ElGamal

FUNDAMENTOS MATEMATICOS

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Propiedades de los Grupos

- **Grupo multiplicativo**
  - $G = <Z_n*, \times>$. El conjunto Z_n* continene aquellos enteros de 1 a 1-n que son relativamente primos
  - $G = <Z_p*, \times>$. Es un grupo cuando p es primo

- **Orden de un grupo |G|**

No. de elementos en un grupo G. En $G = <Z_n*, \times>$ puede probarse que el orden de un grupo es $\phi(n)$

Ejemplo

- $G = <Z_{21}*, \times>$, $|G| = \phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$
  Hay 12 elementos en el grupo 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, y 20. Son relativamente primos con 21.

Propiedades de los Grupos

- **Orden de un elemento (δ(a))**

El orden de un elemento a de un grupo = $<Z_n*, \times>$, es el más pequeño Z^+ k tal que:

$$a^k = \underbrace{a \circ a \circ \ldots \circ a}_{k\ times} = 1$$

Hasta obtener el elemento identidad de Z_n. (1 es el elemento identidad)

Ejemplo

Determinar el δ(a) en Z_{11} a=3

$$\begin{aligned}
a^1 &= 3 \\
a^2 &= a \cdot a = 3 \cdot 3 = 9 \\
a^3 &= a^2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \bmod 11 \\
a^4 &= a^3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \bmod 11 \\
a^5 &= a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \bmod 11
\end{aligned}$$

$$\begin{aligned}
a^6 &= a^5 \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11 \\
a^7 &= a^5 \cdot a^2 \equiv 1 \cdot a^2 \equiv 9 \bmod 11 \\
a^8 &= a^5 \cdot a^3 \equiv 1 \cdot a^3 \equiv 5 \bmod 11 \\
a^9 &= a^5 \cdot a^4 \equiv 1 \cdot a^4 \equiv 4 \bmod 11 \\
a^{10} &= a^5 \cdot a^5 \equiv 1 \cdot 1 \equiv 1 \bmod 11 \\
a^{11} &= a^{10} \cdot a \equiv 1 \cdot a \equiv 3 \bmod 11 \\
&\vdots
\end{aligned}$$

El δ(3) = 5

Propiedades de los Grupos

- **Orden de un elemento (**$\delta(a)$**)**

Ejemplo

- Encontrar el orden de todos los elementos en $G = \langle Z_{10}^*, \times \rangle$.
- **Solución:**

  El grupo tiene $\phi(10) = 4$ elementos 1, 3, 7, 9. El orden de cada elemento es:

  $1^1 \equiv 1 \bmod (10) \rightarrow \delta(1) = 1.$

  $3^4 \equiv 1 \bmod (10) \rightarrow \delta(3) = 4.$

  $7^4 \equiv 1 \bmod (10) \rightarrow \delta(7) = 4.$

  $9^2 \equiv 1 \bmod (10) \rightarrow \delta(9) = 2.$

Propiedades de los Grupos

- **Orden de un elemento: Teorema de Euler**

Teorema de Euler

Si a es un elemento de $G = \langle Z_n*, \times \rangle$ entonces :

$$a^{(\phi)} = 1 \bmod n$$

Relación $a^i = 1 \bmod n$ cuando $i = \phi(n)$

Ejemplo

– Muestre los resultados de $a^i \equiv x \pmod 8$ para $G = \langle Z_8*, \times \rangle$.

– **Solución**:

$\phi(8) = 4$. Los elementos son 1,3,5,7

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$	$i = 7$
$a = 1$	$\boxed{\mathbf{x: 1}}$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 3$	x: 3	$\boxed{\mathbf{x: 1}}$	x: 3	x: 1	x: 3	x: 1	x: 3
$a = 5$	x: 5	$\boxed{\mathbf{x: 1}}$	x: 5	x: 1	x: 5	x: 1	x: 5
$a = 7$	x: 7	$\boxed{\mathbf{x: 1}}$	x: 7	x: 1	x: 7	x: 1	x: 7

- El área sombreada muestra el resultado del Teorema de Euler: $5^4 = 1 \bmod 8$.
- El valor de x puede ser 1 para algunos valores de i, el valor de i da el orden del elemento: δ(1)=1, δ(3)=2, δ(5)=2, δ(7)=2

Propiedades de los Grupos

- **Orden de un elemento: Teorema de Euler**

Teorema

El orden de un elemento δ(a) divide a |G |

Ejemplo

– Cuáles son los posibles órdenes de los elementos en Z_{11}?

