TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Curso 2024-25

Hoja nº 1

Criptografía Simétrica

1. Recibes el mensaje VEILRÑW, cifrado usando una clave de Cesar en el alfabeto castellano de 27 letras (con Ñ). Lee el mensaje, da las transformaciones para cifrar y descifrar, y cifra el mensaje GRACIAS utilizando la clave correspondiente.

2. Utilizando el análisis de frecuencias, descifra el siguiente mensaje, del que sabes que está escrito en inglés (26 letras) y que ha sido cifrado con una clave de Cesar:
PXPXKXENVDRUXVTNLXHYMXGMAXYKXJNXGVRFXMAHWGXXWLEHGZXKVBIAXKMXQM

3. La distribución de frecuencias (en porcentaje) en castellano de las 26 letras (es decir, sin W) es aproximadamente la siguiente.

A	B	C	D	E	F	G	H	I	J	K	L	M
12,6	1,0	5,1	5,7	13,7	0,9	0,8	0,5	7,0	0,2	0,0	4,6	3,2
N	$\tilde{N}$	O	P	Q	R	S	T	U	V	X	Y	Z
7,0	0,1	8,8	2,9	1,1	6,6	7,2	5,1	3,9	0,8	0,1	0,6	0,3

Recibes un mensaje escrito en castellano (con ese alfabeto) que ha sido cifrado con el criptosistema de Cesar. Las dos letras más frecuentes en el texto cifrado son, por ese orden, la J y la N. Deduce razonadamente cual puede haber sido la clave utilizada para cifrar.

4. Interceptamos un mensaje en el que dos profesores hablan de las asignaturas del plan de estudios de Matemáticas. El mensaje es el siguiente:

DONQONHOSDGXQKCHDKSNSJSDOQOBDCUQ

Sabemos que el mensaje ha sido cifrado utilizando una sustitución simple en el alfabeto castellano de 27 letras (con Ñ), y sospechamos que en el mensaje original aparecía la palabra CALCULO. Lee el mensaje.

5. En un alfabeto de 28 letras, las 27 del castellano y el espacio=27, utiliza la clave afín sobre letras $f(m) = 13m + 9$ para cifrar el mensaje "MUY BIEN".

6. Una unidad de texto (en claro) m se dice que es *fija* para una transformación para cifrar si $f(m) = m$. Supongamos que estamos usando transformaciones afines sobre letras en un alfabeto de N letras, $f(m) = a \cdot m + b$ con $a \neq 1$.

1. Demuestra que si N es primo hay exactamente una letra fija.
2. Demuestra que para N arbitrario cualquier transformación lineal (es decir, con $b = 0$) tiene al menos una letra fija, y que si N es par cualquier transformación lineal tiene al menos dos letras fijas.
3. Da un ejemplo de una transformación afín (para algún N) sin letras fijas.

7. Sabemos que el enemigo está utilizando transformaciones afines sobre letras para cifrar mensajes escritos en inglés con el siguiente alfabeto de 37 letras: los números 0,...,9 que se codifican como ellos mismos; las letras A,...,Z (sin Ñ), que corresponden a 10,...,35; y el espacio en blanco=36. Interceptamos el siguiente mensaje cifrado

OH7F86BB46R3627O266BB9 (Atención, no hay ceros, sólo Os)

Sabiendo que el mensaje original acaba con la firma 007 (cero, cero, siete), ¿qué dice el mensaje?

8. El enemigo escribe en inglés y, para cifrar sus mensajes, utiliza transformaciones afines sobre digrafos en el siguiente alfabeto de 30 letras: las letras A,...,Z (sin Ñ) corresponden a 0,...,25; el espacio=26; ?=27; !=28; '=29. Interceptamos el siguiente mensaje cifrado:

DXM SCE DCCUVGX

Un análisis de frecuencias sobre texto interceptado con anterioridad muestra que los digrafos más frecuentes son, por este orden, “M ”, “U ” e “IH”.
En inglés escrito con este alfabeto los digrafos más frecuentes son, por orden, “E ”, “S ” y “ T”.

