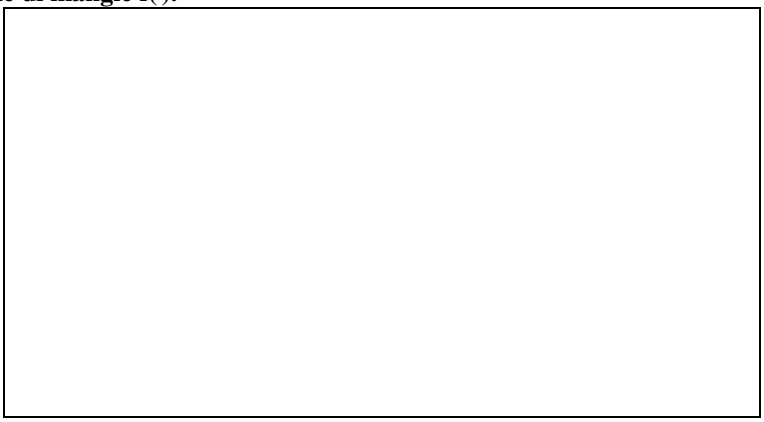
# Corso di Sicurezza nelle reti
# a.a. 2009/2010

## Raccolta di alcuni quesiti del corso da 5CFU
## e prima parte del corso da 9CFU

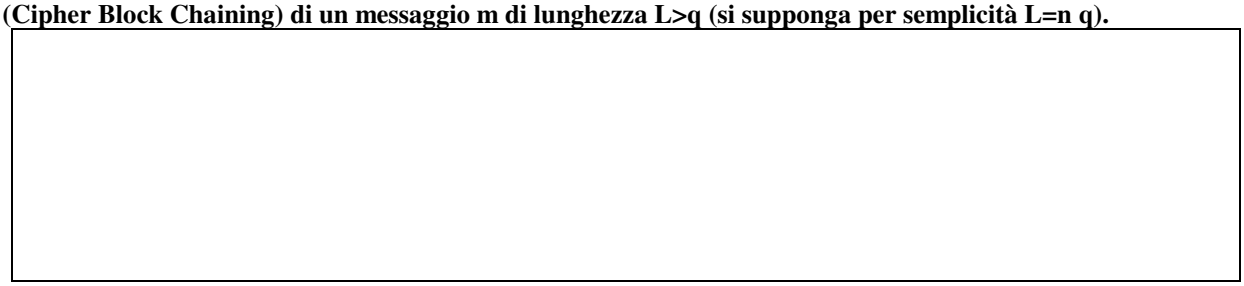
**1) Si consideri un semplice cifrario a sostituzione con shift (tipo cifrario di Cesare), con un alfabeto di N caratteri (con N=21 o 26 a scelta), con chiave K=4. Si cripti la stringa "SEGRETO"**

| ***Plain text*** | ***Cipher text*** |
|---|---|
| SEGRETO | |

**2) Si indichi lo schema di un singolo round del DES$^-$ (o anche di un generico cifrario di Feistel), senza entrare nel dettaglio della funzione di mangle f(·).**

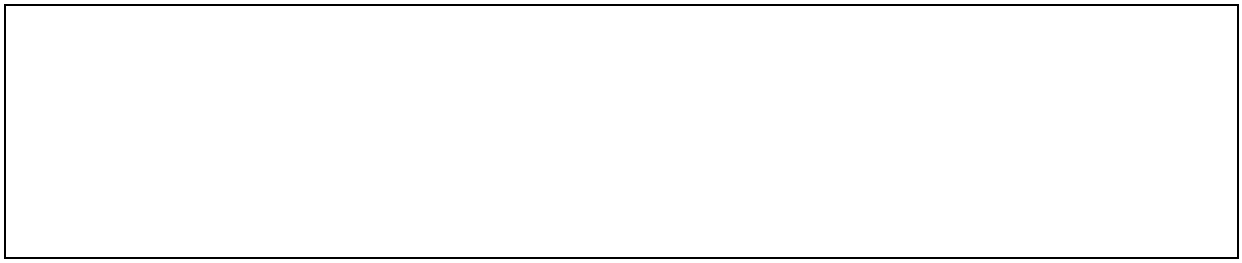


**3) Dato un algoritmo $E_K(\cdot)$ di crittografia a blocchi di lunghezza q, si descriva lo schema di codifica di tipo CBC (Cipher Block Chaining) di un messaggio m di lunghezza L>q (si supponga per semplicità L=n q).**