– **Solución**:

- | Z_{11} | = 10
- 1, 2, 5, 10 dividen a 10

$$
\begin{aligned}
\mathrm{ord}(1) &= 1 & \mathrm{ord}(6) &= 10\\
\mathrm{ord}(2) &= 10 & \mathrm{ord}(7) &= 10\\
\mathrm{ord}(3) &= 5 & \mathrm{ord}(8) &= 10\\
\mathrm{ord}(4) &= 5 & \mathrm{ord}(9) &= 5\\
\mathrm{ord}(5) &= 5 & \mathrm{ord}(10) &= 2
\end{aligned}
$$

Raíz Primitiva

- En $G = \langle Z_n^*, \times \rangle$, cuándo el orden de un elemento es el mismo que $\phi(n)$, entonces es llamado raíz primitiva del grupo

Ejemplo

- El $G = \langle Z_8^*, \times \rangle$ no tiene raíz primitiva porque ningún elemento tiene orden igual a $\phi(8) = 4$.

Raíz Primitiva

Ejemplo

- Cuáles son las raices primitivas de $G = <Z_7*, \times>$
- **Solución**: 3 y 5
  - $\phi(7) = 6$
  - $a^i \equiv x \pmod 7$

Table 9.5 *Example 9.50*

		$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
	$a = 1$	$\boxed{x: 1}$	$x: 1$	$x: 1$	$x: 1$	$x: 1$	$x: 1$
	$a = 2$	$x: 2$	$x: 4$	$\boxed{x: 1}$	$x: 2$	$x: 4$	$x: 1$
Primitive root →	$a = 3$	$x: 3$	$x: 2$	$x: 6$	$x: 4$	$x: 5$	$\boxed{x: 1}$
	$a = 4$	$x: 4$	$x: 2$	$\boxed{x: 1}$	$x: 4$	$x: 2$	$x: 1$
Primitive root →	$a = 5$	$x: 5$	$x: 4$	$x: 6$	$x: 2$	$x: 3$	$\boxed{x: 1}$
	$a = 6$	$x: 6$	$\boxed{x: 1}$	$x: 6$	$x: 1$	$x: 6$	$x: 1$

  - $\delta(1)=1$, $\delta(2)=3$, **$\delta(3)=6$**, $\delta(4)=3$, **$\delta(5)=6$**, $\delta(6)=2$

Raíz Primitiva

- El $G = \langle Z_n*, \times \rangle$ tiene raices primitivas solo si $n=2,4,p^t$ ó $2p^t$

Ejemplo

– Para cada valor de n, el grupo $G = \langle Z_n*, \times \rangle$ tiene raíz primitiva? : n= 17, 20, 38, y 50?

– **Solución**:

$G = \langle Z_{17}*, \times \rangle$ tiene raíz primitiva, 17 es primo. (p^t,t es 1)

- b. $G = \langle Z_{20}*, \times \rangle$ no tiene raíz primitiva
- c. $G = \langle Z_{38}*, \times \rangle$ tiene raíz primitiva, $38 = 2 \times 19$ (19 primo)
- d. $G = \langle Z_{50}*, \times \rangle$ tiene raíz primitiva, $50 = 2 \times 5^2$ (5 ptimo)

Raíz Primitiva

Si $G = \langle Z_n^*, \times \rangle$ tiene una raíz primitiva, el número de raices primitivas es $\phi(\phi(n))$.

Ejemplo

- $G = \langle Z_{17}^*, \times \rangle$ es $\phi(\phi(17)) = \phi(16) = 8$

Grupo cíclico

Si G = <Z_n*, ×> tiene una raíz primitiva, es cíclico. Cada raíz primitiva es llamado elemento generador

$$Z_n* = \{g^1, g^2, g^3, \ldots, g^{\phi(n)}\}$$

Ejemplo

- El elemento a=2, es una raíz primitiva en Z_{11}?

i	1	2	3	4	5	6	7	8	9	10
a^i	2	4	8	5	10	9	7	3	6	1

2 es un elemento generador y Z_{11} es un grupo.

