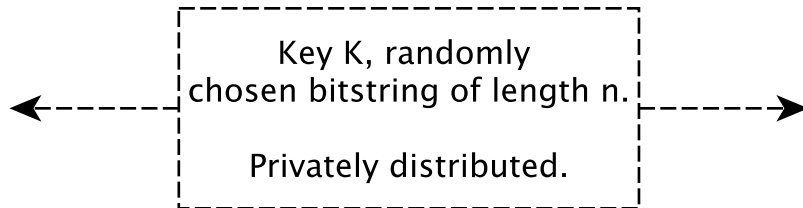


Alice

Bob

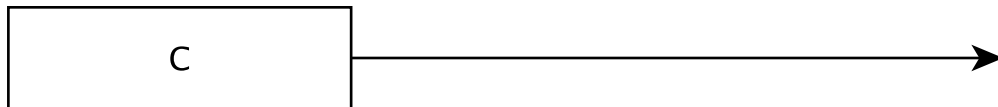


Alice choses a plaintext M

Alice computes:

$Enc(M) = M \text{ (xor) } K$

$C := Enc(M)$



Bob computes:

$Dec(C) = C \text{ (xor) } K = M$