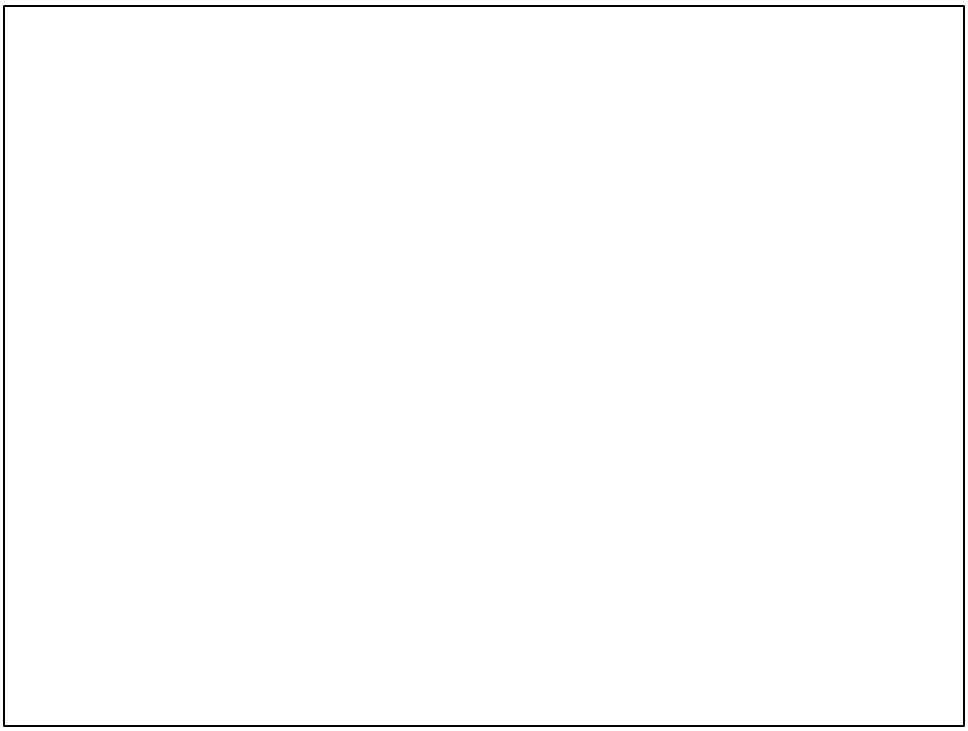
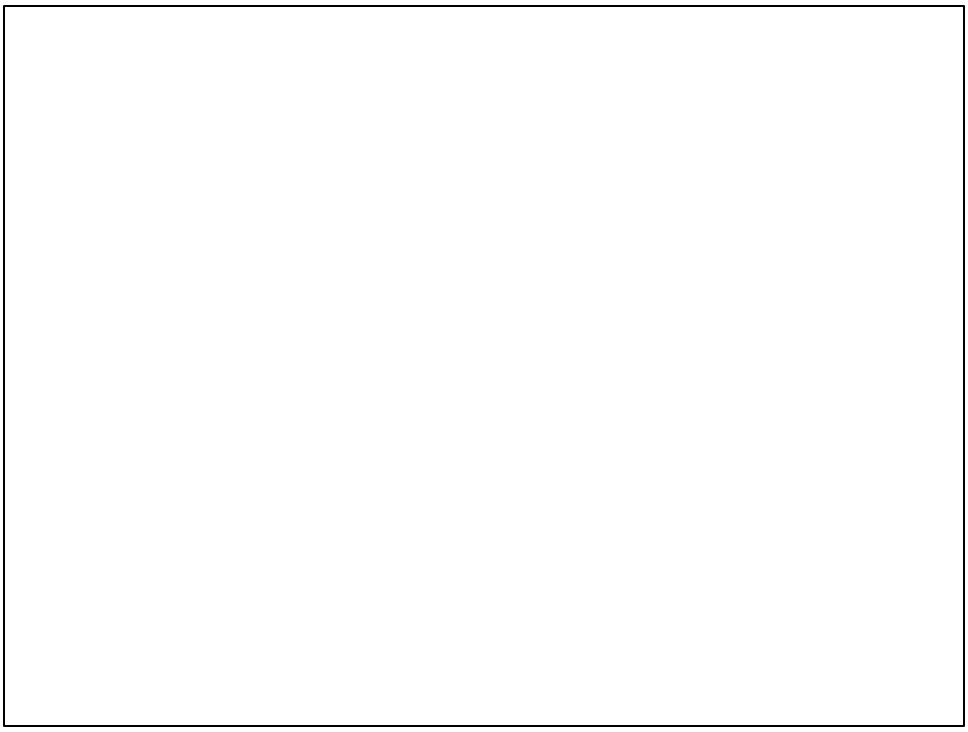
