Introduction to Modern Cryptography, Exercise # 3

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

20 September 2011
(to be handed in by Tuesday, 27 September 2011, 9:00)

1. Exercise 3.1 from [KL].
2. Exercise 3.3 from [KL].
3. Exercise 3.5 from [KL].
4. Exercise 3.6 from [KL]. Prove your answers. **Clarification:** in (a), the input to G, $s0^{|s|}$, is the concatenation of the string s with the all-zero string of the same bit-length as s.

Image credit: `https://secure.flickr.com/photos/topher76/293277608`.