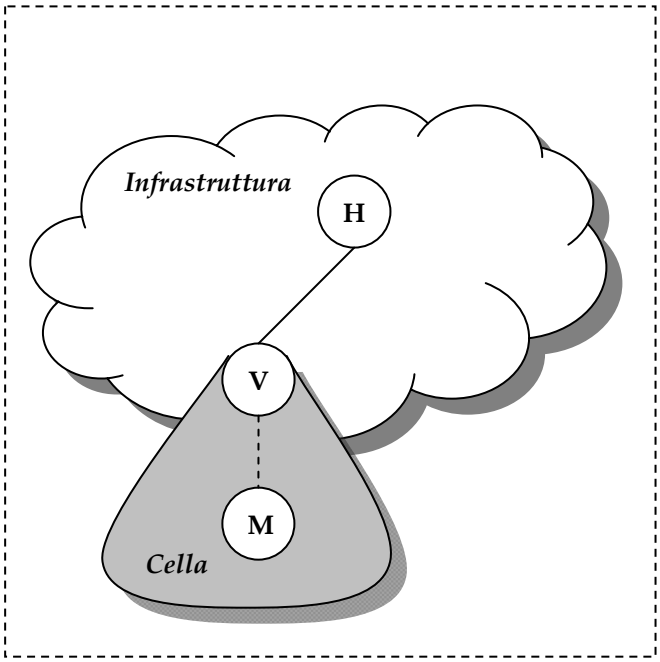
ESERCIZIO 2: Si consideri il sistema di *roaming* riportato in figura in cui una stazione mobile *M*, il cui *home server* è *H*, si trova in visita nella cella gestita dal server *V*. La stazione mobile *M* ed l'home server *H* condividono la chiave k_{mh}. I server *H* e *V* fanno parte dell'infrastruttura fissa e condividono la chiave k_{vh}. Progettare un protocollo che soddisfi i seguenti requisiti:

1. permette l'autenticazione mutua di *M* e *V* quando *M* entra nella cella *V*;
2. permette di distribuire una chiave di sessione k_{mv} tra *M* e *V*;
3. fornisce la prova a *V* che *M* possiede k_{mv} e viceversa;
4. mantiene la segretezza della chiave k_{mh};
5. è resistente ad attacchi di replay.

Si assuma che *M*, *H*, *V* utilizzino lo stesso cifrario e che i loro clock non siano sincronizzati. Il candidato argomenti brevemente ed informalmente, ma con precisione matematica e proprietà di linguaggi, che il protocollo proposto soddisfa i requisiti posti.



Soluzione

Nella soluzione indichiamo con $E(k, m)$ la cifratura del messaggio m con la chiave k e con $a \| b$ la concatenazione della quantità a con la quantità b.

1. $M \rightarrow V$: A, n_m
2. $V \rightarrow H$: A, n_m, n_v
3. $H \rightarrow V$: $E(k_{hm}, V \| n_m \| k), E(k_{hv}, A \| n_v \| n_m \| k)$
4. $V \rightarrow M$: $E(k_{hm}, V \| n_m \| n_v \| k), E(k, V \| M \| n_m)$
5. $M \rightarrow V$: $E(k, M \| V \| n_v + 1)$