- El G = <Z_{10}*, ×> tiene dos raices primitivas, $\phi(10) = 4$ and $\phi(\phi(10)) = 2$. Las raices son 3 and 7. 3 y 7 son elementos generadores del grupo.

$$g = 3 \;\rightarrow\; g^1 \bmod 10 = 3 \quad g^2 \bmod 10 = 9 \quad g^3 \bmod 10 = 7 \quad g^4 \bmod 10 = 1$$
$$g = 7 \;\rightarrow\; g^1 \bmod 10 = 7 \quad g^2 \bmod 10 = 9 \quad g^3 \bmod 10 = 3 \quad g^4 \bmod 10 = 1$$

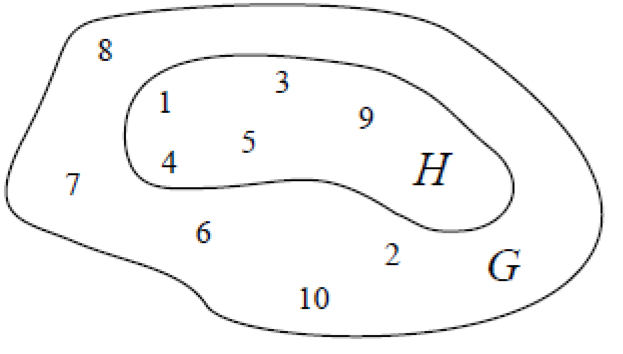
El grupo G = <Z_n*, ×> es un grupo cíclico si tiene raices primitivas
El grupo G = <Z_p*, ×> siempre es un grupo cíclico

SUB-GRUPOS

Teorema:
Dado (G,*) un grupo cíclico. Cada elemento de a ϵG con $\delta(a) = s$ es el elemento primitivo de un subgrupo cíclico con s elementos.

- El $G = \langle Z_{11}^*, \times \rangle$ con $\delta(3) = 5$. Las potencias de 3 genera el sub-conjunto H={1,3,5,9}

× mod 11	**1**	**3**	**4**	**5**	**9**
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4



▪

Escoger Generadores de un Grupo

Sea G = <Z_n*, ×> un grupo cíclico y m =|G|. Y la factorización prima de m = $p_1^{\alpha 1} \ldots p_n^{\alpha n}$, m_i=m/p_i para i=1,...,n. Entonces g ϵ G es un elemento generador si y sólo si para todo i=1,...,n: $g^{mi} \neq 1$

Ejemplo

- Determine todos los generadores de Z_{11}

  Solución:

  – m=ϕ(11)=10, la factorización de 10= 2x5. El test si un dado aϵ es un generador se Z_{11} da por $a^2 \neq 1$ mod 11 y $a^5 \neq 1$ mod 11

a	1	2	3	4	5	6	7	8	9	10
a^2 mod 11	1	4	9	5	3	3	5	9	4	1
a^5 mod 11	1	10	1	1	1	10	10	10	1	10

