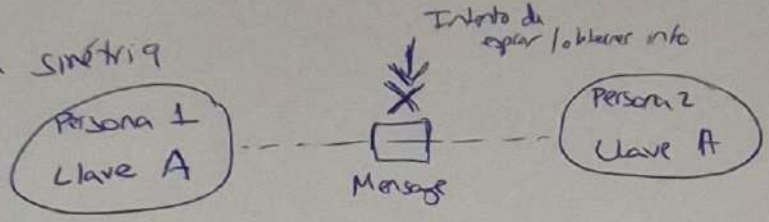
EVOIAOMSFGKCOHBYTPUGOWKRALF

3.- Esquema de la comunicación en ámbito digital



Esquema general de la criptografía simétrico

0241823
Enrique Ulises Bueno Tapia



4) Tiene 497 empleados

$$C(n,2) = \frac{n(n-1)}{2}$$

$$C(497,2) = \frac{497(496)}{2} = \frac{246512}{2}$$

↳ 123,256 llaves

5)

CBC es más seguro porque oculta patrones en los datos.

EBC cifra el bloque completo y de forma independiente, por lo que 2 bloques idénticos en claro, van a ser idénticos cifrados.

CBC combina la cifrada con el bloque anterior (XOR)

entonces 2 bloques iguales se verán diferentes.

6) RBAC

a) Completo → permisos de acuerdo a los roles. Muchas personas con tareas similares.

- Rol: acceso basado en mínimos privilegios.
- TI: acceso técnico completo con permisos de acción de acuerdo al subrol
- Jurídico: solo acceso a documentos
- RH acceso a gestión
- Ventas: ventas, CRM
- POS: Facturas, Inventarios
- Efectivos: acceso general

0241823 Enrique Ulloa Bien Grave Inglés

b) PYME

DAC

No conocemos la sensibilidad de los datos. No conocemos el organigrama ni qué personas participan.

Entonces DAC es flexible y escalable de forma simple.

Identificar recursos. Asignar dueños que tengan acceso directo y que pueda añadir personas.

II) Criptoanálisis

1) se repiten zsvqbsuk
rkxnc
zKv|wobc

Palabras cortas
iye ny

los artículos en español son de 2 pero en inglés son de 3

Para lenguaje normal y tiene símbolos

iye → you

ny → do

C → 3 S → 19

h = 16

Alfabeto de 16 letras

+16 = -10

original: ABC DEFGHIJKLMNOPQRSTUVWXYZ
Desplazado: KLMNOPQRSTUVWXYZABCDEFGHIJ

Good pilgrim, you do wrong your hand too much, which manner devotion shows in this; for saints have hands that pilgrims hands do touch, and palm to palm is holy palmer's kiss.

02413623

Enrique Ulises
Barca Gomez Tapia

2) No hay patrones tan repetitivos en textos es polialfabético

F → I 3 posiciones →
X → a 23 posiciones ←

Pos	Cifr	Des	Clave
1	f	+3	D
2	i	-3	X
3	f	+3	D
4	s	-3	X
5	o	+3	D
6	r	-3	X

Que fi
if f lb pr qr x
pues son costas, seguro es
en mayus de 1ovo
la f o y es I o a
como es fi
la f → I x → a
fi → rf lp → rs
wtr → two
qr → to

If I profane with my unworthiest hand
this holy shrine, the gentle sin is this.
my lips, two blushing pilgims, ready
stand to smooth that rough touch with ~~tears~~
< tender kiss

5) Con el dato de la llave en base 64 se saca la clave

C3BpcmlOdXM=
↓ spiritus (BB) → (IV)
size

Decodificar con la llave

DES en CBC

3DES
usa 16 y 24 Bytes

mayúsculas y minúsculas
signos +, /
números
} Base 64

multiplo de 4 X= = 12
se rellena con "="

se intenta que es DES

le fuimos que quite los relleno

no tenemos IV entonces
ponemos el V[0]

como declaramos un vector de inicialización se uso CBC

Usamos python
y fuerza bruta los pesos para encontrarlo

el relleno del bloque es para tener
múltiplo de DES 8 bytes

0241823 Enrique Ulises Bocanegra

'Tis but thy name that is my enemy.
Thou art thyself though not a Montague
What's Montague? It is nor hand, nor foot,
Nor arm, nor face. O, be some other name
Belonging to a man.
What's in a name? That which we call a rose
By any other word would smell as sweet
So Romeo would, were he not Romeo called,
Retain that dear perfection which he owes
Without that title, Romeo, doff thy name,
And for thy name, which is no part of thee,
Take all myself.