UNIDAD 1

Tema 2: ARITMETICA MODULAR

RSA

Discrete Mathematics and Its Applications (Cap. 4)

7ma. Ed.

1. DIVISIÓN DE LOS ENTEROS

Definición:
ALGORITMO DE LA DIVISION

- Si a,b $\in$ Z, con b > 0, entonces existen q, r $\in$ Z únicos tales que:

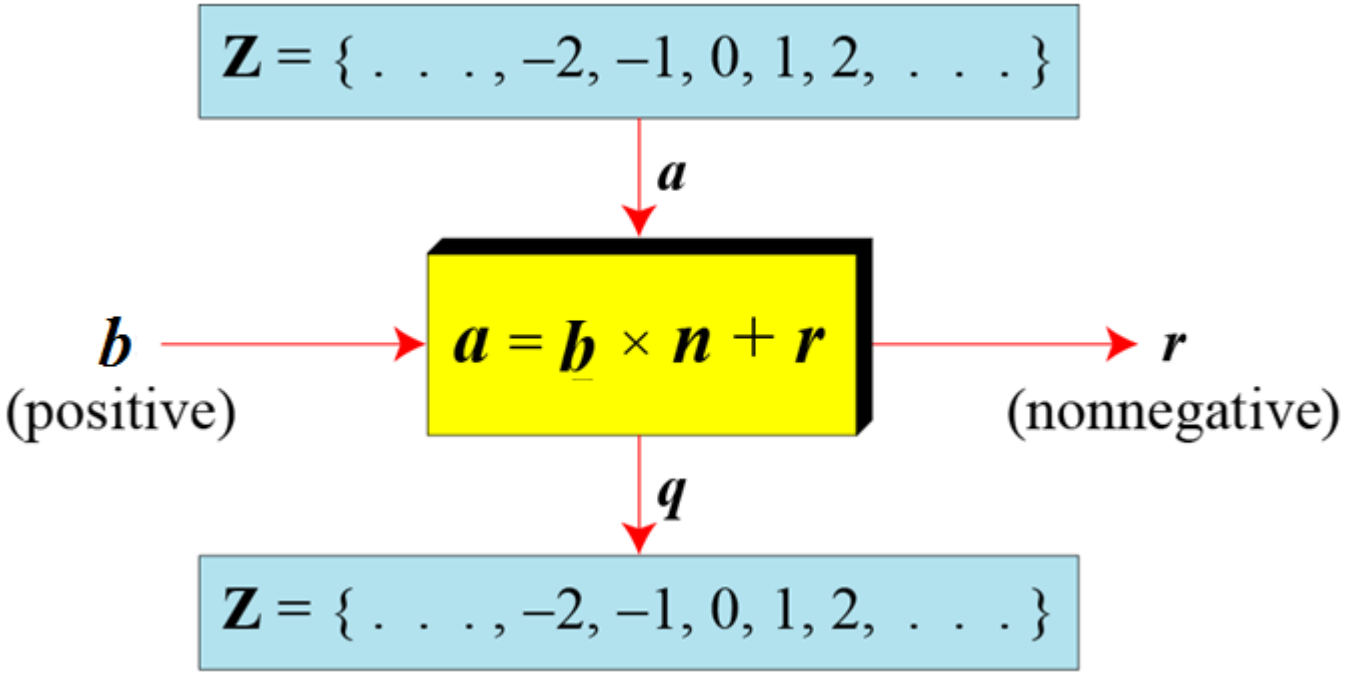
$$a = q \times b + r \quad \text{con } 0 \leq r < b$$

- El **residuo** de una división se denota como "a mod b", mientras el **cociente** se denota como a div b.

- Si a=16 y b=3 => 16 = 3.5 + 1, por tanto q=5, r=1

ALGORITMO DE LA DIVISION

- Dos restricciones:
  - Divisor un entero positivo (b>0)
  - Resto un entero no negativo (r≥0)



ARITMETICA MODULAR

PARTE 1

- **División**
- **Algoritmo de la división**

PARTE 2

- Aritmética Modular - Congruencia

PARTE 3

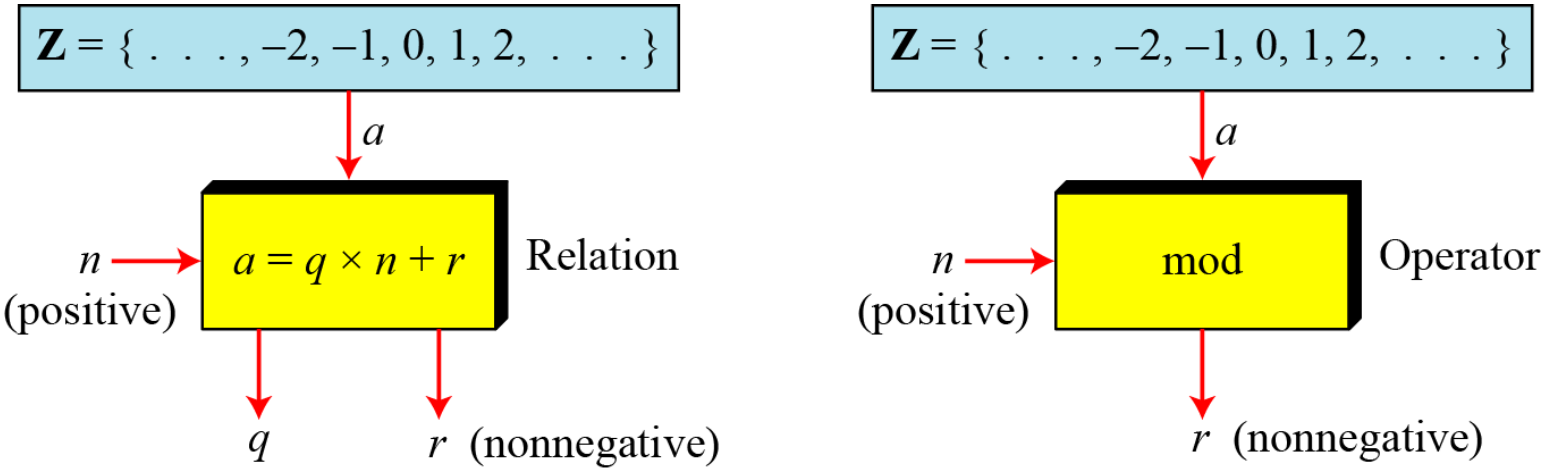
- Suma y Resta módulo de N
  - Criptografía de clave privada.
- Multiplicación y División módulo N
  - Criptografía de clave pública
- Inversa módulo N
- Exponenciación módulo N
- Aplicación RSA

