

# Exercise Sensor Networks

## Lecture 9: Security in sensor networks

### Exercise 9.1: RSA public key encryption

Prove the multiplicative homomorphic property of RSA

### Exercise 9.2: Domingo-Ferrer encryption

a) Prove the probabilistic behavior of the Domingo-Ferrer encryption in contrast to the deterministic behavior of RSA using the following values:

$$d=2, g=28, r=3, \text{ and } g'=7$$

b) Prove the additive homomorphic property of the Domingo-Ferrer encryption