CS 5158/6058 Data Security and Privacy, Spring 2018
Homework 4

Instructor: Dr. Boyang Wang

Due Date: 03/22/2018 (Thursday), 11:59pm.
Format: Please **type** your solutions and submit a pdf of your solutions in Blackboard.
Total Points: 6 points

Problem 1 (1 point). In the Birthday Problem, we assume there are $D = 365$ days each year, and the birthdays are uniformly distributed. If there are n students in a room, then the probability that there are two students having a same birthday can be calculated as

$$p = 1 - \frac{D!}{D^n \cdot (D-n)!} = 1 - \frac{365!}{365^n \cdot (365-n)!} \tag{1}$$

(a) Please explain why this probability can be computed using Eq. 1;

(b) Assume the output of a hash function has $l = 30$ bits, an attacker is trying to find a collision using a brute-force attack. If this attacker tries $10,000$ different inputs in total, then what is the probability that there is a collision? Note: here we assume this attacker chooses different inputs uniformly. For this problem, you only need to compute an approximate probability using Taylor series.

(c) (**One additional question for CS6058 only**) We learned that Eq. 1 can be approximately computed as

$$p \approx 1 - e^{\frac{-n^2}{2D}} \tag{2}$$

in one of our lectures. Please explain why Eq. 1 can be computed as Eq. 2 using Taylor series ($e^x \approx 1+x$, if $x \ll 1$).

Problem 2 (1 point). Given a set $\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, we say that $\mathbb{Z}_{13}$ is an additive group mod 13.

(a) What is the identity of this group? and what is the order of this group?

(b) We define a function $f_e : \mathbb{Z}_{13} \rightarrow \mathbb{Z}_{13}$, where $f_e(g) = e \cdot g$, e is an integer and g is an element of this group $\mathbb{Z}_{13}$. If we choose $e = 3$, then is this function f_e a permutation of this group $\mathbb{Z}_{13}$? If it is a permutation when $e = 3$, then please explain why and compute the output of each input using this function f_e.

(c) Based on this additive group $\mathbb{Z}_{13}$, please list all the elements in multiplicative group $\mathbb{Z}^*_{13}$. What is the identity of group $\mathbb{Z}^*_{13}$ and what is the order of $\mathbb{Z}^*_{13}$?

(d) Please list all the elements in group $\mathbb{Z}_{20}$ and all the elements in group $\mathbb{Z}^*_{20}$

Problem 3 (1 point). Given $N = p \times q$, where p is a prime and q is a prime,

(a) Prove that the number of elements in multiplicative group $\mathbb{Z}^*_N$ is equal to $(p-1)(q-1)$.

(b) Given $N = p_1 \cdot p_2 \cdot p_3 = 13 \times 5 \times 7$, what is the group order of multiplicative group $\mathbb{Z}^*_N$?

Problem 4 (2 points). In textbook RSA key generation function, assume we have chosen two primes $p = 29$ and $q = 47$.

(a) According to the key generation algorithm, can we choose integer e as $e = 7$? If we can choose $e = 7$, please explain the reason, and calculate the public key and private key of textbook RSA using extended Euclidean algorithm. If we cannot choose $e = 7$, please also explain the reason.

(b) According to the key generation algorithm, can we choose integer e as $e = 15$? If we can choose $e = 15$, please explain the reason, and calculate the public key and private key of textbook RSA using extended Euclidean algorithm. If we cannot choose $e = 15$, please also explain the reason.

(c) Given a message $m = 2$, if $e = 7$ is a valid parameter, then what is the ciphertext of message m in textbook RSA? if $e = 15$ is a valid parameter, then what is the ciphertext of message m in textbook RSA?

(d) (**One additional question for CS6058 only**) Given a ciphertext $c = 2$, if $e = 7$ is a valid parameter, then what is the output of the decryption algorithm in textbook RSA? if $e = 15$ is a valid parameter, then what is the output of the decryption algorithm in textbook RSA?

Problem 5 (1 point). In ransomware, an attack essentially leverages the main idea of hybrid encryption to attack users. Without paying Bitcoins to the attacker, a user cannot recover its data.

(a) Please explain/describe how ransomware encrypts data on a user's computer using hybird encryption.

(b) If an attacker can only leverage symmetric-key encryption to encrypt users' data in a ransomware, then what are the major steps in this attack such that this attacker can still provide a copy of a decryption key if a user pays Bitcoins. From the perspective of this attacker, compared to using hybrid encryption, what are the limitations of this attack if it only uses symmetric-key encryption?