

# Assignment 5

● Graded

## Group

ANANYAE KUMAR BHARTARI

ABHAYA PRATAP SINGH

NAVEEN KUMAR MATHUR

 [View or edit group](#)

## Total Points

60 / 60 pts

## Question 1

Teamname

0 / 0 pts

✓ + 0 pts Correct

+ 0 pts Incorrect

## Question 2

Commands

5 / 5 pts

+ 0 pts Incorrect

✓ + 5 pts go/back, wave, dive, go, read

## Question 3

Analysis

50 / 50 pts

✓ + 10 pts Encoding used in the cryptosystem, i.e., odd positions contains [f-m] whereas even positions contains [f-u]

✓ + 30 pts Analysis for finding the preimage of the password. Matrix A is a lower triangular matrix. Finding the preimage can be done in two ways. 1) Finding the matrix A and vector E or 2) finding the mapping between ith input byte and ith output byte by brute force.

✓ + 10 pts Converting the preimage to password (i.e., converting the plaintext to ASCII)

+ 0 pts Wrong answer or NA

#### Question 4

##### Password

Resolved 5 / 5 pts

✓ + 5 pts Correct

+ 0 pts Incorrect

🔄 Regrade Request

Submitted on: Apr 08

Sir, the password is correct as we clear the level with the same password. So please take a look at it and regrade it.

yes, but you provided team name as "NAA" in Q1. Hence your team name is not there in the names of teams who cleared level 5.

Reviewed on: Apr 08

🔄 Regrade Request

Submitted on: Apr 10

Dear Sir we have mailed a screen shot with our team name that is being shown in the terminal please do check it out.

fixed.

Reviewed on: Apr 11

#### Question 5

##### Codes

0 / 0 pts

✓ + 0 pts Correct

### Q1 Teamname

0 Points

NAA

### Q2 Commands

5 Points

List the commands used in the game to reach the ciphertext.

go ,wave, dive, go ,read

### Q3 Analysis

50 Points

Give a detailed description of the cryptanalysis used to figure out the password.  
(Explain in less than 100 lines and use Latex wherever required. If your solution is not readable, you will lose marks. If necessary, the file upload option in this question must be used TO SHARE IMAGES ONLY.)

We know that a 7 bit has a total of 128 possible combinations hence we tried and enter various random plain text. We found out that there is a mapping of the form 'ff'-0 and so on to 'mu'- 127.

Now to break the EAEAE encryption we are going to use a modified form of Square attack.

Observation: Matrix A is a lower triangular matrix.

Reason: on changing one byte all the ciphertext after the given byte change hence we can safely conclude that the matrix is a lower triangular one.

Part One- Breaking E and diagonal of A.

we use 8 sets of plaintext-ciphertext (each set contains 128(plaintext and ciphertext)) each set has one byte different and the rest are zero('ff') basically they are the form PC7. hence we can easily see the corresponding output to one set will be  $(((((input^{ei}) * a_{ii})^{ei}) * a_{ii})^{ei})^{ei})$ , hence we can apply brute force and guess the various pairs(ei,a<sub>ii</sub>) of value that satisfy the above equation.

We get three pairs corresponding to each row.

E is -

[[22, 37, 68], [66, 77, 111], [29, 43, 55], [17, 41, 69], [18, 21, 88], [52, 99, 103], [26, 113, 115], [24, 28, 75]]

A diagonal is-

[[[84, 40, 49], [], [], [], [], [], []], [], [37, 86, 70], [], [], [], [], []], [], [], [108, 43, 86], [], [], [], [], [], [], [68, 95, 12], [], [], [], [], [64, 100, 112], [], [], [], [], [], [11, 73, 103], [], [], [], [], [], [27, 20, 124], [], [], [], [], [], [38, 33, 53]]]

Part two- breaking the complete A

we can choose plaintext such that two bytes are non zero input<sub>i</sub>,input<sub>j</sub> will be zero so we will be able to brute force our way to attaining a<sub>ij</sub> of the Matrix A. and if we don't find the values we discard the following E and A diagonal that we found earlier.

hence through our algorithm, we were able to find that E is

[[22], [111], [43], [69], [88], [52], [26], [24]]

and A transpose is


[[84, 112, 17, 102, 101, 30, 20, 88],  
[0, 70, 27, 20, 60, 47, 123, 9],

```
[0, 0, 43, 24, 13, 29, 11, 72],  
[0, 0, 0, 12, 108, 45, 98, 23],  
[0, 0, 0, 0, 112, 97, 25, 14],  
[0, 0, 0, 0, 0, 11, 92, 69],  
[0, 0, 0, 0, 0, 0, 27, 3],  
[0, 0, 0, 0, 0, 0, 0, 38]]
```

then we brute force to find which input would lead to the specific output (The ciphertext to break ) and found the answer to be after converting bytes to their respective ascii value-

vptkzysubk000000

we remove the padding and enter the password

 No files uploaded

#### Q4 Password


5 Points

What was the final command used to clear this level?

vptkzysubk

#### Q5 Codes

0 Points

 No files uploaded