Corso di Sicurezza nelle reti di telecomunicazioni
a.a. 2008/2009

Soluzione dei quesiti sulla prima parte del corso

1) Si consideri un semplice cifrario a sostituzione con shift (tipo cifrario di Cesare), con un alfabeto di N caratteri (con N=21 o 26 a scelta), con chiave K=4. Si cripti la stringa "SEGRETO"

SOLUZIONE
Nel caso si consideri un alfabeto di 21 caratteri, c = $E_k(m) = E_4$("SEGRETO") = "ZIMVIAS"
Nel caso si consideri invece un alfabeto di 26 caratteri, c = "WIKVIXS"

2) Si costruisca una coppia di chiavi privata/pubblica per RSA, utilizzando come coppia di numeri primi *p* e *q* i seguenti valori: p=3, q=11. Con tale chiavi si cripti il messaggio m=2.

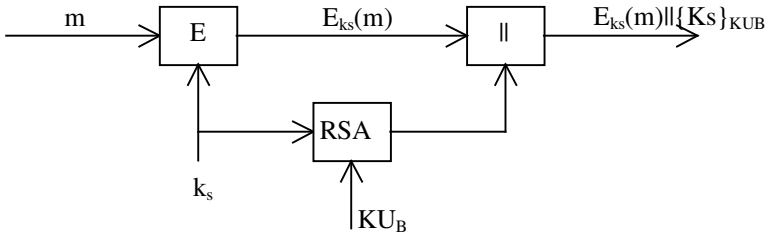
SOLUZIONE
n=pq=33
$\phi(n)=(p-1)(q-1)=20$
possibili candidati alla coppia e,d sono: 1,3,7,9,11,13,17,19
se si sceglie *e*=7, si trova che il moltiplicativo inverso di *e* modulo $\phi(n)$ è *d*=3; infatti ed=1 mod 20
e e *d* possono essere usate rispettivamente come chiave pubblica e privata per cifrare decifrare m; quidi:
$c=E(m)=2^7 \bmod 33=29$
si può verificare che:
$m=D(c)=29^3 \bmod 33=((29x29) \bmod 33) \bmod 33)=16x29 \bmod 33=2$

3) Si faccia un esempio di creazione di chiave condivisa tra A e B con Diffie-Hellman, utilizzando per il generatore g e il numero primo p i seguenti valori: g=2, p=11.

SOLUZIONE
Supponendo che A scelga il segreto x_a=5, mentre B scelga il segreto x_b=3, si ha:
A invia a B $ya=g^{xa} \bmod p=10$
B invia ad A $ya=g^{xb} \bmod p=8$
dati ya e xb, B costruisce: $Kba=ya^{xb} \bmod p=10^3=100x10=1x10=10$
dati yb e xa, A costruisce $Kab= yb^{xa} \bmod p=8^5=(8^2)^2x8=2^2x8=4x8=10$
giustamente si ha Kab=Kba

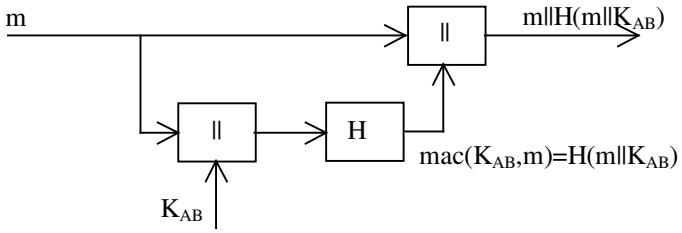
4) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO la confidenzialità dei dati inviati. Per la cifratura del messaggio si utilizzi un algoritmo di crittografia simmetrica. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano tra loro solo le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

SOLUZIONE



5) 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, supponendo che A e B condividano una chiave segreta K_{AB}, e che dispongano solo di un algoritmo di hash H().

SOLUZIONE



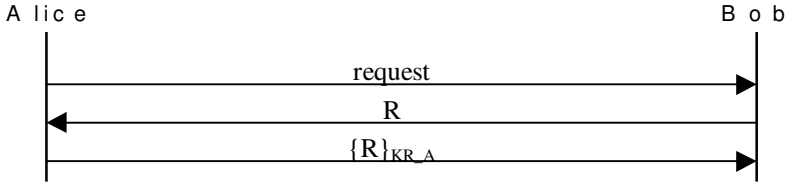
6) Dato un algoritmo $E_K(\cdot)$ di crittografia a blocchi di lunghezza q, si descriva lo schema di codifica di tipo CBC (Cipher Block Chaining) di un messaggio m di lunghezza L>q (si supponga per semplicità L=n q).

SOLUZIONE
$m=m1||m2|| \ldots ||m_n$
$c=IV||m1||m2|| \ldots ||m_n$

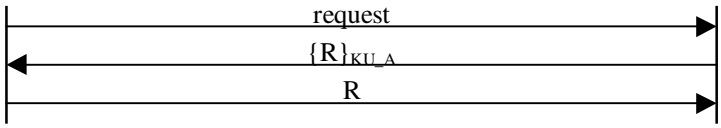
con:
$c_0=IV$
$c_i=Ek(m_i \oplus c_{i-1})$

7) Indicare un possibile schema sicuro di autenticazione tra Alice (supplicant) e Bob (authenticator), nell'ipotesi che Alice e Bob condividano le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

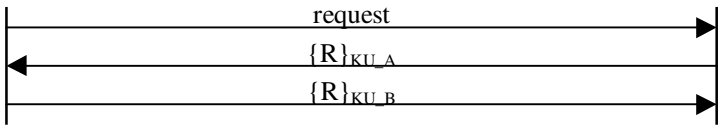
SOLUZIONE



oppure:



oppure:



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

SOLUZIONE