1. Encuentra la clave para descifrar y lee el mensaje.

2. Encuentra la clave para cifrar y encripta el mensaje YES I’M JOKING!

9. Ciframos un mensaje utilizando una transformación afín sobre n-grafos en un alfabeto de N letras vistos como elementos de $\mathbb{Z}/N^n\mathbb{Z}$. Escribimos el texto original como $m_1m_2m_3\dots$ y el texto cifrado como $c_1c_2c_3\dots$, donde cada m_i y cada c_i es una letra.
a) Demuestra que c_{in} depende sólo de m_{in}, esto es, que cada "n-ésima"letra cifrada depende sólo de la correspondiente letra sin cifrar.
b) Utiliza la observación anterior para explicar cómo alguien que intercepte el mensaje, que sepa que la clave es afín en n-grafos, pero que desconozca n, puede utilizar el índice de coincidencia para romper la clave.

10. Interceptamos cuatro mensajes cifrados. Sabemos que tanto los mensajes en claro como los mensajes cifrados han sido escritos utilizando el alfabeto inglés de 26 letras. Las frecuencias con que cada letra aparece en cada mensaje son las siguientes:

1 :	A	B	C	D	E	F	G	H	I	J	K	L	M
	7	6	9	3	5	6	8	3	4	7	13	10	7
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	5	3	6	8	5	4	8	4	8	5	5

2 :	A	B	C	D	E	F	G	H	I	J	K	L	M
	5	3	10	0	1	4	9	0	0	9	3	10	5
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	0	6	5	10	4	2	0	0	1	0	8	0

3 :	A	B	C	D	E	F	G	H	I	J	K	L	M
	3	0	3	6	17	1	0	1	5	1	8	6	2
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	7	0	4	1	5	0	1	4	1	13	1	0	9

4 :	A	B	C	D	E	F	G	H	I	J	K	L	M
	3	7	4	2	8	5	6	4	10	5	8	6	8
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	3	7	9	5	6	4	9	5	7	3	7	6	3

¿Cúales de los mensajes han sido cifrados utilizando sustituciones simples sobre letras?

11. Los siguientes mensajes están cifrados usando el cifrado de Vigenère con alfabeto de 26 letras. Encontrar los mensajes originales:

1. KWPEDWWOXGGESBESGSGFLKSYUCYNSYUSCFCDIIPLSYWA ZKFLRCYFCDWFLI IPWLTKHPSZRMBLJOKGBAGFWSEFWHPESCIIPWGESAZKSBMWGGQLVCD

2. VWXRRRVYHECEDVDRXMGRRXMOIVRXBRHYMFERWJHEEEXRRJSVNEJGWZOV W XRRRVYHELRBBRFRWGERXIDUVTWEQLIARAJZMTEKEZVAES

12. Interceptas el mensaje [escrito en inglés] “!IWGVIEX!ZRADRYD”que se ha cifrado usando una transformación lineal sobre vectores de $(\mathbb{Z}/29\mathbb{Z})^2$, donde $0, ..., 25$ equivalen a las letras $A, ..., Z$, 26 es el espacio en blanco, 27=? y 28=!. Sabes que las 5 últimas letras del mensaje son la firma, $MARIA$.
a) Descifra el mensaje.
b) Encuentra la matriz para cifrar y, haciéndote pasar por Jo, que es la amiga a quién escribía María, envía cifrado el siguiente mensaje: “DAMN FOG! JO”[=¡‘Maldita niebla! Jo”].

13. Interceptas el mensaje [escrito en inglés] "KVW? TA!KJB?FVR "[ojo, acaba con un espacio en blanco] que se ha cifrado usando una transformación lineal sobre vectores de $(\mathbb{Z}/30\mathbb{Z})^2$, donde $0, ..., 25$ equivalen a las letras $A, ..., Z$, 26 es el espacio en blanco, 27=?, 28=! y 29 es el punto. Descifra el mensaje sabiendo que comienza con las 6 letras "C.I.A.".

