Autenticazione su canale insicuro

Message Authentication Code (MAC)

- mittente e destinatario concordano una chiave segreta simmetrica k (per esempio con DH);
- il mittente allega ad ogni messaggio m (eventualmente cifrato con un'altra chiave k') il MAC $A(m, k)$;
- il destinatario riceve la coppia, calcola indipendentemente $A(m, k)$ e verifica che combaci con il MAC ricevuto.

Garantisce identificazione (solo il mittente conosce k) e integrità (se m venisse alterato il MAC non combacerebbe).

Per esempio, $A(m, k) = h(mk)$ dove h è una funzione hash one-way.

CBC

Usare l'ultimo blocco di un crittogramma creato con CBC come MAC, visto che dipende da tutti gli altri blocchi.