Fall 2019

CS134: Computer and Network Security

Homework 1

Due: 10/22/19: 11:59pm

Full Name:
UCI ID Number:
Sources:

Guidelines:

- Use any word processor (or handwrite and scan your answers). Upload your solutions **in PDF** to Gradescope.
- No collaboration is allowed. The only people you may consult are the TA-s and the instructor.
- Looking up, paraphrasing or copying answers from the Internet or other sources is not allowed; doing so is a violation of academic honesty. You must cite any sources you use, e.g., reference books, Wikipedia, etc.

Warning: any submissions not following the above guidelines will receive a score of zero.

P1	P2	P3	P4	P5	Total
/10	/20	/20	/20	/30	/100

Problem 1: One Time Pad

Recall OTP. Assume that the RNG stopped working in the middle of the key generation and generated k_1, a key which length is half the length of message m. Answer the following questions.

(a) If we use k_1 two times (i.e. use $k_1||k_1$ as the key, where $||$ denotes concatenation) to encrypt m using the OTP scheme, will the resulting ciphertext be secure? Why or why not? Justify your answer.

(b) You generate another key, k_2, using the same RNG so that if concatenated with k_1, the total key length will be same with m (i.e. $\text{len}(k_1||k_2) = \text{len}(m)$). If you use $k_1||k_2$, instead of generating a totally new key k' where $\text{len}(k') = \text{len}(m)$, to encrypt m using the OTP scheme, would it affect the confidentiality of the resulting ciphertext? Why or why not? Justify your answer. (Assume that RNG is working correctly.)

NOTE: Answer to each problem in 3 to 5 lines (including the justification). An answer without a justification will result in an automatic 0.

Solution:

Problem 2: DES

Recall the Data Encryption Standard (DES). Note: function DES() denotes the encryption of a block using DES, the key size is 56-bits, and the plain text size is 60-bits.

1. Consider 2-DES, i.e., $c = DES(k_2, DES(k_1, m))$. What are the worst-case time complexity (worst-case number of attempts) and the average-case time complexity (average-case number of attempts) of the brute-force attack?
2. Consider 3-DES, i.e., $c = DES(k_3, DES(k_2, DES(k_1, m))$. Describe how an adversary can launch the meet-in-the-middle (MITM) attack against 3-DES and answer the average-case time complexity.
3. Consider 4-DES, i.e., $c = DES(k_4, DES(k_3, DES(k_2, DES(k_1, m))$. Describe how an adversary can launch the meet-in-the-middle (MITM) attack against 4-DES and answer the average-case time complexity.
4. Compare the average-case time complexities of the MITM attack against 2-DES, 3-DES and 4-DES. How does the number of DES affect the time complexity? (2-3 sentences are enough.)

Solution:

Problem 3: Block Cipher Modes of Operation

Suppose Alice sends Bob a block-cipher encrypted message. Alice and Bob share a secret key, but Bob does not know the IV Alice used to encrypt the message. For each of the following block-cipher modes, explain how much of the message Bob is able to decrypt:

1. CBC
2. CTR
3. OFB
4. CFB

Limit your answers to four lines each.

Solution:

Problem 4: Probability of Collision
In the university of Crapoptamia, every student can design their own student ID. Here is the rules for getting the student ID:

1. The first character should be an upper-case English letter. Students can randomly pick one letter.
2. The following two digits should be the month of student's birthday.
3. The last four characters are 4 digits chosen by each student.

For example, **Z051133** is an valid ID for a student who was born in May.

We assume that each student will randomly choose the first English letter and the four digits.

In a Computer Science class, the instructor tells the class that there is at least a 99% possibility that two or more students share the same **first four characters** in their student ID.

(a) At least how many students are there in the class? Explain your solution. (Assume that the distribution of the birth months is uniform.)

(b) One student says that the first four characters are **'A019'** and asks his classmates to raise the hand if someone has the same first four characters. However, no one responds. Has the instructor made a mistake? Think about relevant properties of hash functions and contrast the instructor's logic and the student's question.

Solution:

Problem 5: Group Theory

Recall that four properties (closure, associativity, identity, inverse) must be satisfied for a set G and an operator @ to be a group. For the following sets and operations, show whether each property holds (you must show the work for all four properties), and decide if (G,@) is a group. If you think it is a group determine whether the resulting group is cyclic and whether it's abelian (explain). If the group is cyclic, show a generator for the group.

(a) $G =$ (2 × 2 non-invertible matrices with entries in $\mathbb{R}$) $= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{R}) | ad - bc = 0\}$, @ = matrix multiplication (denoted by "$\cdot$")

(b) $G =$ The set of real and complex roots of the polynomial $z^4 - 1$ (i.e., the set of solutions to $z^4 - 1 = 0$). @ = multiplication

(c) $G = \mathbb{Z}_{13}^* = \{a \in \mathbb{Z}_{13} | a \text{ is co-prime to } 13\}$, @ = modular multiplication (denoted by "$*$")

Solution: