Fundamentos de Seguridad

Cifrado por sustitución

Propuestos y Resueltos

Ejercicio 1. Un intruso capta parte de un mensaje cifrado con un método monoalfabético de bajo nivel, al parecer sustitución afín, y que va dirigido al presidente de la empresa "Arroz La Lluvia". Si el criptograma en cuestión es: C = … HFLXF JQKNK GFZHL CLCQB COFBK XCICI KCLLF AXCXX QSRCZ CDCBC ….

a) ¿Cuál es la operación de cifra y sus parámetros?

b) Encuentre el alfabeto de cifrado.

c) Descifre el mensaje que se esconde.

Solución:

a) Como el sistema de cifra es monoalfabético, es muy posible que los caracteres repetidos LL y XX del criptograma se correspondan con los caracteres RR y LL de "Arroz la Lluvia" por lo que supondremos esta correspondencia de texto en claro con el criptograma para plantear el sistema de ecuaciones que nos dé la solución a los valores de a y b en la ecuación C = (a*M + b) mod n:

L = (a*R + b) mod n 11 = (a*18 + b) mod 27 (ecuación 1)

X = (a*L + b) mod n 24 = (a*11 + b) mod 27 (ecuación 2)

Restando la ecuación 2 de la 1, se tiene:

-13 = a*7 mod 27 a = (-13) *inv(7,27) mod 27

a = -13*4 mod 27 = -52 mod 27 = 2

Reemplazando este valor en la ecuación 2:

24 = (2*11 + b) mod 27 b = (24 – 2*11) mod 27 = 2

La ecuación de cifra será: C = (2*M + 2) mod 27

b) Mediante la ecuación del punto a) se encuentra el siguiente alfabeto de cifra:

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	26
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
C	E	G	I	K	M	Ñ	P	R	T	V	X	Z	B	D	F	H	J	L	N	O	Q	S	U	W	Y	A

c) Usando la tabla anterior se encuentra el mensaje:

C = HFLXF JQKNK GFZHL CLCQB COFBK XCICI KCLLF AXCXX QSRCZ CDCBC

M = PORLO QUESE COMPR ARAUN ATONE LADAD EARRO ZLALL UVIAM AÑANA

M = … por lo que se comprará una tonelada de arroz la lluvia mañana …

Ejercicio 2. Se recibe el criptograma que se indica:

UV IW GZ VC DF ZN QV PD VN FZ CQ WD WP VB CS QO FC QW NI VN QW VP ZN EO DS QV PC KW FC QW GZ VP ON BO XM CQ VC BL VN PO WN CB LW EV MK WZ NC WM CP OW NG ZV VD ML VS WB LW BO MO CS WH EO CS BC FW CM OV LU WH CL WN MW NC

DK CT CP QV PZ NW EO CS IV CN ZD WS IV CU LO HZ DW SI OK WN WL NW QO PO IZ DW BZ VP CZ NG ZV VD NW IH LV UV CP WI HL VG ZO VN WH LC CP OU OV NV ZN NW IH LV SV PV NW IH LV VP VD QV MK ZD WD CE VN FC NX CQ VQ WN IV NQ WB VQ LW IZ RW XP VM CT WL NC QC BL OI VL C

Sabemos que ha sido cifrado mediante una sustitución monoalfabeto afín trabajando en módulo 27, es decir, sólo letras mayúsculas.

a) Encuentre el algoritmo de cifra: valores de las constantes a y b (Vea la Ayuda).

b) Complete el alfabeto de cifrado (faltan 10 caracteres).

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
_	_	_	_	_	_	F	K	O	T	Y	D	I	N	R	W	B	G	L	P	U	Z	E	_	_	_	_

c) Descifre los primeros 23 caracteres del criptograma (cuatro palabras).

AYUDA: Las letras más frecuentes en el criptograma y su frecuencia relativa son: C = 10,345%, V = 12,853%, W = 11,599%.

Solución:

a) Supondremos que dos de las tres letras más frecuentes en el criptograma C, V y W se corresponden con las letras A y E del alfabeto, siendo la E la más frecuente. Por lo tanto podemos plantear las siguientes ecuaciones:

Texto en claro E Texto cifrado V

Texto en claro A Texto cifrado C

(a*E + b) mod 27 = V (a*4 + b) mod 27 = 22

(a*A + b) mod 27 = C (a*0 + b) mod 27 = 2

Por lo tanto, b = 2

Reemplazando: (a*4 + 2) mod 27 = 22 a*4 mod 27= 20

Como inv (4, 27) = 7 a = 20*7 mod 27 = 140 mod 27 = 5

Como a y b son valores válidos para cifrar en el cuerpo, la función de cifra sería:

C = (5*M + 2) mod 27 siendo M el carácter del mensaje

Como el primer elemento del texto en claro debe ser la letra T según apartado b):

C = (5*T + 2) mod 27 = (5*20 + 2) mod 27 = 102 mod 27 = 21 = U.

