Apéndice E | PROBLEMAS DE CRIPTOLOGÍA

1. ENUNCIADOS

1.1. Criptología clásica

1. Uno de los siguientes criptogramas fue enviado por César Augusto y el otro por Julio César. Decidir cuál envió cada uno (se utiliza el alfabeto internacional, es decir, sin eñes).

```
OD VXHUWH DBXGD D ORV DXGDFHV
BQSFTVSBUF DPO MFOUJUVE
```

2. Cifrar el siguiente mensaje utilizando una escítala lacedemonia de 8 líneas y 3 columnas:

```
UN AGUILA NO CAZA MOSCAS
```

3. ¿Cuál sería el mensaje correspondiente al siguiente criptograma obtenido utilizando la misma escítala?

```
MIRIEEAMCNBOILRMADOAATLR
```

4. Un criptoanalista asegura que el siguiente criptograma se ha realizado con un criptosistema monoalfabético, ¿será cierto?

ANXDUIMNOSUIDADJJJJADUFDS

5. Decidir cuáles de las siguientes posibles palabras clave son las más adecuadas para un cifrado de tipo Vigenère:

DOS, MAMA, TREN, DISCO, COMPUTADOR

6. El siguiente criptograma se ha cifrado con el método de Vigenère, del que se sabe que la palabra clave es una de las siguientes: «ESMERALDA», «DIAMANTE», «TOPACIO» y «ZAFIRO». Determinar la clave y descifrar el mensaje.

DAIETVKEQ ML BRRLMGMNFE QXP FWNSRRLS
B ML BRRLMGMNFE QXP VMNMDB

7. Determinar el mensaje original que corresponde al criptograma siguiente, si se sabe que la clave está relacionada con un gran descubrimiento geográfico:

FP MGTGDDSMVKFRCQ SIOGSMMQ FW NN
EI JOFVREB TXT DVRUUSKCM GXNPR

8. Utilizando el alfabeto internacional de 26 letras y asignando un valor a cada una de ellas de modo que $A \to 0$, $B \to 1$, ..., $Z \to 25$, se define un cifrado afín por la expresión $\mathcal{C}(m) = 3m + 7 \pmod{26}$, siendo m la letra a cifrar.

a) Encriptar, mediante este criptosistema, la siguiente frase:

ESTE CRIPTOSISTEMA NO ES SEGURO

b) Determinar la función de descriptado.

c) Descriptar el mensaje anterior.

1.2. Métodos matemáticos

1. Calcular el orden de la permutación

$$\begin{pmatrix} 2 & 5 & 8 & 9 & 20 & 12 & 13 & 1 & 14 & 3 & 7 & 10 & 11 & 6 & 19 & 18 & 15 & 16 & 17 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \end{pmatrix}$$

2. ¿Cuántos divisores tiene 945? Listarlos.

3. Calculando los restos potenciales de 10 módulo 7, deducir el criterio de divisibilidad por 7 para un número de cinco cifras y para uno de siete cifras. Como aplicación, calcular los valores de *c* y *d* para

que el número $N = 32cd1$ sea divisible por 7. ¿Se podría deducir el criterio de divisibilidad por 7 para un número con cualquier número de cifras?

4. Determinar la potencia de cada uno de los siguientes primos: 2, 3, 5 y 7 que dividen exactamente a 100!.

5. Para cada uno de los siguientes pares de enteros, encontrar su máximo común divisor (mcd = d) y expresar d como combinación lineal de dicha pareja:

a) 26, 19.
b) 187, 34.
c) 841, 160.
d) 1547, 560.
e) 1729, 1001.
f) 2613, 2171.

6. Calcular el mínimo común múltiplo de $a = 2345$ y $b = 737$ usando la fórmula $a \cdot b = \text{mcd}\,(a, b) \cdot \text{mcm}\,(a, b)$.

7. En ocasiones resulta conveniente llevar a cabo el algoritmo de Euclides utilizando también restos por defecto, es decir, llevando a cabo las siguientes divisiones:

$$r_j = q_{j+2} \cdot r_{j+1} - r_{j+2}$$

tanto como

$$r_j = q_{j+2} \cdot r_{j+1} + r_{j+2}$$

En este caso se tiene que

$$r_{j+2} \leq \frac{1}{2} r_{j+1}$$

Realizar este algoritmo con la pareja (2613, 2171).

8. Calcular los valores del $\text{mcd}\,(f(x), g(x)) = d(x)$ para las siguientes parejas de polinomios, y en cada uno de los casos determinar los polinomios $u(x)$ y $v(x)$ tales que $d(x) = u(x) f(x) + v(x) g(x)$.

a) $f(x) = x^4 + x^2 + 1$, $g(x) = x^2 + 1$.
b) $f(x) = x^4 - 4x^3 + 6x^2 - 4x + 1$, $g(x) = x^3 - x^2 + x - 1$.

9. Se sabe que un polinomio tiene raíces múltiples si y sólo si tiene algún factor común con su derivada. En este caso, las raíces múltiples del polinomio $f(x)$ son las del $\text{mcd}\,(f(x), f'(x))$. Encontrar las raíces múltiples del polinomio $f(x) = x^4 - 2x^3 - x^2 + 2x + 1$.

10. Escribir los números enteros a que verifican cada una de las siguientes congruencias:

a) $a \equiv 0 \pmod 3$, $a \equiv 1 \pmod 3$, $a \equiv 2 \pmod 3$.
b) $a \equiv 0 \pmod 7$, $a \equiv 3 \pmod 7$, $a \equiv 4 \pmod 7$.
c) $a \equiv 2 \pmod{23}$, $a \equiv 5 \pmod{23}$, $a \equiv 15 \pmod{23}$.

11. Representar en sendas tablas las operaciones de suma y producto módulo 4.

12. Calcular $160^{-1} \pmod{841}$; es decir, el inverso de 160 módulo 841. Encontrar también el inverso de 15 módulo 127.

13. Calcular el orden de 5 módulo 1367.

14. Determinar las unidades y decenas de 7^{123}.

15. Calcular el valor de la función phi de Euler (ϕ) para los siguientes números:

a) 81.
b) 1960.
c) 1996.
d) 41503.

16. Determinar el último dígito en base 7 de $2^{1.000.000}$.

17. Calcular todas las soluciones de las siguientes congruencias:

a) $3x \equiv 4 \pmod 7$.
b) $3x \equiv 4 \pmod{12}$.
c) $9x \equiv 12 \pmod{21}$.
d) $27x \equiv 25 \pmod{256}$.
e) $27x \equiv 72 \pmod{900}$.
f) $103x \equiv 612 \pmod{676}$.

18. Resolver el siguiente sistema de ecuaciones módulo 5: $3x + 2y = 2$, $x + 3y = 1$.

19. Encontrar el número entero decimal de tres cifras que arroja un resto de 4 al ser dividido por 7, 9 y 11.

20. Determinar el menor entero positivo que da un resto de 1 al dividirlo por 11, un resto de 2 al dividirlo por 12 y un resto de 3 al dividirlo por 13.

21. Encontrar la menor solución no negativa de cada uno de los siguientes sistemas en congruencias:

a) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$, $x \equiv 5 \pmod{16}$.
b) $x \equiv 12 \pmod{31}$, $x \equiv 87 \pmod{127}$, $x \equiv 91 \pmod{255}$.
c) $19x \equiv 103 \pmod{900}$, $10x \equiv 511 \pmod{841}$.

22. Para calcular de forma rápida la exponenciación modular, es decir, el valor de $a^n \pmod m$, con n y m grandes, se utiliza el método de las *potencias cuadradas sucesivas*. Este método consiste en expresar, en primer lugar, n en base 2, $n = n_0 + 2n_1 + 2^2n_2 + \ldots + 2^k n_k$, siendo $n_i \in \{0,1\}$. A continuación se calcula cada una de las potencias $a_j \equiv a^{2^j\, n_j} \pmod m$, $j = 1, \ldots, k$, sin más que elevar al cuadrado, módulo m, la potencia anterior. Finalmente se multiplican los valores a_j obtenidos. Utilizando este método, determinar el valor de $38^{75} \pmod{103}$.

23. Calcular $2^{1.000.000} \pmod{77}$.

24. Utilizar el algoritmo de Euclides para determinar el máximo común divisor $d(X) = \text{mcd}(f(X), g(X))$, con $f, g \in \mathbb{F}_p[X]$, en los siguientes casos, y para cada uno de ellos, determinar $u(X)$ y $v(X)$, de modo que $d(X) = u(X) f(X) + v(X) g(X)$:

a) $f(X) = X^3 + X + 1$, $g(X) = X^2 + X + 1$, $p = 2$.
b) $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, $g(X) = X^4 + X^2 + X + 1$, $p = 2$.
c) $f(X) = X^3 - X + 1$, $g(X) = X^2 + 1$, $p = 3$.
d) $f(X) = X^5 + X^4 + X^3 - X^2 - X + 1$, $g(X) = X^3 + X^2 + X + 1$, $p = 3$.
e) $f(X) = X^5 + 88X^4 + 73X^3 + 83X^2 + 51X + 67$, $g(X) = X^3 + 97X^2 + 40X + 38$, $p = 101$.

25. Encontrar todas las raíces múltiples de $f(X) = X^7 + X^5 + X^4 - X^3 - X^2 - X + 1 \in \mathbb{F}_3[X]$ en su cuerpo de descomposición.

26. Si $\alpha \in \mathbb{F}_{p^2}$, satisface el polinomio $X^2 + aX + b$, con $a, b \in \mathbb{F}_p$, probar que:

a) α^p también verifica el mismo polinomio.
b) Si $\alpha \notin \mathbb{F}_p$, entonces $a = -\alpha - \alpha^p$ y $b = \alpha^{p+1}$.
c) Si $\alpha \notin \mathbb{F}_p$ y $c, d \in \mathbb{F}_p$, entonces $(c\alpha + d)^{p+1} = d^2 - acd + bc^2 \in \mathbb{F}_p$.
d) Sea i una raíz cuadrada de -1 en $\mathbb{F}_{19^2}$. Utilizar el apartado *c*) anterior para calcular $(2 + 3i)^{101}$, es decir, escribirlo en la forma $a + bi$ con $a, b \in \mathbb{F}_{19}$.

27. Calcular el par que corresponde al entero 13 en el isomorfismo $\mathbb{Z}_{143} \approx \mathbb{Z}_{11} \times \mathbb{Z}_{13}$. Recíprocamente, determinar el entero módulo 143 que corresponde al par (7,11).

28. Calcular $\log_2 667$ en $\mathbb{Z}_{683}$.

29. Si n no es un cuadrado perfecto y se verifica que $n-1 > \phi(n) > n - n^{2/3}$, probar que n es el producto de dos primos distintos.

30. Pruébese que $n^5 - n$ es siempre divisible por 30.

31. Sea n un entero producto de dos primos distintos y sean e y d dos enteros positivos tales que $e \cdot d - 1$ es divisible por $p - 1$ para cada divisor primo de n (por ejemplo, este es el caso si $e \cdot d \equiv 1 \pmod{\phi(n)}$). Probar que $a^{e \cdot d} \equiv a \pmod{n}$ para cualquier entero a.

1.3. Complejidad computacional

1. Expresar el número binario $11001001_{(2}$ en base decimal.

2. Calcular $160 \cdot 199$ en base 7.

3. Calcular $11001001_{(2} : 100111_{(2}$.

4. Expresar 10^6 en las bases 2, 7 y 9.

5. Si se utiliza la base $b = 26$, se pueden usar las letras del alfabeto en lugar de números, sin más que asignar a las letras A-Z del alfabeto internacional, los números 0-25. Con esta convención, determinar los valores en base decimal de «$\texttt{MAL}_{(26}$» y de «$\texttt{M.AL}_{(26}$».

6. Determinar los valores de las siguientes constantes en base 2 y en base 26:

a) $\pi = 3{,}1415926\ldots$

b) $e = 2{,}7182818\ldots$

7. Dividir «$\texttt{131B6C3}_{(16}$» entre «$\texttt{1A2F}_{(16}$».

8. Estimar el tiempo requerido para convertir un entero k-bit en su representación en base 10.

9. El algoritmo de Euclides extendido proporciona el valor de las constantes u y v de modo que si $d = \text{mcd}(a,b)$, entonces $d = u \cdot a + v \cdot b$. Determinar el tiempo de ejecución para este algoritmo.

10. Si se verifica que $\text{mcd}(a,m) = 1$, calcular el tiempo necesario para encontrar el inverso de a módulo m, es decir, para determinar un entero b tal que $a \cdot b \equiv 1 \pmod{m}$.

11. Determinar el tiempo necesario para calcular $\lfloor \sqrt{n} \rfloor$, siendo n un número muy grande escrito en binario y si $\lfloor m \rfloor$ representa el mayor entero menor que m.

12. Como ejemplo del algoritmo usado en el problema anterior, determinar en binario el valor de $\lfloor \sqrt{116} \rfloor$.

13. Estimar el tiempo requerido para calcular en binario el valor de 3^n.

14. Determinar el tiempo que hace falta para calcular n^n.

15. Calcular el tiempo necesario para multiplicar todos los números primos menores que un número dado n, supuesto que se tiene la lista de todos esos primos. (*Nota*: para calcular el número de primos menores que n se debe utilizar el teorema de los números primos.)

16. Sea $n = p \cdot q$ el producto de dos primos diferentes. Demostrar que puede calcular $\phi(n)$ a partir de p y q en $O(\log n)$ operaciones bits, y que se pueden calcular p y q a partir de $\phi(n)$ en $O(\log^3 n)$ operaciones bits.

17. Comprobar que el tiempo necesario para calcular $a^n \pmod m$ es $O(\log n \cdot \log^2 m)$.

18. Sea $\mathbb{F}_q$ un cuerpo finito de $q = p^m$ elementos y sea $F(X)$ un polinomio irreducible de grado m sobre $\mathbb{F}_p$. Probar que dos elementos de $\mathbb{F}_q$ pueden ser multiplicados en $O(\log^3 q)$ operaciones bits.

19. Con las mismas condiciones del problema anterior, si k es un entero positivo, entonces un elemento de $\mathbb{F}_q$ puede elevarse a la potencia k en $O(\log k \cdot \log^3 q)$ operaciones bits.

20. Justificar que el siguiente algoritmo para calcular el mcd $(n_1, n_2) = d$ de dos números, debido a Stein, es correcto:

Entrada: dos enteros positivos n_1 y n_2.
Salida: $d = \text{mcd}\,(n_1, n_2)$.

a) $c \leftarrow 0$.
b) Si n_1 y n_2 son pares, entonces $n_1 \leftarrow n_1/2$, $n_2 \leftarrow n_2/2$, $c \leftarrow c + 1$. Repetir el paso *b*).
c) Si n_1 es impar y n_2 es par, entonces $n_1 \leftrightarrow n_2$.
d) Si n_1 es par, entonces $n_1 \leftarrow n_1/2$. Repetir el paso *d*).
e) $\Delta = n_1 - n_2$.

f) Si $\Delta < 0$, entonces $n_2 \leftarrow n_1$, $\Delta \leftarrow -\Delta$.
g) $n_1 \leftarrow \Delta/2$.
h) Si $n_1 \neq 0$, entonces ir al paso *d*).
i) Si $n_1 = 0$, entonces $d = 2^c n_2$.

