Iván Domínguez Lugo

PARTE I. DEFINICIONES Y ASPECTOS TEÓRICOS.

1.- Cifrado: se refiere a las operaciones que se hacen sobre el texto plano para transformarlo a un texto que no sea legible.

- Codificado: este concepto se refiere más al cambio de formato que se le aplica a algún texto o archivo.

- ISO - 7498 - 1:

Esta norma habla del modelo OSI, el cual es un estándar sobre la arquitectura de una red de comunicación, este estándar incluye 7 capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

Tiene una fuerte relación con las redes de datos, pues justamente describe cómo deben de estructurarse estas.

- ISO - 7498 - 2:

En esta norma se aborda todo el tema relacionado a la seguridad en las redes y contempla algunos servicios en este ámbito, los cuales son: confidencialidad, integridad, disponibilidad, autenticación, no repudio y control de accesos.

Está fuertemente ligada a la criptografía, pues se trata de la protección de la información, y la criptografía nos ofrece técnicas para lograr esto.

2.- - César: es un tipo de cifrado que hace un corrimiento a la derecha o a la izquierda de los caracteres del texto plano considerando su posición en el alfabeto y la cantidad de lugares que se quiere recorrer.

- Monosustitución: es un tipo de cifrado en el que se crea un alfabeto que no está en orden, ya sea aleatoriamente o personalizada. Lo que se hace es sustituir la letra original por la letra del alfabeto desordenada usando las mismas posiciones.

Es superior al cifrado César pues la cantidad de permutaciones posibles aumenta en gran escala.

- Vigenere: este tipo de cifrado consiste en tener el texto plano junto con una llave. Lo que se hará es sumar los caracteres uno por uno, usando el primero del texto plano con el primero de la llave y así sucesivamente. Si la llave no es suficientemente larga, se repite las veces que sean necesarias hasta completar la longitud con la misma del texto plano. Después de hacer las sumas se saca el módulo de cada una, 26 en inglés o 27 en español. Una vez se tengan los resultados, el texto cifrado será simplemente sustituir el número con el caracter correspondiente a esa posición.

- Playfair: se requiere que tanto la llave (↳ sin letras repetidas) como el texto plano estén normalizados.

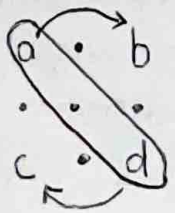
1. Para armar la matriz con la llave se escriben en orden las letras de la llave normalizada y después se completa la matriz con las letras faltantes (considerando n y ñ, también i y j como la misma).

2. Luego se separan las letras del texto plano normalizado en tuplas de 2, si se repite una letra en la misma tupla, se cambia por un caracter neutro que se puede definir previamente.

3. Para cifrar se siguen tres reglas: (buscando las letras de cada tupla en la matriz).
   ① Si las letras están en la misma fila se toma la de la derecha y se sustituye en la cadena.
   ② Si están en la misma columna se usa la de abajo para sustituir.

   (En ambos casos, si es la última letra, se regresa a la primera)

   ③ Si la columna y fila no coinciden se toma una matriz más pequeña que tiene como esquinas las dos letras y para sustituir se toma la que este en el vértice opuesto, ejemplo:



ad → bc

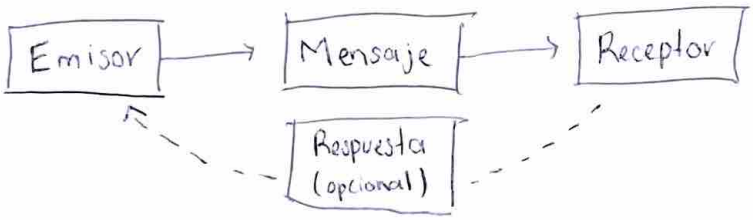
-Hill: este método de cifrado es mucho más fácil de entender con la fórmula:

$$C = PK \bmod 26 \xrightarrow{m=3} (C_1 C_2 C_3) = (P_1 P_2 P_3) \begin{bmatrix} K_{11} & K_{12} & \cdots \\ K_{21} & & \\ \vdots & & \end{bmatrix} \bmod 26$$

Para obtener el texto cifrado, se toma el texto plano, cuyos caracteres van a ser los elementos de una matriz $1 \times m$, esta se multiplica por la matriz llave, que es de $m \times m$, lo cual resultará en otra matriz $1 \times m$ que se le aplica módulo 26 y el resultado será el texto cifrado.

