Assignment # 2

Ayesha munir

221014

BSIT-VI-B

	Otway-Rees protocol	Needham-schroeder protocol
Computation complexity	• 4 encryptions: 2 by Alice, 2 by KDC • 2 decryptions: by KDC	• 3 encryptions: 1 by KDC, 2 by Bob • 2 decryptions: 1 by Alice, 1 by Bob
	Uses session key K_AB	Uses session key K_AB
	Total time: 4 encryptions (8 ms) + 2 decryptions (4 ms) = 12 ms	**Total time:** 3 encryptions (6 ms) + 2 decryptions (4 ms) = 10 ms
Communication overhead	Message 1: ID_A (64) + ID_B (64) + R (128) + encrypted(R_A + IDs) (≈512)	Message 1: ID_A (64) + ID_B (64) + R_A (128)
	Message 2: similar content sent to KDC	Message 2: encrypted part

		(≈512) with R_A, Bob ID, Alice ID
	Message 3: Encrypted data sent to Alice & Bob (~1024 bits total)	Ticket for Bob (~256) + encrypted session info (~512)
	Approx total bits: ~1800–2000 bits	**Approx total bits**: ~1500–1600 bits
Security characteristics	• Provides nonce-based freshness (R & R_A) • Prevents replay if KDC is trusted • No mutual authentication (relies on KDC integrity) • Less vulnerable to replay (compared to NS)	• Includes nonce R_B from Bob • Replay protection • No forward secrecy • Bob verifies freshness via R_B – 1 • Can be replayed if old ticket reused (Denning-Sacco attack)