Ejercicios

2. Semana 2

2.1. Inversos modulares. Teorema chino del resto. Cifrado afín II

1. En caso de que exista, calcular $a^{-1} \mod b$ y comprobar el resultado.

   a) $a = 3$, $b = 26$.

   b) $a = 22$, $b = 28$.

   c) $a = 15$, $b = 28$.

   (Utilizar el resultado del Problema 3 de la Sección 1.4).

2. Resolver el siguiente sistema de ecuaciones

$$\left.\begin{array}{l} 4a + b \equiv 23 \mod 26 \\ 19a + b \equiv 20 \mod 26 \end{array}\right\}$$

3. *a*) Probar

$$4x \equiv 4y \mod 28 \text{ si y sólo si } x \equiv y \mod 7.$$

   b) Resolver los siguientes sistemas:

   (i)
$$4a' \equiv 4 \mod 28,$$

   (ii)
$$12a' \equiv 8 \mod 28.$$

4. *a*) ¿Es $(\mathbb{Z}_{12}, +, \cdot)$ cuerpo?

   b) Encontrar en $\mathbb{Z}_{12}$ dos elementos diferentes de 0 y tales que su producto sea 0.

   c) Calcular la función de Euler de $n = 12$, $\phi(12)$.

   d) Calcular $\mathbb{Z}_{12}^*$. ¿Es $(\mathbb{Z}_{12}^*, \cdot)$ grupo?

5. Utilizar el Pequeño Teorema de Fermat para calcular:

   a) $4^{10} \mod 11$, $5^{10} \mod 11$, $5^{20} \mod 11$, $5^{21} \mod 11$.

   b) $19^{186} \mod 47$.

6. *a*) Calcular $\phi(85)$.

   b) Utilizando el Teorema de Euler-Fermat, calcular:

$$11^{64} \mod 85, \quad 11^{129} \mod 85.$$

7. *a*) Sean a, x números enteros, $x \geq 0$, y sea p un número primo. Demostrar que
$$a^x \equiv (a \mod p)^{(x \mod (p-1))} \mod p.$$
Es decir, al calcular una potencia módulo un primo p, la base puede reducirse módulo p y el exponente puede reducirse módulo $p-1$.

   b) Utilizar el resultado anterior para calcular $1002^{34} \mod 5$.

8. Sean a, b, p, q números enteros con p, q primos relativos. Sea
$$x = qq_1a + pp_1b,$$
donde
$$q_1 \equiv q^{-1} \mod p, \quad p_1 \equiv p^{-1} \mod q.$$
Probar que
$$\begin{aligned} x &\equiv a \mod p, \\ x &\equiv b \mod q. \end{aligned}$$
Sugerencia: tener en cuenta que $pp_1 \equiv 0 \mod p$ y $qq_1 \equiv 0 \mod q$.

9. Utilizando el Teorema chino del resto calcular la solución x del sistema
$$\begin{aligned} x &\equiv 3 \mod 4, \\ x &\equiv 2 \mod 3, \\ x &\equiv 0 \mod 5. \end{aligned}$$
Comprobar el resultado.

10. Utilizando el Teorema chino del resto calcular la solución x del sistema
$$\begin{aligned} x &\equiv 5 \mod 7, \\ x &\equiv 4 \mod 6. \end{aligned}$$
Comprobar el resultado.

11. En este Problema veremos un ejemplo de criptoanálisis por análisis de frecuencias.

Supongamos que el carácter más frecuente en un mensaje cifrado largo es "1" y el segundo más frecuente es "W". Sabemos que ha sido cifrado usando una transformación afín sobre el alfabeto de $N = 28$ caracteres:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*
0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\tilde{N}$	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	1
14	15	16	17	18	19	20	21	22	23	24	25	26	27

En español las letras más frecuentes son "E" y "A", en ese orden. Entonces, es razonable pensar que el descifrado de "1" es "E" y el de "W" es "A".

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{M} \\ \text{"1"} = 27 & \mapsto & \text{"E"} = 4 \\ \text{"W"} = 23 & \mapsto & \text{"A"} = 0 \end{array}$$

Si la clave de descifrado es (a', b') se tiene que

$$\left.\begin{array}{l} 27a' + b' \equiv 4 \mod 28 \\ 23a' + b' \equiv 0 \mod 28 \end{array}\right\}$$

de donde obtenemos

$$4a' \equiv 4 \mod 28, \tag{1}$$

$$b' \equiv -23a' \mod 28. \tag{2}$$

Hemos visto en el Problema 3 de esta Sección que la ecuación (1) tiene 4 posibles soluciones

$$a' = 1, \quad a' = 8, \quad a' = 15, \quad a' = 22.$$

Como debe ser $\mathrm{mcd}(a', N) = 1$, sólo tenemos dos posibilidades:

$$a' = 1 \text{ ó } a' = 15.$$

De la ecuación (2) obtenemos:

- Si $a' = 1$, entonces $b' \equiv -23a' \equiv -23 \equiv 5 \mod 28$.
- Si $a' = 15$, entonces $b' \equiv -23a' \equiv -345 \equiv 19 \mod 28$.

Entonces, las dos posibles claves son:

$$(a', b') = (1, 5) \text{ ó } (a', b') = (15, 19).$$

Tenemos dos opciones:

- Probar con las 2 posibilidades hasta encontrar un mensaje con sentido.
- Seguir con el análisis de frecuencias: supongamos que la siguiente letra más frecuente es "X". En español la tercera letra más frecuente es "O".

