

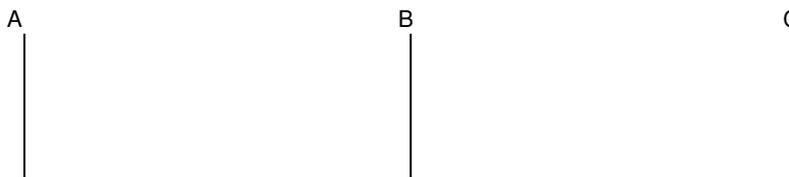
Corso di Sicurezza nelle reti di telecomunicazioni  
a.a. 2008/2009

Esempio di quesiti sulla seconda parte del corso

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

- i) A possiede un certificato digitale X.509  $Cert_A$  (con chiave pubblica  $PU_A$ ) e relativa chiave privata  $PK_A$ ;
- ii) C possiede il certificato di A;
- iii) B e C condividano una chiave segreta  $K_{BC}$ ;
- iv) B e C non dispongano di alcun canale di comunicazione tra loro.

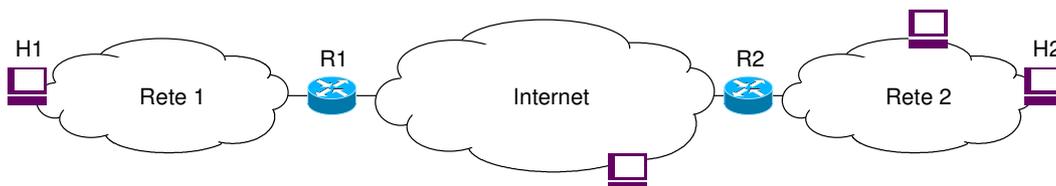
Si chiede di indicare un possibile schema di comunicazione tramite il quale sia possibile instaurare una associazione sicura tra A e B ( $K_{AB}$ ).



2) 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).



3) 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).

