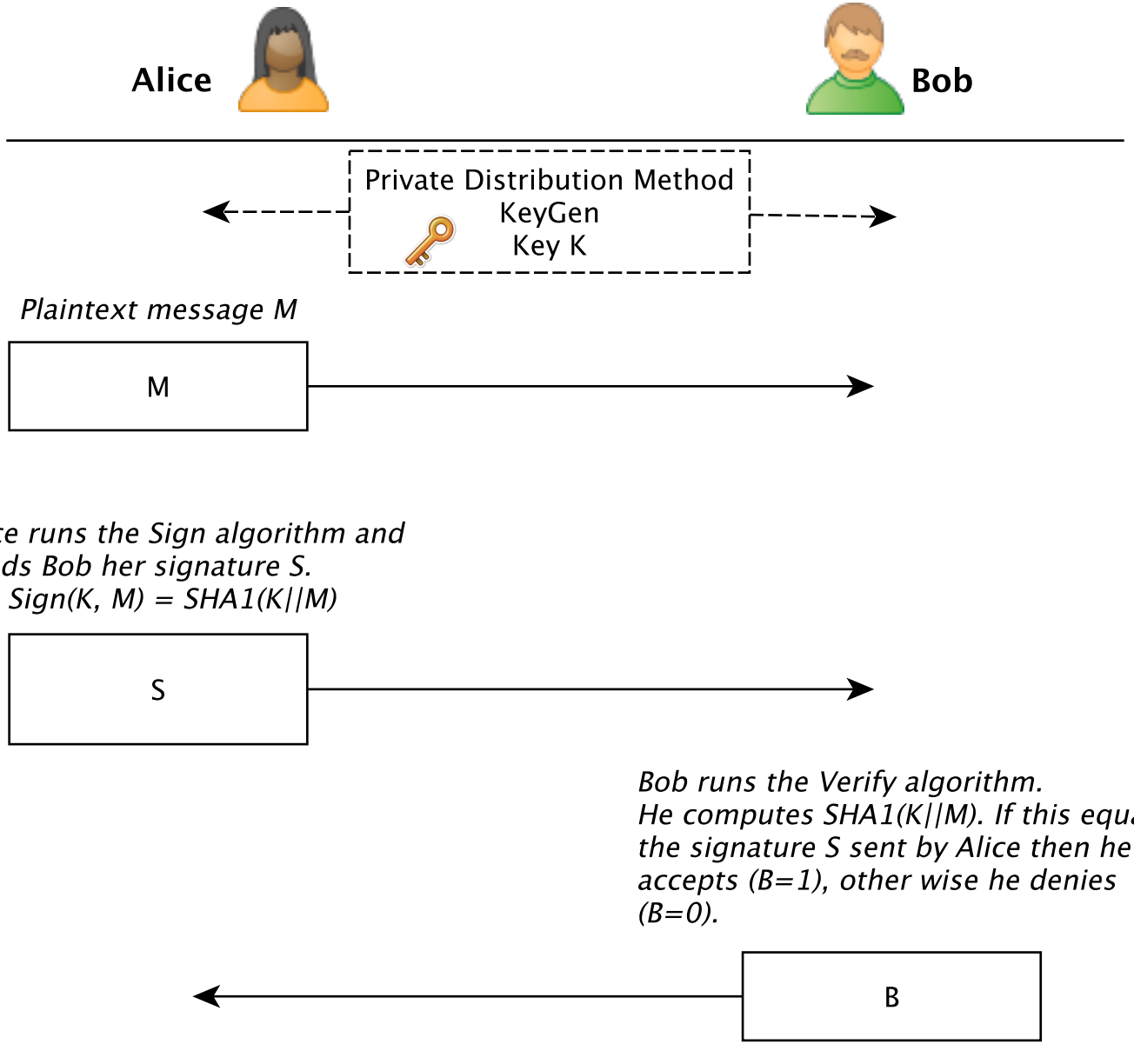
Alice
Bob
Private Distribution Method
KeyGen
Key K
Plaintext message M
M
Alice runs the Sign algorithm and
sends Bob her signature S.
S = Sign(K, M) = SHA1(K||M)
S
Bob runs the Verify algorithm.
He computes SHA1(K||M). If this equals
the signature S sent by Alice then he
accepts (B=1), other wise he denies
(B=0).
B