**4) Indicare lo schema del HMAC in funzione di un algoritmo di hash H(.), e calcolare il numero di passate che devono essere svolte con H durante il calcolo dell'HMAC di un messaggio m lungo N.M dove M è la dimensione di blocco che H elabora in una singola passata (e.g. M=512bit nel caso di MD5 e SHA1).**

Schema dell'HMAC



Numero di passate necessarie per calcolare l'HMAC di un messaggio lungo N·M dove M è la dimensione di blocco di H:

**5) Costruire uno schema di crittografia simmetrica per criptare messaggi m di qualsiasi lunghezza tramite chiave segreta K, basato su algoritmo di crittografia a blocchi $E_K()$ (e.g. AES) ma SENZA effetto valanga, cioè in modo che la modifica di un bit del testo cifrato abbia effetto su un solo bit del testo in chiaro (Suggerimento, nello schema utilizzare anche l'operazione XOR).**

| |
|---|
| |

**6) 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 quali 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).**

| Invio | Ricezione |
|---|---|
| | |

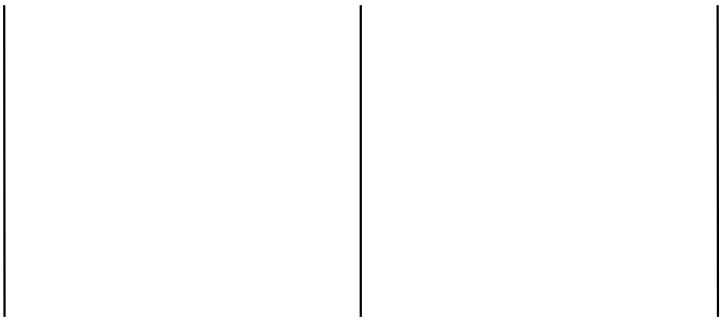
**7) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO l'autenticità/integrità dei dati inviati. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano una chiave segreta $K_{AB}$, e che dispongano solo di un algoritmo di hash H().**

| Invio | Ricezione |
|---|---|
| | |

**8) 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).**

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


**10) Si consideri uno schema di scambio di chiavi tra A e B di tipo Diffie-Hellman, e si indichi come questo può essere attaccato con successo da una terza parte C.**



**11) Perché il seguente schema di distribuzione di chiave di sessione Ks tramite crittografia simmetrica non è sicuro? (si è indicato con Ka e Kb le chiavi segrete condivise rispettivamente tra KDC e A, e KDC e B; con Ks la chiave di sessione)**

| | | | |
|---|---|---|---|
| A | → | KDC: | IDa, IDb |
| KDC | → | A: | IDb, Ks |
| A | → | B: | IDa, Ks |

**b) E il seguente?**

| | | | |
|---|---|---|---|
| A | → | KDC: | $ID_A$, $ID_B$ |
| KDC | → | A: | IDb, {Ks}Ka ,{Ks}Kb |
| A | → | B: | IDa, {Ks}Kb |

**c) Come è possibile migliorare il precedente schema?**

**12) Nell'ipotesi che date tre entità A, B e C:**

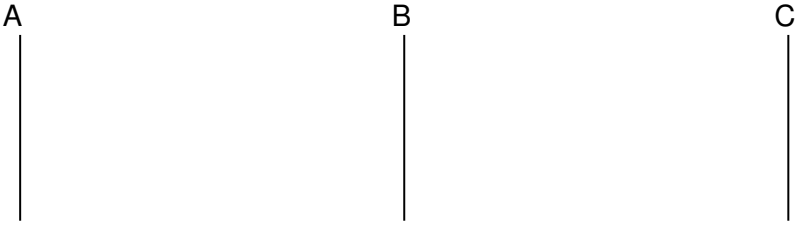
**i) A possieda una coppia di chiavi privata/pubblica $PK_A$ e $PU_A$;**

