Q1 Team Name
0 Points

Group Name

hustler

Q2 Commands
5 Points

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

go --> wave --> dive --> go --> read

Q3 Cryptosystem
5 Points

What cryptosystem was used at this level?

The cryptosystem is EAEAE cipher which is a variant of AES Cipher

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.

After entering the above commands we reached the screen which says :
" you can see the coded password by simply whispering

'password' near the screeen....."

After entering "password " we get ciphertext as "jggkfrkginlmlsgrlhjhlpmqgmmjhrlt"

This is the password/ciphertext that we have to decode to clear the level.

After entering several inputs some observations were made:

1.) On entering some values like "sdddfihio" ,''akjiojeneio'' etc. the window died out. So the plaintext and the ciphertext must exist within a specific range of letters.
2.) After trying more we figured that the inputs which were being accepted can contain only 16 letters from "f" to "u".
3.) Each alphabet represented 4 bits and is mapped from 0 to 15 with "f" being "0 " and "u" being 15. Also, group of 2 alphabets made 8 bits or 1 byte.
4.) It is known that field F_{128} has each byte from range 0 to 127 . Thus the possible alphabet pairs are from "ff" to "mu". The most significant bit is 0.
5.) Since the input is 8 byte block so the plaintext is of 16 alphabets as two letters make 1 byte with each byte varying from "ff" to "mu".
6.) For a plaintext of "ffffffffffffffff" the ciphertext generated is "ffffffffffffffff".
7.)It was observed that giving various inputs that has few starting bytes as 'ff' and then changing the bytes the output came out with same number of starting bytes as "ff" and changing the rest bytes. This indicated that the linear transformation matrix is a lower triangulation matrix.

Calculation of Transformation matrix A and E:

We know from spirit of cave that E is exponentian vector of dimension 8 * 1 and A is linear transformation matrix of dimension 8 * 8 . Also, A is lower triangular matrix.

Let $a_{i,j} \in$A where i,j is row and column index, and

Let $e_i \in E$

We then generated plaintexts of form $C_{8-i}PC_{i-1}$ where C = 'ff' and P ∈ ['fg','mu']. Thus 8 sets of plaintexts with each set containing 128 different values were obtained and stored in plaintexts.txt.

Corresponding Ciphertexts were generated for each plaintexts and stored in ciphertexts.txt

Due to input plaintext format used by us , only 1 block is non - zero per input and we could conduct an iteration on every feasible value of diagonal element and exponents . If a non zero block i had the value p , the its output had the value

$$C = (A^* (A^*(p)^E)^E)^E \quad \text{.....(1)}$$

The encryption process is performed over field F_{128} constructed using degree 7 polynomial $x^7 + x + 1$ over F_2 . Addition is performed as XOR operation in F_{128}

Now for each ciphertext plaintext pair we iterate using values from [0,127] for A and [1,126] for E (as told by spirit of cave) and compare the output whether they map to ciphertext or not.
All possible pairs where output matched we stored those values and found that there are 3 possible pairs per block as below:

Block 0: aii -> [84,46,96], ei -> [24,28,75]
Block 1: aii -> [29,52,70], ei->[6,7,114]
Block 2:aii -> [43,17,15], ei ->[39,106,109]
Block 3: aii-> [6,9,12], ei->[11,34,82]
Block 4: aii-> [47,112,96], ei->[65,92,97]
Block 5: aii-> [11,106,70], ei->[40,89,125]
Block 6: aii-> [27,71,92], ei->[23,48,56]
Block 7: aii-> [126,38,71], ei->[8,25,94]

Now we need to find the true pair and eliminate other pairs from above. Also we need to find the diagonal elements. For this we used some more plaintext and ciphertext combination

and iterated aver the above pairs such that equation (1) is satisfied.

	aii	ei
Byte 0:	84	24
Byte 1:	70	114
Byte 2:	43	39
Byte 3:	12	82
Byte 4:	112	92
Byte 5:	11	40
Byte 6:	27	23
Byte 7:	38	25

The $a_{i,j}$ can be found by using input where jth block is non-zero and looking at the output of ith block. The following elements should be known for finding $a_{i,j}$:

$$Q_{i,j} = \{ a_{n,m} \mid n > m,\ j \leq n, m \leq i \} \subset \{ a_{n,n} \mid j \leq i \}$$

These elements forms a right angle triangle. The non - diagonal elements are searched iteratively with $a_{i+1,i}$ first followed by $a_{i+2,i}$ and so on.

Final linear transformation matrix is :

$$A = \begin{bmatrix} 84 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 118 & 70 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 31 & 43 & 0 & 0 & 0 & 0 & 0 \\ 123 & 16 & 12 & 12 & 0 & 0 & 0 & 0 \\ 98 & 61 & 0 & 105 & 112 & 0 & 0 & 0 \\ 25 & 47 & 18 & 33 & 96 & 11 & 0 & 0 \\ 15 & 125 & 8 & 102 & 4 & 88 & 27 & 0 \\ 76 & 14 & 73 & 26 & 11 & 66 & 3 & 38 \end{bmatrix}$$

Final Exponent Vector:

$$E = \begin{bmatrix} 24 & 114 & 39 & 82 & 92 & 40 & 23 & 25 \end{bmatrix}$$

To Decode the password:

Using above found values of linear transformation vector A and Exponent vector E , we can decrypt the password by applying the reverse of eq (1) on each 8 byte block as following:

$$E^{-1}(A^{-1}(E^{-1}(E^{-1}(C))))$$

where C is the encrypted password

Our encrypted password is "jggkfrkginlmlsgrlhjhlpmqgmmjhrlt" which is of 32 letters. Thus the password is broken into two pieces and then decoded as

password : "xspxdmpven000000"

The 00s are found to be padding and thus the password is:

"xspxdmpven"

Q5 Password

10 Points

What was the password used to clear this level?

xspxdmpven

Q6 Code

0 Points

Please add your code here. It is MANDATORY.

Hustler.zip Download

```
1  Binary file hidden. You can download it using the button above.
```

Assignment 5

● Graded

Group

ABHIVADAN
SANDULA LAVANYA
SHRUTIKA ANIL JADHAV
View or edit group

Total Points

90 / 100 pts

Question 1

Team Name — **0** / 0 pts

Question 2

Commands — **5** / 5 pts

Question 3

Cryptosystem — **5** / 5 pts

Question 4

Analysis — **70** / 80 pts

Question 5

Password — **10** / 10 pts

Question 6

Code — **0** / 0 pts