Authenticated encryption

Combinazione tra cifratura e autenticazione del messaggio: garantisce confidenzialità, autenticità e integrità.

encrypt-then-MAC $m' = C(m,k) \parallel \mathrm{MAC}(C(m,k),k')$

encrypt-and-MAC $m' = C(m,k) \parallel \mathrm{MAC}(m,k)$

MAC-then-encrypt $m' = C(m \parallel \mathrm{MAC}(m,k),k)$ (TLS)