

Corso di Sicurezza nelle reti di telecomunicazioni
a.a. 2004/2005

Esempio di quesiti sulla prima parte del corso

- 1) Si consideri un semplice cifrario a sostituzione con shift (cifrario di Cesare), con un alfabeto di N caratteri (con $N=21$ o 26 a scelta), con chiave $K=8$. Si cripti la stringa "GIALLO"
- 2) Si supponga di voler inviare in modo sicuro un messaggio m da A a B , garantendo SOLO l'autenticità/integrità dei dati inviati. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, avendo a disposizione SOLO un algoritmo di crittografia asimmetrica e le chiavi pubbliche e private di A e B (K_U =chiave pubblica, K_R =chiave privata).

Invio	Ricezione

- 3) Dato un algoritmo $E_K(\cdot)$ di crittografia a blocchi di lunghezza q , si descriva lo schema di codifica di tipo CBC (Cipher Block Chaining) di un messaggio m di lunghezza $L > q$ (si supponga per semplicità $L = n \cdot q$).

- 4) Indicare un possibile schema di mutua autenticazione (forte) tra due utenti Alice e Bob, basato sull'uso di una funzione hash $H(\cdot)$ e su un segreto condiviso K_{AB} .