PARTE 3

- Sistemas de ecuaciones módulo N.
- Teorema del Resto Chino

Operador módulo

- Algoritmos de la división y operador módulo



a mod n = r

Operador módulo

a mod n = r

- 27 mod 5
- 36 mod 12
- -18 mod 14
- -7 mod 10

Conjunto de residuos en Zn

- La operación de módulo crea un conjunto, que en aritmética modular es llamado como el conjunto mínimo de residuos módulo de n (Zn)

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$\mathbf{Z}_2 = \{ 0, 1 \}$ $\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$ $\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$

- Se tiene un conjunto de enteros Zn, pero tenemos infinitas instancias del conjunto de residuos.

Conjunto de Residuos Zn

- El resultado de la operación módulo n es siempre un entero entre 0 y n-1

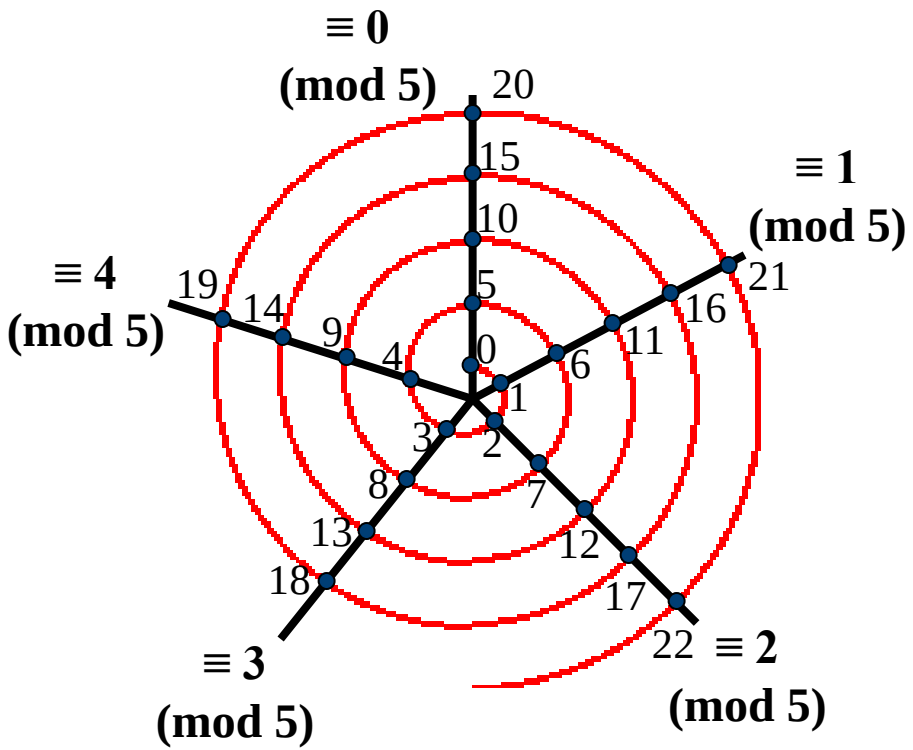
[0]	0	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90
[1]	1	7	13	19	25	31	37	43	49	55	61	67	73	79	85	91
[2]	2	8	14	20	26	32	38	44	50	56	62	68	74	80	86	92
[3]	3	9	15	21	27	33	39	45	51	57	63	69	75	81	87	93
[4]	4	10	16	22	28	34	40	46	52	58	64	70	76	82	88	94
[5]	5	11	17	23	29	35	41	47	53	59	65	71	77	83	89	95

Aritmética Modular

Congruencias

Congruencia en Criptografía

- Es igualdad.
- Mapear de Z a Zn no es de uno
  - ≡ (Mapea de muchos a uno)



1,6,11,16,21 son llamados congruente mod 5

$1 \equiv 6 \bmod 5$

Mapeo

- Relación de 1 a muchos

[0]	0	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90
[1]	1	7	13	19	25	31	37	43	49	55	61	67	73	79	85	91
[2]	2	8	14	20	26	32	38	44	50	56	62	68	74	80	86	92
[3]	3	9	15	21	27	33	39	45	51	57	63	69	75	81	87	93
[4]	4	10	16	22	28	34	40	46	52	58	64	70	76	82	88	94
[5]	5	11	17	23	29	35	41	47	53	59	65	71	77	83	89	95

CONGRUENCIAS MODULO N

- Si n ∈ Z+, n > 1. Para a,b ∈ Z, decimos que a es congruente con b módulo n, y escribimos a ≡ b(mod n), si

$$\mathbf{n \mid (a-b)}.$$

- Obs: a≡ b(mod n); si a=b+*k*n para algún *k* ∈ Z.
- Ejemplo:

