



**f1(bit[] array\_secret, bit[] valor\_aleatorio):**

->  $p = \text{array\_secret} + \text{valor\_aleatorio}$   
 ->  $p = p \ll 1$   
 ->  $p = p \bmod \text{valor\_aleatorio}$

**f2(bit[] array\_secret, bit[] valor\_aleatorio):**

->  $p = \text{array\_secret} \bmod \text{valor\_aleatorio}$   
 ->  $p = p + 3$   
 ->  $p = p \gg 1$

**Note:** The server and the player knows:  $\text{SHA-3}(\text{password})$