*Se incluyen los códigos en el repositorio compartido.

3. Esquema de comunicación en el ámbito digital.



Esquema de comunicación con cifrado simétrico.

4. Usamos la fórmula $\frac{n(n-1)}{2}$

$$\frac{497(497-1)}{2} = \frac{497(496)}{2} = \frac{246,512}{2} = 123,256 \text{ llaves}$$

5. El problema con ECB es que toma de manera independiente cada bloque para ser cifrado, por lo que si hay dos bloques iguales (misma frase, por ejemplo) el bloque cifrado resultante será el mismo para los dos, esto facilita a ciberdelincuente el criptoanálisis.

La manera en la que CBC lo resuelve es haciéndolo de manera serial, esto es que toma en cuenta el bloque anterior resultante para cifrar el siguiente, por lo que el criptoanálisis es más complicado.

6 a. Para Capuleto sería bueno usar MAC, esto principalmente por la cantidad tan alta de empleados y lo bien definidas que están las áreas de la empresa.

Sin duda, MAC sería de mucha utilidad para asegurarse de que los empleados solo accedan a los recursos que son propios de su área y de su puesto.

Lo que haría sería categorizar los recursos dependiendo de su importancia y confidencialidad, posteriorme, al momento de crear a los usuarios le asignaría roles específicos para solamente puedan acceder a lo que está a su nivel.

Si bien puede resultar tedioso al inicio estructurar todo, me parece la mejor opción para garantizar la confidencialidad y tener un control más estructurado.

b. En el segundo caso, en "Rey de los Gatos", como son muy pocos empleados y no se habla de alguna división clara de áreas, considero de DAC sería una buena opción en este caso.

Para implementarlo simplemente le asignaría a cada empleado los permisos para acceder a los recursos que necesita y si es necesario hacer un cambio sería más fácil hacerlo considerando que se tiene un menor volumen de cuentas que manejar.

Parte II. Criptoanálisis.

Texto 1.

- El primer tipo de cifrado que podemos probar es César.
- Analizando el texto cifrado nos damos cuenta de dos cosas:
  - No hay $\bar{n}$.
  - Hay apóstrofes.
- Esto nos hace pensar que el texto está en inglés.
- Sobre los apóstrofes vemos que están después de una 'c' al final de cada palabra. En inglés cuando se usa el apóstrofe al final es porque se usa el posesivo de alguna palabra que termina en 's' (regularmente plurales).
- Podemos probar el corrimiento para $S \rightarrow C$, que en el alfabeto inglés son 16 posiciones de diferencia, por lo que el alfabeto recorrido quedaría así:

cifrado	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
clave	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p

- El mensaje resultante quedaría como

"Good pilgrim, you do wrong your hand too much,
Which mannerly devotion shows in this; For saints have hands
that pilgrims' hands do touch, And palm to palm is holy
palmers' kiss."

Usando Vigenere: Texto 2.

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

f i f s o r c d K h t q K j b r q t r o w e l b v q K x q a

① 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2

②	5	5	14	2	10	19	16	9	11	19	14	4	1	16	23	0									
(-23)	-18	-18	-9	-21	-13	-4	-7	-14	-6	-4	-9	-19	-22	-7	0	-23									
mod 26	8	8	17	5	13	22	19	12	20	22	17	7	4	19	0	3									
P	i	i	r	f	n	w	t	m	u	w	r	h	e	t	a	d									

w e l p k l o v v e u f q b, w e h d h k w i h p l k l p w e l p:

① 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1

②	4	15	11	21	4	5	1	4	3	10	8	15	10	15	4	15									
(-23)	-19	-8	-12	-2	-19	-18	-22	-19	-20	-13	-15	-8	-13	-8	-19	-8									
mod 26	7	18	14	24	7	8	4	7	6	13	11	18	13	18	7	18									
P	h	s	o	y	h	i	e	h	g	n	l	s	n	s	h	s									

p v o f s p, w t r y o r v e l k j m l i j o l j v, o h x g v v q d k g

① 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1

②	21	5	15	19	24	17	4	10	12	8	19	9	14	23	21	16	10								
(-23)	-2	-18	-8	-4	1	-6	-19	-13	-11	-15	-9	-14	-9	0	-2	-7	-13								
mod 26	24	8	18	22	1	20	7	13	15	11	17	12	17	0	24	19	13								
P	y	i	s	w	b	u	h	n	p	l	r	m	r	a	y	t	n								

q r p p l r q k q K x w o r r j e w l x z k t l q k x w b q a h o

① 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2

②	16	15	11	16	16	23	14	17	4	11	25	19	16	23	1	0	14								
(-23)	-7	-8	-12	-7	-7	0	-9	-6	-19	-12	2	-4	-7	0	-22	-23	-9								
mod 26	19	18	14	19	19	0	17	20	7	14	2	22	19	0	4	3	17								
P	t	s	o	t	t	a	r	u	h	o	c	w	t	a	e	d	r								

n f v p.

