Basada en el problema del logaritmo discreto: Alice genera su clave pública $(p, g, A = g^a)$ y su clave privada a.El protocolo usando la firma digital Elgamal sin cifrado es el siguiente:

Firma digital Elgamal

Algoritmo 6 Firma Elgamal

Entrada: Clave pública $(p, g, A = g^a \bmod p)$ clave privada de Alice a.

Salida: Mensaje M y la firma (r, f).

1: Alice calcula el resumen (hash) del mensaje a firmar: $h(M) = m$.

2: Alice genera la clave de sesión: elige al azar un número secreto, x, $1 \leq x \leq p-2$, primo con $p-1$, tal que verifica $\text{mcd}(x, p-1) = 1$. Clave efímera, diferente para cada mensaje.

3: Alice calcula su rúbrica,

$$r = g^x \bmod p.$$

4: Alice calcula su firma,

$$f = x^{-1}(m - a \cdot r) \bmod p - 1.$$

5: **return** $M, (r, f)$