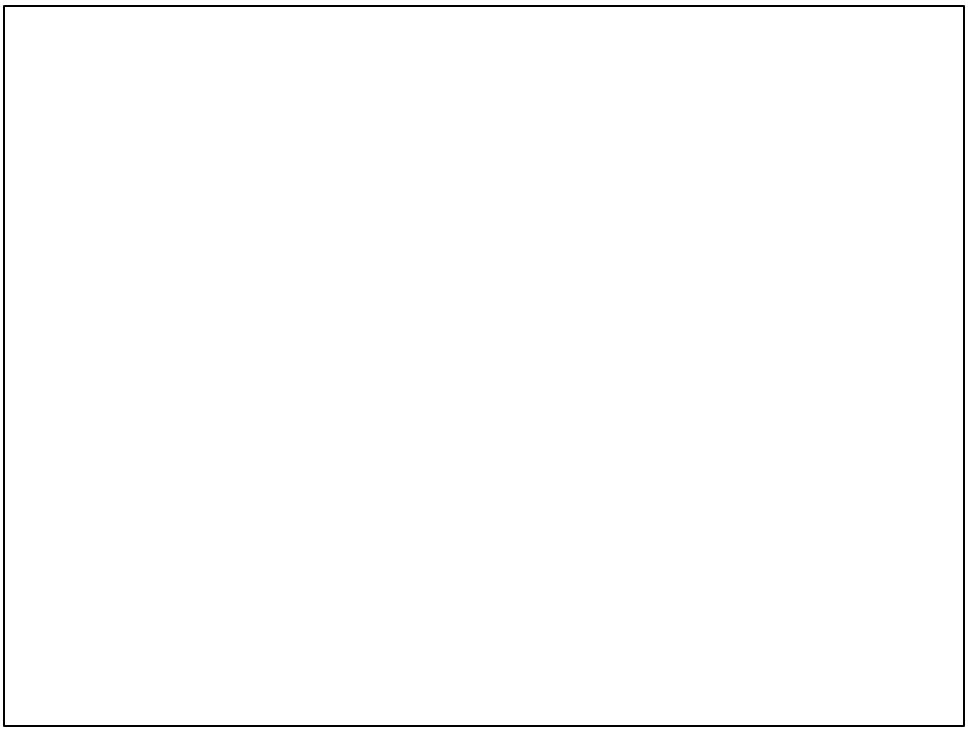
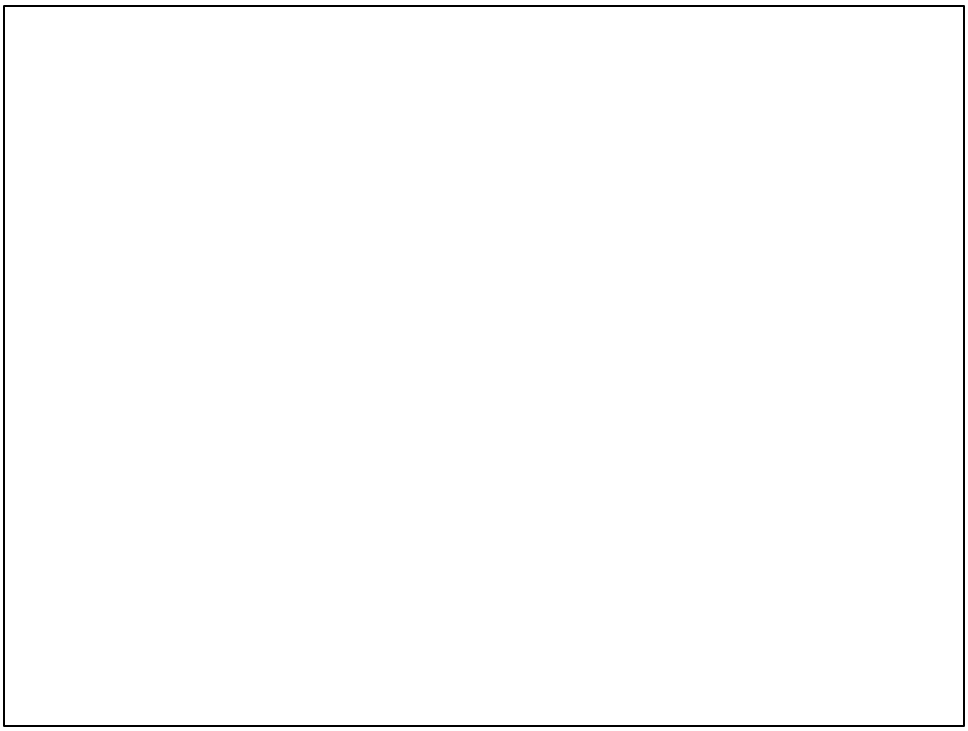