① 2 1 2 1

② / 5 / 15

(-23) -18 -8

mod 26 8 18

P i s

NOTA: descartamos Cesar y monosustitución por "pplrqk", pues en inglés no hay palabras que empiecen con la misma letra, y asumimos que es en inglés porque no hay 'ñ'

① Nos damos cuenta que si usamos una llave de dos caracteres, el caracter correspondiente para 'f y x' correspondería el mismo. Sabiendo que solo la 'i' y la 'a' pueden estar solas en el idioma inglés, primero intentamos aplicar la fórmula para obtener la posible llave que nos dé que $a \to f$ o que $i \to f$ y probamos con 'x' para ver si se cambia a 'a' o 'i'.

i) Para que $a \to f$: $0 = 5 - K \bmod 26 \Rightarrow K = 5 \therefore K = f$

(a) (f)

Probamos con $P = 23 - 5 \bmod 26 \Rightarrow P = 18 \Rightarrow P = s$ X

Dado que no resulta que $a \to f$, entonces:

ii) Probamos $i \to f$:

$$\underset{(i)}{8} = \underset{(f)}{5} - K \bmod 26 \Rightarrow K = 23 \Rightarrow 5 - 23 \bmod 26 = -18 \bmod 26 = 8$$

$\therefore K_1 = x$

Probamos con x

$$P = 23 - 23 \bmod 26 \Rightarrow P = 0 \Rightarrow P = a \checkmark$$

La primera letra de la llave es 'x'

② En el segundo paso aplicamos que x sea la primera letra de la llave para ver si nos da alguna pista de cuál puede ser la segunda letra.

③ Una vez aplicada la primera letra de la llave para desencriptar, se puede notar que

t?   t? → qr

La única palabra de dos letras que empieza con 't' en inglés es "to", por lo que buscamos ahora que o → r

$$\underset{(o)}{14} = \underset{(r)}{17} - K \bmod 26 \Rightarrow K = 3 \Rightarrow K_2 = d$$

④ Ahora probamos decifrar el resto de caracteres usando la llave

fi f sorcdKh tlqK jb rqtrowelbvq Kxqa

	8	18	17	3	7	11	10	1	16	17	22	11	21	10	16
(-3)	5	15	14	0	4	8	7	-2	13	14	19	8	18	7	13
mod 26	5	13	14	0	4	8	7	24	13	14	19	8	18	7	13
P	f	p	o	a	e	i	h	y	n	o	t	i	s	h	n

welp klov veufqb, weh dhKwih plK lp welp:

	22	11	10	14	21	20	16	22	7	7	22	7	11	11	22	11
(-3)	19	8	7	11	18	17	13	19	4	4	19	4	8	8	19	8
P	t	i	h	l	s	r	n	t	e	e	t	e	i	i	t	i

pv ofsp, wtr yorvelKj mlijoljv, ohxgv vqdK g

	15	14	18	22	17	14	21	11	9	11	9	11	21	7	6	21	3	6
(-3)	12	11	15	19	14	11	18	8	6	8	6	8	18	4	3	18	0	3
P	m	l	p	t	o	l	s	i	g	i	g	i	s	e	d	s	a	d

	qr	pplrqk			qkxw		orrje		wlxzk			tlqk		x	wbqaho			
	17	15	17	10	10	22	17	9	22	23	10	11	10		22	16	7	
(−3)	14	12	14	7	7	19	14	6	19	20	7	8	7		19	13	4	
p	o	m	o	h	h	t	o	g	t	u	h	i	h		t	n	e	

	n	f	vp
		13	21
(−3)		10	18
	p	k	s

(5) Combinando ambos textos nos queda ~~el~~ mensaje descifrado:

"if i profane with my unworthiest hand this holy shine, the gentle sin is this: my lips, two blushing pilgrims, ready stand to smooth that rough touch with a tender kiss"

:)