TEMA
Nociones matemáticas para RSA

El propósito principal en estas páginas es presentar una base matemática necesaria para la posterior comprensión de un criptosistema asimétrico llamado RSA. El estudio y conocimiento de los fundamentos matemáticos de la criptografía asimétrica ha adquirido un interés práctico que se le añade al intrínseco interés teórico del que gozan todas las matemáticas.

La teoría de números y la aritmética modular han adquirido un enorme interés práctico gracias a la aparición, en 1976, de la criptografía de clave pública, de la mano de **Whitfield Diffie y Martin E. Hellman** con su histórico artículo titulado "**New Directions in Cryptography**" [14]. El algoritmo que presentaron permitía a dos usuarios ponerse de acuerdo en el valor de una clave secreta a través de un canal inseguro o público. La matemática que sustentaba su algoritmo era la aritmética modular, y la operación básica la exponenciación.

Dos años más tarde del trabajo de Diffie y Hellman, los investigadores **Ronald L. Rivest, Adi Shamir y Leonard M. Adleman** presentaron un algoritmo de clave pública que ha hecho fortuna: se trata del criptosistema que lleva como nombre las tres iniciales de estos tres autores: **RSA** [2].

En las siguientes páginas se recogen algunas nociones matemáticas, necesarias para el estudio y la comprensión del criptosistema RSA. Este trabajo está dividido en dos partes. En la primera parte se recogen unas nociones matemáticas previas. Compartimentado en cinco epígrafes o secciones, se recogen algunas nociones sobre los enteros (sección 1); nociones algebraicas sobre conjuntos (sección 2); una breve presentación de la noción de relación de equivalencia y, en concreto, de la relación de congruencia (sección 3). En una cuarta sección se muestra una presentación intuitiva y visual de los conceptos recogidos hasta ese momento. Y en la sección 5 se aborda el problema concreto de la búsqueda de inversos en aritmética modular y se muestra el procedimiento empleado en la creación de las claves para RSA.

En la segunda parte, en tres secciones, se muestra con detalle el criptosistema RSA. En la sección 6 se presenta una descripción del algoritmo; en la sección 7 se muestran los procedimientos básicos de factorización de enteros, que exigen —como allí se ve— algunas restricciones en la creación de las claves del criptosistema: esas restricciones quedan señaladas en el octavo y último epígrafe de este capítulo.

En este documento no quedan recogidas las demostraciones de los sucesivos teoremas que se enuncian: pretende ser una recopilación de conceptos, y no se ha querido extender más la presentación, ni complicarla con demostraciones, aunque todas ellas son bastante sencillas y en muchos casos casi inmediatas. En la bibliografía recogida al final de estos folios se indica expresamente dónde puede encontrarse cada demostración.

PRIMERA PARTE.
NOCIONES MATEMÁTICAS PREVIAS

1. DEFINICIÓN DEL CONJUNTO DE LOS ENTEROS. ALGUNAS PROPIEDADES.

En la obra Formulario Matemático, publicada en 1889, Guiseppe Peano (1858–1932) presentó una descripción del **CONJUNTO DE LOS ENTEROS NO NEGATIVOS** ($\mathbb{Z}^+$) a partir de tres términos indefinidos: **cero**, **número** y **sucesor** (cfr. [3] §4.6.). Su formulación fue la siguiente:

a. Cero (0) es un número.

b. Para cualquier número n, su sucesor es un número.

c. Ningún número tiene a cero como su sucesor.

d. Si dos números m y n tienen el mismo sucesor, entonces $m = n$.

e. Si T es un conjunto de números donde $0 \in T$, y donde el sucesor de n está en T, siempre que n esté en T, entonces T es el conjunto de todos los números.

Vamos a presentar algunas propiedades del conjunto de los enteros. Especialmente aquellas que hacen referencia a la divisibilidad.

Definición 1.1. Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b divide a a si existe un entero n tal que $a = b \cdot n$. Cuando esto ocurre, decimos que b es **DIVISOR** de a o que a es **MÚLTIPLO** de b.

Definición 1.2. ALGORITMO DE LA DIVISIÓN: Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$, únicos, tales que $a = q \cdot b + r$, con $0 \leq r < b$. Al entero q lo llamamos **COCIENTE** y al entero r **RESTO** o **RESIDUO**. A la operación aritmética destinada a calcular el resto o residuo de dividir dos enteros $a, b \in \mathbb{Z}$ la denotamos $a \bmod b$.

Definición 1.3. Si $a, b \in \mathbb{Z}$, un entero positivo c es **DIVISOR COMÚN** de a y de b si c divide a a y c divide a b.

Definición 1.4. Sean $a, b \in \mathbb{Z}$, al menos uno de los dos distinto de cero. Entonces $c \in \mathbb{Z}^+$ es el **MÁXIMO COMÚN DIVISOR** ($c = mcd(a, b)$) de a y de b si

a. c es divisor común de a y de b.

b. Para cualquier divisor común d de a y b, tenemos que d divide a c.

En definitiva, el máximo común divisor de dos enteros a y b, es el mayor entero que divide a a y divide a b. Se cumple que $mcd(a, b) = mcd(b, a)$.

Se verifica que $mcd(a, 0) = mcd(0, a) = a$.

Teorema 1.1. Para cualesquiera dos enteros positivos $a, b \in \mathbb{Z}^+$ existe un único $c \in \mathbb{Z}^+$ que es el máximo común de a y de b .

Teorema 1.2. Dados dos enteros de a y b con $mcd(a, b) = d$. Entonces $mcd(a/d\ , b/d\ ) = 1$.

Definición 1.5. El método más usual de obtener el máximo común divisor de dos enteros $a, b \in \mathbb{Z}^+$ con $b \neq 0$ es el **ALGORITMO DE EUCLIDES**.

Este algoritmo establece que $mcd(a, b) = mcd(b, a \bmod b)$.

Otra formulación: Sea $r_0 = a$ y $r_1 = b$, enteros tales que $a \geq b$, $a \neq 0$. Si aplicamos el algoritmo de la división de forma sucesiva obtenemos la siguiente secuencia de ecuaciones:

$r_0 = r_1 \cdot q_1 + r_2$, con $0 < r_2 < r_1$; si $r_2 = 0$ se termina la secuencia de ecuaciones y $mcd(a, b) = r_1$.

$r_1 = r_2 \cdot q_2 + r_3$, con $0 < r_3 < r_2$; si $r_3 = 0$ se termina la secuencia de ecuaciones y $mcd(a, b) = r_2$.

(…)

$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$, con $0 < r_n < r_{n-1}$; si $r_n = 0$ se termina la secuencia de

ecuaciones y $mcd(a\,,b) = r_{n-1}$.

$r_{n-1} = r_n \cdot q_n$. Suponemos que efectivamente ya hemos llegado al caso en que $r_{n-1} = 0$. Tenemos que $mcd(a\,,b) = r_n$: el último resto distinto de cero.

Definición 1.6. Se puede demostrar que si $d = mcd(a\,,b)$, entonces existen números enteros s, t, tales que $d = s \cdot a + t \cdot b$. Es decir, podemos expresar d como una combinación lineal de a y de b.

El algoritmo de Euclides ofrece una herramienta para lograr expresar d como una combinación lineal de a y de b, gracias a las diferentes ecuaciones que se genera en su desarrollo. Queda definido un algoritmo, llamado **ALGORITMO EXTENDIDO DE EUCLIDES**, que recibe como entrada dos enteros a y b, genera dos sucesiones s_n y t_n, y proporciona a su salida dos números, s y t tales que $d = s \cdot a + t \cdot b$, donde $d = mcd(a\,,b)$. Las secuencias s_n y t_n se generan de acuerdo con el siguiente procedimiento:

$s_0 = 1\,;\; s_1 = 0\,;\; t_0 = 0\,;\; t_1 = 1;\qquad s_j = s_{j-2} - q_{j-1} \cdot s_{j-1};\qquad t_j = ts_{j-2} - q_{j-1} \cdot t_{j-1}$

para $j = 2, 3, \ldots, n$ y donde q_j son los cocientes en las divisiones del algoritmo de Euclides cuando se usa para el cálculo del máximo común divisor de a y b.

Como se verá más adelante, el algoritmo extendido de Euclides es la herramienta necesaria para la generación de las claves del algoritmo RSA. Mas adelante volveremos sobre él, con un ejemplo ya recogido en el artículo de presentación del algoritmo RSA [2].

Definición 1.7. Si seguimos analizando el conjunto $\mathbb{Z}^+$, observaremos que para todo $n \in \mathbb{Z}^+$, $n > 1$, el entero n tiene al menos dos divisores positivos; 1 y el mismo n (a estos dos divisores se les conoce como **DIVISORES** o **FACTORES TRIVIALES**). Algunos números, como 2, 3, 5, 7, 11, 13, 17,…, tienen como únicos divisores los dos positivos triviales: estos enteros reciben el nombre de **PRIMOS**. Todos los demás enteros positivos (mayores que 1 y que no sean primos) se llaman **COMPUESTOS**, y sus divisores, excepto el 1 y el n, se llaman **DIVISORES** o **FACTORES PROPIOS**.

Teorema 1.3. TEOREMA FUNDAMENTAL DE LA ARITMÉTICA. Cada entero $n > 1$

puede escribirse como un producto de primos de forma única, excepto por el orden de éstos.

Definición 1.8. Diremos que los enteros $a, b \in \mathbb{Z}$ son **PRIMOS RELATIVOS** si $mcd(a, b) = 1$. Decimos también que a y b son **RELATIVAMENTE PRIMOS** o **COPRIMOS**.

Recapitulación de algunas ideas presentadas. Ya sabemos que dados dos enteros positivos cualesquiera $a, b \in \mathbb{Z}^+$ siempre existe un valor $c \in \mathbb{Z}^+$, $c = mcd(a, b)$, y que este entero es único. Además el valor del máximo común divisor es el menor entero positivo que se puede escribir como una combinación lineal de a y de b: de todos los valores $c = a \cdot x + b \cdot y$ $(x, y \in \mathbb{Z})$, el menor de ellos será el máximo común divisor de a y b. Entonces, si tenemos dos enteros a y b primos relativos ($mcd(a, b) = 1$), entonces existen $x, y \in \mathbb{Z}$ tales que $a \cdot x + b \cdot y = 1$.

Teorema 1.4. Hay infinitos números primos.

2. ALGUNAS NOCIONES ALGEBRAICAS SOBRE CONJUNTOS.

Los grupos, anillos y cuerpos son los elementos fundamentales de una rama del saber matemático que llamamos álgebra abstracta, o álgebra moderna. El objeto de esta matemática es el conocimiento de aquellos conjuntos con los que podemos operar algebraicamente: es decir, aquellos conjuntos de los que podemos combinar (operar) cualesquiera dos de sus elementos para obtener un tercer elemento del conjunto. Estas operaciones están sujetas a un conjunto de reglas que vienen definidas por la misma naturaleza del conjunto.