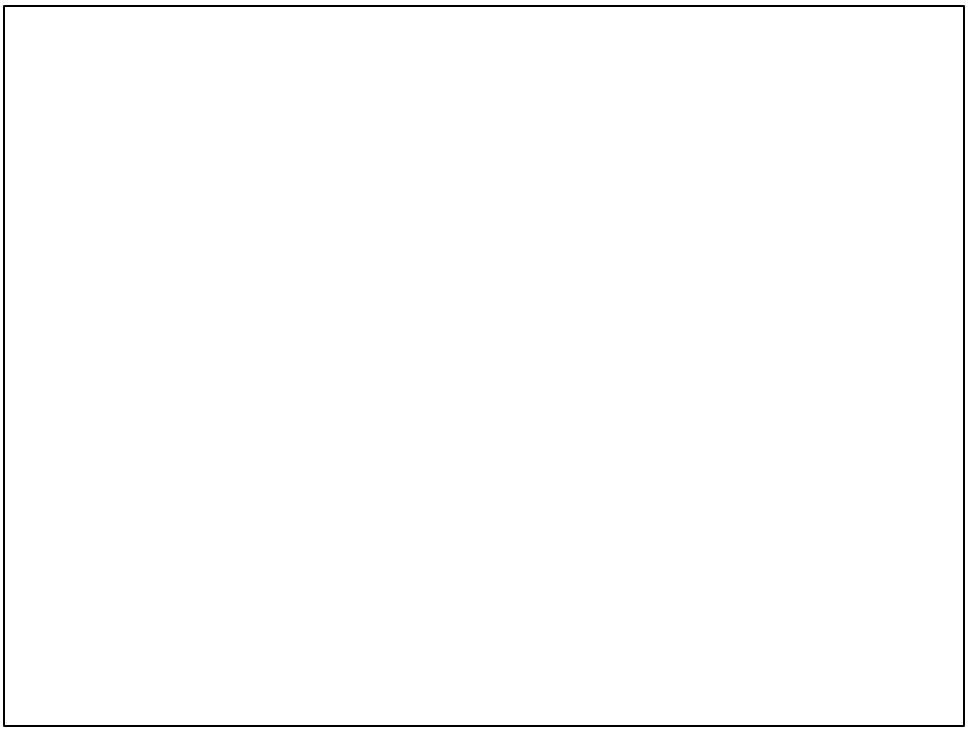
Vulnerabile a reply attack, poiché B dimentica R e A può inviare una coppia R, K{R} registrata da una sessione precedente.