$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

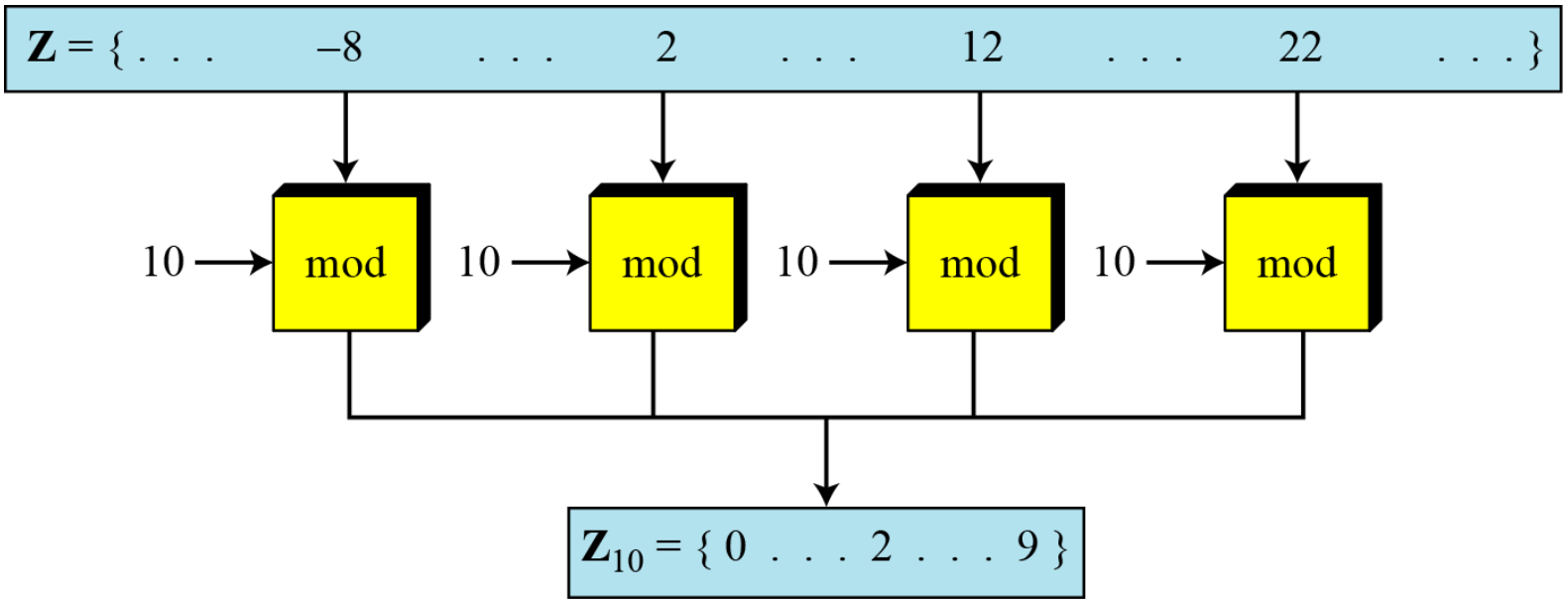
CONGRUENCIAS MODULO N

- Ejercicio:
  - 49 ≡ mod 8
  - -24 ≡ mod 8
  - 18 ≡ mod 8
  - -19 ≡ mod 8
  - 28 ≡ mod 8
  - 46 ≡ mod 8
  - -5 ≡ mod 8
  - 15 ≡ mod 8

CONGRUENCIAS MODULO N

- Propiedades:
  - $a \equiv a \pmod{n}$ (Reflexiva)
  - $a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$ (Simétrica)
  - $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$ entonces $a \equiv c \pmod{n}$ (Transitiva)

CONGRUENCIAS MODULO N: Relación



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

Clases de Residuos [a] ó equivalencia

- **Definición**: Sea Z un conjunto y R una relación de equivalencia en Z, la congruencia módulo n divide a Z en n clases de equivalencia, con $n \geq 2$.

$$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$
$$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$
$$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$
$$[3] = \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\}$$
$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

- En que línea está localizado:
  - El número 124, 327, 440, 1234565 en que clase de equivalencia está ubicado?

CONGRUENCIAS MODULO N

- Teorema 14.11
  - La congruencia módulo *n* es una relación de equivalencia sobre Z
    - Relación de equivalencia de un conjunto A :
      - Reflexiva
      - Simétrica
      - Transitiva.

Relación de Equivalencia

- R es una relación de Equivalencia?

$$R=\{(a,b), (a,a), (b,a),(b,b),(c,c),(d,d)(d,e),(e,e), (e,d)$$
$$(e,f),(f,e),(f,f),(f,d),(d,f)\ \}$$

  - Partición del conjunto R $\{a,b\}, \{c\}, \{d,e,f\}$
  - Las clases de equivalencia son:
    - $[a]=\{a,b\}$
    - $[b]=\{a,b\}$
    - $[c]=\{c\}$
    - $[d]=\{d,e,f\}$
    - $[e]=\{d,e,f\}$
    - $[f]=\{d,e,f\}$

Relación de Equivalencia

- R es una relación de Equivalencia?

$$R=\{(1,1), (1,2), (2,1),(2,2),(3,4),(4,3)(3,3),(4,4)\}$$

Operaciones en Zn

Operaciones en Zn

- Las operaciones de suma, resta y multiplicación en Z pueden ser definidas en Zn. El resultado es mapeado en Zn usando el operador módulo

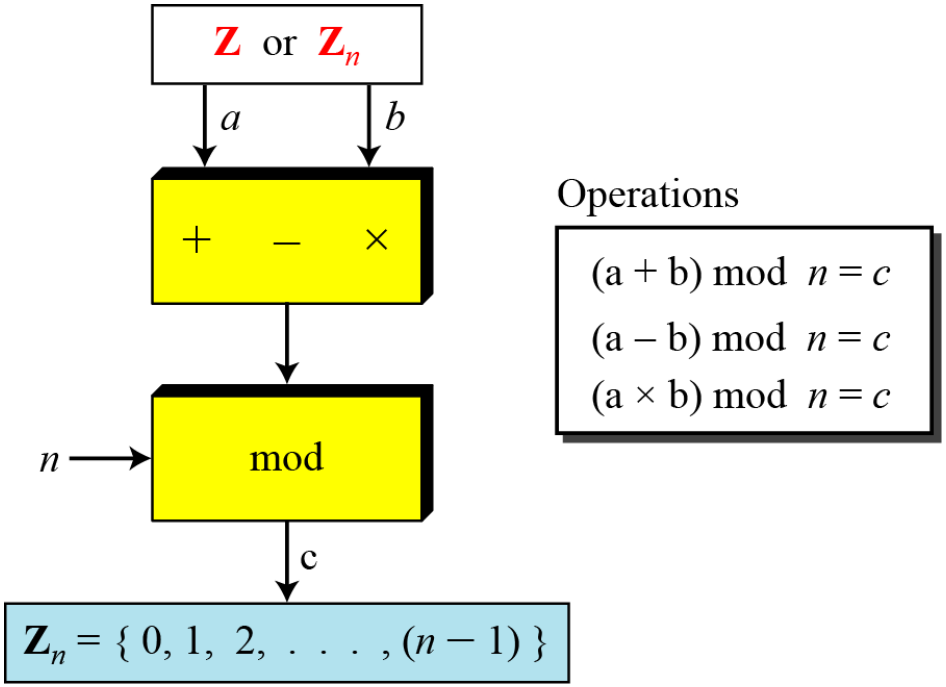


Fig. Operaciones Binarias en Zn

ENTEROS MODULO N

- Ejemplo:

  Para [a], [b] ϵ Zn, definimos + y . Como:

  [a] + [b] = [a+b] y [a] . [b] = [a][b]=[ab]

  Por ejemplo, si n= 7, entonces

  [2]+[6] = [2+6]=[8] = [1]

  [2] . [6] = [2.6] =[12] = [5]

Ejemplo:

- Realizar las siguientes operaciones (entradas desde Zn):
- a. Sumar 7 a 14 en Z_{15}.
- b. Restar 11 de 7 en Z_{13}.
- c. Multiplicar 11 por 7 en Z_{20}.

