Introduction to Modern Cryptography
Exercise Sheet #2

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Monday, 8 September 2014
(to be handed in by Monday, 15 September 2014, 11:00)

Homework

1. Exercise 2.3 from [KL]. 10 p.
2. Exercise 2.4 from [KL]. **Hint:** Use part (a) in part (c). 15 p.
3. Exercises 2.7 and 2.8 from [KL]. 20 p.
   You do *not* need to prove Exercise 2.6. You can just use the result.
4. Exercise 3.1 from [KL]. 10 p.
5. Exercise 3.3 from [KL]. 10 p.
6. Exercise 3.5 from [KL]. 15 p.
7. 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. 10 p.

Figure 1: During Jimmy Carters presidency, the red phone was a hotline to the Kremlin in Moscow. A U.S. president could pick up the phone and speak directly to Soviet leaders in times of crisis. However, the phone on the picture is a replica and was never used, according to this article, see `http://en.wikipedia.org/wiki/Moscow-Washington_hotline`.