Introduction to Modern Cryptography, Exercise # 11

University of Amsterdam, Master of Logic
Lecturer: Christian Schaffner
TA: Joachim Schipper

22 November 2011
(to be handed in by Tuesday, 29 November 2011, 9:00)

1. **El Gamal Variant:** Exercise 10.11 in [KL].
2. **Secure Coin-Flipping:** Exercise 10.17 in [KL].
3. **Paillier Encryption:**
   (a) Exercise 11.16 in [KL].
   (b) Exercise 11.15 in [KL].
   (c) Show that the hardness of the decisional residuosity problem with respect to $\mathsf{GenModulus}$ (as in Definition 11.31) implies the hardness of factoring with respect to $\mathsf{GenModulus}$ (as in Definition 7.45). **Hint:** use (b).

Dr. Taher Elgamal
Image credit: `wikimedia.org`.