  – Los generadores de Z_{11} = {2,6,7,8}

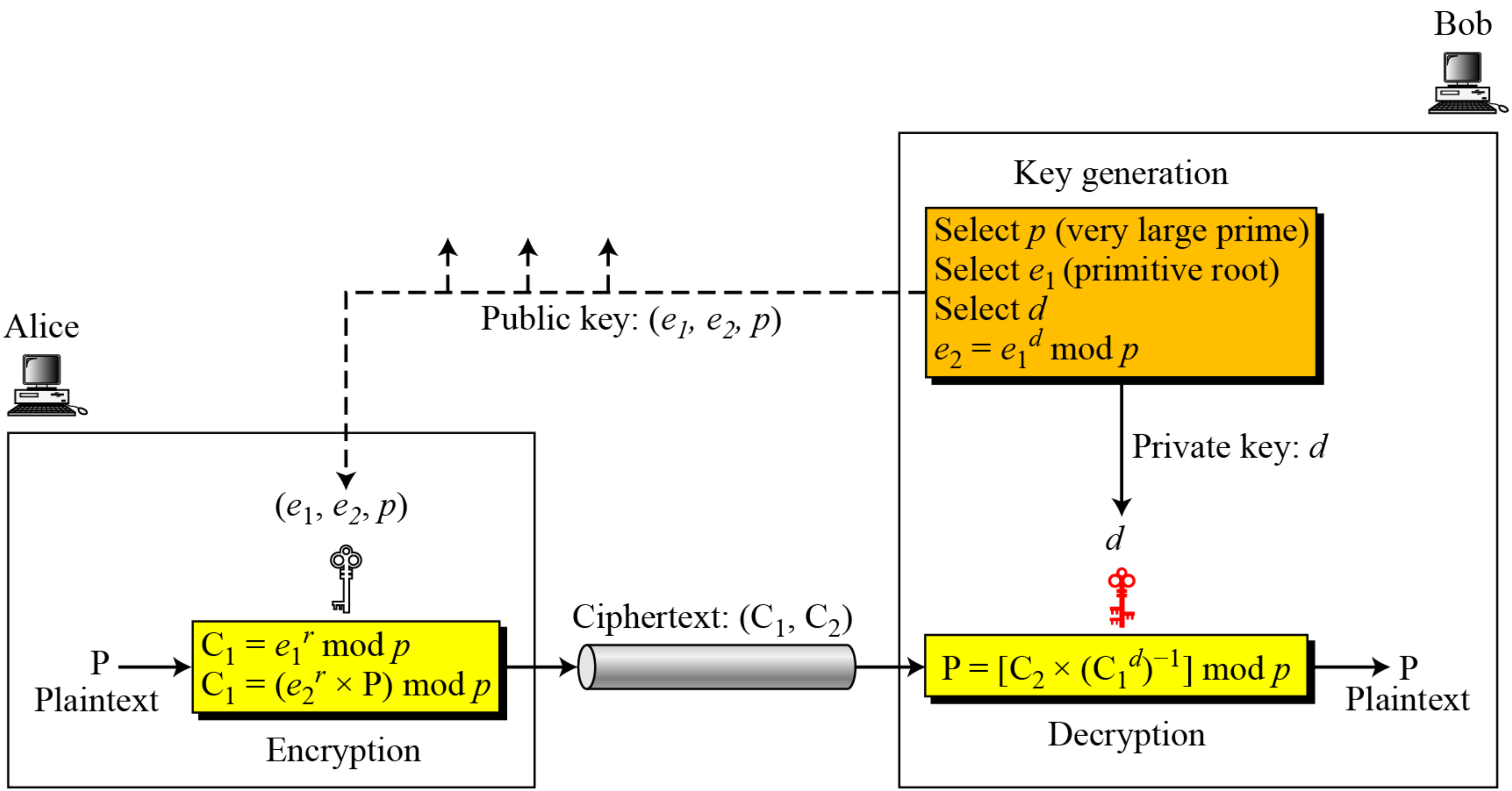
Algoritmo

- Elija un primo p=2q+1. Para algún primo q.

Algorithm FIND-GEN(p)
$q \leftarrow (p-1)/2$
$\mathsf{found} \leftarrow 0$
While ($\mathsf{found} \neq 1$) do
  $g \xleftarrow{\$} \mathbf{Z}_p^* - \{1, p-1\}$
  If ($g^2 \bmod p \neq 1$) and ($g^q \bmod p \neq 1$) then $\mathsf{found} \leftarrow 1$
EndWhile
Return g

CRIPTOSISTEMA ELGAMAL

El-Gamal



Bob
Key generation
Select p (very large prime)
Select e_1 (primitive root)
Select d
$e_2 = e_1^{\,d} \bmod p$
Public key: (e_1, e_2, p)
Private key: d
Alice
(e_1, e_2, p)
d
P
Plaintext
$C_1 = e_1^{\,r} \bmod p$
$C_1 = (e_2^{\,r} \times P) \bmod p$
Encryption
Ciphertext: (C_1, C_2)
$P = [C_2 \times (C_1^{\,d})^{-1}] \bmod p$
Decryption
P
Plaintext

