Criptología - Curso 07-08

Primer examen

11 de abril de 2008

1 Dados los números 141.525 y 37.037:

(a) Usa el algoritmo de Euclides para calcular su máximo común. Calcula los coeficientes. r_k, q_k, x_k e y_k.

(b) Resuelve, si es posible, la ecuación $141.525x + 37.037y = 370$.

Solución:

(a) Tenemos la siguiente tabla:

k	r_k	q_k	x_k	y_k
0	141.525	-	1	0
1	37.037	3.813	0	1
2	30.414	1	1	3
3	6.623	4	1	4
4	3.922	1	5	19
5	2.701	1	6	23
6	1.221	2	11	42
7	259	4	28	107
8	185	1	123	470
9	74	2	151	577
10	37	2	425	1.624
11	0	-		

Por tanto, $37 = (-1)^{10} \cdot 425 \cdot 141525 + (-1)^{11} \cdot 1624 \cdot 37037$

(b) La ecuación $141.525x + 37.037y = 370$ tiene solución ya que $37|370$. Basta multiplicar por 10 la ecuación de más arriba y obtenemos:

$$370 = (-1)^{10} \cdot 4250 \cdot 141525 + (-1)^{11} \cdot 16.240 \cdot 37037$$

2 Sea la matriz A:

$$A = \begin{pmatrix} -2 & 12 & 11 \\ 2 & 7 & -10 \\ 1 & 10 & -2 \end{pmatrix}$$

(a) Comprueba que define un criptosistema de bloque con el alfabeto español. Usa la correspondencia $\{\text{a} \longrightarrow 0, \cdots, \text{z} \longrightarrow 26\}$.

(b) Descrifa el mensaje `tgm`.

Solución: El determinante de A es 7, que es distinto de 0 módulo 27. Por tanto, la transformación de cifrado tiene inversa y el criptosistema está bien definido. La inversa de A es:

$$A^{-1} = \begin{pmatrix} 20 & 23 & 22 \\ 3 & 26 & 8 \\ 25 & 20 & 10 \end{pmatrix}$$

Si tomamos la habitual correspondencia $\{\text{a} \longrightarrow 0, \cdots, \text{z} \longrightarrow 26\}$, tenemos que `tgm` se transforma en el vector $(20, 6, 12)$:

$$\begin{pmatrix} 6 & 1 & 11 \\ 13 & 7 & 12 \\ 14 & 22 & 11 \end{pmatrix} \begin{pmatrix} 20 \\ 6 \\ 12 \end{pmatrix} = \begin{pmatrix} 19 \\ 15 \\ 11 \end{pmatrix}$$

Pasándolo a caracteres obtenemos la palabra `sol`.

3 Dada la permutación:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 8 & 2 & 1 & 11 & 9 & 5 & 6 & 3 & 4 & 10 \end{pmatrix}$$

(a) Descompón π en ciclos.

(b) Halla el orden de π.

(c) Calcula $\pi \circ \pi$ y $\pi^{-1} \circ \pi^{-1}$.

Solución:

(a) La descomposición de la permutación en ciclos es $\pi = (1\ 7\ 5\ 11\ 10\ 4)(2\ 8\ 6\ 9\ 3)$.

(b) El orden de π es el mínimo común múltiplo de las longitudes de los ciclos de su descomposición. En este caso esas longitudes son 6 y 5, y el orden es m.c.m.$(6, 5) = 30$.

(c) Para $\pi \circ \pi$ tenemos:

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 6 & 8 & 7 & 10 & 3 & 11 & 9 & 2 & 1 & 4 \end{pmatrix}$$

y para $\pi^{-1} \circ \pi^{-1}$:

$$\pi^{-2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 9 & 6 & 11 & 1 & 2 & 4 & 3 & 8 & 5 & 7 \end{pmatrix}$$

4 Describe con detalle el criptoanálisis del cifrado de Vigènere por palabra clave.

Solución: El cifrado de Vigènere es un cifrado polialfabético, esto es, un cifrado en que el alfabeto de sustitución cambia periódicamente. La manera en que cambia está dada por una palabra clave que se repite periódicamente. El criptoanálisis consta de dos etapas: el cálculo de la longitud de la palabra clave y el descubrimiento de dicha palabra.

Longitud de la palabra clave:

- Método 1: Se basa en el índice de coincidencia, que es la probabilidad de que dos letras elegidas al azar en el criptograma sean iguales. Sigue la fórmula:

$$k = \frac{0'0405 \cdot l}{(0'0775 - IC) + l \cdot (IC - 0'037)}$$

  Para que este método sea útil el texto ha de tener poca variabilidad y ser de una cierta longitud.

