COMP444: Internet Infrastructure Security
Workshop 2: Length Extension Attack

Due at 11:55pm on 5 March 2015
Submission site: https://submit.comp.polyu.edu.hk/

1. (10 marks) Given a secret “password”, a SHA-1 hash 6d5f807e23db210bc254a28be2d6759a0f5f5d77 and an original data “polyu”, please append a new message “computing” to the end of original data. What are the new appended data and the new digest? Please use the “--out-data-format=html” format used in hash_extender for your answer.

2. (10 marks) Given a vulnerable web page http://hacker-heart.appspot.com/comp444/assign.php?d=data&h=4d79fa9cbd624b44ff02df898fda3610d89fed43, please append a new message “attacking” to the end of parameter d and make the web server accept your data (you should see the message "Your hash is correct. Great!" in your browser). Answer the following questions:
   a) (5 marks) Hong long is the secret used by the vulnerable page?
   b) (5 marks) What is the new digest after you successfully append “attacking”?

3. (10 marks) Given a block size of 512 bits, is it possible that the size of the padding content larger than 512 bits? If no, please elaborate your reason. If yes, please give examples.
   Hint: Each padding must have a 64-bit padding length and at least one bit.