

F. Autreau
P. Lafourcade
JL. Roch

P. Lafourcade.

SET 4

Date: 22.10.2007

Exercise 1

Find an attack on CBC encryption with counter IV , (proving that this encryption mode is not IND-CPA secure). In this scheme the first IV used is 0 and for generating the next IV we just increase by one the value of the previous IV .

Exercise 2

Prove that CBC with random IV is not IND-CCA1 secure. This time IV is a random number. But notice that this mode is IND-CPA secure.

Exercise 3

Find an attack on Needham Schroeder protocol:

1. $A \rightarrow B : \{N_a, A\}_{pk(B)}$
2. $A \leftarrow B : \{N_a, N_b\}_{pk(A)}$
3. $A \rightarrow B : \{N_b\}_{pk(B)}$