Ejemplo:

- Realizar las siguientes operaciones (entradas desde Zn):
- a. Sumar 7 a 14 en Z_{15}.
- b. Restar 11 de 7 en Z_{13}.
- c. Multiplicar 11 por 7 en Z_{20}.

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

Ejemplo:

- Realizar las siguientes operaciones (entradas desde Zn):
- a. Sumar 17 a 27 en Z_{14}.
- b. Restar 34 de 12 en Z_{13}.
- c. Multiplicar 123 por -10 en Z_{19}.

Ejemplo:

- Realizar las siguientes operaciones (entradas desde Zn):
- a. Sumar 17 a 27 en Z_{14}.
- b. Restar 34 de 12 en Z_{13}.
- c. Multiplicar 123 por -10 en Z_{19}.

Solution

$$
\begin{aligned}
(17 + 27) \bmod 14 &\rightarrow (44) \bmod 14 = 2 \\
(12 - 43) \bmod 13 &\rightarrow (-31) \bmod 13 = 8 \\
(123 \times (-10)) \bmod 19 &\rightarrow (-1230) \bmod 19 = 5
\end{aligned}
$$

Propiedades

- Mapear las entradas a Zn (si están en Zn) antes de aplicar las tres operaciones binarias (+,-,x)

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Ejemplo:

Los siguientes ejemplos muestran las propiedades:

1. $(1\ 723\ 345 + 2\ 124\ 945) \bmod 11 =$
2. $(1\ 723\ 345 - 2\ 124\ 945) \bmod 16 =$
3. $(1\ 723\ 345 \times 2\ 124\ 945) \bmod 16 =$

Ejemplo:

Los siguientes ejemplos muestran las propiedades:

1. $(1\ 723\ 345 + 2\ 124\ 945) \bmod 11 = (8 + 9) \bmod 11 = 6$

2. $(1\ 723\ 345 - 2\ 124\ 945) \bmod 16 = (8 - 9) \bmod 11 = 10$

3. $(1\ 723\ 345 \times 2\ 124\ 945) \bmod 16 = (8 \times 9) \bmod 11 = 6$

Ejemplo:

- En aritmética a menudo necesitamos encontrar potencias de 10

$10^n \bmod x = (10 \bmod x)^n$ Applying the third property n times.

$10 \bmod 3 = 1 \rightarrow 10^n \bmod 3 = (10 \bmod 3)^n = 1$

$10 \bmod 9 = 1 \rightarrow 10^n \bmod 9 = (10 \bmod 9)^n = 1$

$10 \bmod 7 = 3 \rightarrow 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7$

Proceso de Cifrado y Descifrado Criptografía

Clave Secreta
Criptografía Clásica

- Emisor y Receptor se ponen de acuerdo sobre una clave secreta
- Ejemplos:
  - Cifrado de Cesar
  - Cifrado de Vigenere

- Para su implementación se usa la aritmética modular
  - Alfabeto: A…Z (0…25) mod 26 ó Z_{26}
  - **a mod n** es el entero no negativo más pequeño **r** tal que:

