VIGINESH KUMAR KARTHIKEYAN RAJALAKSHMI

Name

20424508

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.

K.R-Vigneshkumar.

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?

The input of 64 bit is Z_0 = 0000.....0 (64 zeroes). the permutation at the start has no effecte.

∴ L_0 = 0000.....0 (32-bit zeroes) and $Right_0$ = 0000.....0(32 zero

Applying the fixed permutation on input bits gives K_1 = 000...0 (48 zeroes)

The round gives $R_1 = L_0$ XOR $f(R_0, K_1)$

Expand R_0 into 48-bit long string and it gives 48-bit 0 string

XOR the above result and get 48-bit zero string

48-bit 0 string is divided into 8 * 6 bit chunks. the 000000 gets Mapped with S_i boxes and yield value of 14, 15, 10, 7, 2, 12, 4, 13 the values in binary yield

1110 1111 1010 0111 0010 1100 0100 1101

The above value is permutated by using p table and the value is

1101 1000 1101 1000 1101 1011 1011 1100 = $(f(R_0), K_1)$

L_0 XOR $(f_0(R_0, K_1))$. the $L_0 = 0$ ∴ the Concatenate the both value

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?

Solution:-

The key space size of 112 bit DES is 2^{112}

The size of key space of 56 DES is 2^{56}

∴ the ratio of these two amounts to $2^{112}/2^{56} = 2^{56}$

$2^{56} \simeq 7*10^{16}$

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 - add Round key

b. XOR of the f function output with the left half of the block - Not fiestel cipher

c. The f function - bytesub

d. Permutation P - Row shifting and column mixing

e. Swapping halves of the block - No swapping.

(a) Addround key

(b) AES is not the fiestel cipher so this step is not necessary

(c) Bytesub

(d) shift the row and mix the column

(e) No swapping of halves in AES.

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?

The Cipher block mode creates a dependancy and hence you cannot use that for the individual records.

you need Randomness to access the unrelated records.

The EBC Method can be used but it shows if there are any similar records.

The CTR Method is the Suitable method for this encryption since they give the Randomness to the record and they also use IV - Initialize Vector, which is used only once and it is hard to guess.

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^{40} bytes of data

and each byte has 8 bits ∴ $2^{40} * 8 = 2^{43}$ bits

the logarithmic value of $43 \log_2 2$ = 36 bits

36 bits is the Minimum number needed.

The primitive value is 128 if you subtract 36 from

128 128 - 36 = 92 bits is the Maximum number needed.

∴ 92 bits

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) The exponent e should be relatively prime to N, such that $\gcd(e, \phi(N)) = 1$.

$\phi(N) = \phi(P) \cdot \phi(q) = \phi(41) * \phi(17) = 40 * 16 = 640$

$\gcd(640, 49) = 1$ && $\gcd(640, 32) \neq 1$

$\therefore$ e_2 is the valid RSA exponent. $e_2 = 49$

b) $e * d = 1 \bmod \phi(N)$

$49 * d = 1 \bmod 640$

$640 = 49(13) + 3 \Rightarrow 3 = 640 - 49(13)$

$49 = 16(3) + 1 \Rightarrow 16(640 - 49(13)) + 1$ $\quad 49 - 16(640) - 49 = 208 + 1$

$1 = 49 - 16(640 - 49(13))$

$= 49 - 16(640) - 49(13)(16)$

$1 = 49 - 16(640) - 49(208)$

$\boxed{209 = 49^{-1} \bmod 640.}$

$\therefore$ 209 is the answer.

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?

number of Employees = 120

Each person has to Communicate with other 119 persons and for Every pair it gets reduced by 1

$$\therefore \frac{120 * 119}{2}$$

$= 14280 \div 2$

$= 7140$

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 $\mathbf{Z}^*_{131}$

Order / cardinality of group $Z^*_n = \phi(n)$

$\therefore Z^*_{131} = \phi(131)$

for any prime p $\phi(p) = p-1$

$\therefore \phi(131) = 131 - 1 = 130$

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

Private Key = $K_{pr} = 774$, Prime $p = 131$, $\alpha = 70$

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

$= 70^{774} \bmod 131$

Public Key = 58

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.

Solution:-

If you choose 1, then the acquired public key value would be equal to α. So the attacker can easily guess the private key.

If you choose to use p-1 then the function $\alpha^{p-1} \bmod p$ will yield 1. Since the p is always a prime number and this also enables the attacker to easily guess the private key.