

Proxy



$E(K_A, m)$



Router



m



Server



Kennt K_A, K_B

Kennt K_A

Kennt K_B

$m =$ „Circuit erweitern auf B“; Schlüsselaustausch mit B von K_B