21. Ejecutar el algoritmo anterior para determinar el mcd (24, 36).

1.4. Criptografía de clave secreta

1. Utilizando el cifrado en flujo con la cadena de bits

$$K = 01100011000000010111100000101000$$
$$01111110011110011110011001011010$$

cifrar el mensaje «LADRILLO» usando el código ASCII.

2. Obtener las secuencias cifrantes, utilizando el generador en congruencia lineal $x_{i+1} \equiv (5x_i + 3) \pmod{16}$, para las semillas $x_0 = 1$, 2 y 5.

3. Con la secuencia cifrante cuadrática $x_i \equiv x_{i-1}^2 \pmod{p}$, obtener las secuencias cifrantes para todas las semillas x_0 y para todos los valores primos $p = 17$, 19 y 23.

1.5. Criptografía de clave pública

1. Alicia y Bernardo utilizan como grupo $\mathbb{Z}_{13}^*$ y eligen como generador del mismo $\alpha = 4$. Determinar qué número secreto se intercambiarán por el cambio de clave de Diffie-Hellman, si Alicia elige como número aleatorio $a = 5$ y Bernardo elige $b = 2$.

2. Romper el protocolo utilizado por Alicia y Bernardo en el problema anterior, sabiendo que los números que se intercambian son 3 y 10, respectivamente.

3. Extender el protocolo del cambio de clave de Diffie-Hellman para el caso en el que haya tres participantes.

4. Si se utiliza el criptosistema RSA, determinar el criptograma para el siguiente mensaje M = «1521674902», teniendo en cuenta que los parámetros del destinatario, Bernardo, son: $n_B = 143$, $e_B = 7$, y $d_B = 103$, y los del remitente, Alicia, son: $n_A = 161$, $e_A = 31$ y $d_A = 115$.

5. Bernardo utiliza el criptosistema RSA con la siguiente clave pública: $(n_B, e_B) = (2947, 179)$. Determinar el criptograma que debe enviar a Alicia si el mensaje es M = «MANDA DINERO». En este

caso, las letras A-Z del alfabeto se codifican con 0-25, el punto es el 26 y el espacio en blanco es el 27.

6. Si Alicia tiene como clave pública $(n_A, e_A) = (2773, 17)$, determinar el criptograma que corresponde a la respuesta al mensaje del problema anterior: «NO TENGO».

7. Tratar de romper las claves de Alicia y Bernardo de los dos problemas anteriores.

8. Alicia y Bernardo han decidido cambiar sus claves para estar más seguros a la hora de intercambiarse mensajes. Sus nuevas claves públicas son, respectivamente,

$$(n_A, e_A) = (342723272091234212791, 13)$$
$$(n_B, e_B) = (132954765701773295963, 1031)$$

¿Podrías romper ahora sus claves? ¿Cuál de las dos claves escogerías?

9. ¿Serías capaz de romper un criptosistema cuya clave pública contuviera como n al siguiente número (este número se conoce como RSA–129)?

$n =$ 11438 16257 57888 86769 92357 79976 14661
20102 18296 72124 23625 62561 84293 57069
35245 73389 78305 97123 56395 87050 58989
07514 75992 90026 87954 3541

10. Trata de romper, sin la ayuda de un ordenador, la siguiente clave para el criptosistema RSA: $(n, e) = (536813567, 3602561)$. (*Nota*: los primos de la factorización de n son un tanto especiales.)

11. Enviar el mensaje $M =$ «16» a un amigo que trabaja con el criptosistema de ElGamal. Este amigo utiliza los siguientes parámetros: el primo es $p = 23$, el generador del grupo $\mathbb{Z}_{23}^*$ es $\alpha = 5$ y su clave pública es 19.

12. Descifrar el mensaje que recibe el amigo del problema anterior, si su clave privada es $a = 15$.

13. En el criptosistema de ElGamal se considera el número primo $p = 65537$ y el grupo $\mathbb{Z}_p^*$ con generador $\alpha = 5$. Enviar a Bernardo, cuya clave pública es 23467, un mensaje en el que se indique el tipo de moneda a utilizar en determinada transacción, o sea, $M =$ «PTA».

14. Intentar romper el criptosistema anterior, es decir, determinar b de modo que $5^b \equiv 23467 \pmod{65537}$.

15. Utilizando la codificación usual de letras a dígitos y empleando el criptosistema de ElGamal, se recibe el siguiente criptograma:

(827465920043750348729577 17, 24336907597174300732832413 4)

Si se trabaja en un cuerpo de 29726270500913900677161192 7 elementos (observe que es un número primo) y si la clave privada es a = 10384756843984756438549809, descifrar el criptograma.

16. Sea E una curva elíptica definida por la ecuación (sin raíces dobles) $y^2 = x^3 + ax + b$, sobre un cuerpo de característica diferente de 2 y de 3. Se define la suma de dos de sus puntos afines, $P = (x_1, y_1)$ y $Q = (x_2, y_2)$, como $P + Q = (x_3, y_3)$, donde

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

siendo

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & \text{si } P \neq Q \\ (3x_1^2 + a)/(2y_1), & \text{si } P = Q \end{cases}$$

Sea E la curva elíptica dada por la ecuación $y^2 = x^3 + 4x + 4$ sobre el cuerpo finito $\mathbb{F}_{13}$. Se sabe que el grupo cíclico de dicha curva tiene 15 elementos y que el punto $G = (1, 3)$ es un generador de dicho grupo.

a) Determinar una clave pública para el usuario *B*, de modo que su clave privada sea $b = 4$.

b) Utilizando el criptosistema de ElGamal para curvas elípticas, cifrar el mensaje m cuyo punto de la curva asociado es $P_m = (10, 2)$, utilizando la clave pública anterior del destinatario *B*, eligiendo $k = 7$ como clave de sesión.

c) Descifrar el mensaje recibido.

17. Escribir un algoritmo en pseudocódigo (fácilmente transcribible a un lenguaje de ordenador) de modo que resuelva el problema de la mochila con trampa, es decir, que resuelva el siguiente problema:

Dada una sucesión supercreciente de números $W = \{w_1, w_2, \ldots, w_r\}$, y un entero s, determinar, en el supuesto de que exista, un entero k-bit, $n = (e_{k-1}, e_{k-2}, \ldots, e_1, e_0)_{(2}$, con $e_i \in \{0,1\}$, de modo que

$$\sum_{i=0}^{k-1} e_i w_i = s$$

18. Como ejemplo del algoritmo anterior, considerar el conjunto supercreciente $W = \{2, 3, 7, 15, 31\}$ y el valor $s = 24$.

19. Con el criptosistema de la mochila, enviar a Bernardo, cuya clave pública es $V = \{46, 19, 38, 26, 48\}$, el siguiente mensaje:

$$M = \text{«INTERVENIDO»}$$

20. Descifrar el mensaje del problema anterior si se sabe que la clave privada de Bernardo es 54 y que utiliza el módulo 73.

1.6. Firmas digitales

1. Como ejemplo de función hash sencilla se considera la que lleva a cabo los siguientes pasos:

a) Se divide el texto claro M en seis bloques de caracteres, sin tener en cuenta los espacios en blanco: $M_0M_1M_2M_3M_4M_5$.
b) Se codifican las letras A-Z mediante los dígitos 00-25.
c) Se considera el número $p_1 = 17$ como valor incial de un puntero p_1, y los pesos por los que se multiplicará el puntero en cada vuelta de la función son: 3^0, 3^1 y 3^2.
d) El valor del puntero desde el segundo al último bloque se obtiene seleccionando el valor del carácter, del bloque considerado, al que apunta el puntero anterior, multiplicado por su peso y reducido módulo 6.
e) El resumen de cada bloque, r_i, se obtiene multiplicando el puntero p_i por su peso y se representa como un byte.
f) La acción anterior se repite hasta el último bloque.
g) El resumen del mensaje, también de un byte, se obtiene sumando, bit a bit, los resúmenes parciales anteriores.

Justificar que los pesos asignados anteriormente son adecuados y luego determinar el resumen del mensaje «ESTA FUNCION HASH NOS ENTREGA UN RESUMEN DE UN BYTE».

2. Calcular la firma digital para el criptosistema RSA que corresponde al mensaje $M =$ «152167492» del problema 1.5.4.

3. Comprobar que la firma obtenida corresponde a quien dice ser el remitente del mensaje anterior recibido.

4. Determinar la firma RSA de Alicia para el mensaje que envía Bernardo en el problema 1.5.5 (utilizar los resultados obtenidos en los problemas 1.5.6 y 1.5.7).

5. Hacer el papel de Bernardo verificando que la firma que se recibe es la de Alicia para el mensaje anterior.

6. Escribir la firma RSA del mensaje que responde Bernardo a Alicia en el problema 1.5.6.

7. Hacer ahora el papel de Alicia, comprobando que la firma del mensaje es la que corresponde a Bernardo.

8. Determinar la firma del criptosistema de ElGamal para el mensaje M = «16» que se envía en el problema 1.5.11.

9. Comprobar que la firma digital del problema anterior que se recibe corresponde a quien dice ser quien la envía.

10. Calcular la firma digital, mediante el protocolo de firma digital de ElGamal, del mensaje M = «PTA» que se envía a Bernardo en el problema 1.5.13.

11. Hacer que Bernardo verifique la firma recibida en el problema anterior.

1.7. Aplicaciones criptográficas

1. En una aplicación de lanzamiento de una moneda por teléfono, basado en el protocolo de Blum, se consideran los siguientes casos:

a) $p = 3$, $q = 7$, $n = p \cdot q = 21$.

b) $p = 3$, $q = 5$, $n = p \cdot q = 15$.

Decidir cuál de ellos es preferible si los valores que se intercambian quienes participan en el protocolo son: $y = x^2 \pmod{n}$ y $z = y^2 \pmod{n}$. Es decir, Alicia da a conocer a Bernardo un residuo cuadrático z, y Bernardo tiene que decidir sobre la paridad de su raíz cuadrada principal.

2. Alicia y Bernardo viven en diferentes ciudades y se van a ir de vacaciones al mismo lugar. Deciden que el viaje lo pagará uno de ellos cuando se vean en el lugar elegido. Para ello, seleccionan el protocolo de lanzamiento de una moneda por teléfono, basado en la equivalencia de factorizar n y calcular raíces cuadradas. Desarrollar el protocolo, decidiendo quién pagará, si Alicia escoge $n = 253$ y Bernardo selecciona el entero $u = 35$.

3. Alicia, Bernardo y Carmen quieren jugar al póquer mental, es decir, van a jugar una partida de póquer por teléfono. Para ello se ponen de acuerdo y eligen el entero $n = 11 \cdot 13 = 143$ como módulo para el criptosistema RSA. A continuación cada uno de ellos elige su clave pública y su clave privada, siendo éstas las siguientes: $(e_A, d_A) = (7, 103)$, $(e_B, d_B) = (17, 113)$ y $(e_C, d_C) = (23, 47)$. La codificación de las 52 cartas de la baraja se hace asignando un número a cada una de ellas como sigue:

a) 02 = $A\heartsuit$: as de corazones,…, 14 = $K\heartsuit$: rey de corazones.
b) 15 = $A\diamondsuit$: as de diamantes,…, 27 = $K\diamondsuit$: rey de diamantes.
c) 28 = $A\clubsuit$: as de tréboles,…, 40 = $K\clubsuit$: rey de tréboles.
d) 41 = $A\spadesuit$: as de picas,…, 53 = $K\spadesuit$: rey de picas.

Desarrollar el protocolo del juego de modo que las cartas de cada uno de los jugadores sean las siguientes: Alicia, pareja de ases; Bernardo, pareja de reyes, y Carmen, trío de treses:

A : {03, 15, 22, 28, 38} = {2♥, A♦, 8♦, A♣, J♣}.
B : {14, 25, 27, 34, 45} = {K♥, J♦, K♦, 7♣, 5♠}.
C : {04, 17, 32, 41, 43} = {3♥, 3♦, 5♣, A♠, 3♠}.

4. El director de una empresa establece un premio con el fin de que, al menos, tres de sus cinco empleados —que se odian cordialmente—, se pongan de acuerdo por una vez en la vida. Para recibir el premio, los empleados deben ponerse de acuerdo, compartir la información en un esquema (3, 5)-umbral y acertar la cantidad del premio. El director ha elaborado el esquema umbral con los siguientes módulos: $m_1 = 97$, $m_2 = 98$, $m_3 = 99$, $m_4 = 101$ y $m_5 = 103$. Desarrollar el esquema correspondiente si el valor del premio asciende a 500.000 céntimos de euro.

Comprobar que si los empleados E_2, E_3 y E_4 combinan sus sombras, son capaces de conseguir el premio, mientras que si se unen sólo dos de los empleados, por ejemplo, E_2 y E_5, no son capaces de recuperar el secreto.

5. Alicia y Bernardo desean saber quién de los dos es más rico, pero ninguno de ellos quiere dar a conocer el total de su fortuna al otro. Lo que sí saben es que ambos tienen menos de 10 millones de euros. Desarrollar un protocolo que resuelva el problema del millonario si la fortuna de Alicia es de 3 millones, mientras que la de Bernar-

do es de 5 millones. Para este protocolo los dos se ponen de acuerdo en utilizar el criptosistema RSA, siendo el módulo $n = 115$. Las claves de Alicia son: $(e_A, d_A) = (19, 51)$. Además, Bernardo elige el número secreto $x = 76$ y Alicia elige el primo $p = 23$ (luego deberá elegir $p = 67$, dado que la anterior elección no es adecuada).

6. Desarrollar un protocolo de transferencia inconsciente de modo que, al final del mismo, Bernardo conozca la factorización del número $n = 3145421 = 1583 \cdot 1987$, pero de tal manera que Alicia no tenga forma de saberlo. El otro dato necesario para este protocolo es el valor secreto que elige Bernardo, que es $x = 123456$.

2. SOLUCIONES

2.1. Criptología clásica

1. El primer criptograma se obtuvo con el cifrado de Julio César y el segundo con el de César Augusto. Los mensajes originales son:

```
LA SUERTE AYUDA A LOS AUDACES
APRESURATE CON LENTITUD
```

2. El mensaje cifrado es (los * representan espacios en blanco):

```
UAAN***NMAOOG*SUCCIAALZS
```

3. El mensaje original sería:

```
MI ANIMO TIEMBLA AL RECORDAR
```

4. No es verdad, porque aparecen cuatro letras seguidas iguales, que corresponderían a cuatro letras iguales seguidas en el mensaje original.

5. La palabra `DOS` es mejor que `MAMA`, puesto que la segunda funciona como `MA`. `TREN` es peor que `DISCO`, porque tiene una letra menos. `COMPUTADOR` es, obviamente, la mejor de todas. Así pues, el orden de preferencia de las palabras sería el siguiente:

```
COMPUTADOR > DISCO > TREN > DOS > MAMA
```

6. El grupo de letras `ML BRRLMGMNFE QXP` se repite 24 (= $8 \cdot 3$) letras más adelante, y como no hay palabras clave de tres letras y sólo hay una palabra de ocho letras, resulta que la clave utilizada es DIAMANTE. El mensaje descifrado es:

ASISTIRAN EL PRESIDENTE DEL CONGRESO
Y EL PRESIDENTE DEL SENADO

7. La clave es 1492 (= BEJC), por lo que el mensaje original es:

EL DESCUBRIMIENTO REFERIDO ES EL
DE AMERICA POR CRISTOBAL COLON

8. Pasemos a resolver cada una de las cuestiones planteadas en este problema.

a) Teniendo en cuenta que la función de encriptado está definida en $\mathbb{Z}_{26}$, para encriptar la frase propuesta, procedemos a escribir el mensaje original mediante números en $\mathbb{Z}_{26}$. Tendremos entonces que el mensaje a encriptar es:

4 18 19 4 2 17 8 15 19 14 18 8 18 19 4 12 0 13 14 4 18 18 4 6 20 17 14.