Definición 2.1. Un conjunto de elementos G con la operación binaria + será **GRUPO** si se verifican las siguientes propiedades:

a. **CLAUSURA**: Si $a,b \in G$, entonces $a+b \in G$. Se dice también que G es **CERRADO** respecto a la operación +, o que la operación + es INTERNA en G.

b. **ASOCIATIVA**: Para todas las ternas $a,b,c \in G$, se cumple que $a+(b+c) = (a+b)+c$.

c. **ELEMENTO IDENTIDAD O ELEMENTO NEUTRO**: Existe un elemento $z \in G$ que verifica que $a+z = z+a = a$ para todo elemento $a \in G$.

d. **ELEMENTO INVERSO**: Para cada $a \in G$, existe un elemento $b \in G$ tal que $a+b = b+a = z$.

Decimos que un grupo es **GRUPO ABELIANO** si verifica además la propiedad **CONMUTATIVA**: para el operador +: es decir, para todo par de elementos $a,b \in G$ se verifica que $a+b = b+a$.

Definición 2.2. Sea $\mathbb{R}$ un conjunto no vacío con dos operaciones binarias internas $+$ y $\cdot$, que llamaremos a partir de ahora suma y producto o multiplicación. Entonces $(\mathbb{R},+,\cdot)$ es un **ANILLO** si se cumplen las siguientes condiciones:

a. $(\mathbb{R},+)$ tiene estructura de grupo abeliano a cuyo **elemento neutro** llamaremos normalmente "**cero** (0)".

b. La operación binaria $\cdot$ también verifica la propiedad de clausura, la propiedad asociativa y tiene **elemento neutro**, al que llamaremos normalmente "**uno** (1)": $a \cdot 1 = 1 \cdot a = a$.

c. La operación . es **DISTRIBUTIVA** a la derecha y a la izquierda respecto de la operación +: para todo $a, b, c \in \mathbb{R}$, se verifica que $a \cdot (b + c) = a \cdot c + a \cdot c$ y que $(b + c) \cdot a = b \cdot a + c \cdot a$.

Si además se verifica la propiedad conmutativa para el producto: $a \cdot b = b \cdot a$ para todo $a, b \in \mathbb{R}$, entonces diremos que $\mathbb{R}$ es un **ANILLO CONMUTATIVO**.

Definición 2.3. Sea $\mathbb{R}$ un anillo. Diremos que el elemento $a \in \mathbb{R}$ es una **UNIDAD** si posee un elemento inverso multiplicativo (a la izquierda y a la derecha), al que llamamos **INVERSO** de a, es decir, si existe otro elemento $b \in \mathbb{R}$ que verifica que $a \cdot b = b \cdot a = 1$.

Es inmediato y evidente que el valor $0 \in \mathbb{R}$ no es en ningún caso una unidad. No existe un $x \in \mathbb{R}$ que verifique que $x \cdot 0 = 0 \cdot x = 1$.

Dado un conjunto $\mathbb{R}$, denotaremos $\mathbb{R}^*$ al **CONJUNTO FORMADO POR LAS UNIDADES** de $\mathbb{R}$.

Definición 2.4. Sea $\mathbb{R}$ un anillo. Un elemento $a \in \mathbb{R}$ se llama **DIVISOR DE CERO** (o **DIVISOR PROPIO DE CERO**) si y solo si es distinto de cero y existe $b \in \mathbb{R}$, con $b \neq 0$, tal que $a \cdot b = 0$. Llamamos $\overline{\mathbb{R}}$ al subconjunto de $\mathbb{R}$ que son divisores de cero.

Un elemento $a \in \mathbb{R}$ no puede ser a la vez unidad y divisor de cero. El cero ni es una cosa, ni es la otra. Podemos afirmar que $R^* = \mathbb{R} - \overline{\mathbb{R}} - \{0\}$.

Definición 2.5. Sea $(\mathbb{R}, +, \cdot)$ un anillo conmutativo. Diremos que $\mathbb{R}$ es un **DOMINIO DE INTEGRIDAD** si no tiene divisores de cero. Verifica, por tanto, la **LEY DE CANCELACIÓN DEL PRODUCTO**: para cualesquiera $a, b, c \in \mathbb{R}$, tales que $a \neq 0$ se cumple que si $a \cdot b = a \cdot c$ entonces $b = c$.

Definición 2.6. Un **CUERPO** es un anillo conmutativo $\mathbb{R}$ que verifica que todo elemento distinto de cero es una unidad.

También puede definirse diciendo que es un dominio de integridad $\mathbb{R}$ que verifica la propiedad de existencia de inverso para todo elemento de $\mathbb{R}$, excepto el elemento 0.

El conjunto $\mathbb{R}$, bajo las operaciones suma y producto $(\mathbb{R},+,\cdot)$ tendrá estructura de cuerpo si el $(\mathbb{R},+)$ tiene estructura de grupo abeliano y $(\mathbb{R}-\{0\},\cdot)$ tiene estructura de grupo.

Teorema 2.1. Un dominio de integridad finito $(D,+,\cdot)$ es un cuerpo.

Definición 2.7. Dado un anillo $\mathbb{R}$, un elemento $a \in \mathbb{R}$, $a \neq 0$ diremos que es **NILPOTENTE** si $a^n = 0$ para algún entero $n \geq 1$.

Definición 2.8. Dado un anillo $\mathbb{R}$, un elemento $a \in \mathbb{R}$, $a \neq 0$ diremos que es **IDEMPOTENTE** si $a^2 = a$.

Definición 2.9. Sea $(G,\cdot)$ un grupo. Un subconjunto $H \subseteq G$ es un **SUBGRUPO** si H es cerrado bajo la operación producto y verifica todas las propiedades de grupo respecto a esa operación.

Definición 2.10. Para cualquier grupo $(G,\cdot)$, el número de elementos de G es el **ORDEN DEL GRUPO** G El orden de un grupo de denota como $|G|$. Cuando el número de elementos de un grupo no es finito decimos que G tiene orden infinito.

Definición 2.11. Un grupo $(G,\cdot)$ decimos que es **CÍCLICO** si existe un elemento $a \in G$ tal que, para todo $b \in G$ tenemos que $b = a^n$ para algún $n \in \mathbb{Z}$. El elemento $a \in G$ se llama **GENERADOR** del grupo G.

Teorema 2.2. Dado un grupo $(G,\cdot)$, y $a \in G$, el conjunto $S = \{a^k \mid k \in \mathbb{Z}\}$ es subgrupo de G.

Definición 2.12. Al subgrupo generado como queda dicho en el Teorema 2.2. lo llamamos **SUBGRUPO GENERADO POR** a y se denota como $\langle a \rangle$.

Definición 2.13. Dado un grupo G, y un elemento $a \in G$, definimos **ORDEN DEL ELEMENTO** a al cardinal de subgrupo generado por a ($\langle a \rangle$) y lo denotamos como $\mathcal{O}(a)$.

Algunas consideraciones que se deducen de estas definiciones presentadas. Si el cardinal de $\langle a \rangle$ es 1, entonces a es el elemento neutro del producto: $a = 1$. (cfr. [4] §2A.).

Si el cardinal de $\langle a \rangle$ es finito distinto de uno, entonces $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ es finito, y por tanto el conjunto $\{a, a^2, a^3, \dots\} = \{a^n \mid n \in \mathbb{Z}^+\}$ también es finito. Y por lo tanto, existen $s, t \in \mathbb{Z}^+$ tales que $1 \leq s < t$ y $a^s = a^t$ de donde se deduce que $a^{t-s} = 1$, con $t - s \in \mathbb{Z}^+$. Como $1 \in \{a^n \mid n \in \mathbb{Z}^+\}$, sea m el mínimo entero positivo tal que $a^m = 1$. Entonces podemos afirmar que $\langle a \rangle = \{a, a^2, a^3, \dots, a^m = 1,\}$. Es inmediato ver que el orden del grupo $\langle a \rangle$ es igual al orden del elemento a: $\mathcal{O}(a) = m$.

Teorema 2.3. Sea $a \in G$, $(G,\cdot)$ grupo, con $\mathcal{O}(a) = n$. Si $k \in \mathbb{Z}$ y $a^k = 1$, entonces $n \mid k$.

Teorema 2.4. Teorema de LAGRANGE. Si $(G,\cdot)$ es un grupo finito de orden n y H es un subgrupo de orden m, entonces $m \mid n$.

Teorema 2.5. (Corolario) Si $(G,\cdot)$ es un grupo finito y $a \in G$, entonces $\mathcal{O}(a)$ divide a $|G|$ (cardinal de G).

Teorema 2.6. (Corolario) Cualquier grupo de orden primo es cíclico.

Teorema 2.7. (Corolario) Cada subgrupo de un grupo cíclico es cíclico.

Teorema 2.8. Sea $(G,\cdot)$ un grupo finito cíclico de orden n. Entonces G tiene un subgrupo de orden d para cada divisor d de n, y G no tiene otros subgrupos.

3. RELACIONES DE EQUIVALENCIA. RELACIÓN DE CONGRUENCIA.

Definición 3.1. Sean los conjuntos A y B. Una **RELACIÓN** $\mathcal{R}$ de A en B es cualquier subconjunto de $A \times B$. Si el par (a,b) pertenece a la relación, diremos que $(a,b) \in \mathcal{R}$ ó $a\,\mathcal{R}\,b$. A los subconjuntos de $A \times A$ se les llama relaciones sobre A.

Definición 3.2. Una relación $\mathcal{R}$ sobre un conjunto A es **REFLEXIVA** si para todo $x \in A$ se verifica que $(x,x) \in \mathcal{R}$.

Una relación $\mathcal{R}$ sobre un conjunto A es **SIMÉTRICA** si $(x,y) \in \mathcal{R} \Rightarrow (y,x) \in \mathcal{R}$ para todo $x,y \in A$.

Para un conjunto A, una relación es **TRANSITIVA** si para todo $x,y,z \in A$, si $(x,y) \in \mathcal{R}$ y $(y,z) \in \mathcal{R}$ entonces $(x,z) \in \mathcal{R}$.

Una **RELACIÓN DE EQUIVALENCIA** $\mathcal{R}$ sobre un conjunto A es una relación que verifica las propiedades reflexiva, simétrica y transitiva.

