Homework Assignment #10 – Cryptography I

Practical Cyber Security Fundamentals (CTF), Spring 2017
Department of Computer Science, Florida State University

Points: 45
Due: Beginning of the class (5:15pm) on April 10th, 2017

Submission: You need to submit electronically via Blackboard by uploading a pdf file (named "**hw10-Firstname-Lastname.pdf**") for your answers and programs to the problems; you need to combine all the parts into a single file. Here replace "Firstname" using your first name and replace "Lastname" using your last name in the file name.

All the materials can also be obtained from at
https://github.com/n0l3ptr/IntroToCTFs/tree/master/crypto

Problem 1 (15 points)

Decrypt http://www.cs.fsu.edu/~liux/courses/ctf/assignments/vcipher.txt and find the flag - (Note: non-alpha characters should be unaltered, but do consume a part of the cycle - i.e. the 3rd character uses the 3rd character of the key). Do not use automated tools and show your work.

Problem 2 (15 points)

Decrypt http://www.cs.fsu.edu/~liux/courses/ctf/assignments/feistel.bin - this file has been encrypted with: 8 round Feistel structure len(key) == 16 with F box:

```
def F(block, key):
    s = num2str(str2num(block) ^ key)
    return s[1:] + s[0]
```

Problem 3 (15 points)

Decrypt http://www.cs.fsu.edu/~liux/courses/ctf/assignments/otpcipher.bin - remember that all of these flags start with 'flag{' .