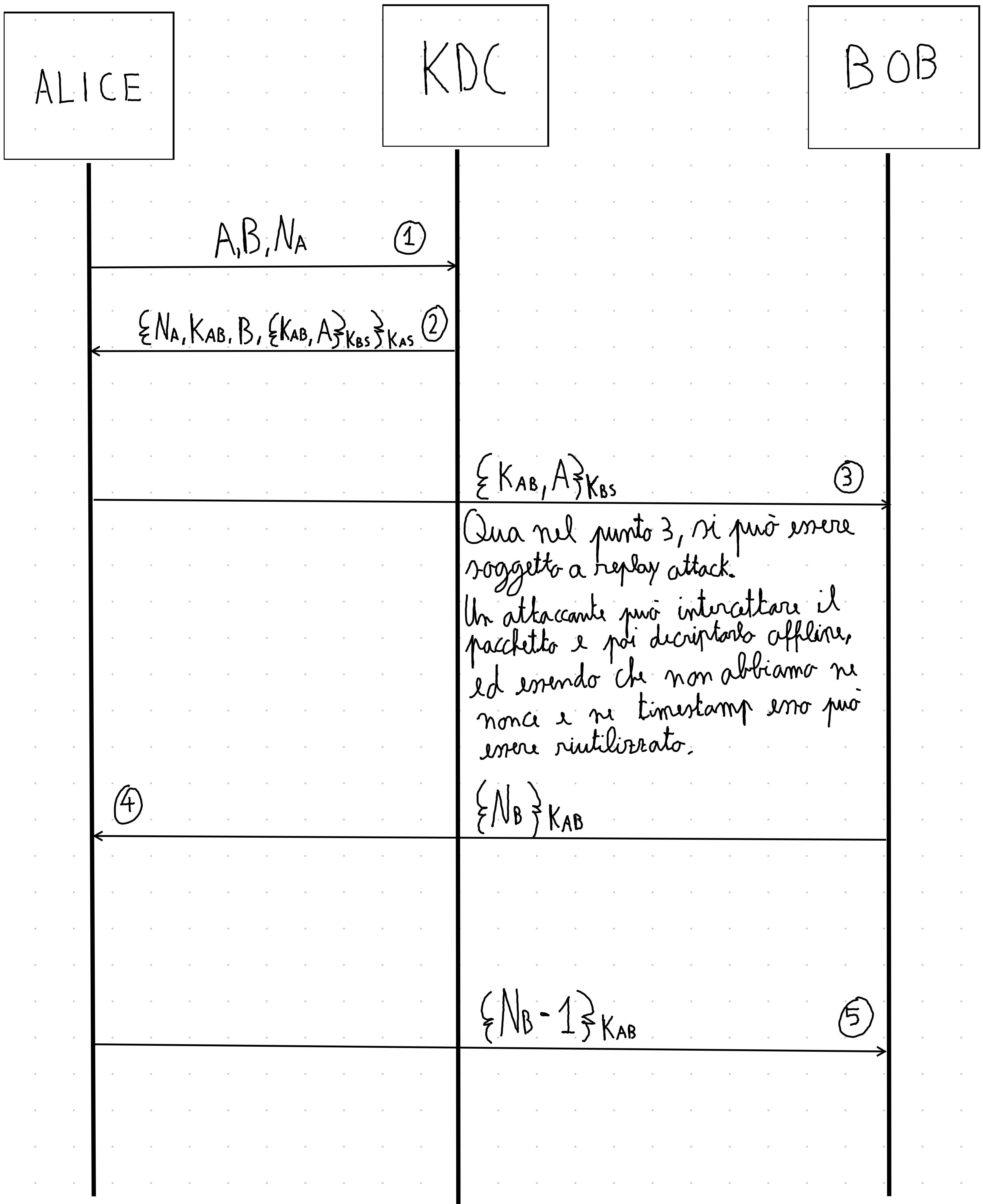
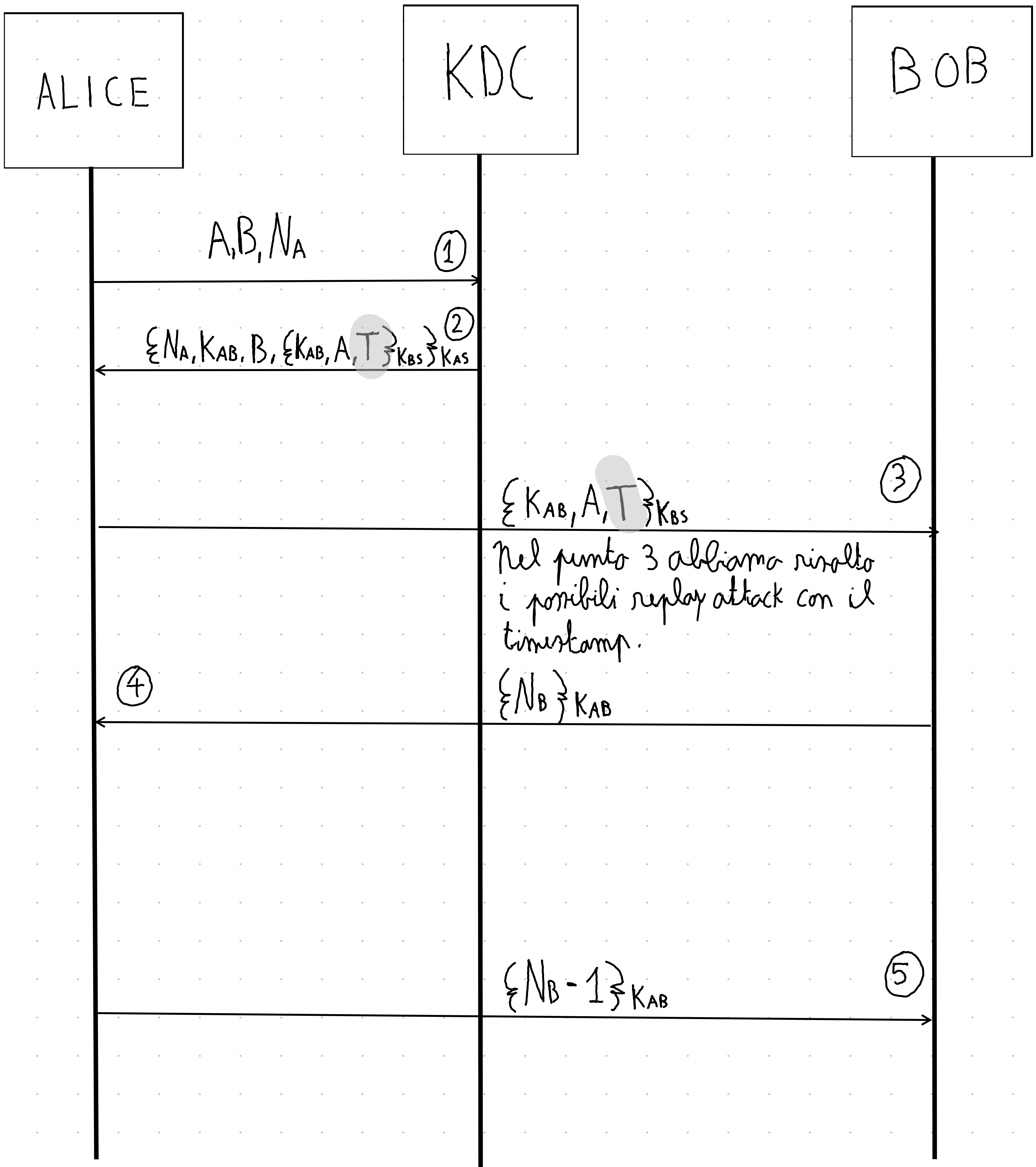


• SHARED KEY (NSSK) (Soggetto a replay attack)



• SHARED KEY (NSSK) (Riparato con Timestamp)



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

ALICE

BOB

$\{A, N_A\}_{K_B}$

①

Con man in the middle Alice ^(Anti fiducia di C) sa di parlare con Charlie ma Charlie cattivo si finge Alice con Bob, e quindi Bob pensa di parlare con Alice ma in realtà sta parlando con Charlie.

②

$\{N_A, N_B\}_{K_A}$

$\{N_B\}_{K_B}$

③

• PUBLIC KEY (NSPK) (Riparato con ritorno identità)

ALICE

BOB

$\{A, N_A\}_{K_B}$

Così siamo sicuri che non è possibile man in the middle

$\{N_A, N_B, B\}_{K_A}$

$\{N_B\}_{K_B}$