Definición 3.3. Dado un conjunto A y un conjunto de índices I, sea $\emptyset \neq A_i \subseteq A$ para cada $i \in I$. Entonces $\{A_i\}_{i\in I}$ es una **PARTICIÓN** de A si:

a. $A = \bigcup_{i\in I} A_i$
b. $A_i \cap A_j = \emptyset$ para todo $i,j \in I$tal que $i \neq j$.

Cada subconjunto A_i es una **CELDA** o **BLOQUE** de la partición. De la definición queda claro que cada elemento de A pertenece a una celda o bloque, y solo a una.

Definición 3.4. Sea $\mathcal{R}$ una relación de equivalencia sobre un conjunto A. Para cualquier $x \in A$, la **CLASE DE EQUIVALENCIA DE** x, que se denota $[x]$, se define como $[x] = \{y \in A \mid y\,\mathcal{R}\,x\}$.

Teorema 3.1. Si $\mathcal{R}$ es una relación de equivalencia sobre un conjunto A, y $x,y \in A$, entonces se verifican las siguientes propiedades:

a. $x \in [x]$.

b. $x \mathcal{R} y$ si y sólo si $[x] = [y]$.
c. Una de dos: o $[x] = [y]$, o $[x] \cap [y] = \emptyset$.

Las tres afirmaciones se deducen rápidamente a partir de la definición 3.3. y se puede adivinar, como se verá a continuación, que el conjunto de clases de equivalencia que se origina en una relación $\mathcal{R}$ de equivalencia sobre A es una partición de A .

Teorema 3.2. (Equivalencia de conceptos: "relación de equivalencia" y "partición"): Sea A un conjunto, entonces:

a. Toda relación de equivalencia $\mathcal{R}$ sobre A induce una partición de A; y
b. Toda partición de A da lugar a una relación de equivalencia $\mathcal{R}$ sobre A.

Teorema 3.3. Para cualquier conjunto A, existe una correspondencia uno a uno entre el conjunto de relaciones de equivalencia sobre A y el conjunto de particiones de A. Este Teorema es especialmente interesante para conjuntos finitos.

Definición 3.5. Sea $n \in \mathbb{Z}^+$, $n > 1$. Para $a, b \in \mathbb{Z}$, decimos que a es **CONGRUENTE CON** b **MÓDULO** n, y escribimos $a \equiv b (mod\, n)$, si $n \mid (a - b)$; o en forma equivalente, si existe algún $k \in \mathbb{Z}$ tal que $a = b + k \cdot n$.

Es decir, dos elementos $a, b \in \mathbb{Z}$ serán congruentes módulo n si el residuo obtenido de dividir a entre n es el mismo que el obtenido al efectuar la división de b entre n. Al entero n se le llama **MÓDULO** de la congruencia.

Si se tiene que $n \nmid (a - b)$ entonces escribimos $a \not\equiv b (mod\, n)$.

Teorema 3.4. La congruencia módulo n es una relación de equivalencia sobre $\mathbb{Z}$.

a. Reflexiva: Si a es un entero, entonces $a \equiv a (mod\, n)$.
b. Simétrica: Si a y b son enteros tales que $a \equiv b (mod\, n)$, entonces $b \equiv a (mod\, n)$.
c. Transitiva: Si a, b y c son enteros con $a \equiv b (mod\, n)$ y $b \equiv c (mod\, n)$, entonces también $a \equiv c (mod\, n)$.

Definición 3.6. Como una relación de equivalencia sobre un conjunto induce una partición sobre éste, para $n \geq 2$, la congruencia módulo n divide a $\mathbb{Z}$ en n clases de equivalencia:

$[0] = \{0 + n \cdot x \mid x \in \mathbb{Z}\}$.

$[1] = \{1 + n \cdot x \mid x \in \mathbb{Z}\}$.

$[2] = \{2 + n \cdot x \mid x \in \mathbb{Z}\}$.

(…)

$[n-1] = \{(n-1) + n \cdot x \mid x \in \mathbb{Z}\}$.

Para cualquier $t \in \mathbb{Z}$, por el algoritmo de la división, podemos escribir $t = q \cdot n + r$, donde $0 \leq r < n$, por lo que $t \in [r]$, ó también, $[t] = [r]$.

Usamos la notación $\mathbb{Z}/n\mathbb{Z}$ para denotar el conjunto $\{[0][1][2] \ldots [n-1]\}$. Este el conjunto de las clases de congruencia módulo n. Y llamaremos $\mathbb{Z}_n$ al conjunto de los menores residuos no negativos módulo n: $\{0, 1, 2, \ldots, n-1\}$.

A cualquier conjunto que verifique que todo $a \in \mathbb{Z}$ es congruente módulo n con un y solo un elemento de ese conjunto se le llama **CONJUNTO COMPLETO DE RESIDUOS MÓDULO** n. $\mathbb{Z}_n$ es uno de esos conjuntos.

Teorema 3.5. Cualquier conjunto de n enteros, todos ellos incongruentes entre sí, forma un conjunto completo de residuos módulo n.

Definición 3.7. A una congruencia de la forma $a \cdot x \equiv b (mod\ n)$, donde x es un entero desconocido la llamamos **CONGRUENCIA LINEAL DE UNA VARIABLE**.

Teorema 3.6. Sean a, b y n enteros tales que $n > 0$ y $mcd(a, n) = d$.

a. Si $d \nmid b$, entonces la congruencia lineal $a \cdot x \equiv b (mod\ n)$ no tiene solución.

b. Si $d \mid b$, entonces $a \cdot x \equiv b (mod\ n)$ tiene exactamente d soluciones, incongruentes entre sí, módulo n.

Definición 3.8. Como corolario a este último teorema es inmediato deducir que

$a \cdot x \equiv 1(mod\ n)$ tendrá solución únicamente si $mcd(a,n) = 1$. Al valor único de x solución de la congruencia $a \cdot x \equiv 1(mod\ n)$ se le llama **INVERSO DE** a **MÓDULO** n. Queda entonces claro que a será un elemento unidad (ver definición 2.3.) en el anillo $\mathbb{Z}_n$ si y solo si $mcd(a,n) = 1$.

Es inmediato deducir también que si p es un entero primo, entonces todos los enteros $a \in \mathbb{Z}_p$ excepto el cero, verifican que $mcd(a,p) = 1$ y, por tanto, todos ellos tienen inverso. Podemos afirmar, por tanto, que $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$: todos los elementos de $\mathbb{Z}_p$, excepto el cero, son unidades.

Definición 3.9. Para $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ definimos las operaciones **SUMA** $(+)$ y **PRODUCTO** $(\cdot)$ como

a. $[a] + [b] = [a + b]$
b. $[a] \cdot [b] = [a \cdot b]$

La definición de estas dos operaciones no depende de la elección de los representantes de las clases y, por tanto, las operaciones están bien definidas: Si $[a] = [c]$ y $[b] = [d]$, entonces $[a] + [b] = [c] + [d]$ y $[a] \cdot [b] = [c] \cdot [d]$.

Algunas propiedades de estas operaciones aritméticas, expresadas en notación modular, son (para $a, b \in \mathbb{Z}$):

a. $(a + b)(mod\ n) = \big((a\ mod\ n) + (b\ mod\ n)\big)(mod\ n)$
b. $(a - b)(mod\ n) = \big((a\ mod\ n) - (b\ mod\ n)\big)(mod\ n)$
c. $(a \cdot b)(mod\ n) = \big((a\ mod\ n) \cdot (b\ mod\ n)\big)(mod\ n)$
d. Si $(a + b) \equiv (a + c)(mod\ n)$, entonces $b \equiv c(mod\ n)$.
e. Si $(a \cdot b) \equiv (a \cdot c)(mod\ n)$, entonces $b \equiv c(mod\ n)$ si $mcd(a,n) = 1$.

Teorema 3.7. Para $n \in \mathbb{Z}^+$, $n > 1$, $\mathbb{Z}_n$ es un anillo conmutativo con elemento unidad igual a $[1]$ en las operaciones binarias cerradas antes definidas.

Por tanto, si sabemos **determinar en qué casos el conjunto $\mathbb{Z}_n$ no tiene divisores de cero**, entonces sabremos determinar cuándo es dominio de integridad. Y como $\mathbb{Z}_n$ es un conjunto finito, sabremos determinar cuándo $\mathbb{Z}_n$ tiene estructura algebraica de cuerpo.

Teorema 3.8. (ver definición 3.8.) En $\mathbb{Z}_n$, a es una unidad (ver definición 2.3.) si y sólo si $mcd(a,n) = 1$.

Teorema 3.9. $\mathbb{Z}_n$ es un cuerpo si y sólo si n es primo. En ese caso, todos los elementos de $\mathbb{Z}_n - \{0\}$ son coprimos con n y, por tanto, $\mathbb{Z}_n$ es dominio de integridad finito, es decir, cuerpo.

Teorema 3.10.: El pequeño teorema de FERMAT. Si p es primo y a es un entero positivo no divisible por p, entonces $a^{p-1} \equiv 1(mod\ p)$. Este teorema permite hallar de forma inmediata el inverso de cualquier elemento $a \in \mathbb{Z}_p$: $a^{p-2}\ mod\ p$.

Definición 3.10. FUNCIÓN DE EULER. Una cantidad importante dentro de la teoría de números es la definida mediante la función de Euler, denotada función Φ donde $\Phi(n)$ es **el número de enteros positivos menores que n y relativamente primos con n**. Se calcula de acuerdo con las siguientes cuatro reglas:

a. Si p es primo, entonces $\Phi(p) = p - 1$.
b. Si p es primo y $n = p^k$, entonces $\Phi(n) = p^k - p^{k-1}$.
c. Si m y n son coprimos entre sí, entonces $\Phi(\mathrm{m} \cdot \mathrm{n}) = \Phi(\mathrm{m}) \cdot \Phi(\mathrm{n})$.
d. Si $n = \prod_{i=1}^{k} p_i^{e_i}$, entonces $\Phi(n) = \prod_{i=1}^{k} p_i^{e_i - 1} \cdot (p_i - 1)$.

La función de Euler Φ ofrece una información muy útil en aritmética modular. Un ejemplo de ello lo veremos en el Teorema 3.11.

¿Existe alguna forma de saber cuántas unidades tiene un anillo determinado $\mathbb{Z}_n$? Por el Teorema anterior sabemos que $[a]$ será unidad (es decir, existe $[a]^{-1}$) si y sólo si $mcd(a,n) = 1$. Por lo tanto, el número de unidades de $\mathbb{Z}_n$ es el número de enteros a tales que $1 \leq a < n$ y $mcd(a,n) = 1$. Este valor podemos obtenerlo, como se acaba de señalar, mediante la función Φ de Euler: $\#\mathbb{Z}_n^* = \Phi(n)$.