Llevando a cabo el encriptado de cada uno de los números anteriores, se tiene:

$3 \cdot 4 + 7 \pmod{26} = 19$, $3 \cdot 18 + 7 \pmod{26} = 9$,
$3 \cdot 19 + 7 \pmod{26} = 12$, $3 \cdot 2 + 7 \pmod{26} = 13$,
$3 \cdot 17 + 7 \pmod{26} = 6$, $3 \cdot 8 + 7 \pmod{26} = 5$,
$3 \cdot 15 + 7 \pmod{26} = 0$, $3 \cdot 14 + 7 \pmod{26} = 23$,
$3 \cdot 12 + 7 \pmod{26} = 17$, $3 \cdot 0 + 7 \pmod{26} = 7$,
$3 \cdot 13 + 7 \pmod{26} = 20$, $3 \cdot 6 + 7 \pmod{26} = 25$,
$3 \cdot 20 + 7 \pmod{26} = 15$.

Por tanto, el mensaje numérico encriptado es:

19 9 12 19 13 6 5 0 12 23 9 5 9 12 19 17 7 20 23 19 9 9 19 25 15 6 23.

Lo que proporciona el siguiente criptograma:

TJMT NGFAMXJFJMTRH UX TJ JTZPGX

b) Para determinar la función de descriptado basta tener en cuenta que si el criptograma de una letra se calcula mediante la expresión $\mathcal{C}(m) = 3m + 7 \pmod{26} = c$. Despejando c en función de m, se tiene la función inversa, que es la de descriptado. De la expresión $3m + 7 \pmod{26} = c$, resulta $m = (c - 7)/3 \pmod{26}$. Ahora bien, como el inverso de 3 módulo 26 es 9, se tiene que

$$m = 9(c - 7) \pmod{26} = 9c - 63 \pmod{26} = 9c + 15 \pmod{26},$$

por lo que $\mathcal{D}(c) = 9c + 15 \pmod{26}$.

c) A la hora de descriptar el criptograma anterior, basta con escribir el texto a descriptar como una colección de números:

19 9 12 19 13 6 5 0 12 23 9 5 9 12 19 17 7 20 23 19 9 9 19 25 15 6 23

y aplicar la función de descriptado a cada uno de los mismos:

$9 \cdot 19 + 15 \pmod{26} = 4$, $9 \cdot 9 + 15 \pmod{26} = 18$,
$9 \cdot 12 + 15 \pmod{26} = 19$, $9 \cdot 13 + 15 \pmod{26} = 2$,
$9 \cdot 6 + 15 \pmod{26} = 17$, $9 \cdot 5 + 15 \pmod{26} = 8$,
$9 \cdot 0 + 15 \pmod{26} = 15$, $9 \cdot 23 + 15 \pmod{26} = 14$,
$9 \cdot 17 + 15 \pmod{26} = 12$, $9 \cdot 7 + 15 \pmod{26} = 0$,
$9 \cdot 20 + 15 \pmod{26} = 13$, $9 \cdot 25 + 15 \pmod{26} = 6$,
$9 \cdot 15 + 15 \pmod{26} = 20$.

A continuación se escriben los números correspondientes:

4 18 19 4 2 17 8 15 19 14 18 8 18 19 4 12 0 13 14 4 18 18 4 6 20 17 14,

y finalmente se recupera el mensaje original:

ESTE CRIPTOSISTEMA NO ES SEGURO

2.2. Métodos matemáticos

1. Para calcular el orden de una permutación π, el procedimiento que se sigue (especialmente cuando dicho orden es elevado) es descomponer π en ciclos con soportes disjuntos; esto es, $\pi = \pi_1 \circ \ldots \circ \pi_k$, donde cada π_i es un ciclo que deja invariantes los puntos que permutan los demás ciclos π_j. El orden de un ciclo es fácil de calcular: es el número de puntos que no quedan invariantes por el ciclo. Por ejemplo, el orden del ciclo

$$\zeta = \begin{pmatrix} 3 & 2 & 5 & 4 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

es 4, porque los elementos que no quedan invariantes son 1, 3, 5, 6. Ello es fácil de comprobar. En efecto,

$$\begin{array}{lllll}
1 \xrightarrow{\zeta} 3 \xrightarrow{\zeta} 5 \xrightarrow{\zeta} 6 \xrightarrow{\zeta} 1 \\
2 \xrightarrow{\zeta} 2 \xrightarrow{\zeta} 2 \xrightarrow{\zeta} 2 \xrightarrow{\zeta} 2 \\
3 \xrightarrow{\zeta} 5 \xrightarrow{\zeta} 6 \xrightarrow{\zeta} 1 \xrightarrow{\zeta} 3 \\
4 \xrightarrow{\zeta} 4 \xrightarrow{\zeta} 4 \xrightarrow{\zeta} 4 \xrightarrow{\zeta} 4 \\
5 \xrightarrow{\zeta} 6 \xrightarrow{\zeta} 1 \xrightarrow{\zeta} 3 \xrightarrow{\zeta} 5 \\
6 \xrightarrow{\zeta} 1 \xrightarrow{\zeta} 3 \xrightarrow{\zeta} 5 \xrightarrow{\zeta} 6
\end{array}$$

y mirando la primera y última columnas se ve que ζ^4 es la identidad. Por otra parte, si los soportes de los ciclos π_i y π_j son disjuntos, los ciclos conmutan; es decir, $\pi_i \circ \pi_j = \pi_j \circ \pi_i$. En este caso, el orden de π es el mínimo común múltiplo de los órdenes de los ciclos factores $\pi_i,\ldots,\pi_k$, con lo cual queda automatizado el cálculo del orden de una permutación. Apliquemos esto a la permutación dada. Se tiene:

$$1 \mapsto 2 \mapsto 5 \mapsto 20 \mapsto 4 \mapsto 9 \mapsto 14 \mapsto 6 \mapsto 12 \mapsto 10 \mapsto 3 \mapsto 8 \mapsto 1$$
$$7 \mapsto 13 \mapsto 11 \mapsto 7$$
$$15 \mapsto 19 \mapsto 7 \mapsto 15$$
$$16 \mapsto 18 \mapsto 16$$

Luego π es el producto de cuatro ciclos disjuntos de órdenes 12, 3, 3, 2, respectivamente. Por tanto, el orden de π es mcm (12, 3, 3, 2) = 12.

2. Dado que $945 = 3^3 \cdot 5 \cdot 7$, el número de divisores es $4 \cdot 2 \cdot 2 = 16$, y éstos son:

1, 3, 5, 7, 9, 15, 21, 27, 35, 45, 63, 105, 135, 189, 315, 945

3. Los restos potenciales de 10 módulo 7 son:

$10^0 \equiv 1 \pmod 7$, $10^1 \equiv 3 \pmod 7$, $10^2 \equiv 2 \pmod 7$,
$10^3 \equiv 6 \pmod 7$, $10^4 \equiv 4 \pmod 7$, $10^5 \equiv 5 \pmod 7$,
$10^6 \equiv 1 \pmod 7$, $10^7 \equiv 3 \pmod 7$, $10^8 \equiv 2 \pmod 7$.

Por tanto, un número de cinco cifras, $M = abcde$, es divisible por 7 si $M = e + d \cdot 10 + c \cdot 10^2 + b \cdot 10^3 + a \cdot 10^4 \equiv 0 \pmod 7$, es decir, si $M = e + d \cdot 3 + c \cdot 2 + b \cdot 6 + a \cdot 4 \equiv 0 \pmod 7$. De forma análoga, un número de siete cifras, $M = abcdefg$, es divisible por 7 si $M = g + f \cdot 3 + e \cdot 2 + d \cdot 6 + c \cdot 4 + b \cdot 5 + a \equiv 0 \pmod 7$.

Según lo anterior, el número $N = 32cd1$ es divisible por 7 si se verifica que $1 + d \cdot 3 + c \cdot 2 + 2 \cdot 6 + 3 \cdot 4 = 25 + 3d + 2c \equiv 0 \pmod 7$. Así pues, los números 32011 y 32501 son divisibles por 7.

Para obtener el criterio de divisibilidad por 7 para un número con cualquier número de cifras basta observar que el resto de $10^6 \pmod 7$ es el mismo que el de $10^0 \pmod 7$, por lo que la serie de los restos potenciales se repite.

4. Tenemos que $100! = 2^{97} \cdot 3^{48} \cdot 5^{24} \cdot 7^{16} \cdot 11^9 \cdot 13^7 \cdot 17^5 \cdot 19^5 \cdot 23^4 \cdot 29^3 \cdot 31^3 \cdot 37^2 \cdot 41^2 \cdot 43^2 \cdot 47^2 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97$.

5. Se tiene que:

a) $\text{mcd}\,(26, 19) = 1 = -8 \cdot 26 + 11 \cdot 19$.

b) $\text{mcd}\,(187, 34) = 17 = 1 \cdot 187 - 5 \cdot 34$.

c) $\text{mcd}\,(841, 160) = 1 = -39 \cdot 841 + 205 \cdot 160$.

d) $\text{mcd}\,(1547, 560) = 7 = 21 \cdot 1547 - 58 \cdot 560$.

e) $\text{mcd}\,(1729, 1001) = 91 = -4 \cdot 1729 + 7 \cdot 1001$.

f) $\text{mcd}\,(2613, 2171) = 13 = -54 \cdot 2613 + 65 \cdot 2171$.

6. Como $\text{mcd}\,(2345, 737) = 67$, se tiene que $\text{mcm}\,(a, b) = 2345 \cdot 737/67 = 25795$.

7. Comparando los dos algoritmos se tiene que:

$$\begin{aligned} 2613 &= 2171 + 442 \\ 2171 &= 4 \cdot 442 + 403 \\ 442 &= 403 + 39 \\ 403 &= 10 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 \end{aligned} \qquad \begin{aligned} 2613 &= 2171 + 442 \\ 2171 &= 5 \cdot 442 - 39 \\ 442 &= 11 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 \end{aligned}$$

8. Se tiene que:

a) $\text{mcd}\,(x^4 + x^2 + 1, x^2 + 1) = 1 = 1(x^4 + x^2 + 1) - x^2(x^2 + 1)$.

b) $\text{mcd}\,(x^4 - 4x^3 + 6x^2 - 4x + 1, x^3 - x^2 + x - 1) = x - 1$, con $x - 1 = (-x/4 + 1/4)(x^4 - 4x^3 + 6x^2 - 4x + 1) + (x^2/4 - x + 5/4)(x^3 - x^2 + x - 1)$.

9. $\text{mcd}\,(x^4 - 2x^3 - x^2 + 2x + 1, 4x^3 - 6x^2 - 2x + 2) = x^2 - x - 1$, por lo que las raíces múltiples del polinomio dado son el número de oro y su conjugado, es decir, $(1 \pm \sqrt{5})/2$.

10. Los conjuntos de números buscados son:

a) $a \equiv 0 \pmod 3 = \{0, 3, 6, 9, 12, \ldots\}$,
$a \equiv 1 \pmod 3 = \{1, 4, 7, 10, 13, \ldots\}$,
$a \equiv 2 \pmod 3 = \{2, 5, 8, 11, 14, \ldots\}$.

b) $a \equiv 0 \pmod 7 = \{0, 7, 14, 21, 28, \ldots\}$,
$a \equiv 3 \pmod 7 = \{3, 10, 17, 24, 31, \ldots\}$,
$a \equiv 4 \pmod 7 = \{4, 11, 18, 25, 32, \ldots\}$.

c) $a \equiv 2 \pmod{23} = \{2, 25, 48, 71, 94, \ldots\}$,
$a \equiv 5 \pmod{23} = \{5, 28, 51, 74, 97, \ldots\}$,
$a \equiv 15 \pmod{23} = \{15, 38, 61, 84, 107, \ldots\}$.

11. La tablas de la suma y del producto módulo 4 son las siguientes:

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

12. Por el problema 2.5.*c*), se tiene que $1 = 205 \cdot 160 - 39 \cdot 841$, por lo que $1 \equiv 205 \cdot 160 \pmod{841}$, es decir, $160^{-1} \equiv 205 \pmod{841}$.

De forma análoga se tiene que $15^{-1} \equiv 17 \pmod{127}$.

13. El orden de 5 módulo 1367 es 1366, es decir, 5 es un generador de $\mathbb{Z}_{1377}$, puesto que 1366 es el menor número tal que $5^{1366} \equiv 1 \pmod{1377}$.

14. Es fácil ver que:

$7^0 \equiv 1 \pmod{100}$, $7^1 \equiv 7 \pmod{100}$, $7^2 \equiv 49 \pmod{100}$,
$7^3 \equiv 43 \pmod{100}$, $7^4 \equiv 1 \pmod{100}$, $7^5 \equiv 7 \pmod{100}$.

Por tanto, como $123 = 4 \cdot 30 + 3$, se tiene que $7^{123} \equiv 7^3 \equiv 43 \pmod{100}$. Luego las unidades de 7^{123} son 3 y las decenas son 4.

15. Descomponiendo en factores cada uno de los números dados se tiene que:

a) $\phi(81) = \phi(3^4) = 3^{4-1}(3-1) = 3^3 \cdot 2 = 54$.
b) $\phi(1960) = \phi(2^3 \cdot 5 \cdot 7^2) = 2^2 \cdot 4 \cdot 7 \cdot 6 = 672$.
c) $\phi(1996) = \phi(2^2 \cdot 499) = 2 \cdot 498 = 996$.
d) $\phi(41503) = \phi(7^3 \cdot 11^2) = 7^2 \cdot 6 \cdot 11 \cdot 10 = 32340$.

16. Consideremos $p = 7$. Como $\phi(7) = 6$ y $1000000 \equiv 4 \pmod{6}$, resulta que $2^{1.000.000} \equiv 2^4 \equiv 16 \equiv 2 \pmod{7}$; así pues, el último dígito en base 7 de $2^{1.000.000}$ es 2.

17. Determinando los inversos correspondientes, se tiene:

a) De $3x \equiv 4 \pmod{7}$ se tiene que $x \equiv 4 \cdot 3^{-1} \equiv 4 \cdot 5 \equiv 20 \equiv 6 \pmod{7}$; por tanto, la solución es $x = 6 + 7n$, con $n \geq 0$.
b) $3x \equiv 4 \pmod{12}$ no tiene solución, pues 3 no tiene inverso módulo 12.

c) Las soluciones son las mismas que las de *a*).
d) $x = 219 + 256n$, $n \geq 0$.
e) $x = 36 + 100n$, $n \geq 0$.
f) $x = 636 + 676n$, $n \geq 0$.

18. Trabajando módulo 5, de la segunda ecuación se tiene que $x = 1 - 3y = 1 + 2y$. Sustituyendo este valor en la primera ecuación es: $3(1 + 2y) + 2y = 2$. De aquí se tiene que $3 + 8y \equiv 2 \pmod 5$, es decir, $3y \equiv 2 - 3 \equiv 2 + 2 \equiv 4 \pmod 5$. Por tanto, $y \equiv 4 \cdot 3^{-1} \equiv 3 \pmod 5$, de donde $x \equiv 2 \pmod 5$.

