Teoría de Códigos y Criptografía

Curso 2009-2010 8 de Julio de 2010

Apellidos y Nombre _____

D.N.I. _____

El examen dura tres horas. No se pueden usar apuntes, libros u otros materiales. Se puede usar calculadoras. Todas las soluciones tienen que estar justificadas (no vale dar sólo las respuestas finales).

1. (2 puntos) Interceptas un texto [escrito en castellano] que se ha cifrado usando una transformación 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 texto original esá firmado por " GALDOS."(hay un espacio al principio y un punto al final). Encuentra el nombre de la obra si el texto cifrado empieza con " WVP"(hay un espacio al principio) y termina con "KNMZNEKF".

   Denotemos por $F(x) = xA + b$ $(x \in \mathbb{Z}_{30}^2)$la transformación lineal afín que descifra el mensaje cifrado (A es una matriz 2 por 2 y b es un vector). Por el anunciado sabemos que F actúa de la siguiente forma:

$$\begin{array}{lllllll} \text{“}KN\text{”} & = & (10,13) & \mapsto & \text{“ }G\text{”} & = & (-3,6) \\ \text{“}MZ\text{”} & = & (12,-4) & \mapsto & \text{‘}AL\text{”} & = & (0,11) \\ \text{“}NE\text{”} & = & (13,4) & \mapsto & \text{“}DO\text{”} & = & (3,15) \\ \text{“}KF\text{”} & = & (10,5) & \mapsto & \text{‘}S.\text{”} & = & (19,-2) \end{array}$$

   Por lo tanto $G(x) = Ax$ actúa como

$$\begin{array}{lll} (2,13) & \mapsto & (3,5) \\ (3,21) & \mapsto & (6,9) \\ (0,-8) & \mapsto & (22,-8) \end{array}$$

   Considerando esta acción módulo 2, 3 y 5 obtenemos que

$$A = \left\{ \begin{array}{ll} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & (\text{mód } 2) \\ \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} & (\text{mód } 3) \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & (\text{mód } 5) \end{array} \right.$$

Por lo tanto $A = \begin{pmatrix} -5 & -4 \\ 1 & 1 \end{pmatrix}$. Como $(10,13)A + b = (-3,6)$, obtenemos que $b = (4,3)$.

Ahora vamos a descifrar el comienzo del texto cifrado aplicando $F(x)$:

$$\begin{array}{rcccccl} \text{“}W\text{”} & = & (-3,23) & \mapsto & (12,8) & = & \text{“}MI\text{”} \\ \text{“}VP\text{”} & = & (22,16) & \mapsto & (0,21) & = & \text{“}AU\text{”} \end{array}$$

El nombre de la obra es “MIAU”.

2. (3 puntos) Consideramos el código lineal sobre $\mathbb{F}_{11}$ que tiene como matriz generadora

$$G = \begin{pmatrix} 1 & -2 & 1 & 0 & 0 \\ 2 & -3 & 1 & 1 & 0 \\ 3 & -4 & 1 & 1 & 1 \end{pmatrix}.$$

Empleamos este código para transmitir palabras castellanas escritas con el alfabeto que tiene 36 letras. Las 26 primeras letras corresponden al alfabeto castellano sin Ñ: 0=A,...,25=Z y las 10 restantes a las 10 cifras: 26=0,...,35=9. Hacemos corresponder a cada digrafo un vector de $\mathbb{F}_{11}^3$: primero vemos el digrafo como un número de dos cifras en base 36, después lo convertimos en un número entero entre 0 y $1295 = (36)^2 - 1$ y a continuación escribimos este número en base 11:

$$AA = (0,0,0), AB = (0,0,1), \ldots, ZZ = (7,7,1), \ldots, 99 = (10,7,8).$$

Antes de transmitir el digrafo que corresponde al vector $x = (x_1, x_2, x_3)$ se codifica como $xG \in \mathbb{F}_{11}^5$.

