Firma con el cifrado ElGamal

José Manuel Cuevas Muñoz

27 de Diciembre de 2019

Índice

Recordando las bases del cifrado

Cifrado ElGamal

- El cifrado ElGamal es un cifrado moderno basado en el intercambio de claves de Diffie-Hellman

Recordando las bases del cifrado

Cifrado ElGamal

- El cifrado ElGamal es un cifrado moderno basado en el intercambio de claves de Diffie-Hellman
- Para generar las claves, primero se escoge un primo **q** y un generador en módulo q, llamado **g**.

Recordando las bases del cifrado

Cifrado ElGamal

- El cifrado ElGamal es un cifrado moderno basado en el intercambio de claves de Diffie-Hellman
- Para generar las claves, primero se escoge un primo **q** y un generador en módulo q, llamado **g**.
- **La clave privada** será **a**, un número aleatorio entre 2 y q-2.
- **La clave pública** será **n**, siendo $n = g^a$ mod q.

Firmar con el cifrado ElGamal

- B quiere enviarle un mensaje a A y la firma para que compruebe el mensaje.

Firmar con el cifrado ElGamal

- B quiere enviarle un mensaje a A y la firma para que compruebe el mensaje.
- B cifra el mensaje que va a enviar a A.

Firmar con el cifrado ElGamal

- B quiere enviarle un mensaje a A y la firma para que compruebe el mensaje.
- B cifra el mensaje que va a enviar a A.
- Ahora, para firmar este mensaje, necesitamos g_B, a_B, q_B.
- B genera un número k, tal que k tenga inverso módulo q_B-1.

Firmar con el cifrado ElGamal

- B quiere enviarle un mensaje a A y la firma para que compruebe el mensaje.
- B cifra el mensaje que va a enviar a A.
- Ahora, para firmar este mensaje, necesitamos g_B, a_B, q_B.
- B genera un número k, tal que k tenga inverso módulo q_B-1.
- B calcula $r = (g_B)^k$ mod q.

Firmar con el cifrado ElGamal

- B quiere enviarle un mensaje a A y la firma para que compruebe el mensaje.
- B cifra el mensaje que va a enviar a A.
- Ahora, para firmar este mensaje, necesitamos g_B, a_B, q_B.
- B genera un número k, tal que k tenga inverso módulo q_B-1.
- B calcula $r = (g_B)^k$ mod q.
- B calcula la inversa de k mod q-1

Firmar con el cifrado ElGamal

- B quiere enviarle un mensaje a A y la firma para que compruebe el mensaje.
- B cifra el mensaje que va a enviar a A.
- Ahora, para firmar este mensaje, necesitamos g_B, a_B, q_B.
- B genera un número k, tal que k tenga inverso módulo q_B-1.
- B calcula $r = (g_B)^k$ mod q.
- B calcula la inversa de k mod q-1
- B devuelve el mensaje firmado $F = (M - a_B * r)k^{-1}$ mod q_B-1 y r.

Confirmar Firma con el cifrado ElGamal

- A recibe el mensaje cifrado y la firma de este mensaje.

Confirmar Firma con el cifrado ElGamal

- A recibe el mensaje cifrado y la firma de este mensaje.
- A descifra el mensaje (M) y utiliza este para comprobar la firma (F).

Confirmar Firma con el cifrado ElGamal

- A recibe el mensaje cifrado y la firma de este mensaje.
- A descifra el mensaje (M) y utiliza este para comprobar la firma (F).
- Ahora, para comprobar la firma de este mensaje, necesitamos g_B, n_B, q_B,r,F y M.
- A calcula g^M mod q.

Confirmar Firma con el cifrado ElGamal

- A recibe el mensaje cifrado y la firma de este mensaje.
- A descifra el mensaje (M) y utiliza este para comprobar la firma (F).
- Ahora, para comprobar la firma de este mensaje, necesitamos g_B, n_B, q_B,r,F y M.
- A calcula g^M mod q.
- A también calcula $n^r r^F$ mod q.

Confirmar Firma con el cifrado ElGamal

- A recibe el mensaje cifrado y la firma de este mensaje.
- A descifra el mensaje (M) y utiliza este para comprobar la firma (F).
- Ahora, para comprobar la firma de este mensaje, necesitamos g_B, n_B, q_B,r,F y M.
- A calcula g^M mod q.
- A también calcula $n^r r^F$ mod q.
- Por último, comprueba si ambos vectores son iguales.

¿Por qué funciona la firma con ELGamal?

Queremos comprobar que g^M mod q$=n^r r^F$ mod q

¿Por qué funciona la firma con ELGamal?

Queremos comprobar que g^M mod q=$n^r r^F$ mod q
Como $F = (M - ar)k^{-1}$ mod q-1 y r=g^k mod q

¿Por qué funciona la firma con ELGamal?