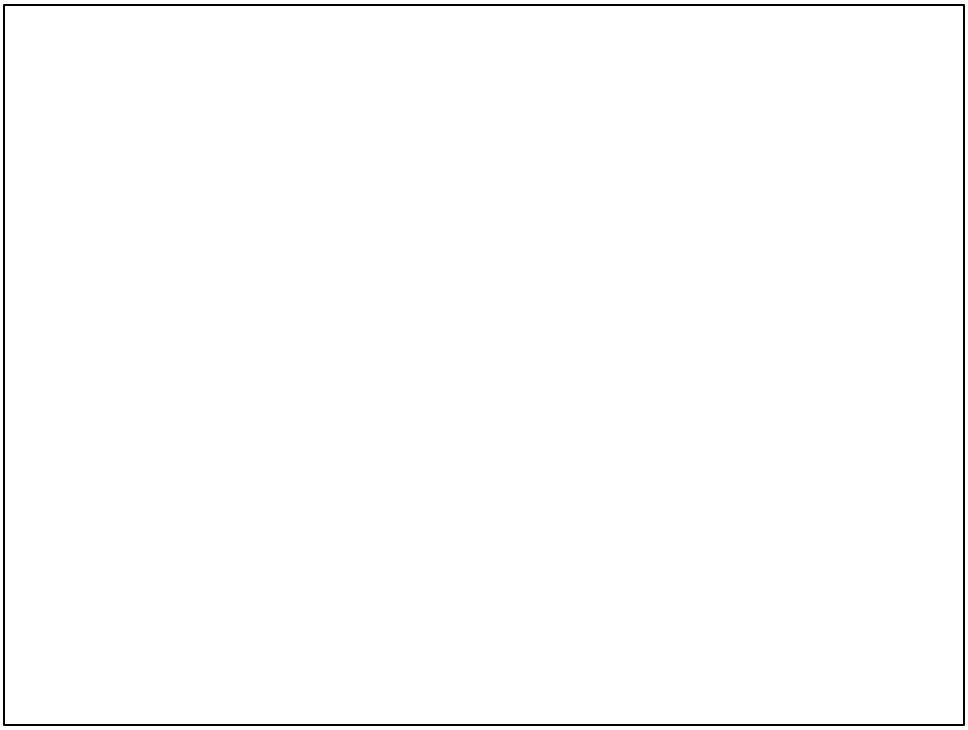


come sopra, non è necessario conoscere R ma solo la coppia $K_B\{R\}$, $K\{R\}$



Alice può ora impersonare solo utenti su una stessa macchina con un reply attack





A $\rightarrow$ R1 $\rightarrow$ B

A $\leftarrow$ $[R1]_B$ $\leftarrow$ B

A $\leftarrow$ R2 $\leftarrow$ B

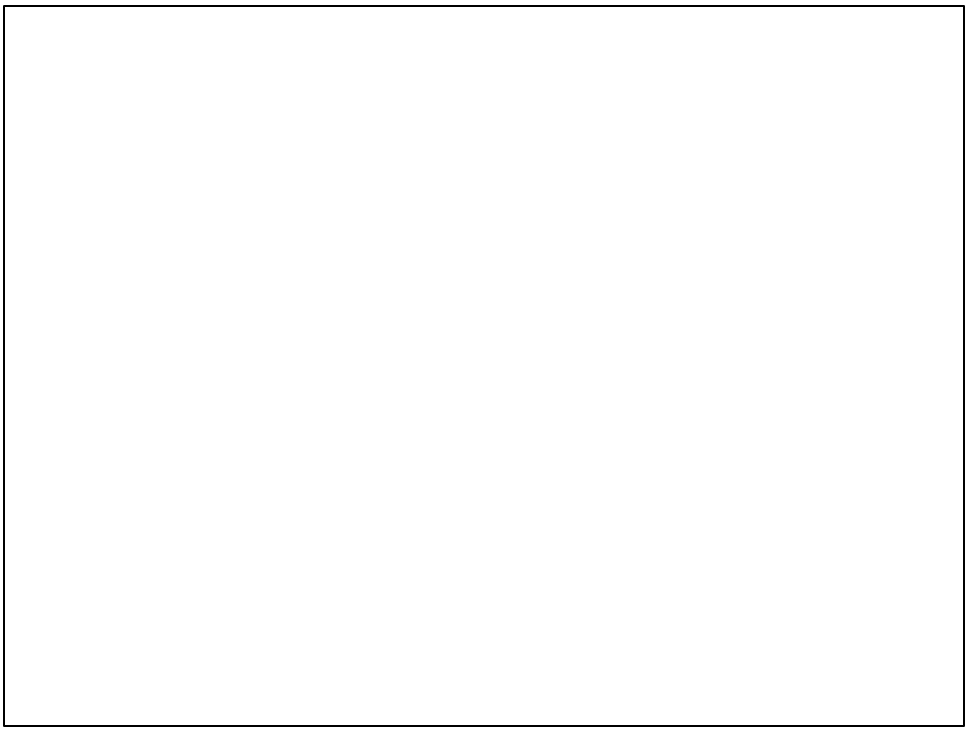
A $\rightarrow$ $[R2]_A$ $\rightarrow$ B

