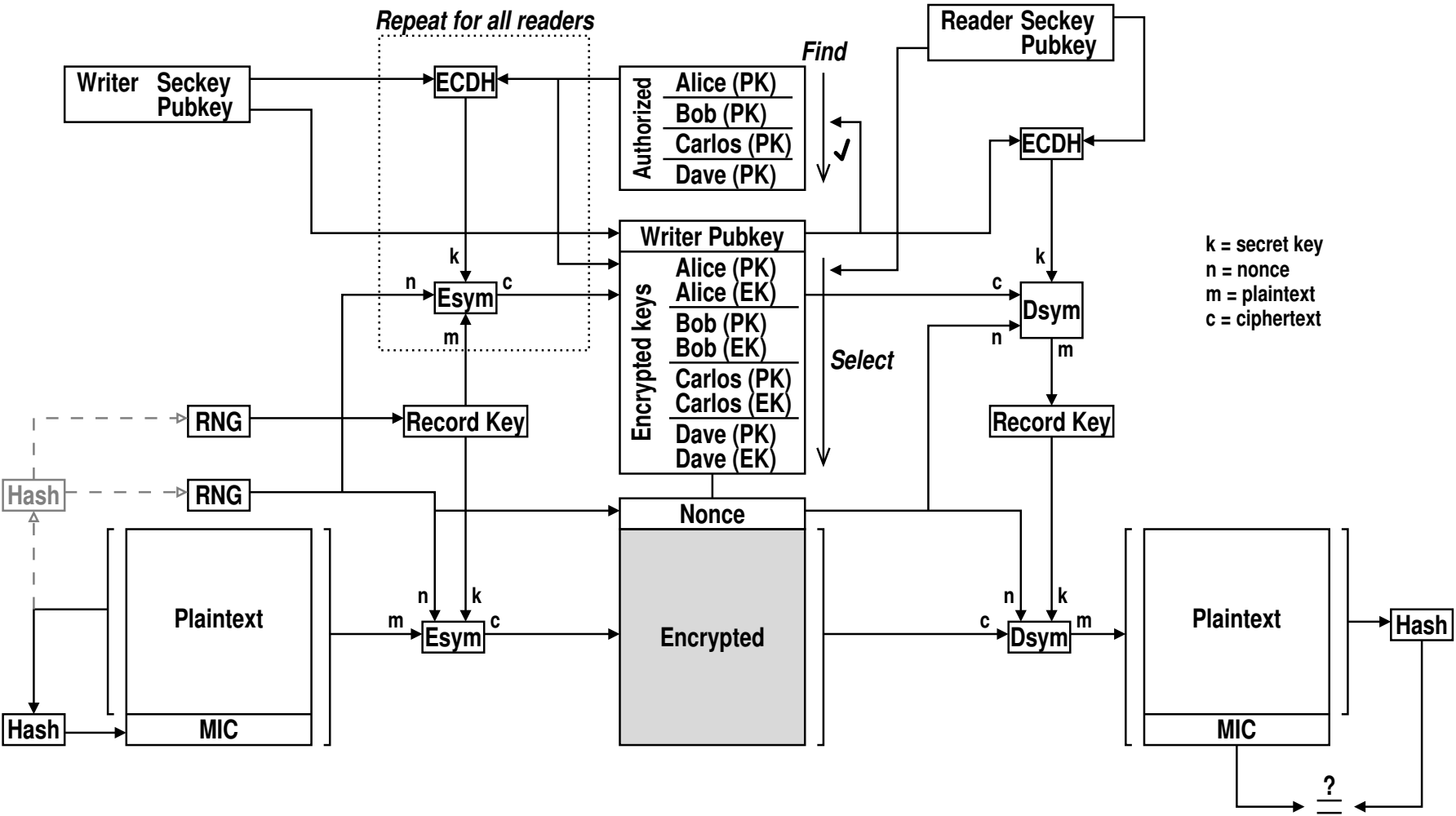
Repeat for all readers
Writer Seckey
Pubkey
ECDH
Authorized
Alice (PK)
Bob (PK)
Carlos (PK)
Dave (PK)
Find
Reader Seckey
Pubkey
ECDH
Writer Pubkey
Encrypted keys
Alice (PK)
Alice (EK)
Bob (PK)
Bob (EK)
Carlos (PK)
Carlos (EK)
Dave (PK)
Dave (EK)
Select
k
n
c
Esym
m
k
c
Dsym
n
m
k = secret key
n = nonce
m = plaintext
c = ciphertext
RNG
Record Key
Record Key
Hash
RNG
Nonce
Plaintext
MIC
Hash
n
k
m
Esym
c
Encrypted
n
k
c
Dsym
m
Plaintext
MIC
Hash
?