19. Es claro que 4 verifica la condición pedida, salvo que no tiene tres cifras. Por otra parte, como $\text{mcd}(7, 9, 11) = 1$ y $7 \cdot 9 \cdot 11 = 693$ tiene tres cifras, la solución es $4 + 693 = 697$.

20. Se puede resolver el problema utilizando el Teorema del Resto Chino utilizando las ecuaciones: $x \equiv 1 \pmod{11}$, $x \equiv 2 \pmod{12}$, $x \equiv 3 \pmod{13}$. Sin embargo, se puede observar que -10 verifica lo pedido, y como en el problema anterior, la solución es: $-10 + 11 \cdot 12 \cdot 13 = 1706$.

21. La solución al sistema de ecuaciones $x_i \equiv a_i \pmod{m_i}$, $i = 1, \ldots, n$, viene dada por el Teorema del Resto Chino, mediante la expresión

$$s = \sum_{i=1}^{n} a_i \cdot M_i \cdot N_i$$

siendo

$$M_i = \left(\prod_{j=1}^{m} m_j\right) / m_i \text{, y } N = M_i^{-1} \pmod{m_i}$$

Por tanto, se tiene que:

a) $x = 2 \cdot 880 \cdot 1 + 3 \cdot 528 \cdot 2 + 4 \cdot 240 \cdot 5 + 5 \cdot 165 \cdot 13 = 20453 \equiv 1973 \pmod{2640}$.
b) $x = 63841$.
c) $x = 58837$.

22. Expresando 75 en base 2 se tiene: $38^{75} = 38^{1 + 2 + 2^3 + 2^6} = 38 \cdot 38^2 \cdot 38^{2^3} \cdot 38^{2^6}$. Por otra parte, se tiene que $38 \equiv 38 \pmod{103}$, $38^2 \equiv 2 \pmod{103}$, $2^2 \equiv 4 \pmod{103}$, $4^2 \equiv 16 \pmod{103}$, $16^2 \equiv 50 \pmod{103}$, $50^2 \equiv 28 \pmod{103}$, y $28^2 \equiv 63 \pmod{103}$. De donde, $38^{75} \equiv 38 \cdot 2 \cdot 16 \cdot 63 \equiv 79 \pmod{103}$.

23. Como $\phi(77) = 60$, se tiene que $2^{\phi(77)} = 2^{60} \equiv 1 \pmod{77}$. Por otra parte, $1000000 \equiv 40 \pmod{60}$, por lo que $2^{1.000.000} \equiv 2^{40} \equiv 2^{2^3 + 2^5}$

(mod 77). Como $2 \equiv 2 \pmod{77}$, $2^2 \equiv 4 \pmod{77}$, $4^2 \equiv 2^{2^2} \equiv 16 \pmod{77}$, $16^2 \equiv 2^{2^3} \equiv 25 \pmod{77}$, $25^2 \equiv 2^{2^4} \equiv 9 \pmod{77}$, $9^2 \equiv 2^{2^5} \equiv 4 \pmod{77}$, resulta que $2^{1.000.000} \equiv 2^{40} \equiv 2^{2^3+2^5} \equiv 25 \cdot 4 \equiv 23 \pmod{77}$.

24. Resolvamos con detalle el primer caso. Los demás se hacen de forma análoga.

a) $X^3 + X + 1 = (X - 1)(X^2 + X + 1) + X$, y $X^2 + X + 1 = X(X + 1) + 1$. Por tanto, $\text{mcd}(X^3 + X + 1, X^2 + X + 1) = 1$. De las igualdades anteriores se obtiene que:

$$\begin{aligned}1 &= X(X + 1) + (X^2 + X + 1)\\ &= ((X^3 + X + 1) + (X + 1)(X^2 + X + 1))(X + 1)\\ &\quad + (X^2 + X + 1)\\ &= (X + 1)(X^3 + X + 1) + (X + 1)^2(X^2 + X + 1)\\ &\quad + (X^2 + X + 1)\\ &= (X + 1)(X^3 + X + 1) + X^2(X^2 + X + 1)\\ &\quad + 2(X^2 + X + 1)\\ &= (X + 1)(X^3 + X + 1) + X^2(X^2 + X + 1)\\ &= (X + 1) f(X) + X^2 g(X).\end{aligned}$$

b) $\text{mcd}(f(X), g(X)) = X^3 + X^2 + 1 = f(X) + (X^2 + X) g(X)$.

c) Se tiene:

$$\begin{aligned}&\text{mcd}(f(X), g(X))\\ &= 1 = (X - 1) f(X) - (X^2 - X + 1) g(X).\end{aligned}$$

d) Se tiene:

$$\begin{aligned}&\text{mcd}(f(X), g(X))\\ &= X + 1 = (X - 1) f(X) - (X^3 - X^2 + 1) g(X).\end{aligned}$$

e) Se tiene:

$$\begin{aligned}&\text{mcd}(f(X), g(X))\\ &= X + 78\\ &= (50X + 20) f(X) + (51X^3 + 26X^2 + 27X + 4) g(X).\end{aligned}$$

25. Como las raíces múltiples de $f(X) = X^7 + X^5 + X^4 - X^3 - X^2 - X + 1 \in \mathbb{F}_3[X]$ son las raíces de $\text{mcd}(f(X), f'(X)) = X^2 + 1$, se tiene que éstas son $\pm\alpha$, siendo α un generador de $\mathbb{F}_9^*$.

26. Resolvamos cada uno de los apartados:

a) Como $0 = \alpha^2 + a \cdot \alpha + b$, elevando esta expresión a la potencia p, se tiene que $0 = (\alpha^2 + a \cdot \alpha + b)^p = (\alpha^2)^p + a^p \cdot \alpha^p + b^p = (\alpha^2)^p + a \cdot \alpha^p + b$.

b) El polinomio tiene dos raíces, α y α^p; por tanto, a es el opuesto a la suma de las raíces y b es su producto.

c) $(c\alpha + d)^{p+1} = (c\alpha + d)^p (c\alpha + d) = (c\alpha^p + d)(c\alpha + d) = c^2 \cdot \alpha^{p+1} + c\alpha^p d + c\alpha d + d^2 = c^2 b + cd(\alpha + \alpha^p) + d^2 = d^2 - acd + bc^2$.

d) Se tiene $(2 + 3i)^{101} = (2 + 3i)^{5(19+1)+1} = (2^2 + 3^2)^5 (2 + 3i) = 14(2 + 3i) = 9 + 4i$.

27. Se tiene que $135 \rightarrow (135 \pmod{11}, 135 \pmod{13}) = (3, 5)$. Por otra parte, es fácil ver que $128 \leftarrow (7, 11)$.

28. Procediendo por fuerza bruta, se tiene que:

$2^1 \equiv 2 \pmod{683}$, $2^2 \equiv 4 \pmod{683}$,
$2^3 \equiv 8 \pmod{683}$, $2^4 \equiv 16 \pmod{683}$,
$2^5 \equiv 32 \pmod{683}$, $2^6 \equiv 64 \pmod{683}$,
$2^7 \equiv 128 \pmod{683}$, $2^8 \equiv 256 \pmod{683}$,
$2^9 \equiv 512 \pmod{683}$, $2^{10} \equiv 341 \pmod{683}$,
$2^{11} \equiv 682 \pmod{683}$, $2^{12} \equiv 681 \pmod{683}$,
$2^{13} \equiv 679 \pmod{683}$, $2^{14} \equiv 675 \pmod{683}$,
$2^{15} \equiv 667 \pmod{683}$.

Por tanto, $\log_2 667 = 15 \pmod{683}$.

29. Es claro que n no puede ser primo porque si así fuera, $\phi(n) = n - 1$. Además, por hipótesis, n no es el cuadrado de un primo. Por otra parte, si n no fuera el producto de dos primos distintos, entonces sería el producto de tres o más primos (no necesariamente distintos). Sea p el menor de estos primos. Como $p < n^{1/3}$, se tiene que

$$\phi(n) \leq n\left(1 - \frac{p}{n}\right) \leq n\left(1 - n^{-1/3}\right) = n - n^{2/3}$$

lo que es contradictorio con la hipótesis.

30. Bastará con demostrar que $n^5 - n$ es divisible por 2, 3 y 5. Como

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n - 1)n(n + 1)(n^2 + 1)$$

resulta que $n^5 - n$ es par. Para probar que es múltiplo de 3 y de 5, basta recordar el Teorema (pequeño) de Fermat para este caso: «si n no es divisible por el primo p, entonces $n^{p-1} \equiv 1 \pmod{p}$». Por tanto, como en la factorización de $n^5 - n$ aparece $n^2 - 1$, y como $n^2 \equiv 1 \pmod{3}$, se tiene que $n^5 - n$ es divisible por 3. Por la misma razón, como $n^4 \equiv 1 \pmod{5}$, se tiene que $n^5 - n \equiv 0 \pmod{5}$.

31. Sea $n = p \cdot q$, siendo $p < q$ dos números primos. Aplicando el Teorema del Resto Chino, bastará ver que se verifica

$$a^{e \cdot d} \equiv a \pmod{p}, \qquad a^{e \cdot d} \equiv a \pmod{q}$$

Probaremos la primera congruencia; la segunda se demuestra igual. Por hipótesis, $e \cdot d - 1 = (p - 1)\,k$, para algún entero k. Si a no es divisible por p, entonces se tiene $a^{e \cdot d} = a^{1 + (p-1)k} = a \cdot (a^{p-1})^k$ y, aplicando la congruencia de Fermat, resulta que $a \cdot (a^{p-1})^k = a \cdot 1^k = a$, con lo que se concluye. Si a es divisible por p, entonces $a = p \cdot l$, para algún entero l, y es obvio que cualquier potencia de a es congruente con a módulo p.

2.3. Complejidad computacional

1. Se verifica lo siguiente: $11001001_{(2} = 1 \cdot 2^0 + 1 \cdot 2^3 + 1 \cdot 2^6 + 1 \cdot 2^7 = 201$.

2. Se tiene que: $160 = 316_{(7}$, y $199 = 403_{(7}$; por tanto,

$$\begin{array}{r} 316_{(7} \\ \times\ 403_{(7} \\ \hline 1254_{(7} \\ 16030_{(7} \\ \hline 161554_{(7} \end{array}$$

3. $11001001_{(2} = 100111_{(2} \cdot 101_{(2} + 110_{(2}$.

4. $10^6 = 11110100001001000000_{(2} = 11333311_{(7} = 1783661_{(9}$.

5. $\mathtt{MAL}_{(26} = \mathtt{L} \cdot 26^0 + \mathtt{A} \cdot 26^1 + \mathtt{M} \cdot 26^2 = 11 \cdot 1 + 0 + 12 \cdot 26^2 = 8123$.

$\mathtt{M.AL}_{(26} = \mathtt{M} \cdot 26^0 + \mathtt{A} \cdot 26^{-1} + \mathtt{L} \cdot 26^{-2} = 12 + 0 + 11/676 = 12 + 11/676 = 8123/676$.

6. Se tiene que:

a) $\pi = 3.1415926 \ldots = 11.001001000011111 \ldots_{(2}$.
b) $e = 2.7182818 \ldots = 10.101101111110000 \ldots_{(2}$.

7. $\mathtt{131B6C3}_{(16} = \mathtt{1A2F}_{(16} \cdot \mathtt{BAD}_{(16}$.

8. El algoritmo para convertir un entero *k*-bit, *n*, en base 10 es el siguiente: se divide *n* entre $10 = 1010_{(2}$. El resto, que ha de ser uno de

los siguientes números: 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, será el dígito de las unidades: d_0. A continuación se reemplaza n por el cociente anterior y se repite el proceso señalado anteriormente, obteniéndose el dígito de las decenas: d_1. Este proceso se debe repetir tantas veces como dígitos decimales tenga n, es decir, $[\log n/\log 10] + 1 = O(k)$ veces. Por otra parte, el número de operaciones bits necesarias es el siguiente: se han hecho $O(k)$ divisiones, cada una de las cuales requiere $O(4k) = O(k)$ operaciones (dividir un número con, a lo más, k bits entre $1010_{(2}$, que tiene 4 bits). Por tanto, el número de operaciones es $O(k^2)$. Como $k = O(\log n)$, se puede escribir:

$$\text{Tiempo (convertir } n \text{ en decimal)} = O(\log^2 n)$$

9. El procedimiento del algoritmo de Euclides extendido para expresar $d = \text{mcd}(a, b) = u \cdot a + v \cdot b$, consiste en utilizar la cadena de divisiones del algoritmo de Euclides, comenzando por la última hasta llegar a la primera, de modo que en cada paso se expresa d en función de los restos anteriores. En cada paso son necesarias una multiplicación y una suma o una resta, por lo que el número de operaciones bits es $O(\log^3 a)$. Así pues,

$$\text{Tiempo(calcular } u, v \text{ con mcd}(a, b) = d = u \cdot a + v \cdot b = O(\log^3 a)$$

10. Si se verifica que $\text{mcd}(a, m) = 1$, por el algoritmo de Euclides extendido, existen u, v con $\text{mcd}(a, m) = d = u \cdot a + v \cdot m$, entonces, tomando $b = u$, se tiene que $a \cdot b \equiv 1 \pmod{m}$. Por tanto, se verifica que

$$\text{Tiempo (calcular el inverso de } a \text{ módulo } m) = O(\log^3 m)$$

11. Para calcular en binario el mayor entero menor que $\sqrt{n}$, $m = \lfloor \sqrt{n} \rfloor$, siendo n un entero k + 1-bits, muy grande, se procede como sigue: como primera aproximación a m se toma 1 seguido de $\lfloor k/2 \rfloor$ ceros. A continuación se trata de encontrar los restantes dígitos de m desde la izquierda hacia la derecha, a partir del 1. Esto se hace cambiando el primer 0 de la izquierda por 1. Este cambio se conserva si el cuadrado de esta aproximación es menor que n, en caso contrario, se mantiene el 0 y se repite el proceso con el siguiente 0. Este proceso requiere $O(\log^3 n)$ operaciones, es decir,

$$\text{Tiempo}\left(\text{calcular } m = \lfloor \sqrt{n} \rfloor\right) = O(\log^3 n)$$

12. Para determinar $m = \lfloor \sqrt{116} \rfloor = \lfloor \sqrt{1110100_{(2}} \rfloor$ procedemos del mismo modo que en el problema anterior. Como 116 tiene 7 dígitos, la primera aproximación será $m_1 = 1000_{(2}$. La segunda aproximación consiste en analizar el cuadrado de $m_2^2 = 1100_{(2}$. Como $m_2^2 = (1100_{(2})^2 = 10010000_{(2} > 1110100_{(2}$, este cambio no es adecuado. Sea $m_3 = 1010_{(2}$. Como $m_3^2 = (1010_{(2})^2 = 1100100_{(2} < 1110100_{(2}$, el cambio se mantiene. Sea por último $m_4 = 1011_{(2}$. Como $m_4^2 = (1011_{(2})^2 = 1111001_{(2} > 1110100_{(2}$, el cambio no es adecuado. Por tanto, el valor buscado es $m = 1010_{(2} = 10$. Por otra parte, puede comprobarse fácilmente que

$$11 = \sqrt{121} > \sqrt{116} \geq \lfloor \sqrt{116} \rfloor \geq \sqrt{100} = 10$$

13. Para calcular en binario 3^n hacen falta $n - 1$ multiplicaciones. En cada producto parcial 3^j tiene $O(n)$ bits y 3 tiene 2 bits, por lo que cada producto parcial necesita $O(n)\, O(2) = O(n)$ operaciones. En total son necesarias $O(n^2)$ operaciones, es decir,

$$\text{Tiempo (calcular en binario } 3^n) = O(n^2)$$

14. Para calcular n^n hacen falta $n - 1$ multiplicaciones y cada una de ellas tiene $O(n \cdot \log n)$ dígitos; por tanto, el tiempo requerido en cada producto parcial es $O(\log n)\, O(n \cdot \log n) = O(n \cdot \log^2 n)$. Luego, el tiempo total es $O(n^2 \cdot \log^2 n)$, es decir,

$$\text{Tiempo (calcular } n^n = O(n^2 \cdot \log^2 n)$$

15. Por el Teorema de los números primos, sabemos que el número de primos menores que un número dado n (denotado por $\pi(n)$) es asintótico a $n/\log n$, por lo que el número de primos es $O(n/\log n)$. Una cota para el número de operaciones bits en una de las multiplicaciones es $O(n \cdot \log n)$. Por tanto, el número de operaciones requerido es $O(n/\log n)\, O(n \cdot \log n) = O(n^2)$, esto es,

$$\text{Tiempo (calcular producto de primos menores que } n) = O(n^2)$$

16. Sea $n = p \cdot q$ el producto de dos primos diferentes, y supongamos que se conocen p y q. Si n es par, la solución es inmediata pues se tiene que $p = 2$, $q = n/2$ y $\phi(n) = n/2 - 1$. Si n es impar, $\phi(n) = \phi(p \cdot q) = \phi(p)\, \phi(q) = (p - 1)\,(q - 1) = n + 1 - (p + q)$, lo cual requiere sólo sumas y restas, es decir, el tiempo es $O(\log n)$.

