Homework 2

Due Date: October 21

Problem 1: Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in cipher block chaining (CBC) mode? How about decryption? [5+10]

Problem 2: If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate? [10]

Problem 3: One local area network vendor provides a key distribution facility, as illustrated in Figure 1.

a. Describe the scheme. [25]

b. Compare this scheme to that of Figure 2. What are the pros and cons? [30]

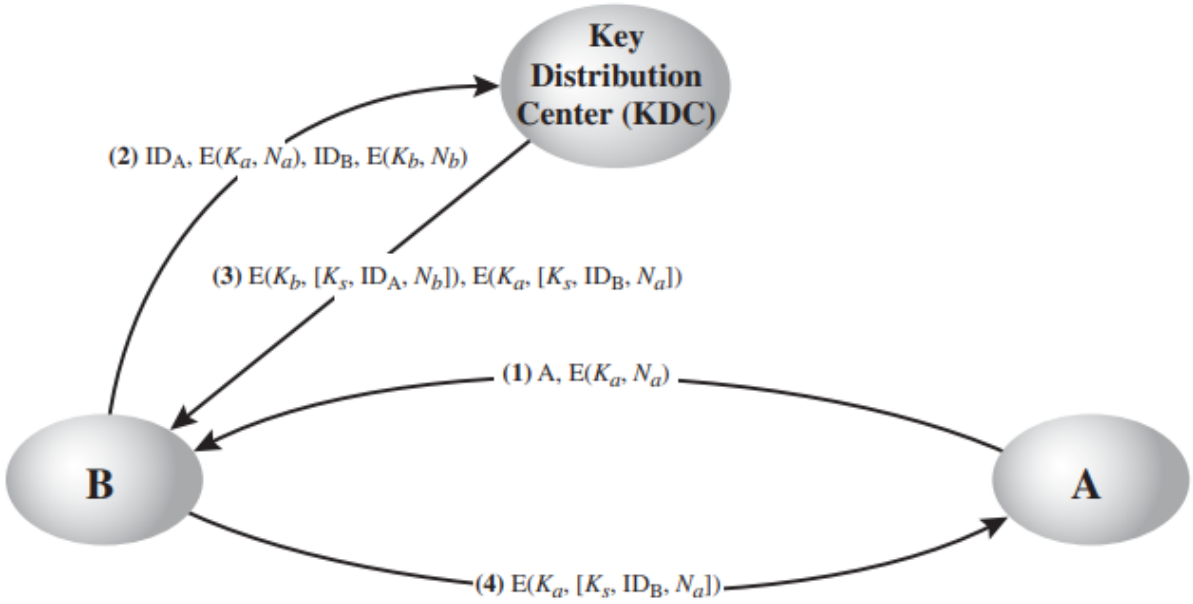

Fig 1.

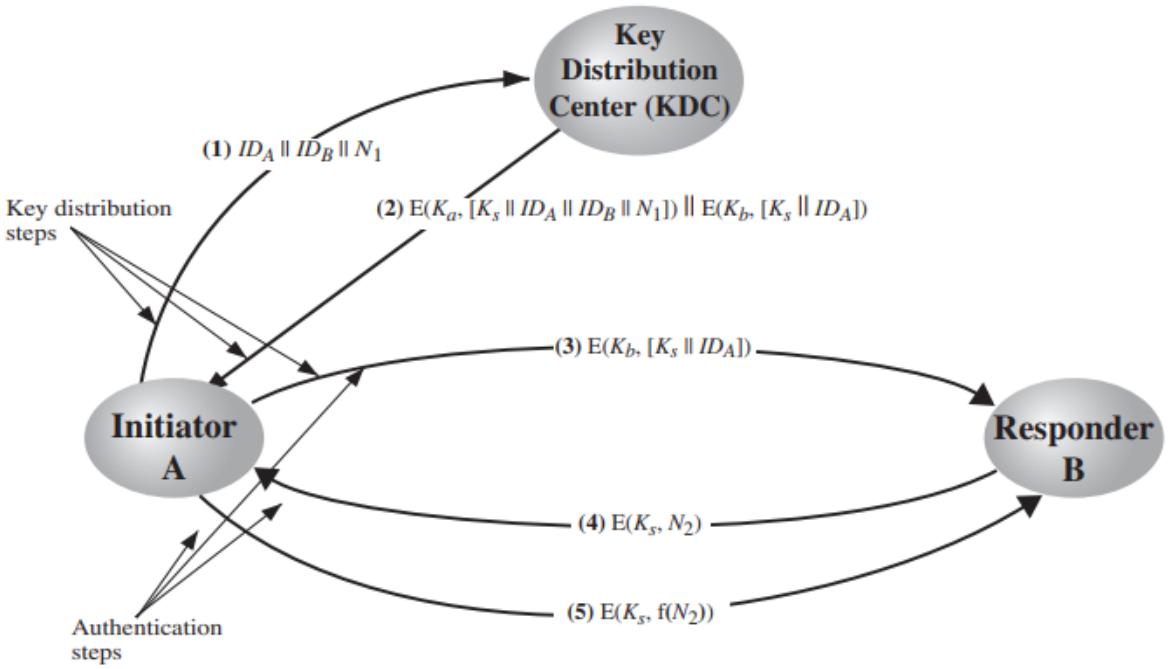

Fig. 2 (we discussed this in the class).

Problem 4: Summarize (i) discretionary access control, (ii) mandatory access control, (iii) role-based access control, and (iv) attribute-based access control. UAH gives all teachers access to Google. What kind of access control is this? [15+5]