Assignment 5

● Graded

Group

Himanshu Karnatak
Bikash Saha
Valeti Lokesh
View or edit group

Total Points

100 / 100 pts

Question 1

Team Name

0 / 0 pts

✔ **+ 0 pts** Correct

+ 0 pts Incorrect / Level not cleared on the server

Question 2

Commands

5 / 5 pts

✔ **+ 5 pts** Correct

+ 0 pts Incorrect / Level not cleared on the server

Question 3

Cryptosystem

5 / 5 pts

✔ **+ 5 pts** Correct

+ 0 pts Incorrect / Level not cleared on the server

Question 4

Analysis

Resolved **80** / 80 pts

- ✔ **+ 5 pts** Encoding used in the cryptosystem, i.e., odd positions contains [f–m] whereas even positions contains [f-u]
- ✔ **+ 5 pts** Reasoning about inputs "ff" to "mu": fall within the range of valid hexadecimal characters and have a guaranteed 0 MSB.

  Solution 1: Computing A and E
- ✔ **+ 10 pts** Correctly explain why A seems to be a lower triangular matrix. Reason: For the ith plaintext byte, changing any byte at j>i does not change the corresponding ith ciphertext byte.
- ✔ **+ 10 pts** However, changing any byte at j<i changes the corresponding ith ciphertext byte
- ✔ **+ 10 pts** Reasoning about the number of minimum possible Plaintext needed
- ✔ **+ 10 pts** Compute diagonal elements of A: Brute force each aii independtly
- ✔ **+ 10 pts** Compute non-diagonal elements of A: Order is important. Explain what elements are required beforehand to brute force aij
- ✔ **+ 10 pts** Correct A: A is a lower triangular matrix with correct values.
- ✔ **+ 10 pts** Correct E

  Solution 2: Brute forcing the plaintext vector

+ 0 pts Incorrect / Level not cleared on the server

Regrade Request **Submitted on: May 02**

Dear Sir,
The minimum number of plaintext-ciphertext pairs required was clearly mentioned in point number 11 of question 4. Additionally, we have included a comprehensive analysis outlining the reasoning behind our solutions. Considering this, we would be grateful if you could review this section of our assignment again. We believe our submission meets the specified criteria and hope you will reconsider the grading accordingly.

done

Reviewed on: May 02

Question 5

Password

10 / 10 pts

- ✔ **+ 10 pts** Correct

+ 0 pts Incorrect / Level not cleared on the server

Question 6

Code

0 / 0 pts

✔ **+ 0 pts** Correct

+ 0 pts Incorrect / Level not cleared on the server

Q1 Team Name
0 Points

Group Name

mod3

Q2 Commands
5 Points

List all the commands in sequence used from the start screen of this level to the end of the level

5
go
wave
dive
go
read
password
uwpjcomzhk

Q3 Cryptosystem
5 Points

What cryptosystem was used at this level?

EAEAE Cipher. It is a Substitution-Permutation Network(SPN) where A is a linear transformation (invertible matrix) and E is the non-linear transformation (exponentiation) as mentioned in the terminal . (Modified version of AES)

Q4 Analysis

80 Points

Knowing which cryptosystem has been used at this level, give a detailed description of the cryptanalysis used to figure out the password.

1. The cryptosystem used in this level uses input block of size 8 bytes. It is given that each byte is an elmenent in F_{128}. This indicates that the values can range from 0 to 127. Though a byte can generally hold a value from 0 to 255. This gives us an important constraint that most significant bit is always 0 while creating plain text bytes.
It is also given that 8x8 linear transformation matrix A also has elements from F_{128}. To apply this transformation we develop functions for arithmetic in F_{128}

2. We observe that input and output strings are made of characters 'f' to 'u' same as in previous level of the game. Here 'f' represents 0 (0x0) and 'u' represents 15 (0xf) to create a hexadecimal representation of the byte stream.

3. Then we generated different plain text pairs. Every byte of the plain text block can take values from 'ff' to 'mu'. We started with all 'ff' and one non zero byte in different places. Then we increase the number of non zero bytes in the plain text. Value of each non-zero bytes can range from 0-127 ('ff' to 'mu'), i.e most significant bit remains 0. Game server was used to generate ciphertexts for each plain text block.