genera S_1 genera S_2

A $\rightarrow$ $[\{S_1\}_B]_A$ $\rightarrow$ B (la firma è necessaria altrimenti vulnerabile ad hijacking)

A $\leftarrow$ $[\{S_2\}_A]_B$ $\leftarrow$ B

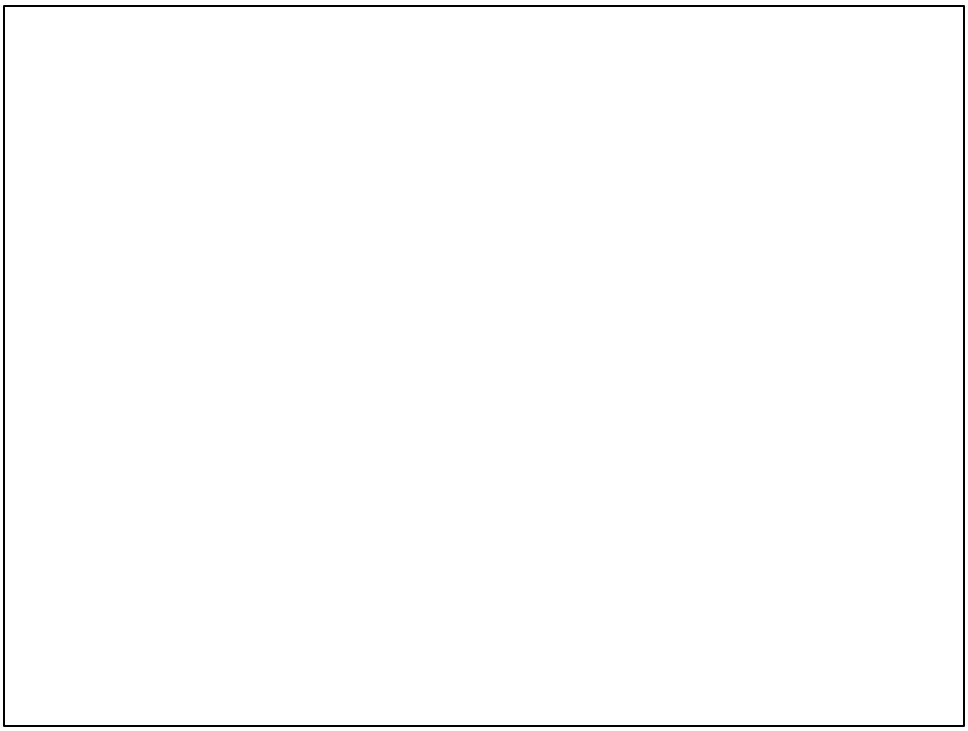
session key= S_1 xor S_2

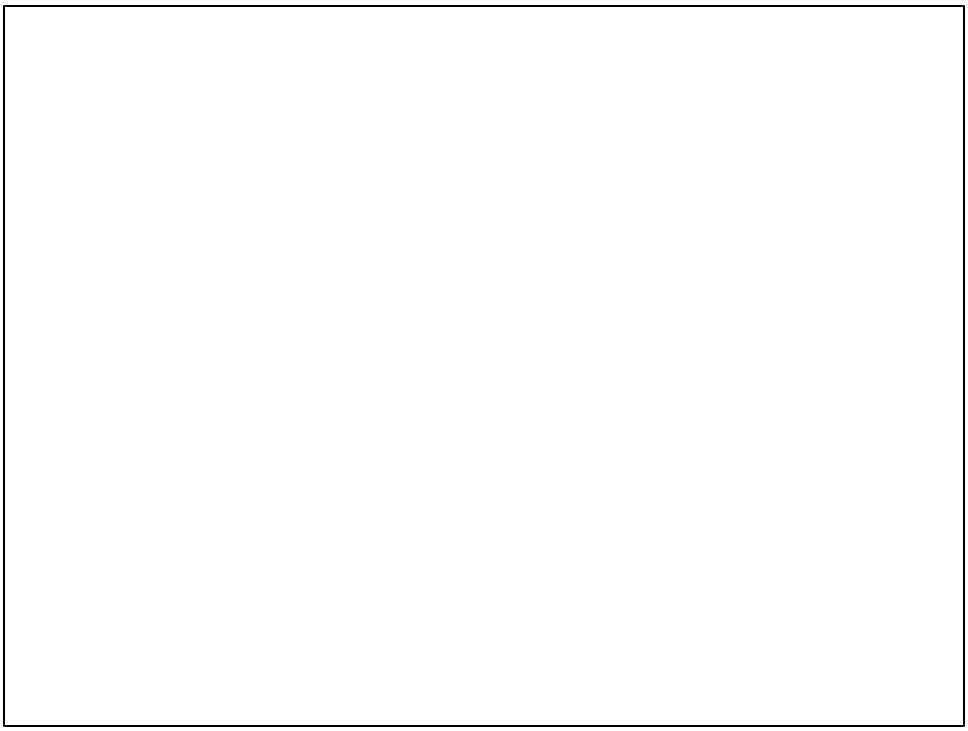


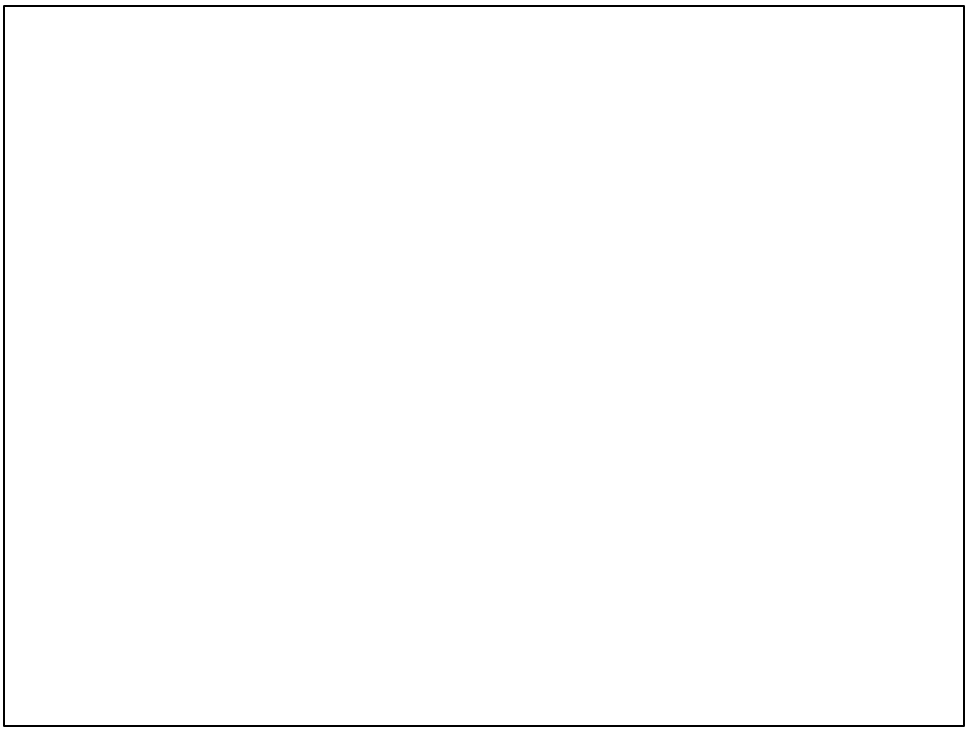
A $\rightarrow \{ S_1 \mid [S_1]_A \}_B \rightarrow$ B

