Computer Security Assignment 1

Due on 15 October 2018

Released on 19 September 2018

Question 1 — **Lamport Signature.** (5 marks) Generate 256 pairs of random numbers, each number being 256 bits in size, that is, a total of $2 \times 256 \times 256$ bits, stored as a two dimensional array $S[0][0]$, $S[0][1]$,…, $S[0][255]$, $S[1][0]$, $S[1][1]$, …, $S[0][255]$. This is kept secret as the private key. The public key is the collection of the hashed values $h(S[0][0])$, $h(S[0][1])$,…, which is also stored as a two dimensional array $P[0][0]$, $P[0][1]$,…, $P[0][255]$, $P[1][0]$, $P[1][1]$, …, $P[0][255]$. Assume that the cryptographic hash function h is preimage-resistant and collision resistant, and is well known.

To sign a message M, we first hash the message to a 256-bit hash sum $h(M)$. Then, for each bit in the hash, based on the value of the bit, pick one number from the corresponding pairs of numbers that comprise the private key (i.e., if the bit is 0, the first number is chosen, and if the bit is 1, the second is chosen). This produces a sequence of 256 random numbers. As each number is itself 256 bits long the total size of the signature will be $8KB$.

Please explain why this is a one-time signature scheme, and how it works. Why the level of security decreases dramatically if it is used for the second time and the third time?

Question 3 — **Cryptanalysis.** (5 marks) Given the ciphertext file 000.txt encoded in substitution cipher, find out its plain text and the key. Recall a key of the substitution cipher is a mapping from $\{a, b, c, \ldots, z\}$ to $\{a, b, c, \ldots, z\}$. They cipher only encrypts English letters, and leave the other characters unchanged. Therefore, you may write down the key as a string of length 26. For example, $edcfghijklmnopqrstuvwxyzab$ maps a to e, b to d, …, and z to b. (Please explain to me how you find out your solution)

(Please send your answer in txt/pdf formats to chenyi_zhang@jnu.edu.cn)