Sabiendo que se trata de una ciudad ¿qué leerías si recibieras el siguiente mensaje

$$(0,-3,1,-2,3); (-2,-4,0,3,0); (5,1,5,4,-4)?$$

Primero calculemos una matriz de paridad de este código:

$$H = \begin{pmatrix} 1 & 0 & -1 & -1 & -1 \\ 0 & 1 & 2 & 1 & 1 \end{pmatrix}.$$

Este código es de distancia 2 (la cuarta y quinta columnas de H son iguales).

Para descifrar vamos a corregir como mucho 1 error.

El sindrome de la primera palabra es $\begin{pmatrix} -2 \\ 0 \end{pmatrix} = -2 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Como $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ es la prmera columna de H, corregimos el primer digito. La palabra corregida es $(2,-3,1,-2,3) = (3,6,3)G$. Entonces podemos calcular el primer digrafo:

$$(3,6,3) \to 3 \cdot 121 + 6 \cdot 11 + 7 = 432 = 12 \cdot 36 \to (12,0) \to \text{“}MA\text{”}$$

El sindrome de la segunda palabra es $\begin{pmatrix} -5 \\ -1 \end{pmatrix} = 5 \begin{pmatrix} -1 \\ 2 \end{pmatrix}$. Como $\begin{pmatrix} -1 \\ 2 \end{pmatrix}$ es la tercera columna de H, corregimos el tercer digito. La palabra corregida es $(-2,-4,-5,3,0) = (3,3,0)G$. Entonces podemos calcular el segundo digrafo:

$$(3,3,0) \to 3 \cdot 121 + 3 \cdot 11 = 396 = 11 \cdot 36 \to (12,0) \to \text{“}LA\text{”}$$

El sindrome de la tercera palabra es $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Entonces la tercera palabra está en el código. Obtenemos que $(5,1,5,4,-4) = (1,8,7)G$. Entonces podemos calcular el tercer digrafo:

$$(1,8,7) \to 1 \cdot 121 + 8 \cdot 11 + 7 = 216 = 6 \cdot 36 \to (12,0) \to \text{“}GA\text{”}$$

La ciudad es “MALAGA”

3. (2 puntos) Sea $f : \mathbb{Z}_{1073} \to \mathbb{Z}_{1073}$ la función que manda x a $x^{11} + 2$. Encuentra la función $g : \mathbb{Z}_{1073} \to \mathbb{Z}_{1073}$ tal que $f(g(x)) = x$.

El número 1073 se descompone como producto de dos primos 29 y 37. Además $MCD(29-1, 37-1) = 252$. Si d satisface $11d \equiv 1 \pmod{252}$, entonces $x^{11d} \equiv x \pmod{1073}$ para todo x. Por lo tanto $g(x) = (x-2)^d$. Entonces nos queda sólo encontrar d. Resolviendo

$$11d \equiv 1 \pmod{4,7,9}$$

obtenemos que $d \equiv 3 \pmod 4$, $d \equiv 2 \pmod 7$ y $d \equiv 5 \pmod 9$. Por lo tanto $d \equiv 23 \pmod{252}$.

4. (3 puntos) (Para obtener los 3 puntos es suficiente resolver correctamente 2 apartados entre los 4 primeros y el apartado e). Los apartados anteriores se puede usar en las demostraciones de los apartados posteriores.)

   Sea n un número natural impar.

   a) Demostrar que n es divisible por un sólo primo si y sólo si la ecuación $x^2 = \bar{1}$ tiene sólo 2 soluciones $(\pm\bar{1})$ en $\mathbb{Z}_n$.

   b) Suponemos que $a^m = \bar{1}$ para todos los $a \in U(\mathbb{Z}_n)$. Demostrar que m es un número par.

   c) Suponemos que $a^m = \bar{1}$ para todos los $a \in U(\mathbb{Z}_n)$ pero existe $b \in U(\mathbb{Z}_n)$ tal que $b^{\frac{m}{2}} \neq \bar{1}$. Demostrar que $c^{\frac{m}{2}} \neq \bar{1}$ por lo menos para la mitad de los elementos c en $U(\mathbb{Z}_n)$.