ElGamal

Bob

Escoge un primo grande p

Escoge el elemento generador $e_1 \epsilon$ Zp (raiz primitiva)

a) Escoge $K_{pr} = d \epsilon \{2,\ldots p-2\}$

b) Calcula $k_{pub} = e_2 \equiv e_1^{d} \bmod p$

Alice

$k_{pub=} (e_1, e_2, p)$ ←

c) Escoge $r \epsilon \{2,\ldots p-2\}$

d) Calcula $C_1 \equiv e_1^{r} \bmod p$

e) Calcula $K_M \equiv e_2^{\,r} \bmod p$

f) Cifra mensaje $P \epsilon$ Zp

$C_2 \equiv P.\, K_M \bmod p$

(C_1, C_2) →

g) Calcula $K_M \equiv C_1^{d} \bmod p$

h)Descifrado $P \equiv C_2.K_M^{-1} \bmod p$

El-Gamal

- Bob

  e_1,e_2 = Clave Privada

  d= Clave Pública

- Alicia

  generar una clave pública y privada cada vez que envía un mensaje.

  r= Clave Privada

  C_1,C_2 = Clave Pública

  P = mensaje

EJEMPLO

El-Gamal: Ejemplo 1

Bob

Escoge p=29

Elemento generador $e_1 = \mathbf{2}$

a) Escoge K_{pr} = d =**12**

b) Calcula e_2=**7** $\equiv 2^{12}$ mod 29

Alice

Mensaje P=26

$\xleftarrow{k_{pub=}\ (\mathbf{29,2,7})}$

c) Escoge r =5

d) Calcula C_1 =**3** $\equiv 2^5$ mod 29

e) Calcula K_M =**16** $\equiv 7^{\ 5}$ mod 29

f) Cifrado mensaje P

C_2 =**10** $\equiv$ 26. 16 mod 29

$\xrightarrow{(\mathbf{3,10})}$

g) Calcula K_M = **16** $\equiv 3^{12}$ mod 29

h)Descifrado 26 $\equiv$ 10.20 mod 29

El-Gamal: Ejemplo 2

- Sara quiere enviar el mensaje “I like math” a Niwar

- Generación de claves por Niwar
  - claves públicas son (3,23,29) =>(e_1,e_2,P)
  - clave privada d= 4

El-Gamal: Ejemplo 2

- Sara cifra el mensaje (3,23,29)
  1. Convierte el mensaje en equivalencias numéricas

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

     Pi= 08 11 08 10 04 12 00 19 07
  2. Selecciona un número $1 < \mathbf{r} < p-2$

     r =5
  3. Calcula $C_1 \equiv e_1^{\,r} \bmod p$ => $C_1 \equiv 3^5 \bmod 29$

     $\mathbf{C_1 \equiv 11}$
  4. Calcula $K_M \equiv e_2^{\,r} \bmod p$ => $K_M \equiv 23^5 \bmod 29$

     $\mathbf{K_M = 25}$
  5. Calcula C_2 para todos los bloques, con bloque < P

     $$C_2 \equiv \mathbf{Pi.\ K_M \bmod p}$$

     $C_{21} = 8.25 \bmod 29 = 26$

     $C_{22} = 11.25 \bmod 29 = 14$

     $C_{23} = 8.25 \bmod 29 = 26$

     $C_{24} = 10.25 \bmod 29 = 18$

     $C_{25} = 4.25 \bmod 29 = 13$

     $C_{26} = 12.25 \bmod 29 = 10$

     $C_{27} = 0.25 \bmod 29 = 0$

     $C_{28} = 19.25 \bmod 29 = 11$

     $C_{29} = 7.25 \bmod 29 = 1$
  6. Concatena C_1C_{2i} , cada C_{2i} es igual al número de dígitos de P

     112614261813100001101

El-Gamal: Ejemplo 2

- Niwar descifra el mensaje (d=4)

  112614261813100001101

1. Calcula $K_M \equiv C_1^d \bmod p$ => $K_M \equiv 11^4 \bmod 29$

   $K_M \equiv 25$

2. Calcula $Pi \equiv C_2.K_M^{-1} \bmod p$

   2.1. Calcula $K_M^{-1} \bmod p = 25^{-1} \bmod 29 = 7$

   2.2. Calcula Pi para cada bloque

   $P_1 = 26.7 \bmod 29 = 08$

   $P_2 = 14.7 \bmod 29 = 11$

   $P_3 = 26.7 \bmod 29 = 08$

   $P_4 = 18.7 \bmod 29 = 10$

   $P_5 = 13.7 \bmod 29 = 04$

   $P_6 = 10.7 \bmod 29 = 12$

   $P_7 = 0.7 \bmod 29 = 00$

   $P_8 = 11.7 \bmod 29 = 19$

   $P_9 = 1.7 \bmod 29 = 07$

3. El mensaje original se obtiene siguiendo los mismos pasos del RSA

   I like math

El-Gamal

- Generación de claves

Algorithm 10.9 *ElGamal key generation*

ElGamal_Key_Generation

{

Select a large prime p

Select d to be a member of the group $\mathbf{G} = <\mathbf{Z}_p^*, \times>$ such that $1 \leq d \leq p-2$