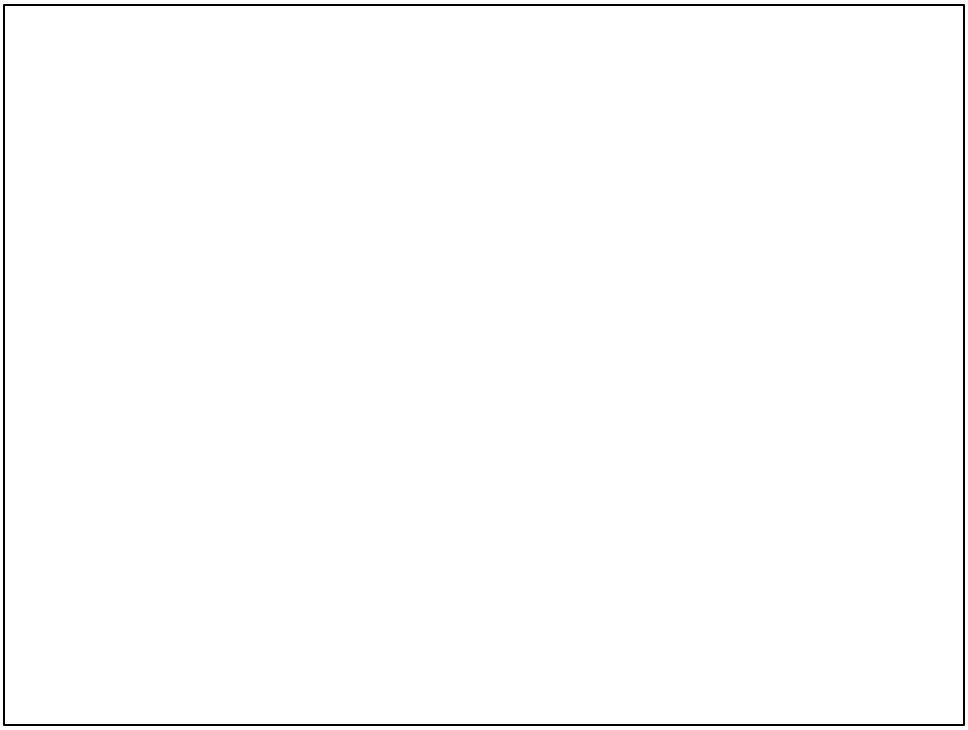
A $\leftarrow \{ S_2 \mid [S_2]_B \}_A \leftarrow$ B

session key= S_1 xor S_2









Supponiamo cha A e B abbiano ciascuna una coppia di chiavi pubbliche.

A genera nuova coppia EA effimera

B genera nuova coppia EB effimera

A $\rightarrow$ { EA.public | $[EA.public]_A$ }$_B$ $\rightarrow$ B

A $\leftarrow$ { EB.public | $[EB.public]_B$ }$_A$ $\leftarrow$ B

A $\rightarrow$ { S_1 }$_{EB}$ $\rightarrow$ B

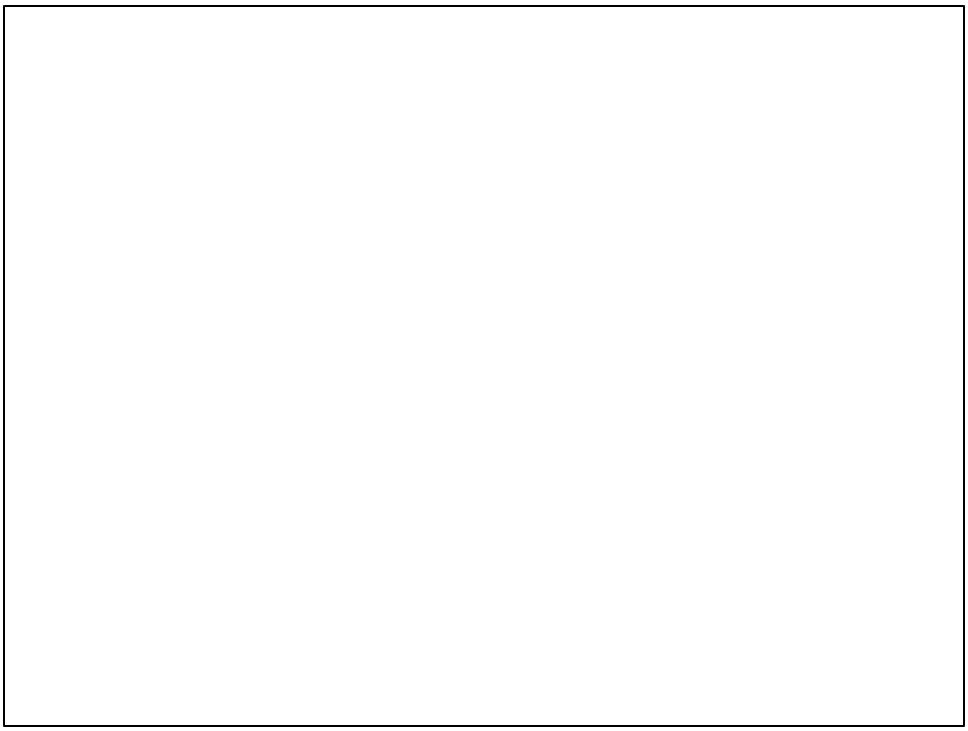
A $\leftarrow$ { S_2 }$_{EA}$ $\leftarrow$ B

