

Άσκηση με KDCs [exercise with KDC]

Η Alice επιθυμεί να επικοινωνήσει εμπιστευτικά με τον Boris μέσω μιας αλυσίδας τριών KDCs (Alice's KDC – CIA KDC, ένα KDC που έχει κοινά κλειδιά τόσο με το KDC της Alice, όσο και με το KDC του Boris – UN KDC, και τελικά το KDC του Boris – KGB KDC). Δώστε σχηματικά την ακολουθία γεγονότων που είναι απαραίτητα για την αποκατάσταση της επικοινωνίας.

[Alice wants to establish a confidential communication with Boris through a chain of 3 KDCs (1. Alice's KDC – CIA KDC, 2. a KDC having common keys with both Alice's KDC and Boris' KDC – UN KDC, 3. Boris' KDC – KGB KDC). Give a diagram showing the sequence of steps required for the establishment of communication].