Select e_1 to be a primitive root in the group $\mathbf{G} = <\mathbf{Z}_p^*, \times>$

$e_2 \leftarrow e_1^{\,d} \bmod p$

Public_key $\leftarrow (e_1, e_2, p)$ // To be announced publicly

Private_key $\leftarrow d$ // To be kept secret

return Public_key and Private_key

}

El-Gamal

- Cifrado

Algorithm 10.10 *ElGamal encryption*

```
ElGamal_Encryption (e1, e2, p, P)                    // P is the plaintext
{
    Select a random integer r in the group G = < Zp*, × >
    C1  ←  e1^r mod p
    C2  ←  (P × e2^r) mod p                          // C1 and C2 are the ciphertexts
    return C1 and C2
}
```

ElGamal_Encryption $(e_1, e_2, p, \mathrm{P})$ // P is the plaintext

{

Select a random integer r in the group $\mathbf{G} = \langle \mathbf{Z}_p^*, \times \rangle$

$C_1 \leftarrow e_1^{\,r} \bmod p$

$C_2 \leftarrow (\mathrm{P} \times e_2^{\,r}) \bmod p$ // C_1 and C_2 are the ciphertexts

return C_1 and C_2

}

El-Gamal

- Descifrado

Algorithm 10.11 *ElGamal decryption*

```
ElGamal_Decryption (d, p, C1, C2)                // C1 and C2 are the ciphertexts
{
    P ← [C2 (C1^d)^-1] mod p                     // P is the plaintext
    return P
}
```

ElGamal_Decryption (d, p, C_1, C_2) // C_1 and C_2 are the ciphertexts

{

$P \leftarrow [C_2 (C_1{}^d)^{-1}] \bmod p$ // P is the plaintext

return P

}

Protocolo ElGamal

- ***Bob***
  - $p = 11$
  - $e_1 = 2$.
  - $d = 3 \;\; e_2 = e_1^{\,d} = 8$.
    - *Clave pública (2, 8, 11)*
    - *Clave privada 3.*
- ***Alice***
  - $r = 4$
  - $P = 7$ *(mensaje)*

Plaintext: 7
$C_1 = e_1^{\,r} \bmod 11 = 16 \bmod 11 = 5 \bmod 11$
$C_2 = (P \times e_2^{\,r}) \bmod 11 = (7 \times 4096) \bmod 11 = 6 \bmod 11$
Ciphertext: (5, 6)

- *Bob Recibe (5 y 6) y calcula*

$[C_2 \times (C_1^{\,d})^{-1}] \bmod 11 = 6 \times (5^3)^{-1} \bmod 11 = 6 \times 3 \bmod 11 = 7 \bmod 11$

Plaintext: 7

ElGamal

- Bob usa un No. aleatorio de 512 bits

p =	115348992725616762449253137170143317404900945326098349598143469219 056898698622645932129754737871895144368891765264730936159299937280 61165964347353440008577
e_1 =	2

d =	1007
e_2 =	978864130430091895087668569380977390438800628873376876100220622332 554507074156189212318317704610141673360150884132940857248537703158 2066010072558707455

ElGamal

- Alicia envía el mensaje P=3200

P =	3200
r **=**	545131
$\mathbf{C_1}$ **=**	88729706938352847102257047149227566312026006725656212501818835142941722359971268111410536366170517305158153318916540097373635508029573678856906061915288 1
$\mathbf{C_2}$ **=**	70845433304892994457701601238079499956743602183619244696177450692124469615516580077945559308034588961440240859952591957920972162887968135058277956643029 50

- Bob calcula el texto plano $P = C_2 \times ((C_1)^d)^{-1} \bmod p = 3200 \bmod p$

P =	3200