Soluciones

1. Semana 1

1.1. Criptografía cásica

1. *a*) "DVWHULA"
   b) "OBELIX"
2. "TEOBALDO"
3. *a*) "KITOVXFZ"
   b) "CIFRADO"
   Hay que tener en cuenta que la clave para cifrar cada bloque del mensaje (a partir del segundo) es el cifrado del bloque anterior.
4. El cifrado del primer mensaje es "OMQ7SXUB6 8A R76ZGXXR RS". MAC1: "R RS".
   El del segundo, "OMQ7SXUB6 8A R76ZPXXRIRS". MAC2: "RIRS".

1.2. Seguridad criptográfica

1. Transparencia 3 de "1_2seguridad".
2. Transparencia 5 de "1_2seguridad".
3. Transparencia 9 de "1_2seguridad".

1.3. Conversión de mensajes. Aritmética modular

1. Como la longitud del mensaje no es múltiplo de 2, hemos añadido una "Z" (se puede añadir cualquier letra que no cree ambigüedad).
   Conversión a números: "CESARZ" $\to (56, 468, 467)$.
   Conversión a bits: Se tiene que
   $$26^2 - 1 = 675 = 2^9 + 2^7 + 2^5 + 2 + 1,$$
   por tanto $26^2 - 1$ se representa con 10 bits. Las cadenas deberán de ser de 10 bits.
   $$\text{"CESARZ"} \to 0000111000011101010001110100 11$$
2. $$117 = 4 \cdot 26 + 13 \to (4, 13) \to \text{"EN"}$$
   $$(117, 214, 312) \to \text{"ENIGMA"}$$

Como $26^2 - 1$ tiene 10 bits, dividimos la secuencia dada en cadenas de 10 bits.

$$0001000010 \to 2^6 + 2 = 66$$

$$66 = 2 \cdot 26 + 14 \to (2, 14) \to \text{“CO”}$$

$$00010000100100101100011110011010000011010 \to \text{“COLOSSUS”}$$

3. $10 + 13 \equiv 8 \mod 15$.

   $10 + (-13) \equiv 12 \mod 15$. $\quad (-3 = (-1) \cdot 15 + 12)$.

   $15 \cdot 10 \equiv 20 \mod 26$.

   $(-15) \cdot 10 \equiv 6 \mod 26$. $\quad (-150 = (-6) \cdot 26 + 6)$.

4. $(\mathbb{Z}_5, +, \cdot)$ es anillo porque

   - $(\mathbb{Z}_5, +)$ es grupo conmutativo:
     - $(+)$ es asociativa.
     - $(+)$ es conmutativa.
     - $(+)$ tiene elemento neutro: 0.
     - Todo elemento $a \in \mathbb{Z}_5$ tiene simétrico para $(+)$: el simétrico de a es $5 - a \in \mathbb{Z}_5$.
   - $(\cdot)$ es asociativa.
   - $(\cdot)$ es conmutativa.
   - $(\cdot)$ tiene elemento neutro: 1.
   - $(\cdot)$ es distributiva con respecto a $(+)$.

   $(\mathbb{Z}_5, \cdot, +)$ no es anillo porque $(\mathbb{Z}_5, \cdot)$ no es grupo conmutativo: $0 \in \mathbb{Z}_5$ no tiene simétrico para $(\cdot)$.

   Tampoco $(+)$ es distributiva con respecto a $(\cdot)$:

   $$2 + (1 \cdot 0) \equiv 2 \mod 5, \quad (2 + 1) \cdot (2 + 0) \equiv 1 \mod 5.$$

5. Solución: $19^{12} \equiv 1 \mod 7$.

   a) $19^{12} \equiv (19 \mod 7)^{12} \equiv 5^{12} \equiv 1 \mod 7$.

   b) $5^{12 \mod 7} \equiv 5^{5 \mod 7} \equiv 3 \mod 7 \neq 19^{12} \mod 7$.

6. a) $38^{75} \equiv 79 \mod 103$; b) $2^{32} \equiv 0 \mod 16$.

1.4. Cifrado afín I. Divisibilidad. Números primos

1. Convertimos "CESAR" en números

$$\text{"CESAR"} \to (2, 4, 18, 0, 17)$$

Ciframos

$$5 \cdot 2 + 10 = 20 \equiv 20 \mod 26$$
$$5 \cdot 4 + 10 = 30 \equiv 4 \mod 26$$
$$5 \cdot 18 + 10 = 100 \equiv 22 \mod 26$$
$$5 \cdot 0 + 10 = 10 \equiv 10 \mod 26$$
$$5 \cdot 17 + 10 = 95 \equiv 17 \mod 26$$
$$(2, 4, 18, 0, 17) \to (20, 4, 22, 10, 17) \to \text{"UEWKR"}.$$

El cifrado de "CESAR" es "UEWKR".

2. *a*) La función de descifrado es:

$$\begin{array}{rccc} f^{-1}: & \mathcal{C} & \longrightarrow & \mathcal{M} \\ & C & \mapsto & M \equiv C - b \mod N \end{array}$$

b) 1) El cifrado de "OBELIX" es "DQTAXM".
2) El descifrado de "PHITGXM" es "ASTERIX".

c) La clave es $b = 23$. El descifrado de "ELIX" es "HOLA".

3. *a*) $\text{mcd}(3, 26) = 1 = 9 \cdot 3 + (-1) \cdot 26$.

b) $\text{mcd}(22, 28) = 2 = (-5) \cdot 22 + 4 \cdot 28$.

c) $\text{mcd}(15, 28) = 1 = (-13) \cdot 15 + 7 \cdot 28$.

4. *a*) $u = -2,\ v = 3$.

b) $u = 2,\ v = 3$.

c) $u = -2,\ v = -3$.

d) $u = 2,\ v = -3$.