Teorema 3.11.: Teorema de EULER. Para todo par de enteros a y n relativamente primos se cumple que $a^{\Phi(n)} \equiv 1(mod\ n)$.

El Teorema pequeño de Fermat queda como corolario del teorema de Euler.

Este teorema permite hallar de forma inmediata el inverso de cualquier elemento $a \in \mathbb{Z}_n^*$: $a^{\Phi(n)-1} mod\ n$. Todo $a \in \mathbb{Z}_n$ será unidad (pertenecerá a $\mathbb{Z}_n^*$) si $mcd(a,n) = 1$. Si n es primo, entonces $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$.

Un corolario inmediato de este teorema, que constituye un fundamento matemático para el algoritmo de cifrado RSA (y que se presentará más adelante), es que para todo par de enteros a y n relativamente primos, donde $n = p \cdot q$, ambos primos, se cumple que $a^{\Phi(n)+1} = a^{(p-1)(q-1)+1} \equiv a(mod\ n)$.

Definición 3.11. Sea $a \in \mathbb{Z}_n^*$ Si el orden de a es $\Phi(n)$ entonces decimos que a es un **GENERADOR**. Si tiene un generador, entonces decimos que $\mathbb{Z}_n^*$ es cíclico (ver definición 2.11).

Definición 3.12. Sea $a <\in \mathbb{Z}_p^*$. Si el orden de a es máximo, es decir, $\mathcal{O}(a) = p - 1$ entonces decimos que a es un **ELEMENTO PRIMITIVO** de $\mathbb{Z}_p^*$.

Es inmediato deducir que un elemento generador de un grupo $\mathbb{Z}_n^*$ donde n es primo es siempre un elemento primitivo.

4. UNA PRESENTACIÓN "VISUAL" DE LA ARITMÉTICA MODULAR, ORIENTADA A LA COMPLETA COMPRENSIÓN DE LA EXISTENCIA DE INVERSOS Y OTROS CONCEPTOS PREVIOS INTRODUCIDOS.

¿Cuándo se puede decir que es posible encontrar un inverso (ver definición 2.3.) en aritmética modular: un valor que multiplicado por otro, y reducido el producto al módulo o cardinal del conjunto, dé como resultado el valor 1? La respuesta a esta pregunta ha quedado recogida en la Definición 3.8. o en el Teorema 3.8.: un elemento $a \in \mathbb{Z}_n$ será unidad (tendrá inverso) si y sólo si $mcd(a,n) = 1$.

15	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	**1**	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	**1**	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	**1**	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	4	11	3	10	2	9	**1**	8
8	8	**1**	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	**1**	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	**1**	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	**1**

Cuadro 1: Productos en aritmética modular, módulo 15.

Veamos, por ejemplo, el Cuadro 1, que recoge todos los productos entre los elementos del conjunto $\mathbb{Z}_{15} - \{0\}$. Quedan señalados en recuadro aquellos productos cuyo valor es el elemento neutro del producto y que, por lo tanto, sus

factores son elementos unidad (definición 2.3.). Y quedan señalados en un recuadro sombreado aquellos productos de productos cuyo valor es el cero y que, por tanto, sus factores son divisores de cero (definición 2.4.). Efectivamente, se observa que los productos iguales a cero se realizan entre elementos de $\mathbb{Z}_{15}$ que no son unidad, es decir, que no tienen inverso. Esos elementos verifican que $mcd(a,15) \neq 1$. Y los elementos que son unidad verifican que $mcd(a,n) = 1$: es el conjunto que se ha llamado conjunto reducido de residuos, y que se denota como $\mathbb{Z}_{15}^*$. Como ya indicamos, el conjunto de divisores de cero será $\overline{\mathbb{Z}_{15}} = \mathbb{Z}_{15} - \mathbb{Z}_{15}^* - \{0\}$.

Cualquier producto en el que intervenga un elemento $c \in \overline{\mathbb{Z}_{15}}$ (un divisor de cero) da como resultado otro elemento de $\overline{\mathbb{Z}_{15}}$, o el cero. De la misma manera, se puede ver que en todos los productos de un determinado c tal que $mcd(c, n = 15 = d > 1$ sólo aparecen valores x de $\mathbb{Z}15$ tales que $mcdx, n = d$. Los ceros aparecen en los productos de dos elementos de $\overline{\mathbb{Z}_{15}}$ que no comparten máximo común divisor. Se puede enunciar esto último diciendo que:

1. Si a y b pertenecen al conjunto $\{0,3,6,9,12\}$ (múltiplos de uno de los factores del módulo: el factor 3), entonces la expresión $a \cdot x \equiv b(mod\ 15)$ tiene tres soluciones. Por ejemplo, la congruencia lineal (ver definición 3.7.) $9 \cdot x \equiv 3(mod\ 15)$ tiene como soluciones los valores $x = 2,7,12$. Así se puede ver y comprobar en el Cuadro 1.

2. Si a y b pertenecen al conjunto $\{0,5,10\}$ (múltiplos de uno de los factores del módulo: el factor 5), entonces la expresión $a \cdot x \equiv b(mod\ 15)$ tiene cinco soluciones. Por ejemplo, la congruencia lineal $5 \cdot x \equiv 5(mod\ 15)$ tiene como soluciones los valores $x = 1,4,7,10,13$. Así se puede comprobar en el Cuadro 1.

3. Si a y b pertenecen al conjunto $\{1,2,4,7,8,11,13,14\}$ (elementos que son coprimos con el módulo 15) entonces la expresión $a \cdot x \equiv b(mod\ 15)$ tiene una solución única. Son los elementos que se han llamado unidades.

Cada elemento de $\mathbb{Z}_{15}^*$ tiene un inverso y solo uno. El conjunto $\mathbb{Z}_{15}^*$ tiene una estructura de grupo abeliano. Es evidente sin embargo que en este nuevo conjunto, definido a partir de $\mathbb{Z}_{15}$, por eliminación de todos los divisores de cero y el mismo cero, no tiene definida una operación suma que verifique la propiedad de clausura. El conjunto $\mathbb{Z}_{15}^*$ y sus productos vienen representados en el Cuadro 2. En ese conjunto, y gracias a lo señalado antes, a la vista del Cuadro 1, la operación producto sí es operación que verifica esa propiedad de clausura.

15	1	2	4	7	8	11	13	14
1	**1**	2	4	7	8	11	13	14
2	2	4	8	14	**1**	7	11	13
4	4	8	**1**	13	2	14	7	11
7	7	14	13	4	11	2	**1**	8
8	8	**1**	2	11	4	13	14	7
11	11	7	14	2	13	**1**	8	4
13	13	11	7	**1**	14	8	4	2
14	14	13	11	8	7	4	2	**1**

Cuadro 2: Productos del conjunto reducido de residuos módulo 15.

Queda claro, a la vista de estos dos primeros cuadros, el enunciado del teorema general de la existencia de inversos (Teorema 3.8.).

Como también sabíamos y cabía esperar, el orden del grupo $\mathbb{Z}_{15}^*$ (definición 2.10), que es el número de elementos del grupo, viene definido por la función de Euler, que en el caso del módulo $n = 15$, producto de los primos $p = 3$ y $q = 15$, es igual (definición 3.10., a y c) al producto de $(p-1)\cdot(q-1) = 8$.

En el Cuadro 3 quedan recogidos los elementos y sus productos para el caso de un módulo primo: en este caso se muestra el módulo $n = 17$. Ahora, con un módulo primo, todos los valores $0 < a < 17$ verifican que $mcd(a, 17) = 1$. Por tanto, cualquier expresión de la forma $a \cdot x \equiv b(mod\ 17)$, donde $0 < b < 17$ tiene una solución única. Y única es la solución para cada valor de a cuando tomamos $b = 1$: en ese caso la solución x será el inverso de a módulo 17. Son los casos recuadrados del Cuadro 3.

Todos los valores recogidos en el intervalo $[1, 16]$ son necesariamente incongruentes entre sí módulo 17 y este intervalo es, por tanto, un conjunto completo de residuos (ver definición 3.6.).

Otra cuestión, una vez se sabe si un elemento de un conjunto de residuos es

unidad o no, es determinar el elemento inverso que le corresponde. Para la respuesta a esta pregunta se dispone de la definida función de Euler (definición 3.10). Gracias al Teorema de Euler (Teorema 3.11) se puede obtener, para un elemento unidad, su inverso correspondiente. Es evidente que el Teorema pequeño de Fermat (Teorema 3.10) es un caso concreto o un corolario del Teorema de Euler: cuando trabajamos en un conjunto $\mathbb{Z}_p^*$ cuyo módulo p es primo, entonces $\Phi(p) = (p-1)$.

17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	**1**	3	5	7	9	11	13	15
3	3	6	9	12	15	**1**	4	7	10	13	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	**1**	5	9	13
5	5	10	15	3	8	13	**1**	6	11	16	4	9	14	2	7	12
6	6	12	**1**	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	**1**	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	**1**	9
9	9	**1**	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	**1**	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	13	7	**1**	12	6
12	12	7	2	14	9	4	16	11	6	**1**	13	8	3	15	10	5
13	13	9	5	**1**	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	**1**	15	12	9	6	3
15	15	13	11	9	7	5	3	**1**	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	**1**

Cuadro 3: Productos en aritmética modular, módulo 17.

De todo lo mostrado hasta el momento se puede presentar una importante conclusión, que es todo un enunciado: Dado el conjunto de los enteros $\mathbb{Z}$, que tiene estructura algebraica de anillo, y dado un entero $p \in \mathbb{Z}$ primo, entonces el conjunto $\mathbb{Z}/p\mathbb{Z}$ (que se puede definir por extensión tomando un representante de cada clase de equivalencia, y en concreto tomando los enteros x comprendidos

en el intervalo $0 \leq x < p-1$) es un conjunto finito formado por p clases de equivalencia, y $\mathbb{Z}_p$ tiene estructura de cuerpo (definición 2.6.).

17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	15	13	9	**1**	2	4	8	16	15	13	9	1
3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	**1**
4	4	16	13	**1**	4	16	13	1	4	16	13	1	4	16	13	1
5	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	**1**
6	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	**1**
7	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	**1**
8	8	13	2	16	9	4	15	**1**	8	13	2	16	9	4	15	1
9	9	13	15	16	8	4	2	**1**	9	13	15	16	8	4	2	1
10	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	**1**
11	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	**1**
12	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	**1**
13	13	16	4	**1**	13	16	4	1	13	16	4	1	13	16	4	1
14	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	**1**
15	15	4	9	16	2	13	8	**1**	15	4	9	16	2	13	8	1
16	16	**1**	16	1	16	1	16	1	16	1	16	1	16	1	16	1

Cuadro 4: Potencias módulo 17. La primera columna recoge las bases. La primera fila los exponentes.

