Introduction to Cryptography - Fall 2015

Homework 5

Due by 11/29

Notes:

- This homework assignment is for individual students. Discussion is encouraged. But you have to form your own solution.
- Only typed or electronic reports (hand drawing okay for figures if necessary and legible) are allowed for homework submission.
- Write in a concise way. The essay solution should not exceed one page for each exercise.
- Submit it through the given link at BlackBoard as a **PDF** file. If there are other files such as Sage codes in a text file, compress all files into one zip file. Verify that the submission is successful.
- If you need more time for this assignment, you need to let me know before the due time.

1. (20pts)

In a public-key system using RSA, you intercept the ciphertext C=9 sent to a user whose public key is e=5, n=35. Now try to crack it. What is the plaintext M? Show very clearly each step in your cryptanalysis. You must use the **Square and Multiply** algorithm as shown in the class whenever applicable in calculation. Show each step clearly in your solution.

2. (30pts)

A simple hash function is done in this way: Choose p, q as primes and compute $N = p*q$. Choose g relatively prime to N and less than N. A number n is hashed as $H = g^n \bmod N$. If there is an m that hashes to the same value as n, then $g^m \equiv g^n \bmod N$, so $g^{m-n} \equiv 1 \bmod N$, which implies that $m–n \equiv 0 \bmod \varphi(N)$. $\varphi(N)$ is the Euler totient function. Breaking this amounts to finding a multiple of $\varphi(N)$.

(a) Write a Sage function that can generate the parameters of such a hash function, i.e. a pair of N and g.

(b) Using N, g, and n as arguments to write a Sage function to perform the hashing.

(c) Write a Sage function that creates a collision given p and q. Note that this function should exploit the above stated condition for a collision to occur for this hash function. It should not be done through a brute force search.