

*F. Autreau*  
*P. Lafourcade*  
*JL. Roch*

*P. Lafourcade.*

## SET 3

Date: 01.10.2007

### Exercise 1

Prove that

$$\begin{aligned} \text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND-XXX}}(\eta) &= \Pr[b' \stackrel{R}{\leftarrow} \text{IND}^1(\mathcal{A}) : b' = 1] - \Pr[b' \stackrel{R}{\leftarrow} \text{IND}^0(\mathcal{A}) : b' = 1] \\ &= 2\Pr[b' \stackrel{R}{\leftarrow} \text{IND}^b(\mathcal{A}) : b' = b] - 1 \end{aligned}$$

### Exercise 2

Prove that the encryption algorithm of an IND-XXX scheme must probabilistic, if it is stateless.

### Exercise 3

Prove that  $DDH \leq CDH \leq DL$

### Exercise 4

Prove that under CDH assumption El-Gamal is OW-CPA.

### Exercise 5

Prove that under DDH assumption El-Gamal is IND-CPA.