Ha quedado claro que la condición de módulo primo es siempre garantía de existencia de inversos. Si se trabaja en una aritmética con módulo n compuesto, el conjunto $\mathbb{Z}_n$ tiene entonces estructura de anillo conmutativo, y entonces al menos se puede asegurar que todo entero coprimo con n (definición 1.8.) tiene inverso. Cuanto mayor sea el valor de la función de Euler (cuantos menos primos factoricen al compuesto y cuanto mayor sea el menor de los primos que lo componen) mayor será el cardinal de las unidades y por tanto más números del intervalo $[0, n-1]$ tendrán inverso en el anillo $\mathbb{Z}_n$.

Para la completa presentación de los conceptos de la aritmética modular, y en concreto para una muestra completa de estos teoremas, de la función de Euler, y otros conceptos previamente presentados, es útil contemplar un cuadro de potencias para un conjunto $\mathbb{Z}_p$ que sea cuerpo: es decir, p primo (ver definición 2.6. y Teorema 3.9.). En el Cuadro 4 quedan recogidos todos los valores de potencia del conjunto $\mathbb{Z}_{17}^*$, tomando como exponentes todos los valores comprendidos entre uno y el valor de la función de Euler: 16 en este caso.

Han quedado señalados con un recuadro las primeras apariciones del valor uno en las potencias de los elementos de $\mathbb{Z}_{17}^*$. Del análisis del cuadro se pueden recalcar algunos conceptos ya presentados:

Los elementos 3, 5, 6, 7, 10, 11, 12 y 14 son elementos generadores (ver definición 3.13). Por ser el módulo ($n = 17$) un valor primo, entonces todos estos elementos generadores son también elementos primitivos (ver definición 3.14.). En sus correspondientes filas se pueden ver <u>todos</u> los elementos de $\mathbb{Z}_{17}^*$ obtenidos mediante las sucesivas potencias. Se alcanza la potencia igual a 1 con el exponente igual al valor de la función de Euler: 16.

15	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1	2	4	8	1	2	4
4	4	1	4	1	4	1	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	8	4	2	1	8	4	2	1	8	4	2	1	8	4
11	11	1	11	1	11	1	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	14	1	14	1	14	1	14	1	14	1	14	1	14	1

Cuadro 5: Potencias de $\mathbb{Z}_{15}^*$. La primera columna recoge las bases. La primera fila los exponentes.

Las potencias de cualquier elemento $a \in \mathbb{Z}_{17}^*$ deben repetirse a partir de un determinado exponente. Para todo $a \in \mathbb{Z}_{17}^*$ existe un α mínimo que verifica que $a^\alpha = 1$. Este valor de α, que se ha llamado orden del elemento (ver definición

2.13), como se ve en el Cuadro 4, es 2, ó 4 u 8, ó 16: así lo enuncia además el **Teorema de Lagrange** (Teorema 2.4.): los divisores de $(p-1)$.

El **Teorema pequeño de Fermat** (Teorema 3.10) queda perfectamente evidenciado en el Cuadro 4: todas las potencias con exponente $(p-1)=16$ son iguales a uno.

En el Cuadro 5, que recoge las potencias de $\mathbb{Z}_{15}^*$, se puede ver el comportamiento de las potencias con exponente $\Phi(n=15)=8$ de acuerdo con el **Teorema de Euler** (Teorema 3.11). En este Cuadro 5 se ve que el orden de todos los elementos de $\mathbb{Z}_{15}^*$ es divisor de 8: ó 2 ó 4. Este conjunto no tiene ningún elemento que sea generador.

Abundando en el orden de los elementos de ambos conjuntos ($\mathbb{Z}_{17}^*$ y $\mathbb{Z}_{15}^*$) al ver que $\mathbb{Z}_{15}^*$ no tiene ningún elemento generador queda claro que $\mathbb{Z}_{15}^*$ no es un grupo cíclico. Sí lo es $\mathbb{Z}_{17}^*$, que tiene varios elementos generadores. Así debía ser, visto el Teorema 2.6. Los subgrupos que se ven en el Cuadro 4, deben ser todos ellos cíclicos (cfr. Teorema 2.7.). Estos subgrupos de $\mathbb{Z}_{17}^*$ son cuatro (ver definición 2.12.): $G_1=\langle 2\rangle=\langle 8\rangle=\langle 9\rangle=\langle 15\rangle=\{1,2,4,8,9,13,15,16\}$; $G_2=\langle 4\rangle=\langle 13\rangle=\{1,4,13,16\}$; $G_3=\langle 16\rangle=\{1,16\}$; $G_4=\langle 1\rangle=\{1\}$ (que es un subgrupo trivial).

17	1	2	4	8	9	13	15	16
1	1	2	4	8	9	13	15	16
2	2	4	8	16	1	9	13	15
4	4	8	16	15	2	1	9	13
8	8	16	15	13	12	2	1	9
9	9	1	2	12	13	15	16	8
13	13	9	1	2	15	16	8	4
15	15	13	9	1	16	8	4	2
16	16	15	13	9	8	4	2	1

17	1	16
1	1	16
16	16	1

17	1	4	13	16
1	1	4	13	16
4	4	16	1	13
13	13	1	16	4
16	16	13	4	1

Cuadro 6:
Subgrupos del Grupo $\mathbb{Z}_{17}^*$.
Falta el subgrupo trivial formado por la unidad.

En el Cuadro 6 podemos comprobar que, efectivamente, estos cuatro conjuntos tienen estructura de grupo para el producto (no queda recogido G_4). El primero de los subgrupos (G_1) está formado por todos los elementos de $\mathbb{Z}_{17}$ excepto los

elementos primitivos; al segundo (G_2) también se le han eliminado los elementos de orden 8; al tercero (G_3) se le han eliminado además los elementos de orden 4, quedando únicamente un elemento de orden 2 y el uno.

En el caso del conjunto $\mathbb{Z}_{15}^*$ los subgrupos que se pueden tomar son el generado por los valores 2 u 8 ($g_1 = \langle 2 \rangle = \langle 8 \rangle = \{1, 2, 4, 8\}$); el generado por los valores 7 ó 13 ($g_2 = \langle 7 \rangle = \langle 13 \rangle = \{1, 4, 7, 13\}$); y los generados por los valores 4 ($g_3 = \langle 4 \rangle = \{1, 4\}$), 11 ($g_4 = \langle 11 \rangle = \{1, 11\}$), ó 14 ($g_5 = \langle 14 \rangle = \{1, 14\}$). También en este caso tenemos el subgrupo trivial, formado por el valor 1. Como señala el Teorema 2.2., todos estos subconjuntos tienen estructura de grupo.

Una última observación, de la mano del Cuadro 7, en el que se aprecian valores que se han llamado nilpotentes (definición 2.7.). Han quedado marcados con un recuadro las primeras apariciones de el valor cero en las sucesivas potencias en cada elemento nilpotente del conjunto $\mathbb{Z}_{16}^*$. **Se tienen elementos nilpotentes siempre que se trabaja con un módulo en cuya factorización aparezca un primo más de una vez**. En este caso concreto, $n = 16 = 2^4$. En el caso, por ejemplo, de $n = 12 = 2^2 \cdot 3$ tenemos un elemento nilpotente en el valor $6 = 2 \cdot 3$: $6^2 mod\ 12 = 0$.

16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	8	0	0	0	0	0	0	0	0	0	0	0	0
4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6	4	8	0	0	0	0	0	0	0	0	0	0	0	0
8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	10	4	8	0	0	0	0	0	0	0	0	0	0	0	0
12	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	14	4	8	0	0	0	0	0	0	0	0	0	0	0	0

Cuadro 7: Potencias módulo 16. Elementos nilpotentes.

Evidentemente, todas las matemáticas presentadas en este epígrafe adolecen de su rigor: sirven para una primera toma de contacto con estos conceptos.

5. CÁLCULO DEL INVERSO EN UNA ARITMÉTICA MODULAR CON MÓDULO COMPUESTO DEL QUE SE DESCONOCEN SUS FACTORES.

La búsqueda de los valores inversos de los elementos que son unidad es tarea sencilla, como ya ha quedado dicho. Un elemento cualquiera x tendrá inverso módulo n si y sólo si se verifica que $mcd(x,n) = 1$ Si n es primo bastará acudir al Teorema pequeño de Fermat (Teorema 3.10). Si n es compuesto el inverso de x se obtiene gracias al Teorema de Euler, a partir del valor calculado de la función de Euler (definición 3.10.).

Pero… ¿Qué ocurre en el caso en que se desconoce el valor de la función de Euler porque se desconocen los factores primos que componen n? Cabría pensar que basta con factorizar primero n y una vez obtenidos esos primos calcular de forma inmediata el valor de la función de Euler. Y ciertamente es así. Pero factorizar un entero es, hoy por hoy, un reto de una complejidad computacional demasiado alta: no se disponen de algoritmos eficientes para lograr obtener los factores primos que componen un entero. La complejidad de la factorización de enteros aumenta de forma exponencial con el tamaño de los primos que componen el entero que se desea factorizar.

Se dispone de otro camino para encontrar el inverso de este valor x: el algoritmo extendido de Euclides (definición 1.6.). Ahora se presenta un desarrollo más extenso de este algoritmo y de las sucesiones de valores que se generan en su proceso.

Sea a coprimo con n. (Si $mcd(a,n) \neq 1$ entonces no cabe buscar un inverso que no existe: cfr. definición 3.8. y teorema 3.8.) El inverso de a será un entero b que verifique que $1 \equiv a \cdot b(mod\, n)$. El proceso de búsqueda de inverso mediante el **algoritmo extendido de Euclides** descansa en el proceso de búsqueda del valor de $mcd(a,n)$, que evidentemente será 1. El proceso comienza con los valores $x_0 = n$, $x_1 = a$ y va generando sucesivamente valores $x_{i+1} \equiv x_{i-1}(mod\, x_i)$ y $q_i = x_{i-1}/x_i$ hasta llegar a un valor $x_{k+1} = 0$. El valor previo (x_k) será igual a 1, pues ese debe ser el máximo común divisor entre a y n.

En el proceso ya antes descrito se generan varias sucesiones finitas de la siguiente forma presentada:

Valores iniciales: $s_0 = 1;\ s_1 = 0;\ t_0 = 0;\ t_1 = 1.$

Generación de las secuencias: $s_j = s_{j-2} - q_{j-1} \cdot s_{j-1}$; $t_j = t_{j-2} - q_{j-1} \cdot t_{j-1}$.

Relación entre ambas secuencias: $x_j = s_j \cdot n + t_j \cdot a$.