$$a = q.n + r \quad 0 \leq r < n$$

- Z_n

Clave Secreta
Suma, Resta mod n

C	A	Z	A	R
2	0	25	0	17
5	3	2	3	20
2	0	-1	0	17
2	0	25	0	17

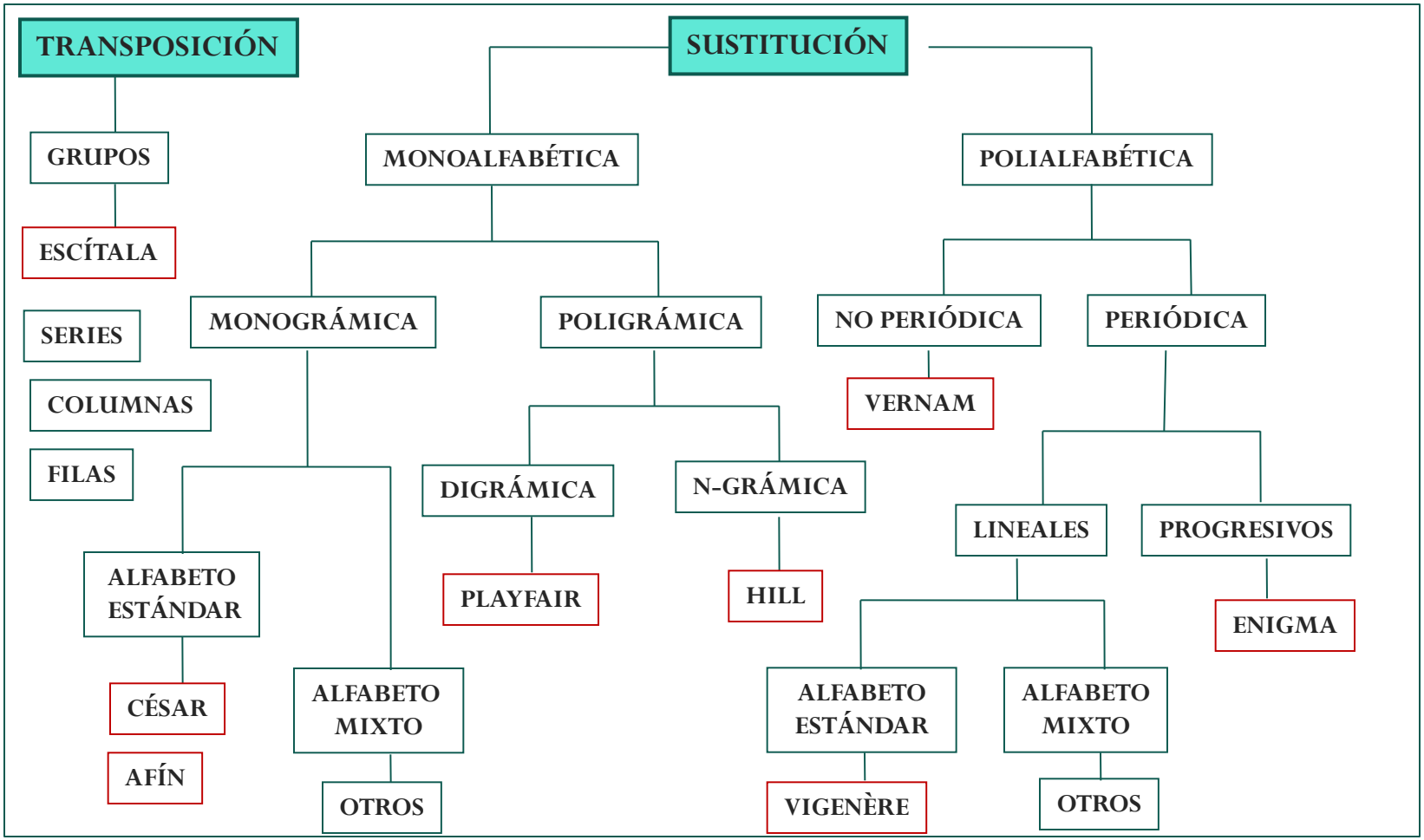
Clave = 3

Cifrado (i) = M(i) + Clave mod 26

Descifrado(i) = C(i) - Clave mod 26

- Calcular:
  - 10 mod 7
  - -10 mod 7

Criptografía Tradicional



Clave Pública
Criptografía

- El emisor y el receptor no acuerdan ninguna clave secreta.
- Cada uno generar una clave privada.
- Generan una clave pública conocida por todos.
- El atacante puede interceptar el mensaje cifrado y puede tener acceso a la clave pública. Difícil descifrar el mensaje.

- Restricción: Claves privada y pública sean inversas.
- Algoritmo de cifrado representativo: RSA.
- RSA: aritmética modular (multiplicación y división).

Criptografía usando multiplicación mod n

- Un posible algoritmo de cifrado es tomar un mensaje **x**, un valor **a** y calcular (Afin)

$$a \cdot x_i \bmod n$$

- El descifrado es dividir a en Zn

- Considerar los 3 casos siguientes:
  a) n=12, a=4, x=3
  b) n=12, a=3, x=6
  c) n=12, a=5, x=7

Criptografía usando multiplicación mod n

- Un posible algoritmo de cifrado es tomar un mensaje **x**, un valor **a** y calcular

$$a \cdot x_i \bmod n$$

- El descifrado es dividir a en Zn
- Considerar los 3 casos siguientes:
  a) n=12, a=4, x=3
  b) n=12, a=3, x=6
  c) n=12, a=5, x=7

- **El mensaje de cifrado y descifrado deben tener una relación de 1 a 1. Se da cuando mcd(a,n)=1**

Inversa multiplicativa módulo N

Teorema
Inversa módulo n

- Un elemento en Zn es invertible si mcd(a,n) =1. En este caso se dice que a y b son **relativamente primos**.
- Suponga que tiene dos elementos a y n, con mcd(a,n)=1. Se tiene un entero x, tal que

$$(a.\ x) \bmod n = 1$$

x es el inverso de a módulo n y tiene una única solución en Zn.

- En Z_9 el inverso de 2 es 5.
  - $2.5 \pmod 9 = 1$

Ejemplos:

- Encontrar la inversa de 8 en Z_{10}.
- Encontrar todas las inversas multiplicativas en Z_5.
- Encontrar todas las inversas multiplicativas en Z_{10}.
- Encontrar todas las inversas multiplicativas en $Z_3, Z_4, Z_6, Z_7, Z_8, Z_9$

.

Ejemplos
Inversa módulo n

- Encontrar todas las inversas multiplicativas en Z_5.

Z_5 a.x (mod 5)

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$1.1 \pmod 5 = 1$
$2.3 \pmod 5 = 1$
$3.2 \pmod 5 = 1$
$4.4 \pmod 5 = 1$

Ejemplos:

- Encontrar la inversa de 8 en Z_{10}.
  - No hay inversa multiplicativa porque mcd(8,10) = 2 ≠ 1

- Encontrar todas las inversas multiplicativas en Z_{10}.
  - Solo los pares (1, 1), (3, 7) y (9, 9). Los números 0, 2, 4, 5, 6, y 8. No tienen inversa

Teorema
Inversa multiplicativa módulo n

Un número entero "a" tiene una inversa multiplicativa en Zn si y solo si existen enteros "x" e "y" tal que

$$ax + ny = 1$$

Si se cumple, entonces el mcd(a,n)=1

Inversa multiplicativa módulo n

Nota

El algoritmo extendido de Euclides encuentra la inversa multiplicativa de “a” en Z_n cuando

$$\text{mcd}(n, a) = 1.$$

La inversa multiplicativa de “a” es el valor de “x” después de ser mapeada en Z_n.

Ejemplos
Inversa módulo n

- ¿Cuál es el inverso de 110 en mod 273?

  - Determinar si mcd(110,273)=1
  - Encontrar ax+by=d (Algoritmo extendido de Euclides)
    - 110x + 273 y= 1
  - El valor de **x** es el inverso de 110 mod 273

  - Nota: x $\in Z^+$

Ejercicios

- Encontrar la inversa multiplicativa de 11 en Z_{26}
- Encontrar la inversa multiplicativa de 23 en Z_{100}
- Encontrar la inversa multiplicativa de 12 en Z_{26}

Exponenciación módulo

Exponenciación a^m

$$\underbrace{a.a.a.a.a.\ldots.a}_{\text{m veces a}}$$

- Mejora: elevar a^2 repetidas veces.
- m expresado como potencias de 2

- Ejemplo: m=29
  - $a^1 = a$
  - $a^2 = a^1 . a^1$
  - $a^4 = a^2 . a^2$
  - $a^8 = a^4 . a^4$
  - $a^{16} = a^8 . a^8$