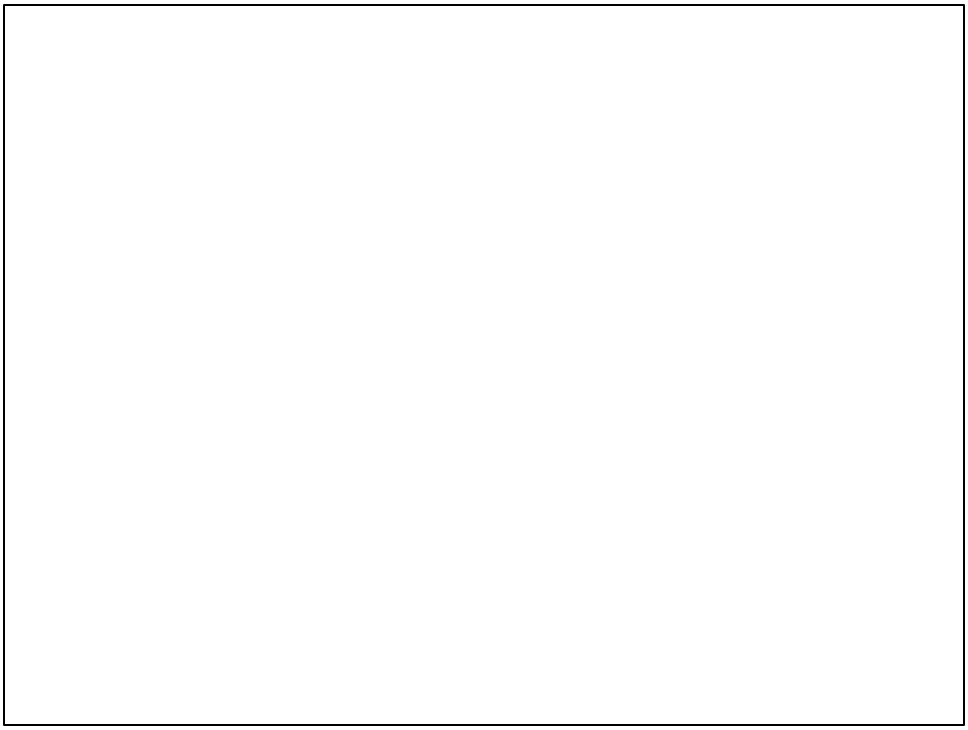
$S=S_1$ xor S_2

A dimentica EA

B dimentica EB

inizia lo scambio dati usando S





Supponiamo cha A e B abbiano ciascuna una coppia di chiavi pubbliche e siano d'accordo su g e p

A genera nuova coppia EA effimera DH: a, $g^a \bmod p$

B genera nuova coppia EB effimera DH: b, $g^b \bmod p$

A $\rightarrow g^a \bmod p \mid [g^a \bmod p]_A \rightarrow$ B

A $\leftarrow g^b \bmod p \mid [g^b \bmod p]_B \leftarrow$ B

$S= g^{ab} \bmod p$

A dimentica a

B dimentica b