N = 2668; a = 157. Ambos valores son coprimos.
Las sucesiones xi y qi son las siguientes:
x0 = 2668
x1 = 157 q1 = 16
x2 = 156 q2 = 1
x3 = 1 q3 = 156
x4 = 0 FIN

Las sucesiones si y ti son las siguientes:
s0 = 1 s1 = 0 t0 = 0 t1 = 1
s2 = s0 - q1 · s1, es decir, s2 = 1 –16 · 0 **= +1**
t2 = t0 – q1 · t1, es decir, t2 = 0 –16 · 1 **= -16**
s3 = s1 – q2 · s2, es decir, s3 = 0 – 1 · 1 **= -1**
t3 = t1 – q2 · t2, es decir, t3 = 1 – 1 ·(-16) **= +17**

Aplicamos los resultados:
x3 = s3 · N + t3 · a, es decir, 1 = (-1)·2668 + 17·157.

Y aplicando módulo 2668 a ambos lados de la ecuación...
1 = 1 modulo 2668 = 17·157 modulo 2668, es decir:

$1 \equiv 17 \cdot 157 \pmod{2668} \Rightarrow$ **$17 \equiv 157^{-1} \pmod{2668}$**

Cuadro 8: Ejemplo de aplicación del algoritmo extendido de Euclides para la búsqueda de un inverso en aritmética modular.

Se calculan los sucesivos elementos de las dos sucesiones t_k y s_k hasta llegar al valor $x_k = 1$. Entonces se habrá llegado a una expresión de la forma $1 = s_k \cdot n + t_k \cdot a$, y aplicando a ambos lados de la expresión el operador $mod\, n$ se llega a que $1 \equiv 0 + t_k \cdot a(mod\, n)$: se tiene, por tanto, un valor t_k que es el inverso de a.

Un ejemplo de este proceso viene recogido en el artículo antes citado de Rivest, Shamir y Adleman [2], en su epígrafe VII.D. Queda recogido en el Cuadro 8, por su interés histórico y también para clarificar este método que es tan usado para la generación de claves del criptosistema RSA. El ejemplo calcula el inverso del valor $a = 157$ módulo el valor $n = 2668$. Como se ve en él, se procede al cálculo de las dos sucesiones s_i y t_i y se llega al valor $t_3 = 17$, que resulta ser el inverso módulo 2668 del valor $a = 157$.

El algoritmo extendido de Euclides es muy sencillo de implementar.

SEGUNDA PARTE.
PROTOCOLO RSA

Cualquier texto plano almacenado en un sistema informático queda codificado mediante ceros y unos. Un texto plano cualquiera puede ser expresado por tanto como un valor numérico tanto más grande cuanto mayor sea el volumen de información codificada. Por ejemplo, "RSA" puede quedar codificado mediante estas tres letras. También pueden ser codificadas por sus valores ASCII que codifican a cada una de las tres letras: 'R' = 82; 'S' = 83; 'A' = 65. En código binario sería: 'R' = 01010010; 'S' = 01010011; 'A' = 01000001. Y concatenando las tres secuencias de bits tenemos que la cadena "RSA" tiene el valor binario 0101 0010 0101 0011 0100 0001 (0x525341), que el base 10 es el entero 5.395.265. Y así, cualquier cadena de caracteres puede quedar unívocamente representada como un valor numérico. O como una secuencia de números si lo que se pretende es "expresar" la información mediante una secuencia de valores numéricos menores que en entero dado como límite superior: en ese último caso, bastará fraccionar el texto plano en bloques siempre menores que una longitud máxima. Y así, se pueden definir procesos de codificación basados en procedimientos matemáticos.

6. ALGORITMO RSA.

Las matemáticas vistas en esta presentación ofrecen suficiente fundamento teórico para la correcta comprensión del algoritmo introducido en 1978 por Rivest, Shamir y Adleman [2] y que se conoce como RSA. Es el criptosistema de clave pública o asimétrico más ampliamente usado. El funcionamiento del criptosistema RSA descansa en las propiedades de la operación **exponenciación en aritmética modular** presentadas en la primera parte.

Sea $m \in \{1, n-1\}$ el mensaje plano, o un bloque del mensaje plano, que se desea cifrar mediante el criptosistema RSA. La operación de cifrado RSA es $c = m^e mod\, n$, donde e y n constituyen los valores de la clave pública de cifrado y se conocen como **EXPONENTE DE CIFRADO** y **MÓDULO DEL CRIPTOSISTEMA**.

La operación de descifrado es $m = c^d mod\, n$, donde d (junto con los factores de n) son las claves privadas del criptosistema; d y n son las claves del descifrado. Al valor de d se le llama **EXPONENTE DE DESCIFRADO**.

RSA necesita, para la generación de sus claves d y e, del **cálculo de inversos en aritmética modular**. La complementariedad existente entre las dos claves de exponente (d y e) y el valor del módulo (n) se basa en el teorema de Euler (Teorema 3.11.). **Basta exigir** (más adelante se verá) **que $\boldsymbol{e \cdot d \equiv 1 (mod\, \Phi(n))}$ para que la función de descifrado sea la inversa de la de cifrado**.

El **protocolo** a seguir **para la generación de claves de RSA** es el siguiente:

1. Cada usuario U elige dos números primos (en el uso práctico se buscan primos de gran tamaño), p y q, y calcula $n = p \cdot q$. El grupo multiplicativo en el que se trabajará será, por tanto $\mathbb{Z}_n^*$. El orden del grupo será $\Phi(n) = \Phi(p \cdot q) = (p-1) \cdot (q-1)$. **Quien desconozca los factores de n no podrá calcular el valor de la función** $\Phi(n)$.
2. U selecciona un entero positivo e de forma que $1 < e < \Phi(n)$ y de forma que sea coprimo con el orden del grupo: $mcd(\Phi(n), e) = 1$
3. U calcula el inverso de e en $\mathbb{Z}_{\Phi(n)}^*$, que será d. Tendremos que $e \cdot d \equiv 1 (mod\, \Phi(n))$, con $1 < d < \Phi(n)$ y d también coprimo con $\Phi(n)$. Como ha quedado explicado, para calcular el inverso de e módulo $\Phi(n)$ utilizamos el algoritmo extendido de Euclides. Se está buscando el inverso de e en una aritmética $mod\, \Phi(n)$ y no en una aritmética $mod\, n$; lo buscamos en $\mathbb{Z}_{\Phi(n)}^*$ y no en $\mathbb{Z}_n^*$.
4. La clave pública del usuario será (n, e). La clave privada será (n, d). Por supuesto, deben permanecer secretos los números p y q y especialmente $\Phi(n)$.

Como ya ha quedado dicho previamente, las operaciones de cifrado y descifrado son

Cifrado: $c = E_e(m) = m^e mod\, n$

Descifrado: $m = D_d(c) = c^d mod\, n$

Donde el mensaje m se obtiene asociando, a cada carácter del alfabeto en que está escrito el mensaje, un valor numérico. Se tiene así un mensaje m a cifrar de una longitud indefinida y, en principio, grande. Este mensaje m se divide en bloques m_i, cada uno de ellos con un valor numérico menor que n. El módulo del

criptosistema determina el límite superior de los tamaños de los mensajes a codificar.

El mensaje cifrado, c, tendrá un tamaño similar en cada uno de sus bloques c_i . Cada bloque se cifra haciendo $c_i = m_i^e mod\ n$ y se descifra haciendo $m_i = c_i^d mod\ n$.

El motivo de que la exponenciación del mensaje cifrado con d sea la operación inversa a la exponenciación del mensaje plano con e queda manifiesto en el modo en que han sido definido los dos exponentes:

$c_i^d = (m_i^e)^d = m_i^{e\cdot d} = m_i \cdot m_i^{e\cdot d-1} = m_i \cdot m_i^{k\cdot\Phi(n)} \equiv m_i mod\ n = m_i$.

Para ello se ha tenido en cuenta que:

1. $e \cdot d \equiv 1(mod\ \Phi(n))$: así se ha buscado el valor de d: por tanto, $e \cdot d - 1 = k \cdot \Phi(n)$.
2. Teorema de Euler (Teorema 3.11.): $m_i^{\Phi(n)} mod\ n = 1$.
3. Se ha supuesto que $mcd(m_i, n) = 1$. De lo contrario el Teorema de Euler no se cumple. Esta disposición no limita el uso de este criptosistema, porque la probabilidad de que no se cumpla esta condición, en el rango de tamaños de los primos p y q y que se emplean para un uso seguro del criptosistema RSA, es enormemente baja.

Una última y breve observación: Si el propietario de un par de claves de RSA (pública e y n, privada d) "cifra" un mensaje con su propia clave privada d, ($c' = m^d(mod\ n)$) entonces todos aquellos que dispongan de su clave pública e podrán "descifrar" ese mensaje y recuperar el mensaje plano original ($m = c'^e(mod\ n) = m^{d\cdot e}(mod\ n)$). Y en ese caso, aunque no se habrá logrado confidencialidad, porque todos pueden llegar de nuevo al texto plano, sí se habrá logrado la autenticación del mensaje, o firma: porque únicamente el propietario de la clave privada d habrá podido realizar la operación correcta para llegar al criptograma c'.

Y aunque lo que se describe a continuación no es el procedimiento habitual para la firma electrónica, se puede ver fácilmente que si el usuario A dispone de las claves (e_A, d_A, n_A), y el usuario B dispone de las claves (e_B, d_B, n_B), entones si el usuario A envía a B el criptograma c_{AB}, donde $f_A = m^{d_A}(mod\ n_A)$; $c_{AB} = f_A^{e_B}(mod\ n_B)$, entonces el usuario B podrá, mediante su clave privada, llegar al valor de f_A (que, desde luego, será aún incomprensible); y luego, mediante la clave pública de A, podrá llegar al mensaje plano original m. Y así, porque sólo él tiene la clave d_B, sólo él puede "deshacer" la operación de exponenciación con su clave pública

e_B; y porque ha logrado "deshacer", con la clave pública de A, e_A, la operación realizada por A con su clave privada d_A, puede tener la certeza de que ha sido, efectivamente, A, quien le ha enviado el criptograma c_{AB}.

Antes de terminar este epígrafe de presentación de RSA, convendrá hacer una corta referencia a dos aspectos del proceso RSA: El primero es el de la complejidad computacional de sus algoritmos. Hay abundante documentación y bibliografía que presenta estas nociones. Pero sí es necesario comentar los modos computacionalmente eficientes de trabajar en RSA: en concreto, nos referimos al modo eficiente en que se puede realizar la operación de exponenciación. El segundo aspecto a reseñar es el de la generación de los primos necesarios para el diseño RSA.

EXPONENCIACIÓN MODULAR.

