Basada en el problema del logaritmo discreto: Alice genera los parámetros de dominio (p, q, g) y calcula su clave pública (y) y su clave privada (x); para verificar la firma Bob, utiliza la clave pública de Alice y la función resumen acordada $h(M) = m$. El protocolo de firma digital Elgamal sin cifrado es el siguiente:

Firma digital DSA

Algoritmo 5 Firma DSA

Entrada: Parámetros de dominio (p, g, q), la clave privada x de Alice y el mensaje M.

Salida: Mensaje M junto con 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, k, $0 < k < q$.

3: Alice calcula su rúbrica,

$$r = (g^k \bmod p) \bmod q.$$

4: Alice calcula su firma,

$$f = k^{-1}(m + x \cdot r) \bmod q.$$

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