14. Interceptas el mensaje [escrito en inglés] "S GNLIKD?KOZQLLIOMKUL.VY"que se ha cifrado usando una transformación lineal sobre vectores de $(\mathbb{Z}/30\mathbb{Z})^2$, donde $0, ..., 25$ equivalen a las letras $A, ..., Z$, 26 es el espacio en blanco, 27 el punto, 28 la coma y 29 el ?. Sabes que las 6 últimas letras corresponden a la firma, "KARLA."[el punto es parte del mensaje]. Descifra el mensaje.

15. Escribes en el alfabeto inglés de 26 letras con las equivalencias usuales. Para aumentar la dificultad de romper tu criptosistema decides cifrar tus mensajes escribiéndolos como vectores-digrafos en $(\mathbb{Z}/26\mathbb{Z})^2$, aplicarles la matriz $\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix}$ mód 26 y luego al resultado aplicarle la matriz $\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$, pero esta segunda vez trabajando mód 29. Así tu mensaje cifrado estará formado por vectores-digrafos en $(\mathbb{Z}/29\mathbb{Z})^2$, que veremos como escritos en el alfabeto de 29 letras donde 0=A,...,25=Z, 26 es el espacio en blanco, 27=? y 28=!. [Observa que multiplicar por dos matrices módulo un mismo n es como multiplicar por una sola matriz, pero que si, como aquí, cambiamos el módulo, el criptosistema es mucho más complicado.]
a) Cifra el mensaje "SEND".
b) Descifra el mensaje "ZMOY".

16. Calcula el número de trasformaciones afines (matriciales) que existen sobre un alfabeto de $N = 26, 27, 28, 29, 30$ letras si utilizamos como unidades de mensaje una sola letra, digrafos o trigrafos vistos como vectores, esto es, como elementos de $(\mathbb{Z}/N\mathbb{Z})^n$.

17. Demuestra que si cifrásemos un mensaje utilizando una aplicación lineal dada por una matriz $A \in M_2(\mathbb{Z}/N\mathbb{Z})$ que no fuese inversible, entonces cualquier unidad de texto cifrado, es decir, un vector (c_1, c_2) donde c_i son letras, podría ser el resultado de cifrar al menos dos unidades de mensaje en claro distintas.

18. Supongamos que estamos cifrando usando transformaciones lineales [=de Hill] dadas por matrices $A \in GL_2(\mathbb{Z}/N\mathbb{Z})$ con $A \neq I$. Un vector digrafo $m = \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$ se dice que es *fijo* para A si $Am = m$.

1. Demuestra que el digrafo "AA"$= \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ es siempre fijo, y encuentra una condición sobre la matriz A que sea equivalente a que "AA"sea el único digrafo fijo.
2. Si N es primo, y si "AA"no es el único digrafo fijo, demuestra que hay exactamente N digrafos fijos.

19. [Un criptosistema ligeramente más complicado.] El texto en claro está escrito en un alfabeto con N letras y el texto cifrado en un alfabeto con M letras, $M > N$. Las unidades de texto en claro serán digrafos vistos como números de dos cifras en base N, es decir, enteros entre 0 y $N^2 - 1$ [o elementos de $\mathbb{Z}/(N^2\mathbb{Z})$]. Análogamente, las unidades de texto cifrado serán enteros entre 0 y $M^2 - 1$ [o elementos de $\mathbb{Z}/(M^2\mathbb{Z})$]. Elegimos tres enteros positivos L, a, b tales que $N^2 \leq L \leq M^2$ y $mcd(a, L) = 1$. La función para cifrar viene dada por $f(m) := am + b$ mód L. Observa que los mensajes en claro son todos los enteros $\{0, \ldots, N^2 - 1\}$, pero como mensajes cifrados obtenemos sólo un subconjunto de $\{0, \ldots, M^2 - 1\}$. Para ver un ejemplo concreto supongamos que el alfabeto en claro tiene $N = 27$ con 0,...,25=A,...,Z [alfabeto inglés], 26=espacio en blanco, y que el alfabeto cifrado tiene $M = 30$, añadiendo al anterior 27=?, 28=!, 29=' [apóstrofe]. Usamos un criptosistema como el descrito con $L = 853$. Sabemos que los digrafos en claro más frecuentes son "E " y "S ", que se cifran respectivamente como "FQ" y "LE". Lee el mensaje cifrado "YAVAOCH'D!"