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{M} \\ \text{"X"} = 24 & \mapsto & \text{"O"} = 15 \end{array}$$

Entonces debe ser:

$$24a' + b' \equiv 15 \mod 28.$$

Se pide:

a) Decidir cuál de las dos posibilidades es la clave de descifrado.

b) Descifrar el criptograma "YNDLOXWVWTDADA".

12. Interceptamos el mensaje "UBTYQT" que sabemos que ha sido cifrado usando una transformación translación (transformación afín de clave $(a = 1, b)$) sobre el alfabeto habitual de $N = 26$ letras.

Supongamos que en un mensaje cifrado razonablemente largo la letra más frecuente es "U". Sabemos que en español la letra más frecuente es "E".

Obtener la clave de descifrado y descifrar el mensaje.

13. Interceptamos el mensaje "QQHMSX" que sabemos que ha sido cifrado en bigramas usando una transformación afín sobre el alfabeto habitual de $N = 26$ letras.

    Supongamos que en un mensaje cifrado largo los bigramas más frecuentes son "EI" y "LD", en ese orden. Sabemos que en español los bigramas más frecuentes son "EN" y "DE".

    Obtener la clave de descifrado y descifrar el mensaje.

14. Estamos intentando criptoanalizar una transformación afín sobre un alfabeto de 37 caracteres. El alfabeto comprende los dígitos 0 a 9, las 26 letras "A"-"Z" y el espacio blanco. Los números están etiquetados con ellos mismos (es decir, con los enteros 0 a 9), las letras con los enteros 10 a 35 y el blanco con 36. Interceptamos el criptograma "43DO6DRBZSM4E " y sabemos que empieza por "ES" y que ha sido cifrado partiendo el mensaje en bloques de una letra. Obtener la clave de descifrado y descifrar el mensaje.

0	1	2	3	4	5	6	7	8	9	A	B	C	D
0	1	2	3	4	5	6	7	8	9	10	11	12	13
E	F	G	H	I	J	K	L	M	N	O	P	Q	R
14	15	16	17	18	19	20	21	22	23	24	25	26	27
S	T	U	V	W	X	Y	Z	" "					
28	29	30	31	32	33	34	35	36					

2.2. Características del cifrado en flujo. Generación de secuencias pseudoaleatorias

1. Supongamos que dos mensajes M_1 y M_2 han sido cifrados con un cifrado de Vernam utilizando la misma clave. Los respectivos criptogramas son:

$$C_1 = 0111010010, \quad C_2 = 11011010.$$

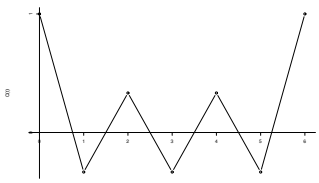
    Sabiendo que $M_1 = 1100111000$, obtener la clave y M_2.

2. Dada la secuencia periódica de período 10,

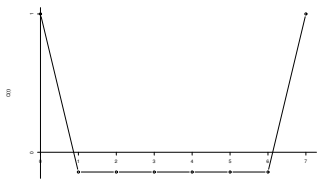
$$(s_i) = (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, \ldots),$$

    hallar la función de autocorrelación $\mathrm{C}(t)$, $0 \leq t \leq 10$, y representarla gráficamente.

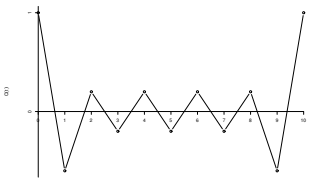
3. Podemos observar que la función de autocorrelación de distintas secuencias de bits es simétrica:



$(s_i) = (1, 0, 1, 0, 0, 0),\ T = 6$



$(s_i) = (0, 0, 1, 0, 1, 1, 1),\ T = 7$



$(s_i) = (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, \dots),\ T = 10$

Probar esta propiedad en general. Es decir, dada la secuencia de bits $(s_i) = (s_0, s_1 s_2, \dots)$ periódica de período T, sea $\mathrm{C}(t)$ su función de autocorrelación. Demostrar que

$$\mathrm{C}(T-t) = \mathrm{C}(t), \quad t = 0, 1, \dots, T-1.$$

Sugerencia: probar que, para $t = 0, 1, \dots, T-1$,

$$\sum_{i=0}^{t-1}(2s_i - 1)(2s_{i+T-t} - 1) = \sum_{j=T-t}^{T-1}(2s_{j+t} - 1)(2s_j - 1),$$

$$\sum_{i=t}^{T-1}(2s_i - 1)(2s_{i+T-t} - 1) = \sum_{j=0}^{T-t-1}(2s_{j+t} - 1)(2s_j - 1).$$

2.3. Generadores congruenciales

1. Dado un generador congruencial lineal de parámetros a, b, m, estudiar si satisface las condiciones para que las secuencias que origina posean período máximo, en los siguientes casos:

   a) $a = 2, b = 3, m = 13$.

   b) $a = 7, b = 5, m = 12$.

2. Obtener las secuencias generadas por los generadores congruenciales lineales indicados a continuación. Estudiar sus períodos y preperíodos y, si no presentan período máximo, indicar por qué.

   a) $a = 2, b = 4, m = 14, x_0 = 1$

b) $a = 3, b = 4, m = 18, x_0 = 2$

c) $a = 1, b = 3, m = 13, x_0 = 1$

3. Si $m = 90$ y $b = 7$, calcular los valores posibles de a para que la secuencia generada por un generador congruencial lineal de parámetros a, b, m tenga período máximo.

4. Los 3 primeros términos de una secuencia generada por un generador congruencial de parámetros a, b, m son $x_0 = 1$, $x_1 = 12$, $x_2 = 17$. Calcular x_3, x_4 sabiendo que $m = 18$.