El cálculo de la clave privada n, obtenida a partir de e y de $\Phi(n)$ se realiza mediante el algoritmo extendido de Euclides. Ese algoritmo resulta muy eficiente. Pero hay que buscar alguna manera eficiente de calcular las exponenciaciones en aritmética modular: no podemos limitarnos a realizar productos y cálculo de restos tantas veces como indique el exponente, porque esa operación haría inviable el algoritmo.

Vamos a ver un algoritmo clásico para el cálculo de la potencia en aritmética modular.

El proceso de potencia no puede realizarse a fuerza de multiplicar la base por sí misma tantas veces como indique el exponente: si el exponente tiene un valor enorme como suele ocurrir habitualmente con los enteros largos, el cálculo de la potencia podría eternizarse.

Para realizar el cálculo de una expresión como $a^x \, mod \, n$ se pueden utilizar algunas técnicas que reducen el número de productos a efectuar. Una técnica muy usada es tomar módulo en sucesivos pasos intermedios. Por ejemplo: $a^8 mod \, n = (a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a) mod \, n$

Pero también podemos decir que $a^8 mod \, n = ((a^2 mod \, n)^2 mod \, n)^2$

Y si el exponente no es potencia de 2, hay que introducir simplemente una sencilla modificación. Por ejemplo, el número 25 queda representado en binario como 11001, es decir: $2^{25} = 2^{16} \cdot 2^8 \cdot 2^1$, y, por tanto: $a^{25} mod \, n = (a \cdot a^{16} \cdot a8 mod \, n = ((((a2 mod \, n \cdot a) 2 mod \, n) 2 mod \, n) 2 mod \, n) \cdot a \, mod \, n$

Necesitamos únicamente seis multiplicaciones.

Información sobre el proceso de exponenciación rápida podemos encontrarla, por ejemplo, en [Bres89]. De esa referencia hemos tomado el algoritmo recogido en Algoritmo 1, para el cálculo de $d = a^e mod\ n$, para $e \geq 0$.

1	Asignar	$d \leftarrow 1$; $E \leftarrow e$; $A \leftarrow a$
2	Mientras $E > 0$ Hacer	
	2.1. Si E es impar, Entonces	$d \leftarrow (d \cdot A) mod\ n$.
	2.2.	$E \leftarrow E/2$. (división entera)
	2.3.	$A \leftarrow A \cdot A\ mod\ n$.
3	Devolver	d.

Algoritmo 1: Algoritmo para el cálculo de potencias, donde tanto la base como el exponente pueden ser enteros grandes.

En C el código tomaría la siguiente forma:

```
typedef unsigned long uli;
uli potencia(uli base, uli exponente, uli modulo)
{
      uli R = 1;
      while(exponente)
      {
            if(exponente & 0x1) R = (R * base) % modulo;
            exponente >>= 1;
            base = (base * base) % modulo;
      }
      return R;
}
```

BÚSQUEDA DE PRIMOS.

RSA requiere el uso de primos de gran tamaño. Entre las características a exigir a esos primos del criptosistema RSA y que luego veremos, hay una principal: que sean de un tamaño suficientemente grande como para que no puedan obtenerse mediante la simple factorización de su producto $n = p \cdot q$.

No se pretende hacer una presentación sobre la generación de aleatorios y de pseudo-aleatorios; o sobre los test de primalidad o de pseudo-primalidad. Existen algoritmos muy variados para la generación de secuencias aleatorias. Y se dispone de algunos test de pseudo-primalidad, como por ejemplo el de Miller-Rabin, o el de Solovay-Strassen. Habitualmente se emplea el primero por ser más eficiente y de más sencilla implementación.

7. CRIPTOANÁLISIS DE RSA. PROPIEDADES EXIGIDAS A LOS PRIMOS QUE COMPONEN EL MÓDULO RSA Y A LAS CLAVES PARA GARANTIZAR SU FORTALEZA FRENTE A POSIBLES ATAQUES.

Un primer peligro que tiene el criptosistema RSA es la posible existencia de mensajes m que verifiquen la propiedad de que $m^e \equiv m(mod\, n)$. A estos mensajes se les llama **MENSAJES INOCULTABLES**. Está demostrado que el número de mensajes inocultables es

$\big(1 + mcd(e-1, p-1)\big) \cdot (1 + mcd(e-1, q-1))$.

Si se eligen p y q y n adecuadamente, el número de mensajes inocultables será muy bajo y su existencia no afecta a la seguridad del criptosistema.

Las características principales exigidas a los factores p y q, del módulo de RSA, se imponen precisamente por la necesidad de ocultar el valor de esos dos primos. La solidez del RSA descansa en la complejidad computacional en las operaciones de factorización de un entero de longitud grande.

De la aritmética elemental es conocido que todo entero n puede ser descompuesto en un producto de factores primos. Y así como resulta elemental conocer el valor de n a partir de sus factores primos, es computacionalmente inabordable el problema general de descomponer cualquier número n en sus factores primos.

RSA fundamenta su seguridad en la dificultad de factorizar números grandes. Sus dos claves (la pública e y la privada d) están vinculadas matemáticamente a través de una relación que mantienen con el cardinal del sistema reducido de residuos módulo n: el valor de la función $\Phi(n)$. Quien conozca el valor de $\Phi(n)$ podrá obtener, mediante el algoritmo extendido de Euclides, el valor de la clave privada d a partir de la clave pública e. Y para conocer el valor de $\Phi(n)$ es suficiente con conocer los factores de n. Los tiempos necesarios para la factorización de enteros puestos en relación con el tamaño de esos números nos indican el grado de seguridad del sistema.

El estudio de técnicas de factorización de números de gran tamaño, y todo posible avance para reducir tiempos en ese proceso, resulta de interés para la

criptografía. No es necesario señalar el interés matemático de la cuestión. El conocimiento de diferentes algoritmos que logran encontrar los factores primos de un determinado compuesto permite definir exigencias concretas que se deben dar en los enteros primos que componen el módulo n para el criptosistema RSA.

El procedimiento teóricamente más sencillo para la búsqueda de los factores primos de un entero dado cualquiera n, consiste en tomar una tabla de los primeros valores primos y proceder a calcular el módulo de dividir n por los sucesivos primos, comenzando por el primero de ellos (el 2). Cada vez que se encuentra un primo p que divide al candidato n se inicia el proceso a partir de ese primo, con $n \leftarrow n/p$. Y así, hasta llegar a $\sqrt{n}$.

Este proceso puede ser útil para enteros pequeños (que no superen el orden de 10^7), pero en cuanto aumenta el tamaño del número a factorizar y, más en concreto, cuando aumenta el tamaño de los primos que componen nuestro entero n, el procedimiento o algoritmo descrito se hace computacionalmente impracticable.

Un siguiente paso en los métodos de factorización se encuentra en el método Rho de Pollard. Este algoritmo está recogido en abundante bibliografía (por ejemplo, [7]). Es una algoritmo eficiente para enteros n en el rango entre 10^6 y 10^{12}.

Otros dos algoritmos útiles en este rango son el algoritmo $(p-1)$ de Pollard y el algoritmo $(p+1)$ de Williams. Ambos vienen documentados en diferentes libros de los señalados más abajo, en al apartado de referencias; especialmente en [7] o en [8]. Estos métodos factorizan con facilidad aquellos compuestos en los que alguno de sus primos sea tal que el entero que resulta de sumarle o restarle la unidad tenga todos sus factores primos menores que un límite superior: por ejemplo, menores que 10^4.

Estos algoritmos de factorización traen consigo unas primeras exigencias para los primos que se tomen para crear las claves del criptosistema RSA. Las propiedades que exigimos a los primos que componen el módulo RSA para garantizar la fortaleza del criptosistema frente a posibles ataques de factorización son las siguientes:

1. p y q deben tener aproximadamente la misma longitud, porque en la medida que un factor de n sea más pequeño, es tanto más fácil de obtener.
2. p y q no deben estar demasiado cerca, de forma que $p-q$ no sea

excesivamente pequeño (cfr. [9] Note 8. 8. ii.). Si son demasiado cercanos, entonces $p \cong \sqrt{n}$ y es sencillo buscarlo mediante el algoritmo de divisiones sucesivas.

3. $mcd(p-1, q-1)$ debe ser "pequeño". En caso contrario, si $mcd(p-1, q-1)$ es "grande", entonces el valor de
   $M = mcm(p-1, q-1) = \Phi(n)/(p-1) \cdot (q-1)$,
   es pequeño, y cada d' tal que $e \cdot d' \equiv 1(mod\, n)$ sirve para descifrar; esto es, se verifica que $m^{e \cdot d'} \equiv m(mod\, n)$ para todo mensaje m.
   Por tanto, si M es "relativamente pequeño" en comparación con el valor de $\Phi(n)$, entonces es computacionalmente posible encontrar un valor d' que rompa el criptosistema.
4. $p-1$ y $q-1$ deben tener un factor primo grande, para hacer frente a los algoritmos de factorización $(p-1)$ de Pollard, y $(p+1)$ de Williams.
5. d debe ser de longitud aproximadamente igual a la de n (cfr. [9], Fact 8. 4. iv.). Si se toma un valor del exponente de cifrado con una cantidad de bits menor que una cuarta parte del total de bits que tiene n, entonces se disponen de algoritmos eficientes para calcular d. Se puede elegir primero d aleatoriamente y luego calcular e.
6. Elegir un valor de e pequeño facilita el cifrado. El menor valor es $e = 3$. Recuérdese que el exponente e debe cumplir que $mcd\big(e, \Phi(n)\big) = 1$ y que el valor de $\Phi(n)$ en el protocolo RSA es siempre múltiplo de 4, por ser el producto de dos pares. Los valores habituales para el exponente de cifrado e son, además del 3, el 17 ó el 65.537 (que es igual a $2^{16}+1$) y que son números que sólo tienen dos unos en su codificación binaria. Estas características del exponente reducen mucho las operaciones de producto para exponenciar, y no compromete la seguridad del criptosistema. Con estas medidas la operación de cifrado es mucho más veloz que la de descifrado; y la operación de reconocimiento de firma mucho más veloz que la de firmado.

Todas estas propiedades o características de los primos p y q dificultan, con los algoritmos hoy conocidos, la factorización de $n = p \cdot q$. Como se ha visto antes, conocidos p y q es inmediato el cálculo de $\Phi(n)$, y es también entonces inmediato el cálculo de la clave privada d una vez se ha hecho pública su correspondiente clave e.

