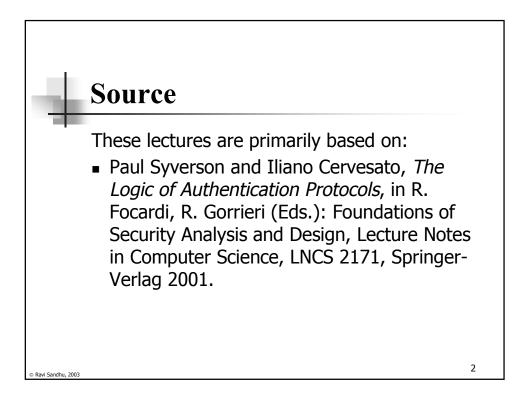
## Logic of Authentication 1. BAN Logic

Ravi Sandhu



## Protocol 1 (Needham-Schroeder Shared-Key) [NS78]

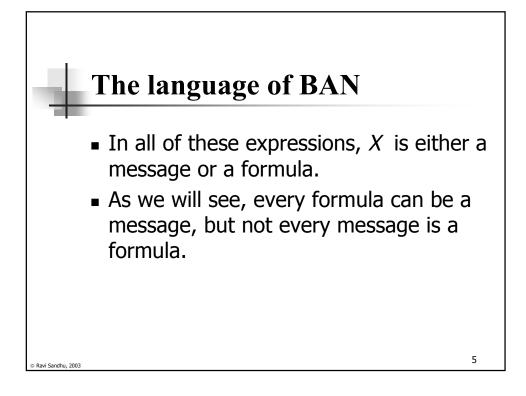
 $\begin{array}{l} Message \ 1 \ A \rightarrow S : A, B, n_A \\ Message \ 2 \ S \rightarrow A : \{n_A, B, k_{AB}, \{k_{AB}, A\}k_{BS}\}k_{AS} \\ Message \ 3 \ A \rightarrow B : \{k_{AB}, A\}k_{BS} \\ Message \ 4 \ B \rightarrow A : \{n_B\}k_{AB} \\ Message \ 5 \ A \rightarrow B : \{n_B - 1\}k_{AB} \\ \end{array}$ Nonces are random unpredictable values generated by a principal and included in messages so that she can tell any messages later received and containing her nonce must have been produced after she generated and

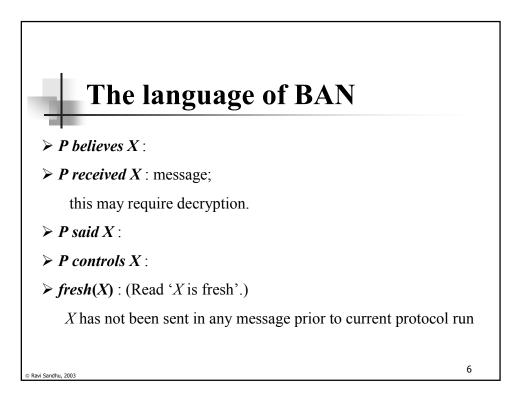
3

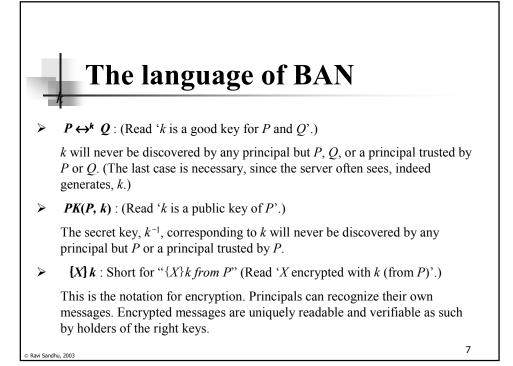
sent the nonce.

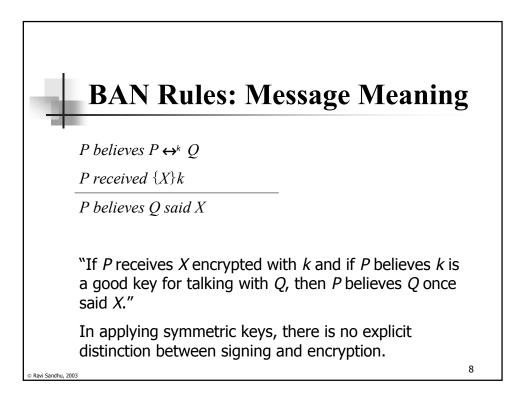
Ravi Sandhu, 2003

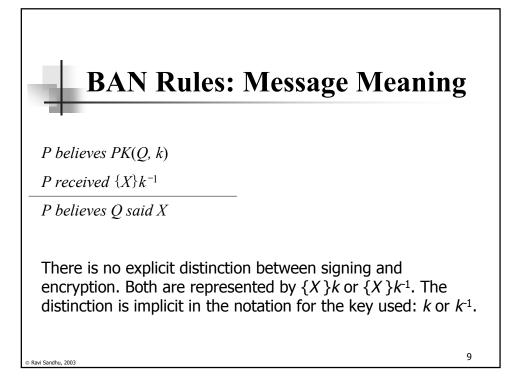
<section-header><list-item><list-item><list-item>