Coincide en este carácter y en los demás, entregando un texto con sentido. Por lo tanto el algoritmo de cifra es C = (5*M + 2) mod 27.

Si hubiésemos supuesto que la letra V de mayor frecuencia del criptograma corresponde con la letra A del texto en claro y que la letra C se corresponde ahora con la letra E del texto en claro, tenemos:

(a*E + b) mod 27 = C (a*4 + b) mod 27 = 2

(a*A + b) mod 27 = V (a*0 + b) mod 27 = 22

Por lo tanto, b = 22

Reemplazando: (a*4 + 22) mod 27 = 2 a*4 = -20 mod 27 = 7

Como inv (4, 27) = 7 a = 7*7 mod 27 = 49 mod 27 = 22

Como a y b son valores válidos para cifrar en el cuerpo n = 27, la función de cifra podría ser C = (22*M + 22) mod 27: No obstante, para el primer elemento del texto que es la letra T se tiene C = (22*T + 22) mod 27 = (22*20 + 22) mod 27 = 462 mod 27 = 3 = D, que no corresponde con el criptograma. Luego, aunque la función de cifra es válida dentro del cuerpo 27, no es la que buscamos.

Algo similar sucede con otras combinaciones.

A igual resultado se puede llegar planteando ecuaciones de relación entre el alfabeto en claro y el cifrado que se entrega.

b) Aplicando bien la fórmula directamente o, más fácilmente, al conocer que el factor de decimación es igual a 5 y el desplazamiento igual a 2, el valor de cifra de la letra A será 0+2 = C y de aquí en adelante se recorre el alfabeto saltando de cinco en cinco:

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

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

c) Leyendo en la tabla anterior se obtiene el mensaje M:

UV IW GZ VC DF ZN QV PD VN FZ CQ WD

TE MO QU EA LG UN DE SL EN GU AD O

Ejercicio 3

La función de cifra para sistemas genéricos de sustitución monográmica es:

a) $C_i = (M_i + b) \bmod n$ Desplazamiento puro
b) $C_i = a * M_i \bmod n$ Decimación pura
c) $C_i = (a * M_i + b) \bmod n$ Sustitución afín

a) Se pide escribir las ecuaciones para descifrar de forma directa un criptograma sin utilizar las correspondencias entre alfabeto en claro y alfabeto cifrado.

b) Si n = 27, a = 7 y b = 3, cifre y descifre el mensaje M = SOL según las ecuaciones dadas y encontradas en el apartado anterior.

Ejercicio 4.

Dos archivos de texto distintos se cifran el primero con un algoritmo de decimación pura y el segundo con uno de sustitución afín. Se procede al ataque del segundo de ellos con éxito.

a) Explique de forma resumida cómo se ha roto la operación de cifra.

b) Si el factor de decimación a en ambos casos es el mismo valor, ¿es posible descifrar con los datos encontrados en el ataque anterior el primero de los archivos y por qué?

Ejercicio 5: Se tiene el siguiente criptograma de 317 letras de una cifra afín módulo 27:

UQBUO KBUFJ QBKVY QÑNFB CFSOK BDQKB YQYFF DQCFS KMFBQ UQÑDF KMTFÑ VOBQS LKMFL BSKMK ÑQNKÑ ZFBDO BNFWK MYOÑF DFGLK MMFTF BYQÑV LNÑFS LÑFKM DKTOC QKBDQ CQTFÑ UQBQU OCQCK MLBQF MQDÑQ UQBRO BMFML BFKBK MTFÑÑ OKMFK BMFMQ BFZOT KKMSO KBDQP FMXFK BNMFB CQTQS OTOKB DQQMF VCKYM FDFPF XLMPS KKMUF YODFB YOÑFD FUFBD FBCQF MKZÑK KBMFY QYFFV OFFLB MFCQF MQDÑQ KLÑQY FPFMM FFVLR ÑKBDK VDFTN LM

En el que se observan las siguientes frecuencias:

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*	*26*
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**
0	31	10	17	0	52	1	0	0	1	34	12	30	6	18	16	4	33	2	8	9	9	7	1	2	11	3

a) Si se sabe que la segunda letra del texto en claro es una vocal, encuentra las constantes a y b de ese cifrado afín. Justifica cómo lo has hecho y comprueba que los valores de a y b son los correctos.
b) Descifra las 7 primeras letras del criptograma, indicando en cada caso las ecuaciones correspondientes con sus respectivos valores numéricos.
c) ¿Por qué crees que precisamente las letras A y E aparece con frecuencia cero el criptograma?