Network Security

Project 1
Hacking the Cipher

Instructor: Shiuhpyng Shieh
TAs: Te-Yu Chang, Po-Hsing Wu

1. Project Goal

   This project is intended for students who wish to tackle the weaknesses of RSA-based network protocols. RSA keys are assumed to be random. However, in practice, RSA keys in use may not be random, thereby causing unexpected security problems.

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.

   Although factorization seems like a very hard problem, a relatively easy problem may be tackled – finding the greatest common divisor (GCD) of two numbers. GCD is the largest integer that divides both numbers.

   If the common divisor is discovered, it will be easy to factorize N into p and q, where N is the modulus used in RSA key generation. Then, we can generate private key easily with known p and q.

   In this project, each student is given a file through the e3 platform with twelve RSA public keys. In these keys, there are two public keys that have a common divisor. Your job is try to find the corresponding private keys of these two public keys.

3. Deliverables

   Each student must work on his own and submit a zip file, named by '<STUDENT ID>.zip', containing:

   - Report in the PDF format about how to get the private keys.
   - The two private keys have a common factor, named by 'private<N>.pem', where N is the number in 'public<N>.pub'. For example, if you restore the private key of 'public2.pub', the private key filename is 'private2.pem'.

Deadline : 2017/10/17 (Tuesday) 23:59:59