German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Hacking Assignment 2 : Break Simple RSA Schemes

Discussion 01/03/2020 - 05/03/2020 **Task Grade** 5%

1 Introduction

In this task you're required to implement an algorithm to break Simple RSA Schemes. You are given **PublicKey(e,n)** and required to break the **PrivateKey(d,n)**.

This can be done by following the steps:

1. Get the prime factors of **n** using the **Sieve of Eratosthenes** algorithm.
2. Once you have obtained the two prime factors p & q, you can then use the extended Euclidean Algorithm to find the private key d using $\Phi(n)$ and the public key e.
3. After finding the private key, you can simply follow the decryption equation to get the decrypted value:

$$\mathbf{M} = \mathbf{C^d} \bmod \mathbf{n}$$

2 Details

You are given a starter code for this assignment containing the base implementation of the task in Python. You will find the starter code for this assignment uploaded on the MET website.

You are required to implement an algorithm that given the values; **n, e and C** encrypted using RSA, returns the both **the private key d and the decrypted message M**.

To compute the prime factors of n, you will apply the Sieve of Eratosthenes algorithm to get all the prime numbers till n. Once you get all the prime numbers till n, you can start to check whether n is divisible by any two of the prime numbers. Once you find p & q; two prime factors of n, you can calculate Euler's Totient, $\Phi(n)$.

Once you acquire $\Phi(n)$, you can use it alongside e to calculate the private key d. This can be done by using the Extended Euclidean Algorithm.

Once you have found the private key d, you can use it along with n to decrypt the provided cipher by following the equation:

$$\mathbf{M} = \mathbf{C^d} \bmod \mathbf{n}$$

You are also provided with a set of test cases within the source code file in order to check your implementation once you are done. The tests should get both the correct d and the correct decrypted message.

3 Submission

You will be required to submit your source code file by maximum one week from the tutorial slot (e.g. if your tutorial slot is on Sunday, your deadline is the following Saturday at 23:59) . Upload the source code file to the MET website in the corespondent submission link for your tutorial group. The source code file should be named as $[ID]\_[TutoiralNumber]\_[Task\_Number]$ (e.g. $[37-1111]\_[T01]\_[Task2]$).

In case there was a problem in the submission through the MET website, then send an email to your TA with the title same as the name of the .java or .py file.