Las cuatro primeras propiedades ya fueron originariamente introducidas por los

autores del criptosistema RSA, y quedan recogidas, en un estilo algo informal, en el artículo [2]. La condición 1 se apunta en [2], apartado IX, A. La condición 2 se apunta en [2], apartado VII, B. La condición 3 queda recogida en [2], IX, C. La cuarta, en [2], IX, A. Y la quinta, de forma más velada, en el epígrafe V y en VII, C.

De forma adicional a estas cinco condiciones (la sexta es una recomendación de comodidad de computación, pero no otorga mayor seguridad al criptosistema), y en consideración a los posibles ataques de factorización, se exige actualmente a los primos que componen el módulo que sean primos robustos. Con esa exigencia, además, se garantiza el cumplimiento de la condiciones 3 y 4 antes señaladas.

Se dice que un primo p es un **PRIMO ROBUSTO** (cfr. Definición 4. 52, de [9]) si verifica las tres siguientes condiciones:

1. $p-1$ tiene un factor primo grande, r.
2. $p+1$ tiene también un factor primo grande, s.
3. $r-1$ tiene también un factor primo grande, t.

La tercera de las propiedades de los primos robustos es una protección contra otro ataque de fuerza bruta que consiste en el intento de obtención de texto plano, a partir del cifrado, mediante el llamado ataque cíclico (descrito en [9], §8, 2.2.vii.), que tiene posibilidades de tener éxito si no se verifica la característica tercera de los primos robustos.

El término "primo robusto" es una traducción del anglosajón "strong prime" ampliamente utilizado en la documentación científica sobre esta área de la ciencia matemática. Otra posible traducción al castellano de esta expresión es hablar de "**primos fuertes**".

Desde el inicio mismo de la existencia del criptosistema RSA ha estado abierto el debate sobre la necesidad de estas exigencias. Es cierto que tomando primos de gran tamaño es estadísticamente muy probable que ambos verifiquen que el valor obtenido al restarles uno tenga un factor primo grande. Finalmente, sin embargo, se ha llegado al consenso general sobre la necesidad de exigir que los primos sean robustos. No para la defensa frente al ataque procedente de un atacante externo, sino también y sobre todo para la defensa contra las insidias de los propios usuarios cuando diseñan y construyen sus propias claves. En circunstancias normales, la probabilidad de que, de forma fortuita o accidental,

se toman valores de claves débiles es extraordinariamente baja. Sin embargo, existe la posibilidad de que una de las partes haga trampa y de forma deliberada intente generar una clave débil. Luego, esa persona podría repudiar mensajes firmados por ella, argumentando que su clave ha sido rota por una atacante y ha sido, por tanto, suplantado.

Desde luego, se conocen y estudian otros muchos algoritmos de factorización de enteros, mucho más eficaces que los aquí señalados. En [13] se recoge un resumen de algunos de ellos.

REFERENCIAS BIBLIOGRÁFICAS DONDE ENCONTRAR MÁS AMPLIO DESARROLLO DE LAS DEFINICIONES Y TEOREMAS PRESENTADOS EN LOS EPÍGRAFES 1, 2 Y 3.

Definición 1.1.	[10] §1.4.; [5] §I.2.; [11] §1.2.; [3] D. 4.1.
Definición 1.2.	[10] Th. 1.7.; [3] T. 4.5.
Definición 1.3.	[9] 2.85.; [3] D. 4.2.
Definición 1.4.	[10] §3.2.; [11] §1.2.; [7] §1.2.; [9] 2.86; [3] D. 4.3.
Teorema 1.1.	[3] T. 4.6.
Teorema 1.2.	[10] Th. 3.6.; [3] T. 4.7.
Definición 1.5.	[10] §3.3.; [5] §I.2.; [11] A. 1.1.; [12] §4.3.; [7] §1.3. y A. 1.7.; [9] 2.104.
Definición 1.6.	[10] Th. 3.13.; [11] §1.2.; [9] 2.107.
Definición 1.7.	[10] §3.1.; [5] §I.2.; [9] 2.92.
Teorema 1.3.	[10] Th. 3.14.; [5] §I.2.; [11] §1.2.; [7] Th. 1.4.; [9] 2.97; [3] T. 4.11.
Definición 1.8.	[10] §3.2.; [9] 2.91.
Teorema 1.4.	[10] Th. 3.1.; [11] Th. 4.1.; [7] Th. 2.1. ; [9] 2.94; [3] T. 4.4.
Definición 2.1.	[4] 1.4.; [12] §4.1.; [8] D. A1.2.; [9] 2.162; [3] D. 16.1.
Definición 2.2.	[12] §4.1.; [8] D. A1.7.; [9] 2.175; [3] D. 14.1.
Definición 2.3.	[9] 2.178; [3] D. 14.2.c y 14.3.
Definición 2.4.	[3] D. 14.2.b.
Definición 2.5.	[12] §4.1.; [3] D. 14.4.a.
Definición 2.6.	[12] §4.1.; [9] 2.181; [3] D. 14.4.b.
Teorema 2.1.	[3] T. 14.8.
Definición 2.7.	[4] Pr 12.10.
Definición 2.8.	[4] Pr 12.13 y C. 13.16.
Definición 2.9.	[4] 2.1.; [9] 2.166; [3] D. 16.3.
Definición 2.10.	[4] §1A; [8] D. A1.3.; [9] 2.163; [3] D. 16.2.
Definición 2.11.	[4] §2A; [12] §4.1.; [8] D. A1.6.; [9] 2.167; [3] D. 16.14.
Teorema 2.2.	[4] §2A.
Definición 2.12.	[4] §2A; [9] 2.169.
Definición 2.13.	[4] §1A; [3] D. 16.7.
Teorema 2.3.	[4] 2.8.; [3] T. 16.6.
Teorema 2.4.	[4] 2.23; [8] Th. A1.3.; [9] 2.171; [3] T. 16.9.
Teorema 2.5.	[3] C. 16.1.
Teorema 2.6.	[3] corolario 16.2.
Teorema 2.7.	[4] 2.7.; [9] 2.172; [3] T. 16.8.
Teorema 2.8.	[4] 2.9.; [9] 2.172.
Definición 3.1.	[3] D. 7.1.
Definición 3.2.	[3] D. 7.2, D. 7.3, D. 7.4 y D. 7.7.

Definición 3.3.		[3] D. 7.21.
Definición 3.4.		[3] D. 7.22.
Teorema 3.1.		[3] T. 7.6.
Teorema 3.2.		[3] T. 7.7.
Teorema 3.3.		[3] T. 7.8.
Definición 3.5.		[10] §4.1.; [11] §4.3.; [1] §11.3.; [8] App 2.; [9] 2.110.; [3] D. 14.7.
Teorema 3.4.		[10] Th. 4.2.; [5] §I.3.; [9] 2.112.; [3] T. 14.11.
Definición 3.6.		[10] §4.1.; [12] §4.2.; [9] 2.113.
Teorema 3.5.		[10] Lemma 4.1.
Definición 3.7.		[10] §4.2.
Teorema 3.6.		[10] Th. 4.10.; [11] Pr. 2.2.
Definición 3.8.		[10] §4.2.; [5] Pr. I.3.1.; [11] Pr. 1.16.; [8] Th. A2.5. ; [9] 2.115; [9] 2.117.
Definición 3.9.		[10] §4.1.; [12] §4.2.; [1] §11.3.
Teorema 3.7.		[3] T. 14.12.
Teorema 3.8.		Ver definición 3.8. [3] T. 14.14.
Teorema 3.9.		[5] §I.3. C 1 of Pr I.3.1. ; [9] 2.184.; [3] T. 14.13.
Teorema 3.10.		[10] Th. 6.3.; [5] Pr. I.3.2.; [11] Th. 2.6.; [12] §8.2.; [1] §11.3.; [7] Th. 3.2.; [8] Th. A2.8.; [9] 2.127.
Definición 3.10.		[10] §6.3.; §7.1.; [5] §I.2.; [11] Ch. 3.; [12] §8.2.; [1] §11.3.; [9] 2.100.
Teorema 3.11.		[10] Th. 6.14.; [5] Pr. I.3.5.; [11] Th. 3.7.; [12] §8.2.; [1] §11.3.; [7] Th. 3.4.; [8] Th. A2.8.; [9] 2.126.
Definición 3.11.		[9] 2.131.
Definición 3.12.		[9] 2.131.

En general, una buena referencia para los conceptos de divisibilidad, congruencia y grupos es [15] en sus capítulos 1 y 3. Una referencia sencilla que presenta una breve descripción de los algoritmos matemáticos y de la base matemática básica para RSA es [16]: es un libro breve y sencillo.

REFERENCIAS

[1] "Applied Cryptography. Protocols, Algorithms and Source Code in C" Bruce Schneier. John Wiley & Sons, Inc. 2nd edition. 1996.

[2] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" R. L. Rivest, A. Shamir and L. Adleman. Communication of the ACM. Vol. 21, nº 2. February 1978. pages 120−130.

[3] "Matemáticas discreta y combinatoria. Una introducción con aplicaciones". Ralph P. Grimaldi. Prentice may. 3ª. Edición. 1998.

[4] "Algebra. A Graduate Course". I. Martin Isaacs. Brooks/Cole Publishing Company. 1994.

[5] "A course in Number Theory and Cryptography". Neal Koblitz. Graduate Text in Mathematics, 114. Springer. 2nd Edition 1994.

[6] "Técnicas Criptográficas de Protección de Datos". Amparo Fuster y otros. Ra–ma 2000.

[7] "Factorization and Primality Testing". David M. Bressoud. Springer−Verlag, 1989.

[8] "Prime Numbers and Computer Methods for Factorization". Hans Riesel. Birkhäuser Boston, Inc. 2nd edition, 1987.

[9] "Handbook of Applied Cryptography". A. Menezes, P. van Oorschot, and S. Vanstone. CRC Press, Inc. 1997.

[10] "Elementary Number Theory and its applications" Kenneth H. Rosen. Addison Wesley Longman, Inc. 4th edition. May 2000.

[11] "A Course in Computational Number theory". David Bressoud and Stan Wagon. Key College Publishing. Springer. 2000.

[12] "Cryptography and Network Security. Principles and practices". William Stallings. Prentice Hall. Pearson Education. Third edition. 2003.

[13] "El criptosistema RSA". Raúl Durán Díaz, Luis Hernández Encinas y Jaime Muñoz Masqué. Ra – Ma.

[14] "New Directions in Cryptography". Whitfield Diffie and Martin E. Hellman. IEEE Transactions on information theory, vol IT–22 nº 6, November 1976, pp. 644–654.

[15] "Algebra Lineal y Geometría". Manuel Castellet e Irene Llerena. Ed. Reverté, S.A., 2000.

[16] "The mathematics of ciphers. Number theory and RSA cryptography", S. C. Coutinho. A.K. Peters Ltd. 1999.