Network Security

Project 1
Hacking the Cipher

Instructor: Shiuhpyng Shieh
TAs: Wei-Ti Su, Xin-Yu Wang

1. Project Goal
   Chosen cipher attack is an attack model that If an attacker can gather information by obtaining the decryption of cipertexts, attacker can then retrieve the plaintext without having the key.

2. Project Description
   RSA is an important encryption technique first publicly invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. RSA security is based on the factoring problem -- the problem of factoring a large integer number into two prime numbers.
   In this project, each student is given a public key, an encrypted flag and a source code of the decrypter running on the server. Your goal is to use chosen ciphertext attack to retrieve the flag. The decrypt server is at 140.113.194.66, port 8888.

3. Deliverables
   Each student must work on his own and submit a zip file, named by '<STUDENT ID>.zip', for example 0656000.zip, containing:
   - flag: the decrypted message - 30%
   - report.pdf: a report about how to decrypt flag.enc - 70%
   - any code or script you write

Deadline : 2018/04/03 (Tuesday) 23:59:59