

2) DIGITAL SIGNATURE and DIGITAL CERTIFICATE

$$(b)$$
 $\beta - (-1) - A$

3) SECURITY PROTOCOL

(TYPE FLAW)
ATTACK

A LICE	VA
A, NA	
2 ENAZKAB, NB	ENA3KAB, NB
	Nel punto 2 EVA interesta 2 rahva NB.
	ENB KAB
(A) {NB} KAB	EK3KAB
Nel punto 4 Eva sostituisce il messaggio intercettato da B	
con il messaggio precidementemente salvato, struttando il fatto che	
NB = K & che A,B non effektum il typing dei messaggi, per esempio utilizzare i primi due	
bit di un messaggio per identificare se i un No una K.	