**ii) C possieda la chiave pubblica di A, $PU_A$;**

**iii) B e C condividano una chiave segreta $K_{BC}$;**

**iv) B e C non dispongano di alcun canale di comunicazione tra loro.**

**Si chiede di indicare un possibile schema di comunicazione tramite il quale sia possibile instaurare una associazione sicura tra A e B ($K_{AB}$).**



**13) Nell'ipotesi che A possieda i seguenti certificati digitali: $cert_{A|CA3}$, $cert_{CA3|CA2}$, $cert_{CA2|CA1}$, e $cert_{CA1|CA1}$ (dove è indicato con $cert_{X|Y}$ il certificato di X firmato da Y), indicare cosa è necessario che A invii a B in modo tale che B possa comunicare in modo sicuro con A, nei seguenti casi:**

| B possiede: | A deve inviare a B: |
|---|---|
| $cert_{CA1\|CA1}$ | |
| $cert_{A\|CA3}$ | |
| $cert_{CA2\|CA1}$ | |
| $cert_{CA1\|CA1}$, $cert_{A\|CA3}$ | |

**14) Se A possiede $cert_{A|B}$ e $cert_{B|C}$ (dove si è indicato con $cert_{X|Y}$ il certificato di X firmato da Y), mentre D possiede $cert_{D|E}$, indicare:**
**a) cosa deve possedere A per autenticare D, e un possibile schema di autenticazione?**

**b) cosa deve possedere D per autenticare A, e un possibile schema di autenticazione?**

**15) 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.**

**16) 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.**


**17) Tramite l'algoritmo di Euclide determinare il massimo comune divisore gcd( , ) tra:**
**a) 36, 15**
**b) 47, 20**
**c) 43, 35**

**18) Determinare $\lambda, \mu \in \mathbb{Z}$ tali che$25\,\lambda + 32\,\mu = 1$, per mezzo dell'Algoritmo di Euclide esteso, ed utilizzare il risultato ottenuto per risolvere l'equazione $25\,x \equiv 4 \bmod 32$**

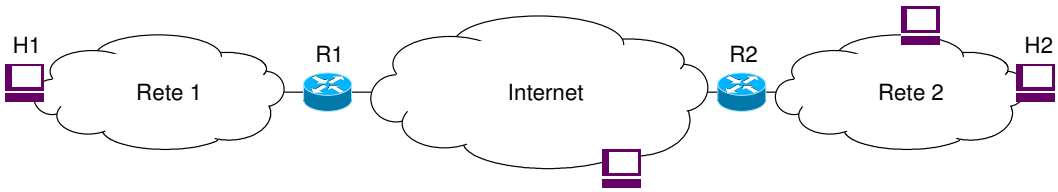
**19) Si costruisca una coppia di chiavi privata/pubblica per RSA, utilizzando come coppia di numeri primi *p* e *q* i seguenti valori: p=7, q=11 e come chiave pubblica KU=<e,n> con e=13. Con tale chiavi si decripti il messaggio c=2.**

**20) Si consideri lo schema di rete rappresentato in figura in cui due sottoreti aziendali sono interconnesse tra loro in VPN tramite rete IP pubblica attraverso IPSec.**

**Nell'ipotesi che la VPN sia instaurata tra i router R1 e R2 utilizzando ESP e AH (con AH che protegge anche il contenuto di ESP), e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili (transport/tunnel), si chiede di:**

**i) indicare lo schema dei pacchetti che transitano nel tratto di rete esterna inviati da H1 a H2;**

**ii) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA).**




**21) Si consideri uno scenario tipo road-warrior in cui un nodo H1 si collega tramite IPSec alla sua rete aziendale e comunichi in modo sicuro con un nodo interno H2, come rappresentato in figura.**

**Nell'ipotesi che H1 si colleghi alla sua rete tramite il router R1 in IPSec/ESP, che H1 protegga la sua comunicazione con il nodo H2 tramite IPSec/ESP, e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili, si chiede di:**

**iii) indicare lo schema dei pacchetti che transitano nel tratto di rete esterna inviati da H1 a H2;**

**iv) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA).**