Teoría de Códigos y criptografía
Curso 2009-2010

Hoja 2 (Criptografá clásica)

1. Un general espartano recibe el siguiente mensaje de un amigo de Cantoblanco:
SONFAUHPINPEOCTOHRIANEQLSGCUTUOHEEEQOENRUBSETEIDRELEIT
¿Qué dice el mensaje?

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

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

4. 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.

5. 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 W), y sospechamos que en el mensaje original aparecía la palabra CALCULO. Lee el mensaje.

6. 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".

7. 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.

8. 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 (con W, 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?

9. Sea A un anillo conmutativo con 1. Diremos que $a \in A$ es un *divisor de 0* si existe $b \in A, b \neq 0$ y tal que $ab = 0$ (con esta definición, que no es la normal, 0 es un divisor de 0, pero no importa, simplifica los enunciados). Diremos que $a \in A$ es una *unidad* si existe $b \in A$ tal que $ab = 1$.

1. Demostrar que $\{\text{Unidades de } A\} \cap \{\text{Divisores de 0 en } A\} = \emptyset$.
2. Dado $a \in A$, definimos la aplicación "multiplicar por a", $m_a : A \longrightarrow A$ como $m_a(x) = ax$. Caracterizar los divisores de 0 (o quizá los no divisores de 0) y las unidades de A en términos de propiedades de la correspondiente aplicación m_a.
3. Utilizar la caracterización anterior para demostrar que si A es un anillo finito se tiene

   $$\{\text{Unidades de } A\} \cup \{\text{Divisores de 0 en } A\} = A.$$

   (Esto generaliza lo que sucede en los anillos de congruencias $\mathbb{Z}/N\mathbb{Z}$.)
4. Demostrar que la hipótesis de finitud es esencial en el apartado 3).

10. 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 (con W, 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!

11. 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 $m_1m_2m_3\ldots$ y el texto cifrado como $c_1c_2c_3\ldots$, 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.

12. 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?

13. El siguiente mensaje esta cifrado usando el método de Vigenere y usa el alfabeto castellano de 26 letras (sin Ñ). Encontrar el mensaje.

KWPEDWWOXGGESBESGSGFLKSYUCYNSYUSCFCDIIPLSYWAZKFLRCYFCDWFLI
IPWLTKHPSZRMBLJOKGBAGFWSEFWHPESCIIPWGESAZKSBMWGGQLVCD

14. El siguiente mensaje esta cifrado usando el método de Vigenere y usa el alfabeto castellano de 26 letras (sin Ñ). Encontrar el mensaje.

VWXRRRVYHECEDVDRXMGRRXMOIVRXBRHYMFERWJHEEEXRRJSVNEJGWZOVW
XRRRVYHELRBBRFRWGERXIDUVTWEQLIARAJZMTEKEZVAES