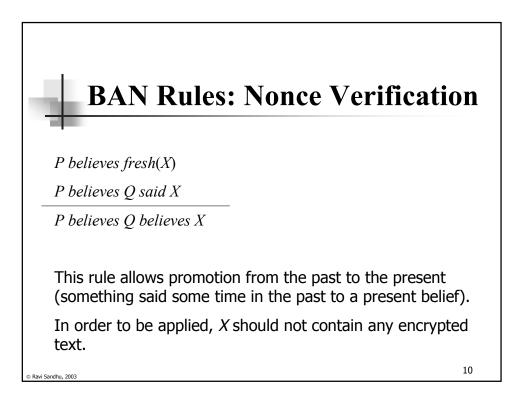


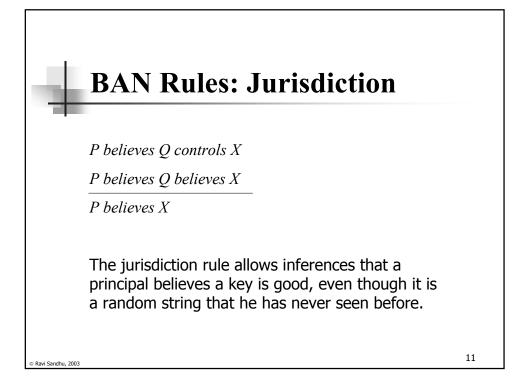


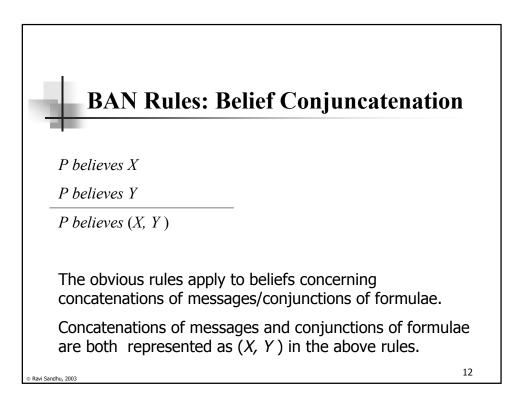




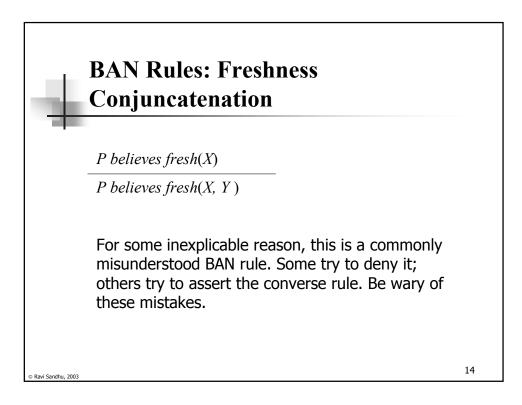


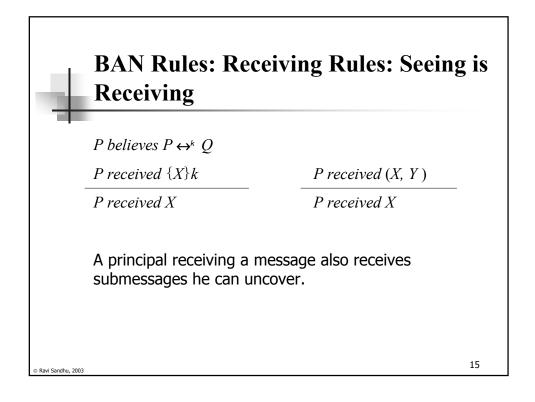


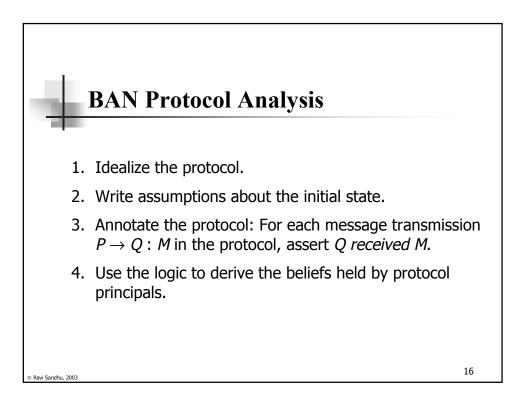




P believes Q believes (X, Y)	P believes $Q$ said $(X, Y)$
P believes Q believes X	P believes Q said X
We do not list all of the rules, representative sampling.	; we give only a







## Protocol 1 (Needham-Schroeder Shared-Key) [NS78]

$$\begin{split} &Message \ 1 \ A \to S : A, B, n_A \\ &Message \ 2 \ S \to A : \{n_A, B, k_{AB}, \{k_{AB}, A\}k_{BS}\}k_{AS} \\ &Message \ 3 \ A \to B : \{k_{AB}, A\}k_{BS} \\ &Message \ 4 \ B \to A : \{n_B\}k_{AB} \\ &Message \ 5 \ A \to B : \{n_B - 1\}k_{AB} \end{split}$$

17

© Ravi Sandhu, 2003