$29 = 1+4+8+16$

Exponenciación a^m
Elevando al cuadrado repetidas veces

1. Inicialmente x =a
2. Se calcula m mod 2

   Si es 1 significa que el valor de x al cuadrado está incluido en el resultado
3. Al resultado se multiplica por x

x	m	m mod 2	Resultado	m/2
a^1	29	1	a	14
a^2	14	0	--	7
a^4	7	1	a. a^4	3
a^8	3	1	a. a^4. a^8	1
a^{16}	1	1	a. a^4. a^8. a^{16} =a^{29}	0

Exponenciación a^m mod n
Elevando al cuadrado repetidas veces

- **a^2 mod n = [(a mod n) (a mod n)] mod n**
- Ejemplo: 572^{29} (mod 713)

x	m	m mod 2	Elevado al cuadrado		Resultado mod 713	n/2
572^1	29	1	572	572	572	14
572^2	14	0	572^2 mod 713 = 327184 mod 713=**630**			7
572^4	7	1	(572^2 mod 713)(572^2 mod 713) =630^2 mod 713=**472**	572.572^4	572.472 (mod 713)=**470**	3
572^8	3	1	(572^4 mod 713)(572^4 mod 713) =472^2 mod 713=**328**	$572.572^4.572^8$	470.328 (mod 713)=**152**	1
572^{16}	1	1	(572^8 mod 713)(572^8 mod 713) =328^2 mod 713=**634**	$572.572^4.572^8.572^{16}$	152.634 (mod 713)=**<u>113</u>**	0

Sistema de Ecuaciones módulo enteros

Sistemas de Ecuaciones módulo enteros

- Congruencia lineal: Ecuaciones de la forma

$$ax \equiv b \pmod{n}$$

  - Donde a,b son enteros fijos, n> 1, y *x* es indeterminado
  - Puede no tener soluciones o un número limitado "d" de soluciones:

$$mcd(a,n) = d$$

Si d | b, hay d soluciones

  - Todos los enteros x que son solución de la congruencia son de la forma
    - $x = nk + r \qquad k \in z$

Sistemas de Ecuaciones módulo enteros

- Pasos:
  - Reducir la ecuación por dividir ambos lados de la ecuación (incluyendo el módulo) por d.
  - Multiplicar ambos lados de la ecuación reducida por la inversa multiplicativa de a, para encontrar la solución particular x_o.
  - La soluciones generales son:

$$\mathbf{x = x_o + k(d/n)\ , para\ k=0,1,\ldots,(d-1)}$$

Sistemas de Ecuaciones módulo enteros

- $14x \equiv 12 \pmod{18}$
- $3x + 4 \equiv 6 \pmod{13}$

Sistemas de Ecuaciones módulo enteros

a) $3x + 4 \equiv 5 \pmod 6$

b) $5x + 2 \equiv 5 \pmod 7$

c) $7x \equiv 6 \pmod 9$

d) $3x + 4 \equiv 6 \pmod{13}$.

Sistemas de Ecuaciones módulo enteros

$$x \equiv a_1 \pmod{p_1}$$
$$x \equiv a_2 \pmod{p_2}$$
$$x \equiv a_3 \pmod{p_3}$$
$$\ldots.$$
$$x \equiv a_n \pmod{p_n}$$

Teorema del Resto Chino

Teorema del Resto Chino

- Sean $a_1, a_2, \ldots a_n \in Z$, y $p_1, p_2, \ldots, p_n \in Z^+$, verificando:
  - i) $p_1 > 1$, γ $i=1,2,\ldots,n$
  - ii) $mcd(p_i, p_j) = 1$

  Entonces el sistema

$$x \equiv a_1 \pmod{p_1}$$
$$x \equiv a_2 \pmod{p_2}$$
$$x \equiv a_3 \pmod{p_3}$$
$$\ldots.$$
$$x \equiv a_n \pmod{p_n}$$

Tiene una solución módulo el producto $P= p_1,* p_2 *,\ldots, p_n$

Teorema del Resto Chino

- Resuelva el sistema de ecuaciones:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

1. p_1, p_2, p_3 **deben ser primos entre sí,**
   $P = 3 \times 5 \times 7 = 105$
2. $P_i = P/p_i$
   $P_1 = 105/3 = 35;\ P_2 = 105/5 = 21;\ P_3 = 105/7 = 15$
3. **Para cada i existirá un** q_i **tal que**
   $q_i.P_i \equiv 1 \bmod p_i$ $\quad q_1 = 2;\ q_2 = 1;\ q_3 = 1$
4. **Sea entonces** $x_o = a_1 \times P_1 \times q_1 + a_2 \times P_2 \times q_2 + a_3 \times P_3 \times q_3 \pmod P$
   $x_o = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 23 \pmod{105}$
5. **Todas las soluciones del sistema serán:**
   $X = x_o + P.k$ $\quad X = 23 + 105k$

Práctica

- Resuelva el siguiente sistema de congruencias:

$$x \equiv 2 \bmod 9$$

$$x \equiv 3 \bmod 7$$

$$x \equiv 1 \bmod 4$$

$$x \equiv -1 \bmod 5$$

- Resolver:

$$x \equiv 2 \bmod 5$$

$$2x \equiv 1 \bmod 7$$

$$3x \equiv 4 \bmod 11$$

Práctica

- En el conjunto Z7 se define la relación:

  xRy (x=y) ó (xy=1)

  (a) Demuestre que R es una relación de equivalencia

  (b) Hallar todas las clases de equivalencia

  (c) Determinar el conjunto cociente.

