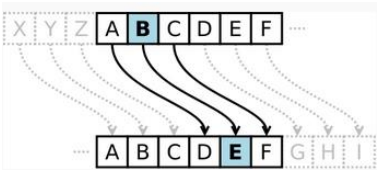
HOJA FINAL DE REPASO

Serie 1

El cifrado césar mueve cada letra un determinado número de espacios en el alfabeto, tal como se observa en el ejemplo, se usa un desplazamiento de tres espacios:



Dicho cifrado se puede transformar en un cifrado simétrico, la cual consiste en colocar la llave dentro del contexto (Creando así un nuevo contexto), por lo tanto:

- Construya el nuevo contexto, tomando en cuenta que, por cada 3 símbolos del contexto, se debe Insertar un símbolo de la llave.
    - El contexto "**BCDFHIJKLMNOPQRVWXYZE**"
    - La llave "**AGU_ST**"
- Dado el nuevo contexto, y un desplazamiento de 3, encripte el mensaje "**HOLA_MUNDO**"
- Dado el nuevo contexto, y un desplazamiento de 3, desencripte el mensaje "**DXEWOFEOWI**"
- Dado la operación de cifrado por bloques (ECB), con las siguientes características:
    - Bloques de 4 caracteres
    - Puede existir al menos un bloque que contenga menos de 4 caracteres.
    - Se utilizará el cifrado cesar anterior (utilizando el nuevo contexto), tomando en cuenta que los bloques pares se utilizará un desplazamiento de 3, y los bloques impares un desplazamiento de 5.
    - Los índices de bloques comienzan con 0 (e.g. [b0, b1, b2, …, bn]

  Encripte el mensaje: "**ESTO_ES_UNA_PRUEBA_ECB**"

Serie 2

El banco "Tu Ahorro S.A.", tiene un sistema de cambios de cheques, las cuales consiste en verificar la firma digital de cada cheque (Hecho por un algoritmo SHA), en caso de que coincida dichas firmas, se cambiará el cheque. Por lo tanto, subraye los cheques válidos a cambiar:

BD de cheques Tu Ahorro S.A	**Cheques para cambiar**
559aead08264d5795d390971	2e7d2c03a9507ae265ecf5b53
3e23e8160039594a33894f65	cd0aa9856147b6c5b4ff2b7df
2e7d2c03a9507ae265ecf5b53	aaa9402664f1a41f40ebbc52c
18ac3e7343f016890c510e93f	559aead08264d5795d390971
252f10c83610ebca1a059c0ba	2d711642b726b04401627ca9

Serie 3

Luigi y Mario se esta comunicando en un canal inseguro, dado que es escuchado por Bowser, por lo tanto, decidieron utilizar el método RSA, para encriptar la comunicación, tomando las siguientes características:

- Los caracteres ASCII imprimibles [32,126], son utilizados para desencriptar el mensaje.
- El mensaje encriptado esta formado por un arreglo numérico (e.g. [0,1,2,3, …]).
- Los números primos seleccionado son (p=11,q=23)
- La llave publica es (3,253)
- La llave privada es (147,253)

De acuerdo con las características, realice lo siguientes pasos:

- Encripte el mensaje “HOLA _MUNDO”
- Desencripte el mensaje [19, 229, 123, 85, 32, 102, 131, 144, 85, 131, 229, 92, 102].
- Desarrolle un proceso de validación para comenzar la conversación entre Mario y Luigi, utilizando el protocolo Diffie-Hellman, tomando en cuenta el siguiente contexto:

Contexto Diffie-Hellman:

```
{
 "A":1,
 "B":2,
 "C":3,
 "D":4,
 "E":5,
 "F":6
}
```

Caracteres ASCII imprimibles

32	espacio	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		