Cifratura ibrida

Cifrario simmetrico con chiave segreta scambiata tramite in modo sicuro utilizzando un cifrario a chiave pubblica. La lentezza della cifratura asimmetrica si paga solo per lo scambio, i messaggi sono veloci da cifrare. Risolve anche il problema degli attacchi chosen plain-text.

Esempio:

- Alice ottiene la chiave pubblica di Bob k_{pub} e genera una chiave AES k da 256 bit;
- Alice spedisce $(C_{\text{RSA}}(k, k_{\text{pub}}), C_{\text{AES}}(m, k))$;
- da questo momento tutti i messaggi della sessione vengono cifrati tramite AES con k.

Problemi:

- suscettibile ad attacchi MITM nella fase di ricezione della chiave pubblica – risolto con certificati digitali;
- la generazione di k è interamente a carico di Alice, ma Bob potrebbe non fidarsi – protocollo Diffie-Hellman;
- non garantisce forward secrecy – DH.