Queremos comprobar que g^M mod q$=n^r r^F$ mod q
Como $F = (M - ar)k^{-1}$ mod q-1 y r$=g^k$ mod q

$$n^r r^F \text{ mod q} = g^{ar}(g^k)^{(M-ar)k^{-1}mod(q-1)} \text{ mod q}$$

¿Por qué funciona la firma con ELGamal?

Queremos comprobar que g^M mod q=$n^r r^F$ mod q
Como $F = (M - ar)k^{-1}$ mod q-1 y r=g^k mod q

$$n^r r^F \text{ mod q} = g^{ar}(g^k)^{(M-ar)k^{-1} mod(q-1)} \text{ mod q}$$

Gracias al pequeño teorema de Fermat

$$g^{M \ mod(q-1)} \text{ mod q} = g^{ar}(g^k)^{(M-ar)k^{-1} mod(q-1)} \text{ mod q}$$
$$g^M \text{ mod q} = g^{ar}(g^k)^{(M-ar)k^{-1}} \text{ mod q}$$
$$g^M \text{ mod q} = g^{ar}g^{(M-ar)} \text{ mod q}$$
$$g^M \text{ mod q} = g^{ar+M-ar} \text{ mod q}$$
$$g^M \text{ mod q} = g^M \text{ mod q}$$

Ejemplo de firma ElGamal

Elección de claves

- B genera su q=101 y su g=11

Ejemplo de firma ElGamal

Elección de claves

- B genera su q=101 y su g=11
- B escoge a=29 como clave privada y $n = 11^{29}$ mod 101=61 como clave pública.

Ejemplo de firma ElGamal

Elección de claves

- B genera su q=101 y su g=11
- B escoge a=29 como clave privada y $n = 11^{29}$ mod 101=61 como clave pública.

- B elige "HOLA" como firma.

Ejemplo de firma ElGamal

Elección de claves

- B genera su q=101 y su g=11
- B escoge a=29 como clave privada y $n = 11^{29}$ mod 101=61 como clave pública.

- B elige "HOLA" como firma.
- B pasa la firma al tamaño de dígitos(q)-1.
- "HOLA" = **7 15 11 0**

Ejemplo de firma ElGamal

Elección de claves

- B genera su q=101 y su g=11
- B escoge a=29 como clave privada y $n = 11^{29}$ mod 101=61 como clave pública.

- B elige "HOLA" como firma.
- B pasa la firma al tamaño de dígitos(q)-1.
- "HOLA" = **7 15 11 0**
- B escoge **k**=31 y **r**=8. La inversa de k mod q-1 es 71.

Ejemplo de firma ElGamal

- Firmamos el mensaje con $(M - a_B * r) * inv \bmod q_B$-1

(7-29*8)*71 mod 100=25, (15-29*8)*71 mod 100=93,
(11-29*8)*71 mod 100=9, (0-29*8)*71 mod 100=28.

Ejemplo de firma ElGamal

- Firmamos el mensaje con $(M - a_B * r) * inv \bmod q_B$-1

(7-29*8)*71 mod 100=25, (15-29*8)*71 mod 100=93,
(11-29*8)*71 mod 100=9, (0-29*8)*71 mod 100=28.

- Enviamos a A r=8 y F= 25 93 9 28

Ejemplo de firma ElGamal

- A recibe r=8 y F= 25 93 9 28

Ejemplo de firma ElGamal

- A recibe r=8 y F= 25 93 9 28
- Sabiendo que g=11 y q=101, calculamos g^M mod q.

11^7 mod 101=29, 11^{15} mod 101=60, 11^{11} mod 101=86, 11^0 mod 101=1.

Ejemplo de firma ElGamal

- A recibe r=8 y F= 25 93 9 28
- Sabiendo que g=11 y q=101, calculamos g^M mod q.

11^7 mod 101=29, 11^{15} mod 101=60, 11^{11} mod 101=86, 11^0 mod 101=1.

- Sabiendo que n=61, r=8 y q=101, calculamos $n^r r^F$ mod q.

$61^8 8^{25}$ mod 101=29, $61^8 8^{93}$ mod 101=60, $61^8 8^9$ mod 101=86, $61^8 8^{28}$ mod 101=1.

Ejemplo de firma ElGamal

- A recibe r=8 y F= 25 93 9 28
- Sabiendo que g=11 y q=101, calculamos g^M mod q.

11^7 mod 101=29, 11^{15} mod 101=60, 11^{11} mod 101=86, 11^0 mod 101=1.

- Sabiendo que n=61, r=8 y q=101, calculamos $n^r r^F$ mod q.

$61^8 8^{25}$ mod 101=29, $61^8 8^{93}$ mod 101=60, $61^8 8^9$ mod 101=86, $61^8 8^{28}$ mod 101=1.

¡¡AMBOS SON IGUALES!!