   d) Suponemos que n es producto de 2 primos impares distintos p y q y m cumple que $a^m = \bar{1}$ para todos $a \in U(\mathbb{Z}_n)$ pero existe $b \in U(\mathbb{Z}_n)$ tal que $b^{\frac{m}{2}} \neq \bar{1}$. Sea A el subconjunto de los elementos c de $U(\mathbb{Z}_n)$ tal que $c^{\frac{m}{2}} - \bar{1}$ es divisible exactamente por uno de los primos p or q. Demostrar que A tiene la mitad de los elementos de $U(\mathbb{Z}_n)$.

   e) Suponemos que n es producto de 2 primos impares distintos p y q. . Usando los apartados anteriores dar unas ideas generales como se puede construir un algoritmo probabilístico que dado un algoritmo que rompe RSA (es decir, busca la clave d privada a partir de la clave e pública) descompone n con una probabilidad alta.

a) Primero suponemos que $n = p^k$, donde p es un primo impar y $k \geq 1$. En este caso si $x^2 \equiv 1 \pmod{n}$, entonces $x - 1$ ó $x + 1$ pero no ambos es divisible por p. Por lo tanto $x \equiv \pm 1 \pmod{n}$.

Si $n = p_1^{k_1} \cdots p_s^{k_s}$, donde $p_1, \ldots, p_s$ son primos impares distintos y $k_i \geq 1$, entonces $x^2 \equiv 1 \pmod{n}$ es equivalente al sistema de s congruencias: $x^2 \equiv 1 \pmod{p_i^{k_i}}$. Cada una de estas ecuaciones tiene 2 soluciones y por el Teorema chino del resto esto da 2^s soluciones de $x^2 \equiv 1 \pmod{n}$.

b) Como $(-1)^m \equiv 1 \pmod{n}$ y n es impar, m es par.

c) Sea $H = \{x \in U(\mathbb{Z}_n) : \ x^{m/2} = 1\}$. Entonces H es subgrupo propio de $U(\mathbb{Z}_n)$ y por lo tanto tiene como mucho la mitad de elementos de $U(\mathbb{Z}_n)$.

d) Si x es coprimo con n, entonces $x^{m/2} \equiv \pm 1 \pmod{p, q}$.Por lo tanto $H = U(\mathbb{Z}_n) \setminus A$ es un subgrupo de $U(\mathbb{Z}_n)$ y ademas si $a, b \in A$, entonces $ab \in H$. Luego H tiene índice 2 en $U(\mathbb{Z}_n)$.

e) Observemos primero que si encontramos un $2 \leq a \leq n - 1$ tal que a no es coprimo con n, entonces $MCD(a, n)$ es p o q y por lo tanto obtendremos una factorzación de n. Entonces podemos suponer que si escogemos un $a \neq 0$ entre 2 y $n - 1$, a es coprimo con n. Por lo tanto vamos a trabajar dentro de $U(\mathbb{Z}_n)$.

Como podemos encontrar la clave d a partir de la clave e, podemos calcular $M = de$ que satisface $x^{M-1} = 1$ para todo $x \in U(\mathbb{Z}_n)$.

Usando el apartado c) podemos encontrar con probabilidad alta un m tal que $a^m = \bar{1}$ para todos los $a \in U(\mathbb{Z}_n)$ pero existe $b \in U(\mathbb{Z}_n)$ tal que $b^{\frac{m}{2}} \neq \bar{1}$ (si tenemos un N tal que $a^N \equiv 1 \pmod{n}$ para muchos a escogidos al azar, podemos suponer usando c) que $a^N \equiv 1$ para todos los a coprimos con n y pasamos a analizar $N/2$).

Usando el apartado d) podemos encontrar con probabilidad alta un a tal que $a^{m/2}$ es divisible sólo por uno de los primos. Entonces $MCD(a^{m/2}, n)$ es un divisor propio de n.