(NSSK) (Soggetto a replay attack) · SHARED KEY ENA, KAB, B, EKAB, AZKBSZKAS 2 Qua rel punto 3, si può essere soggetto a replay attack. Un attaccante può interattare il pacchetto e poi decriptorbo afflire. ed essendo che non abbiasso ne nonce en timestamp eno può enere riutilizzato.

· SHARED KEY (NSSK) (Riparato con Timestamp)

ENA, KAB, B, EKAB, A, T > KBS & KAB, A, T 3KBS Nel punto 3 abbiarna risolto i posibili replay attack con il timestamp

· PUBLIC KEY (NSPK) (Soggetto a man in the middle)

ALICE

BOB

EA, NA 3 KB

(1)

Con man in the middle alice (Anithodic) di parlare con Charlie ma Charlie cattivo si finge alice con Bob, e quindi Bob pensa di parlare con alice ma in realta sta parlanda con Charlie

(2)

ENA, NB BKA

ENB3KB

3

· PUBLIC KEY (NSPK) (Riparato con ritamo identità)

ALICE

BOB

E Y Na 3 KB

Con riama riami che non à possibile man in Et middle

ENA, NB, B3KA

ENB3KB