4. We see a pattern in the cipher text blocks generated for our plain text blocks with one non zero byte. Our observation is that changing i^{th} byte of plain text block changes all bytes starting from i^{th} bytes till the last byte in cipher text block. Bytes previous to i^{th} bytes still remain 'ff' i.e 0. A simple glance at cipher texts indicates a triangular pattern.

5. We also observe that in all these plain texts if we look at i^{th} byte, changing any value at byte $j > i$ does not change corresponding i^{th} byte in cipher text.

6. But when we change any value at byte $j < i$, i^{th} byte in cipher text is changed.

7. We know that exponentiation transformation E operates on individual bytes. It's the linear transformation A that mixes bytes in input block. Above observations indicate that only $j <= i$ bytes are involved in creating i^{th} byte of next round. That means all elements below the diagonal elements a_{ii} of A

are zero.

8. It give us an idea about the linear transformation matrix A. It seems to be a triangular matrix. It can be represented as a lower triangular or an upper triangular matrix depending on ordering of elements. As both upper and lower triangular matrices are conjugate of each other.

9. Application of transformation EAEAE on a plain text with only one non zero element can be analysed in following representation.

Let linear transformation matrix A be

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} & a_{18} \\ 0 & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} & a_{28} \\ 0 & 0 & a_{33} & a_{34} & a_{35} & a_{36} & a_{37} & a_{38} \\ 0 & 0 & 0 & a_{44} & a_{45} & a_{46} & a_{47} & a_{48} \\ 0 & 0 & 0 & 0 & a_{55} & a_{56} & a_{57} & a_{58} \\ 0 & 0 & 0 & 0 & 0 & a_{66} & a_{67} & a_{68} \\ 0 & 0 & 0 & 0 & 0 & 0 & a_{77} & a_{78} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{88} \end{bmatrix}$$

Let exponentiation vector be E =

$$\begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \end{bmatrix}$$

Let's take a sample plain text block where only 4^{th} element $(i = 4)$ is non zero.
X=

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ x_4 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Now let us do the transformation $EAEAE(X)$ step by step.
Step1. $E(X)$ =

$$\begin{bmatrix} 0 & 0 & 0 & (x_4)^{e_4} & 0 & 0 & 0 & 0 \end{bmatrix}$$

It is a row vector representation. X is a 8x1 column vector in all transformations.

Step2. $AE(X)$ =

$$\begin{bmatrix} a_{14} \times (x_4)^{e_4} \\ a_{24} \times (x_4)^{e_4} \\ a_{34} \times (x_4)^{e_4} \\ a_{44} \times (x_4)^{e_4} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Step 3. $EAE(X)$ =

$$\begin{bmatrix} (a_{14} \times (x_4)^{e_4})^{e_4} \\ (a_{24} \times (x_4)^{e_4})^{e_4} \\ (a_{34} \times (x_4)^{e_4})^{e_4} \\ (a_{44} \times (x_4)^{e_4})^{e_4} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Step 4. $AEAE(X)$ =

$$\begin{bmatrix} a_{11} \times (a_{14} \times (x_4)^{e_4})^{e_4} + a_{12} \times (a_{24} \times (x_4)^{e_4})^{e_4} + a_{13} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a_1 \\ a_{22} \times (a_{24} \times (x_4)^{e_4})^{e_4} + a_{23} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a_{24} \times (a_{44} \times (\\ a_{33} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a_{34} \times (a_{44} \times (x_4)^{e_4})^{e_4} \\ a_{44} \times (a_{44} \times (x_4)^{e_4})^{e_4} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Step 5. $EAEAE(X)$ =

$$\begin{bmatrix} (a_{11} \times (a_{14} \times (x_4)^{e_4})^{e_4} + a_{12} \times (a_{24} \times (x_4)^{e_4})^{e_4} + a_{13} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a \\ (a_{22} \times (a_{24} \times (x_4)^{e_4})^{e_4} + a_{23} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a_{24} \times (a_{44} \times \\ (a_{33} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a_{34} \times (a_{44} \times (x_4)^{e_4})^{e_4})^{e_4} \\ (a_{44} \times (a_{44} \times (x_4)^{e_4})^{e_4})^{e_4} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

10. Our analysis gives us a clear picture how an i^{th} byte in cipher text is related to i^{th} byte in plain text, when all bytes except i_{th} in plain text are zero. $c_i = (a_{ii} \times (a_{ii} \times (x_i)^{e_i})^{e_i})^{e_i}$. This equation is used to derive the value of all diagonal elements a_{ii} of linear transformation A.