- Sean a,b,c,d,h,m ∈ Z con h≠0 y m>0 demostrar que
  a) Si a≡b (mod m) y c ≡ d (mod m)
     a+c ≡b+d (mod m) y
     a.c ≡b.d (mod m)
  b) Si a≡b (mod m) ha ≡ hb (mod m)

Teorema del Resto Chino

$$
\begin{aligned}
x &\equiv 12 \pmod{25} \\
x &\equiv 19 \pmod{26} \\
x &\equiv 7 \pmod{27}
\end{aligned}
$$

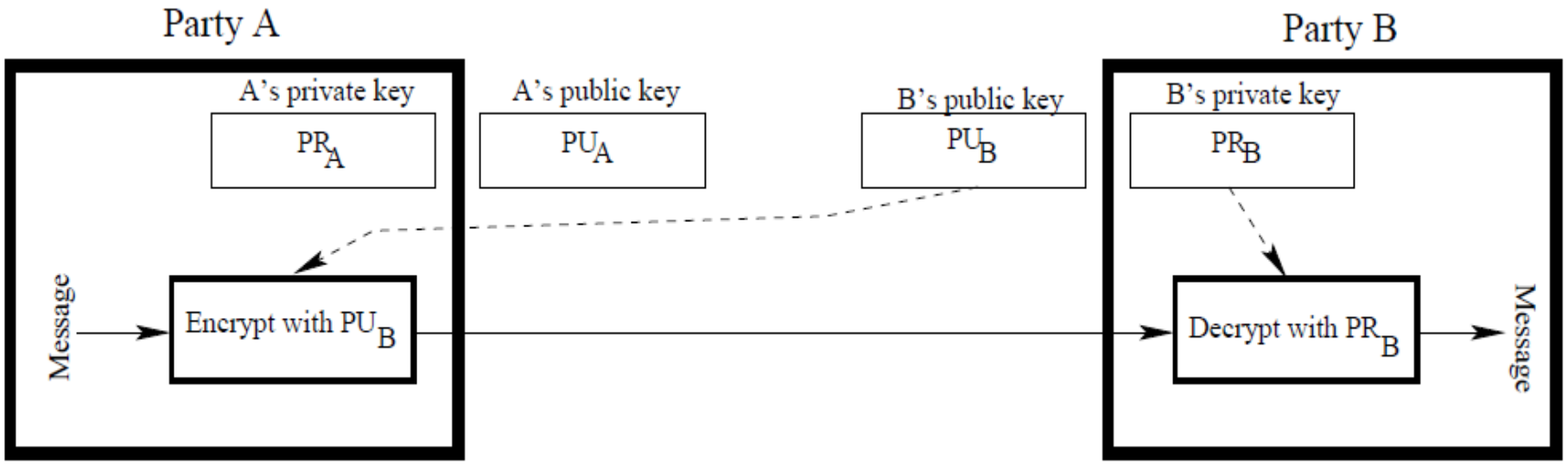
$$
\begin{aligned}
x &\equiv 12 \cdot 702 \cdot 13 + 19 \cdot 675 \cdot 25 + 7 \cdot 640 \cdot 14 \pmod{17550} \\
&\equiv 2437 \pmod{17550}
\end{aligned}
$$

