Exercise Sensor Networks

Lecture 10: Security in sensor networks

Exercise 10.1: RSA public key encryption

Prove to multiplicative homomorphic property of RSA

Exercise 10.2: 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 and g'=7

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

©Thomas Haenselmann – Applied Computer Science IV, University of Mannheim