

nonce

$u(\text{creator}, \text{addressee}, \text{rand})$

$u_p \equiv u(p, -, -)$

$p \xrightarrow{E_q(u_p, p)} q \text{ ----- } \text{enc1}(q, u_p, p) : \text{Cipher1}$

$p \xleftarrow{E_p(u_p, u_q, q)} q \text{ ----- } \text{enc2}(p, u_p, u_q, q) : \text{Cipher2}$

$p \xrightarrow{E_q(u_q)} q \text{ ----- } \text{enc3}(q, u_q) : \text{Cipher3}$

Cipher