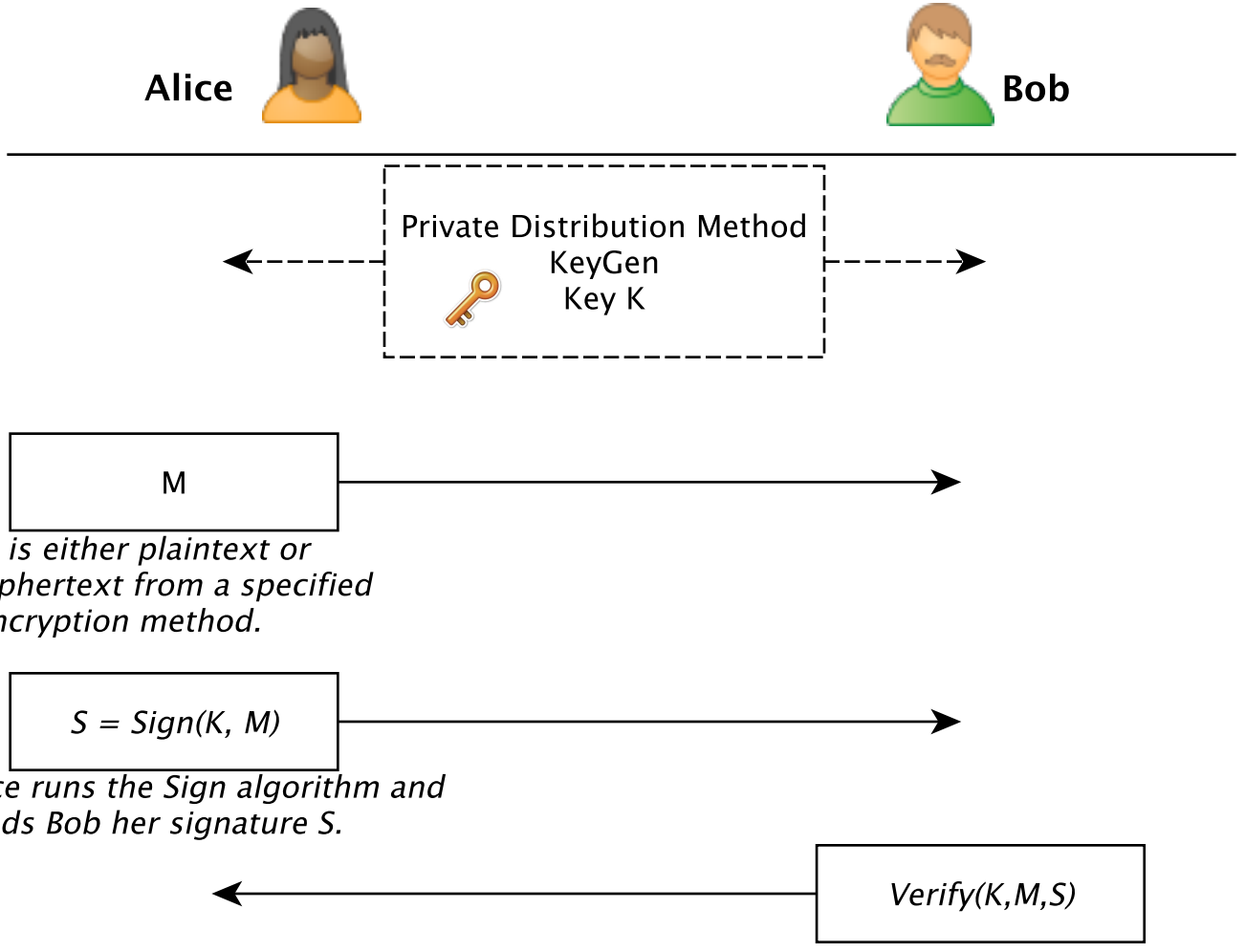
Alice
Bob
Private Distribution Method
KeyGen
Key K
M
M is either plaintext or ciphertext from a specified encryption method.
S = Sign(K, M)
Alice runs the Sign algorithm and sends Bob her signature S.
Verify(K,M,S)
Bob runs the Verify algorithm. Output is a bit 1 (accept) or 0 (do not accept).
The Verify algorithm checks that M hashes to S under key K.