Christopher Morcom	A20385764
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?

Input = x_0 = 000.... (64 bits)

L_0 = 000... (32 bits) R_0 = 000... (32 bits)

① Expansion
② SBox Sub
③ Permutation

$$\left[R_1 = L_0 \oplus f(R_0, k_1)\right]$$

R_0 = 000... (48 bits)

$$000\ldots = 000\ldots \oplus f(000\ldots, k_1)$$

k_1 = 000... (48 bits)

Substitute 6 bit blocks into SBox 1 → 8.

Yields: 14, 15, 10, 7, 2, 12, 4, 13

Permute this on Table P:

Yields: 13, 8, 13, 8, 13, 11, 11, 12 = $f(R_0, k_1)$

$$R_1 = L_0 \oplus \{13, 8, 13, 8, 13, 11, 4, 12\}$$

So Round 1 output is:

0000 0000 0000 0000 0000 0000 0000 0000 1101 1000 1101 1000 1101 1011 1011 1100

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?

Key space $= 2^n$ bits

$$\frac{3DES\ (keyspace)}{DES\ (keyspace)} = \frac{2^{112}}{2^{56}} = 2^{56}$$

Against a 112 bit 3DES a brute force key search would be at worst 2^{56} times slower than 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 — Key addition

b. XOR of the f function output with the left half of the block — No; DES uses a feistel structure but AES does not.

c. The f function - Byte substitution

d. Permutation P — Shift rows sublayer & Mix columns sublayer

e. Swapping halves of the block — AES is NOT feistel structured so there are no halves to swap

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?

Counter mode (CTR) mode would be best because it acts like a stream cipher which encrypts bits individually & is small & fast & usually in embedded devices. Additionally, databases have lots of random accesses and CTR mode is good for that.

Since records are 16 bytes (128 bits), records are broken down Blocks then Encrypted/decrypted on access.

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?

$1\ TB = 2^{43}$ bits $\quad \frac{2^{43}}{128} = 2^{36} \rightarrow$ 36 bits req. for counter

(128 = Block size)

$128 - 36 = 92$ bits

92 Bits is the max number of bits for the initial vector (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.

(a) $\phi(N) = (40)(16) = 640$

$\gcd(32, 640) = 32$

$\gcd(49, 640) = 1 \rightarrow E_2$ is valid exponent

(b) $ed = 1 \bmod (\phi N) \rightarrow 49d = K(640)+1$

$49d = 1 \bmod (640)$ $\rightarrow d = \frac{K(640)+1}{49} \in \mathbb{Z}^+$

By trial & Error on calculator, $K = 16$

$d = \frac{16(640)+1}{49} = 209$

$$\boxed{K_{pr} = (41, 17, 209)}$$

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?

n employees $(n-1)$ connections per user

$n = 120$, $(n-1) = 119$

$\frac{120(119)}{2} = 7140$ keys required.

Question 1.8 (10 Points)

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

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

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$

131 is prime so $\mathbb{Z}_{131}^* = 131 - 1 = \underline{130}$

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

$K_{pr} = 774$ $\quad \alpha = 70, p = 131$

$K_{pub} = \alpha^{K_{pr}} \bmod p$

$K_{pub} = 70^{774} \bmod 131 = 58$

Question 1.9 Extra Credit (5 Points)

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

Given that DHKE uses a symmetric encryption b/c $K_{pub} = \alpha^{K_{pr}} \bmod p$, we see that if K_{pr} is 1, the public key would be constant and guessable. Similarly, $a^{p-1} \bmod p = 1$ and a public key of 1 is also guessable.

additionally, note that if $K_{pr} = 1$, the sets of α & K_{pub} for all α would entirely intersect so interception wouldn't require a great deal of calculation to figure out p & "decrypt" the message.