Name

CWID

Exam

Monday Oct 15, 2018
Due Wed Oct 17 by 10:00am

CS458 - Fall 2018 - Exam 1

Please leave this empty!

1.1 1.2 1.3 1.4 1.5 1.6 1.7 1.8

1.9 Sum

Instructions

- **You have to hand in the assignment using your blackboard**
- **This is an individual and not a group assignment. Fraud will result in 0 points**
- For your convenience the number of points for each part and questions are shown in parenthesis.

BY SUBMITTING THIS EXAM THROUGH THE ONLINE SYSTEM, I AFFIRM ON MY HONOR THAT I AM AWARE OF THE STUDENT DISCIPLINARY CODE, AND (I) HAVE NOT GIVEN NOR RECEIVED ANY UNAUTHORIZED AID TO/FROM ANY PERSON OR PERSONS, AND (II) HAVE NOT USED ANY UNAUTHORIZED MATERIALS IN COMPLETING MY ANSWERS TO THIS TAKE-HOME EXAMINATION.

Question 1.1 (20 Points)

What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros?

Question 1.2 (5 Points)

About how many times more time does a brute force key search take against a 112-bit DES than against a 56-bit DES?

Question 1.3 (15 Points)

Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

a. XOR of subkey material with the input to the f function

b. XOR of the f function output with the left half of the block

c. The f function

d. Permutation P

e. Swapping halves of the block

Question 1.4 (5 Points)

Consider the storage of data in encrypted form in a large database using AES. One record has a size of *16* bytes. Assume that the records are not related to one another. Which mode would be best suited and why?

Question 1.5 (5 Points)

We are using AES in counter mode for encrypting a hard disk with 1 TB of capacity. What is the maximum length of the IV?

Question 1.6 (15 Points)

Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA.

a. Which of the parameters $e_1 = 32$, $e_2 = 49$ is a valid RSA exponent? Justify your choice.

b. Compute the corresponding private key $K_{pr} = (p, q, d)$. Point out every calculation step.

Question 1.7 (10 Points)

Assume a (small) company with 120 employees. A new security policy demands encrypted message exchange with a symmetric cipher. How many keys are required, if you are to ensure a secret communication for every possible pair of communicating parties?

Question 1.8 (10 Points)

Given is a Diffie-Hellman key exchange protocol with the modulus *p=131* and the primitive root element α*=70*

1. What is the order of $\mathbb{Z}_{131}^*$

2. Your private key is 774. Compute the public key

Question 1.9 Extra Credit (5 Points)

In the DHKE protocol, the private keys are chosen from the set *{2,..., p-2}*. Why are the values *1* and *p-1* excluded? Describe the weakness of these two values.

This page left blank intentionally. There are no more questions.