Cifrado El Gamal

1- Elegir un número primo grande p y un valor entero g (α) que sea generador del grupo multiplicativo Z_p

2- Elegir la clave privada x como un entero aleatorio tal que $1 < x < p-1$

3- Calcular $y \equiv g^x \bmod p$. La clave pública es la tripleta (p, g, y)

4- Cifrado: A partir de M se calcula $C = (r, s)$.

- Elegir un entero k en $1 < k < p-1$ que sea primo relativo con $p-1$
- Calcular:

$$r \equiv g^k \bmod p$$

$$s \equiv M y^k \bmod p$$

5- Descifrado: A partir de $C = (r, s)$ se obtiene M como:

$$M \equiv \frac{s}{r^x} \bmod p = s \cdot \left(r^{-1} \bmod p\right)^x \bmod p$$

- Ejemplo

$p = 107$

$g = 32$

$x = 74 \rightarrow$ Clave Secreta

$y = g^x \bmod p \rightarrow y = 32^{74} \bmod 107 = 53$

Clave pública: $(107, 32, 53)$

Diseño: $p > M$

- Cifrado

$M = 82$

$k = 49$

$r = g^k \bmod p \rightarrow r = 32^{49} \bmod 107 = 58$

$s = M \cdot y^k \bmod p \rightarrow s = 82 \cdot 53^{49} \bmod 107 = 28$

$C = (r, s) \rightarrow C = (58, 28)$

- Descifrado

$$M = \frac{s}{r^x} \bmod p = s \cdot \left(r^{-1} \bmod p\right)^x \bmod p \rightarrow M = 28 \cdot \left(58^{-1} \bmod 107\right)^{74} \bmod 107 =$$

$$= 28 \cdot 24^{74} \bmod 107 =$$

$$= (28 \cdot 87) \bmod 107 =$$

$$= 2436 \bmod 107 = \boxed{82 = M}$$

Cifrado El Gamal

1- Elegir un número primo grande p y un valor entero g (α) que sea generador del grupo multiplicativo Z_p

2- Elegir la clave privada x como un entero aleatorio tal que $1 < x < p-1$

3- Calcular $y \equiv g^x \bmod p$. La clave pública es la tripleta (p, g, y)

4- Cifrado: A partir de M se calcula $C = (r, s)$.

- Elegir un entero k en $1 < k < p-1$ que sea primo relativo con $p-1$
- Calcular:

$$r \equiv g^k \bmod p$$

$$s \equiv M y^k \bmod p$$

5- Descifrado: A partir de $C=(r,s)$ se obtiene M como:

$$M \equiv \frac{s}{r^x} \bmod p = s \cdot \left(r^{-1} \bmod p\right)^x \bmod p$$

- Ejemplo

$p = 107$

$g = 32$

$x = 74 \rightarrow$ Clave Secreta

$y = g^x \bmod p \rightarrow y = 32^{74} \bmod 107 = 53$

Clave pública: $(107, 32, 53)$

Diseño: $p > M$

- Cifrado

$M = 82$

$k = 49$

$r = g^k \bmod p \rightarrow r = 32^{49} \bmod 107 = 58$

$s = M \cdot y^k \bmod p \rightarrow s = 82 \cdot 53^{49} \bmod 107 = 28$

$C = (r, s) \rightarrow C = (58, 28)$

- Descifrado

$$M = \frac{s}{r^x} \bmod p = s \cdot \left(r^{-1} \bmod p\right)^x \bmod p \rightarrow M = 28 \cdot \left(58^{-1} \bmod 107\right)^{74} \bmod 107 =$$

$$= 28 \cdot 24^{74} \bmod 107 =$$

$$= (28 \cdot 87) \bmod 107 =$$

$$= 2436 \bmod 107 = \boxed{82 = M}$$