Si se conocen n y $\phi(n)$ y las incógnitas son p y q, resulta que $p \cdot q = n$ y $p + q = n + 1 - \phi(n)$, es decir, p y q son las raíces de la ecuación

de segundo grado $x^2 - (n + 1 - \phi(n))\, x + n = x^2 - 2bx + n = 0$, con lo que bastará con calcular el valor de $b \pm \sqrt{b^2 - n}$. Ahora bien, el mayor tiempo necesario para calcular la expresión anterior lo lleva determinar la raíz cuadrada, pero esto se puede hacer en $O(\log^3 n)$.

17. Utilizando el método de las potencias cuadradas sucesivas, se puede apreciar que para calcular $a^n \pmod m$, siendo n un entero $k + 1$-bits, hay que hacer, en cada paso, una o dos multiplicaciones de números menores que m^2, y que hay que hacer k pasos. Por tanto, cada paso lleva $O(\log^2 m^2) = O(\log^2 m)$ operaciones bits. Así pues, el número de operaciones es $O(\log n)\, O(\log^2 m)$, es decir,

$$\text{Tiempo}(\text{calcular } a^n \pmod m) = O(\log n \cdot \log^2 m)$$

18. Un elemento de $\mathbb{F}_q$ puede verse como un polinomio con coeficientes en $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ módulo el polinomio $F(X)$. Para multiplicar dos elementos de $\mathbb{F}_q$ se multiplican los polinomios —lo que requiere $O(m^2)$ multiplicaciones de enteros módulo p (y algunas sumas de enteros módulo p, que necesitan menos tiempo)— y luego se toma el resto de la división entre $F(X)$. La división de polinomios lleva $O(m)$ divisiones de enteros módulo p y $O(m^2)$ multiplicaciones de enteros módulo p. Por tanto, el número de operaciones necesarias es

$$O(m^2 \cdot \log^2 p + m \cdot \log^3 p) = O((m \cdot \log p)^3) = O(\log^3 q)$$

es decir,

$$\text{Tiempo}(\text{multiplicar dos elementos de } \mathbb{F}_q) = O(\log^3 q)$$

19. Una potencia k-ésima se puede calcular por el método de las potencias cuadradas sucesivas, de forma análoga a la exponenciación modular. Este proceso requiere de $O(\log k)$ multiplicaciones (o cuadrados) de elementos de $\mathbb{F}_q$, y, por tanto, de $O(\log k \cdot \log^3 q)$ operaciones bits, es decir,

$$\text{Tiempo}(\text{elevar a } k \text{ un elemento de } \mathbb{F}_q) = O(\log k \cdot \log^3 q)$$

20. La justificación del algoritmo es como sigue:

a) Inicialización de una variable, c, que contendrá el número de factores 2 que tienen en común n_1 y n_2.

b) Determinación del mayor exponente de 2 que es común a n_1 y a n_2, y almacenamiento de este exponente en c. Por tanto, 2^c es un factor de la salida del algoritmo.

c) n_1 será par, si es que alguno de los factores aún lo es.

d) Si n_1 es impar, se simplifica su valor de modo que pase a ser impar. El factor por el que se divide n_1 para ser impar no importa en la salida, dado que n_2 es impar. Después de este paso, los dos números son impares.

e) Cálculo del discriminante como $\Delta = n_1 - n_2$.

f) El discriminante es un valor positivo.

g) Como Δ es par por ser la diferencia de dos números impares, se simplifica por 2, y al nuevo valor se le llama n_1.

h) Si $n_1 \neq 0$, como n^2 es impar, se vuelve al paso *d*) para repetir el proceso.

i) Si $n_1 = 0$, se tiene que n_2 es el factor común y el algoritmo termina considerando que la salida es el producto de ese factor por la potencia de 2 determinada en el paso *b*).

21. Realicemos paso a paso el algoritmo anterior:

a) $c \leftarrow 0$.

b) $n_1 = 24$ y $n_2 = 36$ son pares, luego $n_1 \leftarrow 24/2 = 12$, $n_2 \leftarrow 36/2 = 18$. Como ambos son pares de nuevo, se repite el proceso, y se tiene que $n_1 \leftarrow 12/2 = 6$, $n_2 \leftarrow 18/2 = 9$.

c) $n_1 \leftarrow 6$ es par, luego $n_1 \leftarrow 6/2 = 3$, que ya es impar.

d) $\Delta = 3 - 9 = -6$.

e) Como $\Delta = -6 < 0$, $n_2 \leftarrow 3$, $\Delta \leftarrow -\Delta = 6$.

f) $n_1 \leftarrow 6/2 = 3$.

g) Como $n_1 = 3 \neq 0$, vamos al paso *d*).

d1.

e1. $\Delta = 3 - 3 = 0$.

f1.

g1. $n_1 \leftarrow 0/2 = 0$.

h1.

i1. Como $n_1 = 0$, $d = 2^2 n_2 = 4 \cdot 3 = 12$.

Por tanto, se tiene que $\text{mcd}\,(24, 36) = 12$.

2.4. Criptografía de clave secreta

1. El mensaje «LADRILLO», en código ASCII, concatenando todas las letras es:

$$M = 01001100010000010100010001010010$$
$$01001001010011000100110001001111$$

Sumando, ahora, bit a bit el mensaje con la cadena cifrante K, se obtiene el mensaje cifrado *C*:

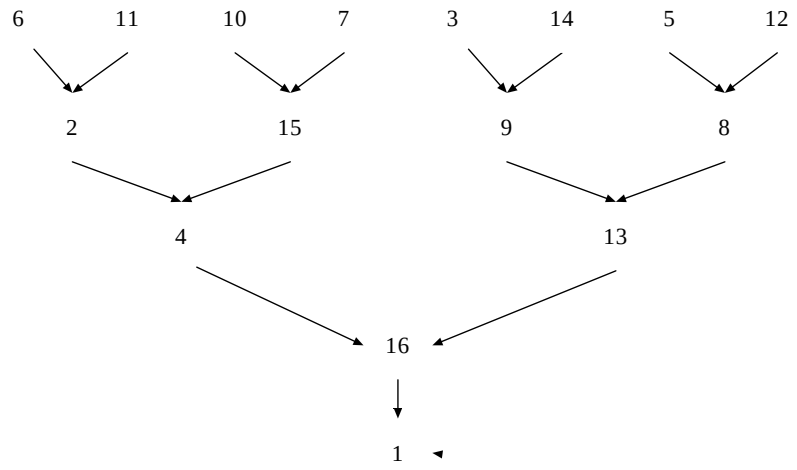
$$M = 01001100010000010100010001010010$$
$$01001001010011000100110001001111,$$
$$K = 01100011000000010111100000101000$$
$$01111110011110011110011001011010,$$
$$C = 00101111010000000011110001111010$$
$$00110111001101011010101000010101$$

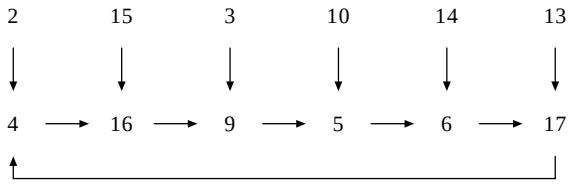
Ahora, escribiendo el criptograma usando el código ASCII, se tiene el mensaje a enviar: «/@< z7;¬§».

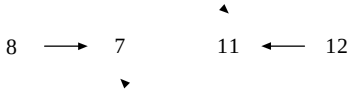
2. Las secuencias cifrantes generadas por $x_{i+1} \equiv (5x_i + 3) \pmod{16}$ son las siguientes:

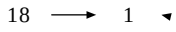
$x_0 = 1 \rightarrow 1, 8, 11, 10, 5, 12, 15, 14, 9, 0, 3, 2, 13, 4, 7, 6, 1, 8, \ldots$
$x_0 = 2 \rightarrow 2, 13, 4, 7, 6, 1, 8, 11, 10, 5, 12, 15, 14, 9, 0, 3, 2, 13, \ldots$
$x_0 = 5 \rightarrow 5, 12, 15, 14, 9, 0, 3, 2, 13, 4, 7, 6, 1, 8, 11, 10, 5, 12, \ldots$

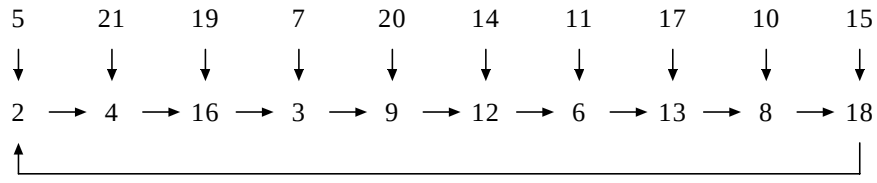
3. Las órbitas obtenidas para el generador $x_i \equiv x_{i-1}^2 \pmod{p}$ con p = 17, 19 y 23, se pueden observar en las siguientes tablas:

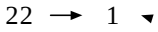












2.5. Criptografía de clave pública

1. Consideramos $\mathbb{Z}_{13}^*$, $\alpha = 4$, $a = 5$ y $b = 2$. Por el protocolo de Diffie-Hellman, se tiene que:

a) *A* elige $a = 5$, calcula $\alpha^a = 4^5 \pmod{13} = 10$, y envía 10 a *B*.
b) *B* elige $b = 5$, calcula $\alpha^b = 4^2 \pmod{13} = 3$, y envía 3 a *A*.
c) *A* recibe 3 y calcula $3^a = 3^5 \pmod{13} = 9$.
d) *B* recibe 10 y calcula $10^b = 10^2 \pmod{13} = 9$.

El número secreto compartido por Alicia y Bernardo es $\alpha^{a \cdot b} = 4^{5 \cdot 2} \pmod{13} = 9$.

2. Para romper el protocolo anterior, dado que los números que se intercambian son muy pequeños, se puede proceder con el ataque por fuerza bruta:

$$\begin{array}{lll} 4^1 \equiv 4 \pmod{13}, & 4^2 \equiv 3 \pmod{13}, & 4^3 \equiv 12 \pmod{13}, \\ 4^4 \equiv 9 \pmod{13}, & 4^5 \equiv 10 \pmod{13}, & 4^6 \equiv 1 \pmod{13}, \\ 4^7 \equiv 4 \pmod{13}, & 4^8 \equiv 3 \pmod{13}, & 4^9 \equiv 12 \pmod{13}, \\ 4^{10} \equiv 9 \pmod{13}, & 4^{11} \equiv 10 \pmod{13}, & 4^{12} \equiv 1 \pmod{13}. \end{array}$$

Como Alicia ha enviado el 10, se sabe que eligió $a = 5$ u 11, mientras que Bernardo eligió $b = 2$ u 8. En este problema no importa el valor concreto elegido por cada uno puesto que

$$\alpha^{a \cdot b} \equiv 4^{5 \cdot 2} \equiv 4^{5 \cdot 8} \equiv 4^{11 \cdot 2} \equiv 4^{11 \cdot 8} \equiv 9 \pmod{13}$$

3. La extensión del protocolo del cambio de clave de Diffie-Hellman para el caso de tres participantes es como sigue:

a) Alicia elige un número aleatorio grande, *a*; calcula $\mathfrak{a} = \alpha^a \pmod{p}$ y se lo envía a Bernardo.
b) Bernardo elige un número aleatorio grande, *b*; calcula $\mathfrak{b} = \alpha^b \pmod{p}$ y se lo envía a Carlos.
c) Carlos elige un número aleatorio grande, *c*; calcula $\mathfrak{c} = \alpha^c \pmod{p}$ y se lo envía a Alicia.
d) Alicia calcula $C = \mathfrak{c}^a \pmod{p}$ y se lo envía a Bernardo.
e) Bernardo calcula $A = \mathfrak{a}^b \pmod{p}$ y se lo envía a Carlos.
f) Carlos calcula $B = \mathfrak{b}^c \pmod{p}$ y se lo envía a Alicia.
g) Alicia calcula $k = B^a \pmod{p}$.
h) Bernardo calcula $k = C^b \pmod{p}$.
i) Carlos calcula $k = A^c \pmod{p}$.

El secreto compartido por Alicia, Bernardo y Carlos es entonces: $k \equiv A^c \equiv (\mathfrak{a}^b)^c \equiv B^a \equiv (\mathfrak{b}^c)^a \equiv C^b \equiv (\mathfrak{c}^a)^b \equiv \alpha^{a \cdot b \cdot c} \pmod{p}$.

4. Dado que $n_B = 143$ tiene tres dígitos y M = «1521674902» tiene diez, se debe dividir el mensaje a cifrar en grupos de dos dígitos, por lo que el mensaje a cifrar será la siguiente cadena de números: $M = M_1, M_2, M_3, M_4, M_5$ = «15, 21, 67, 49, 02». Los criptogramas de cada una de las partes del mensaje son:

$$\begin{aligned} C_1 &= 15^7 \pmod{143} = 115 \\ C_2 &= 21^7 \pmod{143} = 109 \\ C_3 &= 67^7 \pmod{143} = 89 \end{aligned}$$

$$C_1 = 49^7 \pmod{143} = \ \ 36$$
$$C_1 = 02^7 \pmod{143} = 128$$

Por tanto, el criptograma será C = «115, 109, 89, 36, 128».