$$
x = 2437 + 17550k \qquad (k \in \mathbb{Z})
$$

Criptosistema RSA

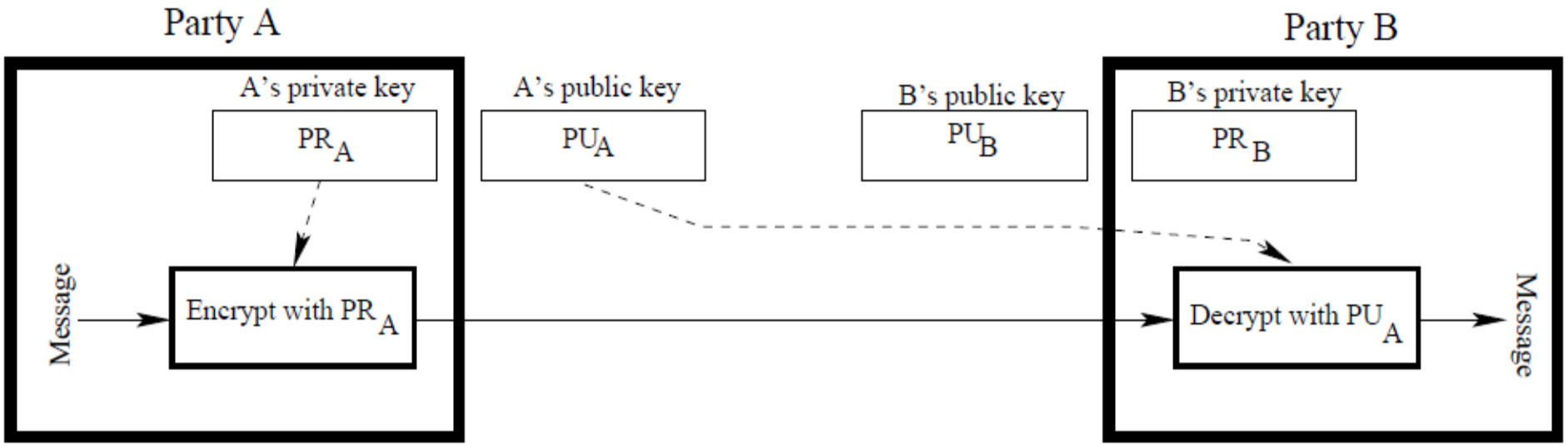
A quiere enviar un mensaje B

- Cuando solo se necesita confidencialidad



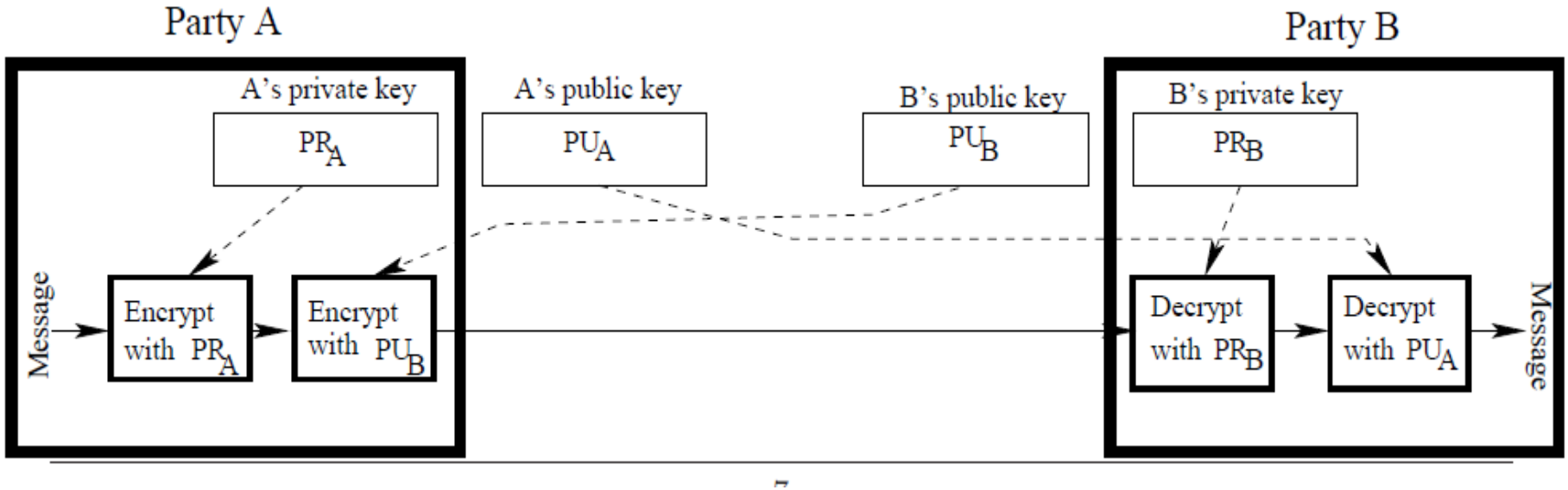
A quiere enviar un mensaje B

- Cuando solo se necesita autentificación



A quiere enviar un mensaje B

- Cuando son necesarios confidencialidad y autentificación



RIVEST-SHAMIR-ADLEMAN (RSA)

- N = módulo
- $\Phi(n)$ = fi de n
- e = un entero que es relativamente primo con $\Phi(n)$
- d= un entero que es la inversa multiplicativa de e módulo $\Phi(n)$

RSA: Generación de claves

- Seleciona dos números primos p y q
- Calcula $n = p \cdot q$
- Calcula $\phi(n) = (p-1)(q-1)$
- Seleciona e tal que $1 < e < \phi(n)$ y $\text{mcd}(\phi(n), e) = 1$
- Calcula d tal que $d \cdot e \bmod \phi(n) = 1$
- La clave pública es $<e, n>$
- La clave privada es $<d, n>$

Cifrado y Descifrado

- Mensaje: M
- Cifrado: $C = M^e \bmod n$
- Mensaje: $M = C^d \bmod n$

El algoritmo RSA (ejemplo)

- Selecciona dos números primos p =7 y q =17
- Calcula $n = p\ q = 119$
- Calcula $\phi(n) = (p\text{-}1)(q\text{-}1) = 96$
- Selecciona e tal que $1 < e < \phi(n)$ y mcd($\phi(n)$, e) = 1, *e.g.*, $e = 5$
- Calcula d tal que $d\ e \bmod \phi(n) = 1$, $d = 77$
- La clave pública es $\{e, n\} = \{5, 119\}$
- La clave privada es $\{d, n\} = \{77, 119\}$

El algoritmo RSA (ejemplo)

- Mensaje: $M = 19$
- Cifrado: $C = M^e \bmod n = 19^5 \bmod 119 = 66$
- Mensaje: $M = C^d \bmod n = 66^{77} \bmod 119 = 19$

Para romper RSA

- Factoriza n, que es público, y así obtienes p y q
- Calcula $\phi(n) = (p-1)(q-1)$
- Calcula d tal que $d\ e \bmod \phi(n) = 1$ (e es público)
- La clave privada es $KR = \{d, n\}$

Ejemplo:

- Siendo la clave pública <23,91>
- Use el RSA para cifrar M=24
- Descifrar el mensaje recibido de la parte a)

a) Cifrar M=24

- $C = M^e \bmod N$
- $C = 24^{23} \bmod 91 = 19$

X	M	M% 2	Elevar cuadrado	Resultado	m/2
24^1	23	1	24	24	11
24^2	11	1	24*24 (mod 91)=30	24*30 (mod 91)=83	5
24^4	5	1	30*30 (mod 91)=81	83*81 (mod 91)=80	2
24^8	2	0	81*81 (mod 91)=9		1
24^{16}	1	1	9*9 (mod 91)=81	80*81 (mod 91)=**19**	0

b) Descifrar mensaje

- $D = M^d \bmod N$
- $D = 19^d \bmod 91$

- Para descifrar se necesita el valor de la clave privada.

Generación de clave privada

- $p = 7$ y $q = 13$
- Calcula $n = p\ q$

  $91 = 7 \times 13$
- Calcula $\phi(n) = (p-1)(q-1)$

  $72 = (7-1)\ (q-1)$
- Selecciona e tal que $1 < e < \phi(n)$ y mcd$(\phi(n), e) = 1$

  $e = 23$ // clave pública
- Calcula d tal que $d = e^{-1} \bmod \phi(n)$

  $d = 23^{-1} \pmod{72}$

Generación de clave privada

- *Cálculo de la inversa :*

  $d = 23^{-1} \pmod{72}$

  - Aplicar algoritmo de Euclides: **mcd(72,23)= 1**

    72= 23(3) + 3 **3 = 72-23(3)**

    23= 3(7) + 2 **2= 23- 3(7)**

    3 = 2(1) + **1** **1= 3 – 2(1)**

    2 = 1(2) + 0

  - Aplicar el algoritmo extendido de Euclides : y=-25, x=8, d= 1

    1 = 3 - 2(1)

    1 = 3 - [**23- 3(7)**]

    1 = 3(8) - **23**

    1 = [**72-23(3)**](8) - **23**

    1 = [**72(8)-23(24)**] – **23**

    1 = **72(8) + 23(-25)**

  - **La inversa de 23 es -25. -25 tiene que ser un entero positivo**
  - **-25 + 72 = 47**

- La clave privada es $\{d, n\} = \{47, 91\}$

b) Descifrar mensaje

- $D = M^d \bmod N$
- $D = 19^{47} \bmod 91 = 24$

X	M	M% 2	Elevar cuadrado	Resultado	m/2
19^1	47	1	19	19	23
19^2	23	1	19*19 (mod 91)=88	19*88 (mod 91)=34	11
19^4	11	1	88*88 (mod 91) =9	34*9 (mod 91)=33	5
19^8	5	1	9*9 (mod 91) =81	33*81 (mod 91)=34	2
19^{16}	2	0	81*81 (mod 91) =9		1
19^{32}	1	1	9*9 (mod 91) =81	81 * 34 (mod 91)=24	0