- Búsqueda de las coincidencias. Dado el criptograma C, se consideran los sucesivos desplazamientos de C por i caracteres a la derecha. Designemos por C_i dichos desplazamientos. Para cada i se cuenta el número de coincidencias entre C y C_i, esto es, se cuenta el número de veces que en la posición j, para $j = 1$ hasta la longitud de C, se encuentra una misma letra. El máximo de esas coincidencias sobre j da la longitud de la palabra clave.

Sabiendo k, los métodos para criptoanalizar Vigènere:

- Una vez conocida k, se divide el criptograma C en k bloques de longitud l/k. Cada bloque está codificado con un cifrado monoalfabético y ya sí responde al análisis de frecuencias.
- Sea W el vector de frecuencias relativas del castellano. Consideremos los bloques antes mencionados $C_1, \ldots, C_k$. Para el bloque i se considera el vector de frecuencias relativas $A_{i,j}$ obtenido por el desplazadamiento de j posiciones a la derecha del vector de frecuencias relativas de C_i; aquí se tiene $j = 0, \ldots, 26$. Se calculan los productos escalares $W \cdot A_{i,j}$, para $0 \leq j \leq 26$. El índice que proporciona el valor máximo de esos productos escalares es el índice de la letra i de la palabra clave.

5 Responde a las siguientes preguntas:

(a) Define los distintos tipos de ataque y pon ejemplos con los cifrados vistos en clase.

(b) La estructura de grupo en un cifrado, ¿aumenta la seguridad del mismo? Razónalo y pon un ejemplo.

(c) Explica qué es el índice de coincidencia.

Solución:

(a) Los tipos de ataque son los siguientes:

- Ataque de criptograma. Se conoce una parte del criptograma, la cual ha sido interceptada en la comunicación entre ambos correspondientes.

- Ataque de texto claro conocido. Se conoce un texto claro y su correspondiente criptograma. De nuevo, ambos han sido interceptados en la comunicación entre los correspondientes.
- Ataque de texto claro escogido. Aquí el fisgón o atacante tiene acceso a la máquina que cifra. Elige un mensaje claro concreto y obtiene el correspondiente criptograma, que posteriormente estudia para conocer la clave.
- Ataque de texto claro escogido y adaptativo. Es como en el caso anterior, pero el fisgón manda varios mensajes claros con la idea de sacar patrones con los que descubrir la clave.

Por ejemplo, para un cifrado de desplazamiento, y dado un criptograma suficientemente largo, basta el análisis de frecuencias para averiguar la clave. Luego un ataque de criptograma es suficiente para el cifrado de desplazamiento. Lo mismo se aplica al cifrado afín. Un ataque de texto claro conocido de tamaño dos basta obtener la clave para ese cifrado. En los cifrados de sustitución, un análisis de frecuencias más refinado permite averiguar la clave también. De nuevo, el ataque de criptograma basta. El ataque de texto claro conocido para el cifrado de sustitución no permite sacar nada más que la correspondencia de las letras del texto claro, aunque, claro es, simplifica el análisis de frecuencias. Un ataque de texto claro escogido rompe por completo la clave. El cifrado de Vigènere no responde al análisis de frecuencias al cambiar periódicamente el alfabeto de sustitución. Sin embargo, con métodos más complejos (incorporando el índice de coincidencia, calculando máximo de coincidencias, etc.) se puede romper el cifrado con un ataque de criptograma. Los cifrados de permutación no responden al análisis de frecuenciass, pero con prueba y error sobre la longitud de las columnas más un diccionario de anagramas se puede conseguir que un ataque de criptograma proporcione el texto claro.

(b) La estructura de grupo en un cifrado no aumenta la seguridad. Si la composición de dos claves k_1, k_2 es equivalente a una tercera clave k_3, entonces el esfuerzo computacional de romper la composición es igual al de romper k_3. Como ejemplo, consideremos el cifrado de desplazamiento:

$$\begin{aligned} E_{k_1}(E_{k_2}(x)) &= E_{k_1}(x+k_2) = \mod 27 = (x+k_2)+k_1 \bmod 27 \\ &= x + (k_1+k_2) \bmod 27 \end{aligned}$$

En este caso romper el cifrado $k_1 + k_2$ es igual que romper el cifrado de desplazamiento cualquiera. En particular, el análisis de frecuencias no cambia por la composición de cifrados de desplazamiento.

(c) El índice de coincidencia de un lenguaje es la probabilidad de que dos letras elegidas al azar sean iguales. En el caso del español, ese índice es igual a la suma de los cuadrados de las frecuencias relativas, y vale $0'0775$. El índice de coincidencia de un criptograma es la probabilidad de que dos letras elegidas al azar de dicho criptograma. Si $n_1, \cdots, n_p$ son las frecuencias absolutas de los símbolos del criptograma (suponemos que hay p símbolos), y n la longitud del criptograma, entonces el índice es:

$$\frac{\sum_{i=1}^{p} n_i(n_i-1)}{n(n-1)}$$