5. Como se utilizan 28 caracteres, tenemos que determinar la longitud de cada parte del mensaje. Dado que $28^2 = 784 < n_B = 2947 < 21952 = 28^3$, resulta que el mensaje hay que romperlo en grupos de dos caracteres. Luego hay que codificar cada uno de estos grupos para que sea un número menor que n_B. Finalmente se procede a determinar el criptograma de cada grupo, y se obtiene el criptograma resultante:

M = «*MANDA DINERO*»,
M' = «*MANDA_DINERO*»,
$M_1 = MA = M \cdot 28 + A = 12 \cdot 28 + 0 = 336$
$\rightarrow 336^{179} \pmod{2947} = 7 = 0 + 0 + 7$
$= AAH = C_1$,
$M_2 = ND = N \cdot 28 + D = 13 \cdot 28 + 3 = 367$
$\rightarrow 367^{179} \pmod{2947} = 397 = 0 + 14 \cdot 28 + 5$
$= AOF = C_2$,
$M_3 = A\_ = A \cdot 28 + \_ = 0 \cdot 28 + 27 = 27$
$\rightarrow 27^{179} \pmod{2947} = 139 = 0 + 4 \cdot 28 + 27$
$= AE\_ = C_3$,
$M_4 = DI = D \cdot 28 + I = 3 \cdot 28 + 8 = 92$
$\rightarrow 92^{179} \pmod{2947} = 1954 = 2 \cdot 28^2 + 13 \cdot 28 + 22$
$= BNW = C_4$,
$M_5 = NE = N \cdot 28 + E = 13 \cdot 28 + 4 = 368$
$\rightarrow 368^{179} \pmod{2947} = 2438 = 2 \cdot 28^2 + 3 \cdot 28 + 3$
$= CDD = C_5$,
$M_6 = RO = R \cdot 28 + O = 17 \cdot 28 + 14 = 490$
$\rightarrow 490^{179} \pmod{2947} = 56 = 0 + 2 \cdot 28 + 0$
$= ACA = C_6$,
C' = «*AAHAOFAE_BNWCDDACA*»,
C = «*AAHAOFAE BNWCDDACA*».

6. Repitiendo el procedimiento llevado a cabo en el problema anterior, se tiene que la respuesta de Alicia es:

M = «*NO TENGO*»
M' = «*NO_TENGO*»

$M_1 = NO = N \cdot 28 + O = 13 \cdot 28 + 14 = 378$
$\rightarrow 378^{17} \pmod{2773} = 1117 = 1 \cdot 28^2 + 11 \cdot 28 + 25$
$= BLZ = C_1,$
$M_2 = \_T = \_ \cdot 28 + T = 27 \cdot 28 + 19 = 775$
$\rightarrow 775^{17} \pmod{2773} = 124 = 0 + 4 \cdot 28 + 12$
$= AEM = C_2,$
$M_3 = EN = E \cdot 28 + N = 4 \cdot 28 + 13 = 125$
$\rightarrow 125^{17} \pmod{2773} = 164 = 0 + 5 \cdot 28 + 24$
$= AFY = C_3,$
$M_4 = GO = G \cdot 28 + O = 6 \cdot 28 + 14 = 182$
$\rightarrow 182^{17} \pmod{2773} = 2278 = 2 \cdot 28^2 + 25 \cdot 28 + 10$
$= BZK = C_4,$
C = «*BLZAEMAFYBZK*».

7. Para romper las claves de Alicia y Bernardo de los dos criptosistemas anteriores, bastará con factorizar $n = p \cdot q$ para luego determinar $\phi(n) = (p - 1)(q - 1)$ y el inverso de e módulo $\phi(n)$: d, mediante el algoritmo de Euclides extendido.

$n_B = 2947 = 7 \cdot 421$, $\phi(2947) = 6 \cdot 420 = 2520$, $d_B = 1619$.
$n_A = 2773 = 47 \cdot 59$, $\phi(2773) = 46 \cdot 58 = 2668$, $d_A = 157$.

8. Se tiene que:

$$\begin{aligned} n_A &= 342723272091234212791 \\ &= 89 \cdot 3850823281923979919, \\ \phi(n_A) &= 3850823281923979918, \\ d_A &= 52134222893740035813. \\ n_B &= 132954765701773295963 \\ &= 148661281 \cdot 894346966523, \\ \phi(n_B) &= 132954764807277668160, \\ d_B &= 70152659607331766711. \end{aligned}$$

Es preferible la clave de Bernardo, porque sus dos primos están más cercanos entre sí que los de la clave de Alicia, que tiene un número primo muy pequeño.

9. La factorización del número RSA-129 es la siguiente:

n = 11438 16257 57888 86769 92357 79976 14661 20102 18296 72124 23625 62561 84293 57069 35245 73389 78305 97123 56395 87050 58989 07514 75992 90026 87954 3541

= 34905 29510 84765 09491 47849 61990 38981 33417 76463 84933 87843 99082 0577 · 32769 13299 32667 09549 96198 81908 34461 41317 76429 67992 94253 97982 88533.

10. Se verifica que $n = 536813567 = 8191 \cdot 65537$. Los factores de n son especiales, puesto que el primero es un primo de Mersenne: $8191 = 2^{13} - 1$, mientras que el segundo es un primo de Fermat: $65537 = 2^{2^4} + 1$. Por último, se tiene que el inverso de $e = 3602561$ módulo $\phi(n) = 536739840$ es $d = 201244481$.

11. Siguiendo el protocolo de ElGamal con los parámetros $p = 23$, $\alpha = 5$, clave pública $19 = 5^b \pmod{23}$, y $M =$ «16», se tiene que:

a) Se elige un númeo aleatorio, $h = 9$, se calcula $\alpha^h \pmod{p} = 5^9 \pmod{23} = 11$.
b) Se determina $(\alpha^b)^h \pmod{p} = 19^9 \pmod{23} = 10$.
c) Se calcula $M \cdot (\alpha^b)^h \pmod{p} = 16 \cdot 10 \pmod{23} = 22$.
d) Se envía el criptograma correspondiente: $(\alpha^h, M \cdot \alpha^{b \cdot h}) = (11, 22)$.

12. Para recuperar el mensaje anterior se procede como sigue:

a) Se calcula $(\alpha^h)^b \pmod{p} = 11^{15} \pmod{23} = 10$.
b) Se determina el cociente:

$$M \cdot \alpha^{b \cdot h} / \alpha^{h \cdot b} \pmod{p} = 22/10 \pmod{23}$$
$$= 22 \cdot 7 \pmod{23} = 16 = M$$

13. Dado que el mensaje, $M =$ «PTA», tiene tres letras, y como $26^3 = 17576 < p = 65537 < 456976 = 26^4$, no hace falta dividir el mensaje en bloques. Se tiene que $M = PTA = P \cdot 26^2 + T \cdot 26 + A = 15 \cdot 26^2 + 19 \cdot 26 + 0 = 10634$, por lo que:

a) Se elige $h = 21$ y se calcula $5^{21} \pmod{65537} = 37684$.
b) Se calcula $23467^{21} \pmod{65537} = 42782$.
c) Se determina $10634 \cdot 42782 \pmod{65537} = 51471$.
d) Se obtiene el criptograma correspondiente: (37684, 51471).

Escribiendo en letras el par anterior, se tiene que:

$$37684 = 10 + 19 \cdot 26 + 3 \cdot 26^2 \cdot 2 \cdot 26^3 = CDTK$$
$$51471 = 17 + 3 \cdot 26 + 24 \cdot 26^2 + 2 \cdot 26^3 = CYDR$$

Por tanto, la pareja a enviar es «(CDTK, CYDR)».

14. Se tiene que $b = 36151$ dado que $\log_5 23467 \pmod{65537} = 36151$, es decir, $5^{36151} \equiv 23467 \pmod{65537}$.

15. Dado que el mensaje recibido es

$$\begin{aligned}&(\alpha^h, M \cdot \alpha^{h \cdot a})\\ &= (827465920043750348729577 17,\\ &\quad 24336907597174300732832413 4),\end{aligned}$$

se eleva el primer número a $a = 10384756843984756438549809$ y luego se divide el segundo entre el valor obtenido, todo ello módulo el número primo $p = 29726270500913900677161192 7$, es decir,

$$\begin{aligned}&(\alpha^h)^a \pmod p\\ &= 827465920043750348729577 17^{10384756843984756438549809}\\ &\quad \pmod{29726270500913900677161192 7}\\ &= 10277040981937509303538788 8.\end{aligned}$$

$$\frac{M \cdot \alpha^{h \cdot a}}{\alpha^{a \cdot h}} \pmod p$$

$$\begin{aligned}&= \frac{24336907597174300732832413 4}{10277040981937509303538788 8}\\ &\quad \pmod{29726270500913900677161192 7}\\ &= 7466224520185525333630.\end{aligned}$$

Ahora, expresando en base 26 el mensaje recibido, se obtiene el texto original:

$$\begin{aligned}&7466224520185525333630\\ &= 14 + 18 \cdot 26 + 11 \cdot 26^2 + 0 \cdot 26^3 + 5 \cdot 26^4 + 18 \cdot 26^5\\ &\quad + 4 \cdot 26^6 + 0 \cdot 26^7 + 12 \cdot 26^8 + 4 \cdot 26^9 + 17 \cdot 26^{10}\\ &\quad + 14 \cdot 26^{11} + 4 \cdot 26^{12} + 19 \cdot 26^{13} + 11 \cdot 26^{14} + 4 \cdot 26^{15}\\ &= \text{ELTEOREMAESFALSO}.\end{aligned}$$

es decir, «EL TEOREMA ES FALSO».

16. Vamos a resolver cada uno de los apartados del problema planteado:

a) Para calcular la clave pública del usuario *B* se puede utilizar el generador de la curva que proporciona el enunciado del problema, de modo que dicha clave estará formada por la propia curva $E : y^2 = x^3 + 4x + 4$, el generador $G = (1, 3)$ y el múltiplo del generador dado por su clave privada $C_B = 4G$.

Así pues, la clave pública es: (E, G, C_B). Determinemos de modo efectivo el valor de C_B. Calculemos en primer lugar $2G = G + G$. Aplicando la fórmula para doblar puntos en una curva elíptica, se tiene:

$$\lambda = (3 \cdot 1^2 + 4) / (2 \cdot 3) = 7 \cdot 6^{-1} = 7 \cdot 11 \pmod{13} = 12,$$
$$x_3 = 12^2 - 1 - 1 \pmod{13} = 12,$$
$$y_3 = 12\,(1 - 12) - 3 \pmod{13} = 8,$$

de donde $2G = G + G = (12, 8)$. Repitiendo el proceso con $4G = 2G$, se tiene:

$$\lambda = (3 \cdot 12^2 + 4) / (2 \cdot 8) = 109 \cdot 4^{-1} = 5 \cdot 10 \pmod{13} = 11,$$
$$x_3 = 12^2 - 12 - 12 \pmod{13} = 6,$$
$$y_3 = 11\,(12 - 6) - 8 \pmod{13} = 6,$$

por lo que $C_B = 4G = (6, 6)$. Así pues, la clave pública del usuario B es:

$$(y^2 = x^3 + 4x + 4, (1, 3), (6, 6)$$

b) Para cifrar el mensaje cuyo punto de la curva es $P_m = (10, 2)$, mediante el criptosistema de ElGamal, hay que elegir la clave de sesión, es decir, un entero aleatorio, que en este caso es $k = 7$. A continuación se determina el par dado por $(k \cdot G, P_m + k \cdot C_B)$. Así pues, hay que calcular $k \cdot G = 7\,(1, 3)$, y luego hallar el valor de $P_m + k \cdot C_B = (10, 2) + 7\,(6, 6)$. Procediendo de forma análoga a como se ha hecho antes, se calcula el valor de $7\,(1, 3)$. Para ello podemos utilizar los resultados del apartado anterior, teniendo en cuenta que

$$7\,(1, 3) = 4\,(1, 3) + 2\,(1, 3) + (1, 3) = (6, 6) + (12, 8) + (1, 3)$$

Ahora bien, $(6, 6) + (12, 8) = (11, 1)$, dado que

$$\lambda = (8 - 6) / (12 - 6) = 1 \cdot 3^{-1} = 1 \cdot 9 \pmod{13} = 9,$$
$$x_3 = 9^2 - 6 - 12 \pmod{13} = 11,$$
$$y_3 = 9\,(6 - 11) - 6 \pmod{13} = 1.$$

Además, como

$$\lambda = (3 - 1) / (1 - 11) = -1 \cdot 5^{-1} = -1 \cdot 8 \pmod{13} = 5,$$
$$x_3 = 5^2 - 11 - 1 \pmod{13} = 0,$$
$$y_3 = 5\,(11 - 0) - 1 \pmod{13} = 2,$$

se tiene que $7\,(1, 3) = (0, 2)$. De forma análoga se determina que $(10, 2) + 7\,(6, 6) = (3, 2)$. Por tanto, el criptograma correspondiente al mensaje $P_m = (10, 2)$ es el par $((0, 2), (3, 2))$.

c) Para recuperar el mensaje original, *B*, que recibe el par ((0, 2) (3, 2)), tiene que utilizar su clave privada y multiplicarla por el primer punto de los dos recibidos, es decir, debe calcular el valor de $b \cdot (k \cdot G)$, esto es, debe hallar $4\,(0, 2)$. Procediendo como antes, se obtiene que $4\,(0, 2) = 4\,(12, 5)$. Ahora, *B* debe restar este valor del segundo de los puntos recibidos en el criptograma:

$$P_m + k \cdot C_B - b \cdot (k \cdot G) = (3, 2) - (12, 5)$$

Para ello se debe tener en cuenta que restar el punto (12, 5) es lo mismo que sumar su opuesto, es decir, su simétrico respecto de la curva. Dicho punto tiene la misma coordenada *x*, y su coordenada *y* es la opuesta, de modo que

$$P_m = (3, 2) - (12, 5) = (3, 2) + (12, -5) = (3, 2) + (12, 8) = (10, 2).$$

17. El problema es difícil para una mochila cualquiera (es un problema **NP**-completo), no lo es para una mochila tramposa. En este último caso, el problema se resuelve eligiendo el mayor número w_i que sea menor o igual al número buscado *s*. Si $w_i \leq s$, el subíndice *i* se almacena en un conjunto de índices $I = \{i\}$, es decir, se toma $e_i = 1$. A continuación se reemplaza *s* por $s - w_i$ y se repite el proceso hasta encontrar un elemento de la lista que sea igual a esta diferencia. De esta forma o se obtiene una colección de w_i cuya suma es *s* o se llega a un entero positivo $s - \sum_{i \in I} w_i$ que es menor que los restantes w_i, con lo que el problema no tiene solución. El pseudocódigo podría ser el siguiente:

a) Se hace $t = s$ y $j = k$.
b) Se hace $e_{j-1} = 0$, $e_{j-2} = 0$, …, hasta que se obtenga el primer subíndice *i*, que se llamará i_0, tal que $w_{i_0} \leq t$. En este momento se hace $e_{i_0} = 1$.
c) Se reemplaza *t* por $t - w_{i_0}$, se hace $j = i_0$, y si $t > 0$, se vuelve al paso *b*).
d) Si $t = 0$ se acaba y la solución es $n = (e_{k-1}, ..., e_0)_{(2}$.
e) Si $t > 0$ y los restantes w_i son mayores que *t*, entonces no hay solución $n = (e_{k-1}, ..., e_0)_{(2}$.

