Security

Key distribution Problem.

- Using symmetric / shared keys.
- Using public / private keys.

Encrypting Function

\[ \text{Encrypt}(M) = E_{K_{pub}}(M) \]

\[ E_{K_{BA}}(M) = D_{K_{BA}}(E_{K_{BA}}(M)) = M \]
The procedure whereby each node generates its public-private key pair & broadcasts the public key has authentication problem.