Teoría de Códigos y criptografía
Curso 2009-2010

Hoja 3 (Álgebra lineal sobre $\mathbb{Z}/N\mathbb{Z}$. La cifra de matrices.)

1. Sean p y q dos primos distintos.

1) Sea $S = \{v_1, v_2, v_3\}$ un subconjunto de $(\mathbb{Z}/p\mathbb{Z})^2$. Demostrar que si S genera $(\mathbb{Z}/p\mathbb{Z})^2$ entonces existe un subconjunto de S que consiste de 2 elementos que también genera $(\mathbb{Z}/p\mathbb{Z})^2$.

2) Encontrar un subconjunto generador W de $\mathbb{Z}/30\mathbb{Z}$ de 3 elementos, tal que cualquier subconjunto de W no es un sistema generador de $\mathbb{Z}/30\mathbb{Z}$.

2. 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"].

3. 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.".

4. 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.

5. 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 $\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix}$ mod 26 y luego al resultado aplicarle la matriz $\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$, pero esta segunda vez trabajando mod 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".

6. 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 $(\mathbb{Z}/N)^n$.

7. 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.

8. 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.

9. Sean $f_1 : \mathcal{M}_1 \to \mathcal{C}_1$ y $f_2 : \mathcal{M}_2 \to \mathcal{C}_2$ dos funciones para cifrar [o criptosistemas]. Si $\mathcal{C}_1 \subset \mathcal{M}_2$ podemos definir el *criptosistema producto* mediante la función $f = f_2 \circ f_1$. Más formalmente, si llamamos $\mathcal{I} := f_1(\mathcal{M}_1) \subset \mathcal{C}_1 \subset \mathcal{M}_2$ [$\mathcal{I} = intermedio$], el criptosistema producto lo define la función f dada por la composición

$$f : \mathcal{M}_1 \to^{f_1} \mathcal{I} \to^{f_2} \mathcal{C}_2.$$

Supongamos que trabajamos con funciones para cifrar afines $f_i : (\mathbb{Z}/n\mathbb{Z})^l \to (\mathbb{Z}/n\mathbb{Z})^l$ con n y l fijos [n no necesariamente primo], que vendrán dadas por $f_i(m) = A_i m + b_i$. Demuestra:

1. El producto de dos translaciones [$f_i(m) = m + b_i$, es decir, $A_i = I$] es una translación.
2. El producto de dos funciones de Hill [=lineales, $f_i(m) = A_i m$, es decir, $b_i = 0$] es una función de Hill.
3. El producto de dos funciones afines cualquiera es una función afín.

10. [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 $f(m) := am + b \mod L$. 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!"

11. [Como combinar las ideas de los dos ejercicios anteriores para, sin mucho esfuerzo, conseguir un criptosistema mucho más difícil de romper.] Sean f_1, f_2 funciones para cifrar como las del ejercicio anterior, es decir, $f_i(m) := a_i m + b_i \mod L_i$, donde N y M son iguales para las dos funciones pero las L, a, b pueden ser distintas. Supongamos $L_2 > L_1$. Podemos construir entonces el criptosistema producto $f = f_2 \circ f_1$ donde, a partir de una unidad de texto en claro m, el correspondiente texto cifrado se obtendrá en dos pasos [$i = intermedio$].

$$i := a_1 m + b_1 \mod L_1 \quad c := a_2 i + b_2 \mod L_2.$$

Observa que este criptosistema producto no es en general un criptosistema afín. Fijados los alfabetos, las claves son sextuplas $(L_1, a_1, b_1, L_2, a_2, b_2)$ sujetas a las condiciones $N^2 \leq L_1 < L_2 \leq M^2, mcd(a_1, L_1) = 1, mcd(a_2, L_2) = 1$.

Para ver un ejemplo concreto supongamos que usamos para los textos en claro y cifrados los alfabetos con $N = 27$ y $M = 30$ letras del problema anterior. Sabiendo que la clave para cifrar es $(757, 247, 109, 881, 675, 402)$, explica cómo descifrar y descifra el mensaje "D!RAJ'KCTN".

12. Interceptas el mensaje [escrito en castellano] que se ha cifrado usando una transformación lineal sobre vectores de $(\mathbb{Z}/30)^2$, donde $0, ..., 26$ equivalen a las letras $A, ..., Z$, 27 es el espacio en blanco, 28=., 29=?. Sabemos que está cifrado usando una cifra matricial afín sobre digrafos y que el mensaje original está firmado por " BAROJA." (hay un espacio al principio y un punto al final). Encontrar las posibles funciones códificadoras $f_{A,b}$ si el mensaje cifrado termina con $Z.MBGPCB$.