18. Aplicando el algoritmo anterior al caso $W = \{2, 3, 7, 15, 31\}$, con $s = 24$, se tiene que:

a) $t = 24,\ j = 4$.
b) Como $w_5 = 31 > 24 = t$, es $e_4 = 0$.
c) Como $w_4 = 15 < 24$, se hace $e_3 = 1$ y se considera $t = 24 - 15 = 9$.
b1. Como $w_3 = 7 < 9$, se hace $e_2 = 1$ y se considera $t = 9 - 7 = 2$.
b2. Como $w_2 = 3 > 2$, se hace $e_1 = 0$.
c1. Como $w_1 = 2 = 2$, se hace $e_0 = 1$.
d1. Como $t = 0$, el proceso termina, y la solución es $n = 01101_{(2}$.

19. Bastará con codificar cada una de las letras del mensaje $M =$ «INTERVENIDO» con la codificación habitual, luego pasar cada número a base 2 y utilizar la mochila de Bernardo.

$$\begin{aligned}
I &= 08 = 01000_{(2} \rightarrow 26\\
N &= 13 = 01101_{(2} \rightarrow 46 + 38 + 26 = 110\\
T &= 19 = 10011_{(2} \rightarrow 46 + 19 + 48 = 113\\
E &= 04 = 00100_{(2} \rightarrow 38\\
R &= 17 = 10001_{(2} \rightarrow 46 + 48 = 94\\
V &= 21 = 10101_{(2} \rightarrow 46 + 38 + 48 = 132\\
E &= 04 = 00100_{(2} \rightarrow 38\\
N &= 13 = 01101_{(2} \rightarrow 46 + 38 + 26 = 110\\
I &= 08 = 00100_{(2} \rightarrow 26\\
D &= 03 = 00011_{(2} \rightarrow 46 + 19 = 65\\
O &= 14 = 01110_{(2} \rightarrow 19 + 38 + 26 = 83
\end{aligned}$$

Por tanto, el criptograma a enviar es el siguiente:

{26, 110, 113, 38, 94, 132, 38, 110, 26, 65, 83}

20. Como la clave privada de Bernardo es 54 y el módulo utilizado es 73, la mochila de Bernardo es:

$$54 \cdot \{46, 19, 38, 26, 48\} \pmod{73} = \{2, 4, 8, 17, 37\}$$

y el criptograma recibido se convierte en:

$$54 \cdot \{26, 110, 113, 38, 94, 132, 38, 110, 26, 65, 83\} \pmod{73} = \{17, 27, 43, 8, 39, 47, 8, 27, 17, 6, 29\}$$

y entonces:

$$\begin{aligned}
17 &= 00100_{(2} \rightarrow I\\
27 &= 17 + 8 + 2 = 01101_{(2} \rightarrow N\\
43 &= 37 + 4 + 2 = 10011_{(2} \rightarrow T\\
8 &= 00100_{(2} \rightarrow E\\
39 &= 37 + 2 = 10001_{(2} \rightarrow R
\end{aligned}$$

$$47 = 37 + 8 + 2 = 10101_{(2} \rightarrow V$$
$$8 = 00100_{(2} \rightarrow E$$
$$27 = 17 + 8 + 28 = 01101_{(2} \rightarrow N$$
$$17 = 00100_{(2} \rightarrow I$$
$$6 = 4 + 2 = 00011_{(2} \rightarrow D$$
$$29 = 17 + 8 + 4 = 01110_{(2} \rightarrow O$$

el mensaje original era «INTERVENIDO».

2.6. Firmas digitales

1. Los pesos asignados son adecuados, porque el mayor valor que puede tomar un resumen parcial es el que corresponde a la letra Z, cuyo valor sería: $25 \cdot 3^2 = 225$, que es un valor menor que el mayor entero que ser puede representar por un byte, que es $11111111_{(2} = 255$.

El proceso para obtener el resumen del mensaje «ESTA FUNCION HASH NOS ENTREGA UN RESUMEN DE UN BYTE», según el procedimiento señalado, consiste en considerar como mensaje al siguiente grupo de bloques: *M* = «ESTAFU NCIONH ASHNOS ENTREG AUNRES UMENDE UNBYTE» y luego hacer lo siguiente:

a) $17 \cdot 3^0 \pmod 6 = 5$, $f_{5\{NCIONH\}} = H = 07$, $r_1 = 017 = 0001\ 0001$.
b) $07 \cdot 3^1 \pmod 6 = 3$, $f_{3\{ASHNOS\}} = N = 13$, $r_2 = 021 = 0001\ 0101$.
c) $13 \cdot 3^0 \pmod 6 = 3$, $f_{3\{NCIONH\}} = R = 17$, $r_3 = 117 = 0111\ 0101$.
d) $17 \cdot 3^0 \pmod 6 = 5$, $f_{5\{NCIONH\}} = S = 18$, $r_4 = 017 = 0001\ 0001$.
e) $18 \cdot 3^0 \pmod 6 = 0$, $f_{0\{NCIONH\}} = U = 20$, $r_5 = 054 = 0011\ 0110$.
f) $20 \cdot 3^0 \pmod 6 = 0$, $f_{0\{NCIONH\}} = U = 20$, $r_6 = 180 = 1011\ 0100$.
g) $20 \cdot 3^0 \pmod 6 = 2$, $r_7 = 020 = 0001\ 0100$.

Aplicando a los resúmenes parciales la operación XOR, se tiene:

$$r_1 \oplus r_2 \oplus r_3 \oplus r_4 \oplus r_5 \oplus r_6 \oplus r_7 = r = 1111\ \ 0101$$

2. Para calcular la firma digital que corresponde al mensaje *M* = «152167492» se divide el mensaje en grupos de dos y se firma cada uno de ellos, tal y como se hizo para determinar su criptograma:

$R_1 = 15^{115} \pmod{161} = 099$, $S_1 = 099^7 \pmod{143} = 044$
$R_2 = 21^{115} \pmod{161} = 014$, $S_2 = 014^7 \pmod{143} = 053$
$R_3 = 67^{115} \pmod{161} = 060$, $S_3 = 060^7 \pmod{143} = 135$
$R_4 = 49^{115} \pmod{161} = 105$, $S_4 = 105^7 \pmod{143} = 118$
$R_5 = 02^{115} \pmod{161} = 009$, $S_5 = 009^7 \pmod{143} = 048$

Por tanto, la firma digital es S = (044, 053, 135, 118, 048).

3. Para comprobar que la firma corresponde a quien dice ser el remitente, se eleva cada una de las partes de la firma a la clave privada del destinatario módulo su clave pública. Luego se repite este proceso con el exponente público del remitente, módulo su clave pública, obteniéndose el mensaje original.

$$F_1 = 044^{103} \pmod{143} = 099, \quad M_1 = 099^{31} \pmod{161} = 15$$
$$F_2 = 053^{103} \pmod{143} = 014, \quad M_2 = 014^{31} \pmod{161} = 21$$
$$F_3 = 135^{103} \pmod{143} = 060, \quad M_3 = 060^{31} \pmod{161} = 67$$
$$F_4 = 118^{103} \pmod{143} = 105, \quad M_4 = 105^{31} \pmod{161} = 49$$
$$F_5 = 048^{103} \pmod{143} = 009, \quad M_5 = 009^{31} \pmod{161} = 02$$

4. Para determinar la firma RSA de Alicia para el mensaje M = «MANDA DINERO» = «336, 367, 27, 92, 368, 490», que envía a Bernardo, se utilizan los resultados obtenidos en los problemas 5.6 y 5.7: $n_B = 2947 = 7 \cdot 421$, $\phi(2947) = 2520$, $d_B = 1619$; $n_A = 2773 = 47 \cdot 59$, $\phi(2773) = 2668$, $d_A = 157$, y se lleva al cabo el protocolo correspondiente:

$$R_1 = 336^{157} \pmod{2773} = 0012$$
$$S_1 = 0012^{179} \pmod{2947} = 1228$$
$$R_2 = 367^{157} \pmod{2773} = 0052$$
$$S_2 = 0052^{179} \pmod{2947} = 0705$$
$$R_3 = 027^{157} \pmod{2773} = 0004$$
$$S_3 = 0004^{179} \pmod{2947} = 0324$$
$$R_4 = 092^{157} \pmod{2773} = 1695$$
$$S_4 = 1695^{179} \pmod{2947} = 1721$$
$$R_5 = 368^{157} \pmod{2773} = 2135$$
$$S_5 = 2135^{179} \pmod{2947} = 2436$$
$$R_6 = 490^{157} \pmod{2773} = 1876$$
$$S_6 = 1876^{179} \pmod{2947} = 0749$$

Es decir, S = (1228, 705, 324, 1721, 2436, 749), que escrito como texto equivale a: «BPYAZFA QCFNDDAA.V».

5. Para verificar la firma de Alicia para el mensaje precedente, teniendo en cuenta los datos del problema anterior, se procede como sigue:

$$F_1 = 1228^{1619} \pmod{2947} = 0012$$
$$M_1 = 0012^{17} \pmod{2773} = 336$$

$$F_2 = 0705^{1619} \pmod{2947} = 0052$$
$$M_2 = 0052^{17} \pmod{2773} = 367$$
$$F_3 = 0324^{1619} \pmod{2947} = 0004$$
$$M_3 = 0004^{17} \pmod{2773} = 027$$
$$F_4 = 1721^{1619} \pmod{2947} = 1695$$
$$M_4 = 1695^{17} \pmod{2773} = 092$$
$$F_5 = 2436^{1619} \pmod{2947} = 2135$$
$$M_5 = 2135^{17} \pmod{2773} = 368$$
$$F_6 = 0749^{1619} \pmod{2947} = 1876$$
$$M_6 = 1876^{17} \pmod{2773} = 490$$

Como el resultado obtenido coincide con el mensaje recibido, la firma se da por buena.

6. La firma de Bernardo a M = «NO TENGO» = «378, 775, 125, 182» es la siguiente:

$$R_1 = 378^{1619} \pmod{2947} = 0882$$
$$S_1 = 0882^{17} \pmod{2773} = 2223$$
$$R_2 = 775^{1619} \pmod{2947} = 2061$$
$$S_2 = 2061^{17} \pmod{2773} = 2156$$
$$R_3 = 125^{1619} \pmod{2947} = 2533$$
$$S_3 = 2533^{17} \pmod{2773} = 0150$$
$$R_4 = 182^{1619} \pmod{2947} = 2240$$
$$S_4 = 2240^{17} \pmod{2773} = 2091$$

Es decir, S = (2223, 2156, 150, 2091) = «CXLCVAAFKCST».

7. Para comprobar la firma de Bernardo, se procede como sigue:

$$F_1 = 2223^{157} \pmod{2773} = 0882$$
$$M_1 = 0882^{179} \pmod{2947} = 378$$
$$F_2 = 2156^{157} \pmod{2773} = 2061$$
$$M_2 = 2061^{179} \pmod{2947} = 775$$
$$F_3 = 0150^{157} \pmod{2773} = 2533$$
$$M_3 = 2533^{179} \pmod{2947} = 125$$
$$F_4 = 2091^{157} \pmod{2773} = 2240$$
$$M_4 = 2240^{179} \pmod{2947} = 182$$

8. Para firmar digitalmente mediante el criptosistema de ElGamal el mensaje M = «16», con los parámetros $p = 23$, $\alpha = 5$, $5^b \pmod{23} = 19$, se debe conocer la clave privada del remitente, en este caso dicha clave es $b = 15$ y luego proceder como se indica:

a) Se elige un número aleatorio h, tal que $\text{mcd}(h, \phi(p)) = 1$, por ejemplo, $h = 5$, dado que $\text{mcd}(5, 22) = 1$.

b) Se calcula $\alpha^h \pmod p = 5^5 \pmod{23} = 20 = r$.

c) Se resuelve la ecuación en congruencia siguiente: $M \equiv (b \cdot r + h \cdot s) \pmod{\phi(p)}$, es decir,

$$16 \equiv (15 \cdot 20 + 5 \cdot s) \pmod{22}$$
$$s \equiv (16 - 15 \cdot 20)/5 \pmod{22} = 18$$

Por lo que la firma digital es la pareja $(r, s) = (20, 18)$.

9. Para verificar la firma digital del problema anterior, se calcula:

a)

$$r^s \pmod p = 20^{18} \pmod{23} = 2$$
$$(\alpha^b)^r \pmod p = 19^{20} \pmod{23} = 13$$

b) $r^s \cdot (\alpha^b)^r \pmod p = 2 \cdot 13 \pmod{23} = 3$, y se comprueba que el valor anterior coincide con el valor de $\alpha^M \pmod p = 5^{16} \pmod{23} = 3$.

10. Para firmar digitalmente el mensaje M = «PTA» = «10634», utilizando como clave privada $a = 17321$, se procede como sigue:

a) Se elige un número aleatorio $h = 165$, primo con $\phi(p) = 65536$.

b) Se calcula $\alpha^h \pmod p = 5^{165} \pmod{65537} = 52273$.

c) Se resuelve la ecuación

$$10634 \equiv (17321 \cdot 52273 + 165 \cdot s) \pmod{65537}$$

cuyo resultado es $s = 33181$.

Por tanto, la firma digital para el mensaje es

$$(r, s) = (52273, 33181)$$

Como $r = 52273 = 13 + 8 \cdot 26 + 2 \cdot 26^2 =$ *CZIN*, y como $s = 33181 = 5 + 2 \cdot 26 + 23 \cdot 26^2 + 1 \cdot 26^3 =$ *BEFD*, resulta que la firma que se envía junto con el mensaje es el par (CZIN, BEFD).

11. Para que Bernardo verifique la firma del problema anterior, basta con tener en cuenta que (CZIN, BEFD) = (52273, 33181) = (r, s). Entonces, Bernardo calcula:

a) $r^s \pmod p = 52273^{33181} \pmod{65537} = 46365$.

b) $(\alpha^a)^r \pmod p = (5^{17321})^{52273} \pmod{65537} = 55108$.

c) Multiplica $46365 \cdot 55108 \pmod{65537} = 59938$, y comprueba que este resultado es el mismo que

$$\alpha^M \pmod p = 5^{10634} \pmod{65537} = 56938$$

2.7. Aplicaciones criptográficas

1. Analicemos cada uno de los casos:

a) $p = 3$, $q = 7$, $n = p \cdot q = 21$. En este caso, n es un entero de Blum, puesto que $3, 7 \equiv 3 \pmod 4$. En esta situación se tienen los siguientes restos cuadráticos módulo $n = 21$:

$x^2 \pmod{21}$	y	z	$x^2 \pmod{21}$	y	z
$1^2 \pmod{21}$	1	1	$11^2 \pmod{21}$	16	4
$2^2 \pmod{21}$	4	16	$12^2 \pmod{21}$	18	9
$3^2 \pmod{21}$	9	18	$13^2 \pmod{21}$	1	1
$4^2 \pmod{21}$	16	4	$14^2 \pmod{21}$	7	7
$5^2 \pmod{21}$	4	16	$15^2 \pmod{21}$	15	15
$6^2 \pmod{21}$	15	15	$16^2 \pmod{21}$	4	16
$7^2 \pmod{21}$	7	7	$17^2 \pmod{21}$	16	4
$8^2 \pmod{21}$	1	1	$18^2 \pmod{21}$	9	19
$9^2 \pmod{21}$	18	9	$19^2 \pmod{21}$	4	16
$10^2 \pmod{21}$	16	4	$20^2 \pmod{21}$	1	1

Estos restos tienen siempre la misma paridad, es decir, tanto en $y = x^2 \pmod{21}$, como en $z = y^2 \pmod{21}$, hay la misma cantidad de números pares que de impares. Los restos cuadráticos son: $R_z(x) = \{1, 4, 7, 9, 15, 16, 18\}$, y resultan aceptables para el problema planteado, dado que la probabilidad de elegir un resto par es la misma que la de elegir un resto impar, es decir, 1/2.

b) $p = 3$, $q = 5$, $n = p \cdot q = 15$. En este caso, n no es un entero de Blum y los restos cuadráticos son los siguientes:

$x^2 \pmod{15}$	y	z	$x^2 \pmod{15}$	y	z
$1^2 \pmod{15}$	1	1	$8^2 \pmod{15}$	4	1
$2^2 \pmod{15}$	4	1	$9^2 \pmod{15}$	6	6
$3^2 \pmod{15}$	9	6	$10^2 \pmod{15}$	10	10
$4^2 \pmod{15}$	1	1	$11^2 \pmod{15}$	1	1
$5^2 \pmod{15}$	10	10	$12^2 \pmod{15}$	9	6
$6^2 \pmod{15}$	6	6	$13^2 \pmod{15}$	4	1
$7^2 \pmod{15}$	4	1	$14^2 \pmod{15}$	1	1

Los restos cuadráticos en este caso son $R = \{1, 6, 10\}$, cuya paridad, como se observa en la tabla anterior, no es la misma.