11. We generated 127 plaintexts for nonzero byte at one index and 0 is all other indexes. In total 1016 distinct plain text- cipher text pairs were used to analyse this cipher. We then iterated through all valid values of e_i (ranging from 1 to 126)and a_{ii} (ranging from 1 to 127) with available plain text cipher text pairs to find out the valid set of values. The possible value pairs turn out to be.

	Possible Value pairs of $a_{i,i}$	Possible value pairs of e_i
Byte 1	73, 84, 20	18, 21, 88
Byte 2	72, 101, 70	53, 83, 118
Byte 3	43, 17, 15	39, 106, 109
Byte 4	37, 126, 12	22, 37, 68
Byte 5	5, 31, 112	78, 85, 91
Byte 6	5, 11, 121	36, 42, 49
Byte 7	27, 14	20, 108
Byte 8	38, 11, 58	29, 43, 55

12. With all possible diagonal elements now know to us, we use this information to find other elements. Matrix representation at Step5 of our analysis point 9, show that for any non-zero element adjacent to diagonal, we can use values of a_{ii} and a_{jj} to figure out value of a_{ij}. This closed triangle formed by these elements seems solvable.

13. In our analysis example, for 4^{th} non-zero element in plain text block, we now look at equation described in 3^{rd} row.
$c_3 = (a_{33} \times (a_{34} \times (x_4)^{e_4})^{e_4} + a_{34} \times (a_{44} \times (x_4)^{e_4})^{e_4})^{e_4}$
Using known plain text- cipher text byte x_4, c_3 and known diagonal values a_{33}, a_{44}, this equation can be used to find value of a_{34}. This can be generalized for finding a_{ij} using neighbor diagonal element a_{ii}, a_{jj}. We need to take care of the order of solving so that equations remain simple enough to solve. This approach is now used to find all elements of the matrix A. It first narrows down the diagonal elements to unique values.

	Value of $a_{i,i}$	Value of e_i
Block 0	84	21
Block 1	70	118
Block 2	43	39
Block 3	12	68
Block 4	112	91
Block 5	11	42
Block 6	27	20
Block 7	38	29

14. And then using the same approach described in previous point we find remaining elements of the matrix. This computation narrows down out possible values of A and E to the following values.

$$A = \begin{bmatrix} 84 & 113 & 14 & 105 & 111 & 24 & 13 & 66 \\ 0 & 70 & 31 & 23 & 57 & 41 & 122 & 3 \\ 0 & 0 & 43 & 2 & 7 & 30 & 20 & 77 \\ 0 & 0 & 0 & 12 & 108 & 53 & 102 & 29 \\ 0 & 0 & 0 & 0 & 112 & 99 & 22 & 14 \\ 0 & 0 & 0 & 0 & 0 & 11 & 95 & 67 \\ 0 & 0 & 0 & 0 & 0 & 0 & 27 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 38 \end{bmatrix}$$

$$E = \begin{bmatrix} 21 & 118 & 39 & 68 & 91 & 42 & 20 & 29 \end{bmatrix}$$

15.We utilize the values of A and E to decrypt the ciphertext from level 5 of the caves. Initially, we split the encrypted password "lhjkfghjjkilgriqmrkrfghhkjljliif" into two halves: "lhjkfghjjkilgriq" and "mrkrfghhkjljliif." Following the decryption method discussed earlier, we obtained the unencrypted password "uwpjcomzhk000000." To derive the final password, we removed the last six zeros, resulting in "uwpjcomzhk." This password allows us to pass this level.

Q5 Password
10 Points

What was the password used to clear this level?

uwpjcomzhk

Q6 Code
0 Points

Please add your code here. It is MANDATORY.

▾ MOD3_Assignment5.zip	Download
1	Binary file hidden. You can download it using the button above.