2. Como Alicia elige el entero $n = 253 = 11 \cdot 23$, y $11, 23 \equiv 3 \pmod 4$, se tiene que n es un entero de Blum. Entonces el protocolo es el siguiente:

a) Alicia elige el entero de Blum $n = 253$, y comunica su valor a Bernardo.

b) Bernardo selecciona un entero $u \in (1, n/2) = (1, 126)$, por ejemplo, $u = 35$. A continuación calcula $z = u^2 \pmod n = 35^2 \pmod{253} = 213$, y comunica este valor a Alicia.

c) Alicia, dado que conoce la factorización de $n = 11 \cdot 23$, determina las cuatro raíces cuadradas de $z = 213$: $\pm x = \pm 35$, $\pm y = \pm 57$, es decir, 35, 218, 57 y 196. Entonces selecciona los dos valores menores, uno de los cuales es u, y determina su expresión en binario: $35 = 100011_{(2}$, y $57 = 111001_{(2}$.

d) Alicia envía a Bernardo su hipótesis sobre cuál de los dos valores que ha elegido es el número u, pero sin revelar totalmente el número, para evitar que Bernardo calcule otra raíz cuadrada de $n = 253$ y factorizarlo. Si se desea que Alicia pague las vacaciones, se supondrá que $u = 57$. Luego comunica a Bernardo: «el segundo bit del número que has pensado es 0» (si se desea que las vacaciones las pague Bernardo, la hipótesis de Alicia será $u = 35$; la respuesta de Alicia será: «el segundo bit del número que has pensado es 1»).

e) Bernardo desvela a Alicia el número que pensó, $u = 35$, probando que $35^2 \pmod{253} = 213$, cuyo segundo bit es 1, con lo que Alicia pierde y paga (en el otro caso, Alicia acierta el número, y quien paga es Bernardo).

3. Para desarollar el protocolo completo, el primer paso consiste en codificar las cartas, cosa que ya se ha hecho. El resto del protocolo es como sigue:

a) Alicia codifica las cartas con su clave pública; es decir, calcula $c_i^{e_A} \pmod n = c_i^7 \pmod{143}$, obteniendo los siguientes valores (que supondremos barajados, aunque en realidad no lo estén):

{128, 42, 82, 47, 85, 6, 57, 48, 10, 132, 12, 117, 53, 115,
3, 30, 138, 46, 136, 109, 22, 23, 106, 64, 104, 14, 63, 94,

134, 125, 98, 110, 122, 139, 75, 93, 25, 52, 105, 24, 81,
43, 99, 111, 84, 31, 126, 36, 41, 116, 13, 92},
que envía a Bernardo para que elija sus cinco cartas.

b) Bernardo selecciona al azar cinco de los números anteriores: {53, 64, 14, 122, 111}, los cuales cifra con su clave pública, $e_B = 17$, obteniendo:

$\{53, 64, 14, 122, 111\}^{17} \pmod{143} = \{92, 103, 53, 122, 89\}$,

y se los devuelve a Alicia. En este momento, ni Alicia ni Bernardo conocen los valores de las cartas elegidas por Bernardo.

c) Alicia descifra los números recibidos de Bernardo con su clave privada, $d_A = 103$, y envía el resultado a éste:

$\{92, 103, 53, 122, 89\}^{103} \pmod{143} = \{53, 64, 14, 34, 67\}$.

d) Bernardo descifra con su clave privada $d_B = 113$ los valores anteriores y conoce su pareja de ases:

$\{53, 64, 14, 34, 67\}^{113} \pmod{143}$
$= \{14, 25, 27, 34, 45\} = \{K\heartsuit, J\diamondsuit, K\diamondsuit, 7\clubsuit, 5\spadesuit\}$

e) Bernardo envía a Carmen los números de las cartas que no ha elegido; es decir, envía la cadena:

{128, 42, 82, 47, 85, 6, 57, 48, 10, 132, 12, 117, ✠, 115,
3, 30, 138, 46, 136, 109, 22, 23, 106, ✠, 104, ✠, 63, 94,
134, 125, 98, 110, ✠, 139, 75, 93, 25, 52, 105, 24, 81,
43, 99, ✠, 84, 31, 126, 36, 41, 116, 13, 92}.

f) Carmen repite el mismo proceso que Bernardo para elegir sus cartas; es decir, de los números recibidos elige cinco al azar y se los manda cifrados, con su clave pública, $e_C = 23$, a Alicia, quien se los descifra con su clave privada, $d_A = 103$, y se los remite de nuevo a Carmen. Ahora Carmen los descifra con su clave privada, $d_C = 47$, y obtiene los valores de sus cartas. Supongamos que Carmen elige los siguientes números: {82, 30, 98, 24, 43}. Entonces, el proceso descrito para obtener su trío de treses: $\{3\heartsuit, 3\diamondsuit, 5\clubsuit, A\spadesuit, 3\spadesuit\}$, es el siguiente:

$\{82, 30, 98, 24, 43\}^{23} \pmod{143} = \{114, 127, 54, 19, 10\}$,
$\{114, 127, 54, 19, 10\}^{103} \pmod{143} = \{75, 62, 76, 72, 10\}$,
$\{75, 62, 76, 72, 10\}^{47} \pmod{143} = \{04, 17, 32, 41, 43\}$.

g) Finalmente, Alicia debe elegir sus cartas. Para ello, Carmen cifra con su clave pública, $e_C = 23$, las cartas que quedan, de

modo que Alicia no sepa el valor de las cartas que aún no han sido repartidas, y se las envía:

{123, 113, ✠, 5, 28, 128, 8, 42, 43, 33, 12, 13, ✠, 136,
126, ✠, 18, 41, 141, 21, 55, 56, 46, ✠, 26, ✠, 6, 139,
140, 31, ✠, 11, ✠, 68, 69, 59, 38, 39, 40, ✠, 9, ✠, 44,
✠, 24, 47, 81, 82, 72, 51, 52, 53}.

Alicia elige, sin cifrar, dado que las cartas que recibe ya estaban cifradas desde el principio del protocolo, cinco de los números recibidos: {113, 136, 127, 6, 38}. A continuación Alicia devuelve a Carmen los cinco números que ha elegido, quien los descifra con su clave privada, $d_C = 47$, y los remite de nuevo a Alicia. Por último, Alicia descifra, con $d_A = 193$, los números recibidos, que corresponden a su pareja de ases: {2♥, *A*♦, 8♦, *A*♣, *J*♣}:

$\{113, 136, 127, 6, 38\}^{47} \pmod{143} = \{42, 115, 30, 63, 25\}$,
$\{42, 115, 30, 63, 25\}^{193} \pmod{143} = \{03, 15, 22, 28, 38\}$.

Una vez que cada jugador conoce sus cartas, se inicia la partida. En este caso, el protocolo podría extenderse de modo que cada uno de los jugadores pudiera descartarse de alguno de los naipes que ya posee y elegir otros nuevos. El procedimiento sería parecido al descrito anteriormente, pero teniendo en cuenta que cada jugador debe descartarse de las cartas que no desee antes de elegir las nuevas, y de modo que los naipes descartados no sean elegidos por ninguno de los restantes jugadores.

4. Desarrollemos el esquema (3, 5)-umbral diseñado por el director de la empresa. Dado que éste ha elegido los módulos que verifican las condiciones del Teorema del Resto Chino: $m_1 = 97$, $m_2 = 98$, $m_3 = 99$, $m_4 = 101$ y $m_5 = 103$, y como el mínimo del producto de tres de los módulos es 941094, y el máximo del producto de dos de ellos es 10403, el valor secreto $S = 500000$ está entre ellos; por lo que se puede proceder a elaborar el esquema.

Se calculan los valores de a_i de modo que $S \equiv a_i \pmod{m_i}$. En este caso se tiene que $a_1 = 62$, $a_2 = 4$, $a_3 = 50$, $a_4 = 50$ y $a_5 = 38$. Estos valores son las sombras que se proporcionan a cada uno de los empleados, con el fin de que tres de ellos, por lo menos, sean capaces de ponerse de acuerdo y compartir esa información.

Comprobemos que los empleados E_2, E_3 y E_4 son capaces de combinar sus sombras para conseguir el premio. En primer lugar calculan los valores de $M_i = m_j \cdot m_k$, con $i \neq j \neq k \neq i$, y los valores de sus inversos módulo m_i:

$$M_2 = 9999,\ M_3 = 9898,\ M_4 = 9702;\ N_2 = 33,\ N_3 = 49,\ N_4 = 17$$

De aquí, y por el Teorema del Resto Chino, se tiene que la solución a la que llegan es:

$$s = \sum_{i=2}^{4} a_i M_i N_i = 4 \cdot 9999 \cdot 33 + 50 \cdot 9898 \cdot 49 + 50 \cdot 9702 \cdot 17$$

$$= 33816668$$

de donde se tiene que $S \equiv s \pmod{98 \cdot 99 \cdot 101} = 500000$.

Veamos ahora que si se unen sólo dos de los empleados, por ejemplo, E_2 y E_5, no son capaces de recuperar el secreto. En efecto, estos dos empleados sólo pueden obtener el siguiente valor:

$$s = 4 \cdot 103 \cdot 59 + 38 \cdot 98 \cdot 41 = 176992 \equiv 5394 \pmod{10094}$$

Tras lo cual sólo saben que el premio es de la forma $5394 + k \cdot 10094$, siendo $1 \leq k \leq 92$, pero sin saber exactamente cuál de estos 92 valores es el que corresponde al premio.

5. Los datos para el protocolo del millonario son los siguientes: $i = 3$, $j = 5$, $n = 115$, $e_A = 19$, $d_A = 51$, $x = 76$ y $p = 23$. Por tanto, Alicia y Bernardo proceden de la siguiente manera (se supone que ninguno de ellos hace trampa, dado que ambos están interesados en resolver el problema):

a) Bernardo elige $x = 76$ y calcula

$$k = x^{e_A} \pmod{n} = 76^{19} \pmod{115} = 11$$

enviando el valor $k - j = 11 - 5 = 6$ a Alicia.

b) Alicia elige $p = 23$ y calcula los valores

$$y_i = (6 + u)^{d_A} \pmod{115}\ ,\ \text{con } 1 \leq u \leq 10$$

Estos valores son:

$$103,\ 27,\ 59,\ 90,\ 61,\ 8,\ 2,\ 79,\ 65,\ 81.$$

c) A continuación Alicia calcula los valores anteriores módulo $p = 23$:

$$11,\ 4,\ 13,\ 21,\ 15,\ 8,\ 2,\ 10,\ 19,\ 12$$

Dado que hay valores entre los anteriores cuya diferencia es menor que 2 (por ejemplo 10, 11, 12 y 13), el número primo elegido por Alicia no es adecuado. Por ello, Alicia elige otro número primo, $p = 67$, y repite la operación anterior, obteniendo:

36, 27, 59, 23, 61, 8, 2, 12, 65, 14

que sí verifican lo pedido.

d) Ahora, como el valor secreto de Alicia es $i = 3$, Alicia envía a Bernardo la sucesión de números anterior modificada, de modo que a partir de la cuarta posición los números se han incrementado en una unidad, y al final se incluye el número primo que ha elegido:

36, 27, 59, 24, 62, 9, 13, 66, 15, 67

e) Dado que el valor secreto de Bernardo es $j = 5$, como el quinto valor de la serie anterior, esto es, 62, verifica que

$$x \pmod p = 76 \pmod{67} = 9 \neq 62$$

Bernardo concluye que $i < j$, es decir, que él es más rico que Alicia.

6. Para el protocolo de la transferencia inconsciente con $x = 123456$ y $n = 3145421 = 1583 \cdot 1987$, se tiene que:

a) Bernardo elige el número $x = 123456$, calcula su cuadrado módulo n, $x_2 = x^2 \pmod n = 123456^2 \pmod{3145421} = 1819191$, y se lo envía a Alicia.

b) Alicia calcula las cuatro raíces cuadradas de $x_2 = 1819191$ módulo 3145421 como sigue:

i. En primer lugar determina

$$x_2 \pmod p = 1819191 \pmod{1583} = 324$$
$$x_2 \pmod q = 1819191 \pmod{1987} = 1086$$

ii. A continuación calcula las raíces cuadradas de los dos números obtenidos módulo los números primos p y q:

$$\sqrt{324} \pmod{1583} = \pm 18,\ \sqrt{1086} \pmod{1987} = \pm 262$$

siendo $-18 \pmod{1583} = 1565$ y $-262 \pmod{1987} = 1725$.

iii. De las cuatro raíces anteriores se queda con las dos menores y calcula, mediante el algoritmo de Euclides extendi-

do, el inverso de cada una de ellas módulo el otro primo, esto es:

$$\pm 18 \cdot 1987 \cdot 192 \pm 262 \cdot 1583 \cdot 1746$$
$$= \{123456, 1275916, 1869505, 3021965\}$$

c) Dado que sólo importan las dos raíces menores, puesto que las otras dos son sus opuestos, Alicia transmite a Bernardo cualquiera de ellas. Como en el problema se pide que Bernardo conozca la factorización del módulo, se supone que Alicia elige aleatoriamente la raíz $y = 1275913$.

d) Bernardo recibe la raíz $y = 1275913$. Ahora bien, como se tiene que $1275916 \pmod{3145421} \neq -123456$, resulta que Bernardo recibe una raíz de x_2 que no conocía, lo que le permite factorizar $n = 3145421$, sin más que calcular:

$$\text{mcd}\,(x + y, n) = \text{mcd}\,(1399372, 3145421) = 1583$$
$$\text{mcd}\,(-x + y, n) = \text{mcd}\,(1152460, 3145421) = 1987$$

con lo que $n = 3145421 = 1583 \cdot 1987$.