Q1 Team Name
0 Points

Group Name

team_13

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 -> password

Q3 Cryptosystem
5 Points

What cryptosystem was used at this level?

EAEAE cipher (a variant of AES)
Polyalphabetic Substitution 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.

spirit whispered that "This is another magical screen. And this one I remember perfectly...
Consider a block of size 8 bytes as 8 x 1 vector over F_{128} -- constructed using the degree 7 irreducible polynomial x^7 + x + 1 over F_2. Define two transformations: first a linear transformation given by invertible 8 x 8 key matrix A with elements from F_{128} and

second an exponentiation given by 8 x 1 vector E whose elements are numbers between 1 and 126. E is applied on a block by taking the ith element of the block and raising it to the power given by ith element in E. Apply these transformations in the sequence EAEAE on the input block to obtain the output block. Both E and A are part of the key. You can see the coded password by simply whispering 'password' near screen..."

ciphertext : gskfgnjiiujogfhhjnjumjmrinjqgklk

Observations:

As spirit whispered, encoding was done on 8 bytes block over F_{128}. The first challenge was to figure out the encoding being done on the input string to convert into the block. We observed that the encrypted password contains alphabets between 'f' and 'u', so we tried some inputs and observed their output pattern. Only certain inputs were accepted. Inputs containing alphabets only from 'f' to 'u' were accepted. So there is a total of 16 letters that can be represented by 4 bits as each alphabet from 'f' to 'u' can be mapped to a number between 0-15. We noticed that the field was F_{128}, which translated to 7 bytes, but the question mentioned 8 bytes. We observed the output pattern for the inputs "ff"-"mu" and came to the conclusion that each byte of input was from "ff"-"mu" mapping to 0-127 with MSB as 0. There was one more observation that when we have some starting bytes as "ff", only part after the "ff" was being encrypted, all the "ff" remains the same. which means "ff" present in each row must be at the end of the row. which means the matrix is a lower triangular matrix.

To decrypt the password, we can find all the elements of the matrix by finding matrix A and matrix B and just brute force all the possible values. by the observations we got, we can find both matrices. Let's denote the members of matrix A as $a_{i,j}$ and members of matrix E as e_i. Now we will iterate through the feasible values of diagonal elements, taking specific input containing only 1 non-zero block and other blocks as "ff". If the non-zero value has value x then output value will be O=$\left(a_{i,i}\left(a_{i,i} * x^{e^i}\right)^{e^i}\right)^{e^i}$. then using the degree 7 irreducible polynomial operation can be applied over the field F_{128}. Then iterate through all the values of $a_{i,i}$ and e_i, and we can get around 3 pairs for each block. Now $a_{i,j}$ can be calculated from $a_{i,i}$ and $a_{j,j}$ using some more plaintext and ciphertext pairs. It will also help in reducing possible

pairs. Then we can find all the values of the matrix by iterating through all the elements using the final value of E matrix and verifying with O.

Final Linear Transformation matrix A:

$[84, 0, 0, 0, 0, 0, 0, 0]$
$[112, 70, 0, 0, 0, 0, 0, 0]$
$[19, 30, 43, 0, 0, 0, 0, 0]$
$[98, 16, 2, 12, 0, 0, 0, 0]$
$[110, 62, 12, 104, 112, 0, 0, 0]$
$[25, 51, 29, 51, 99, 11, 0, 0]$
$[2, 123, 9, 103, 29, 88, 27, 0]$
$[0, 2, 74, 22, 10, 66, 31, 38]$

Exponent matrix E:
$[22, 113, 38, 73, 92, 42, 19, 26]$

Now we can decrypt the password using the same way.

Decrypted Password: vroodolwao (after removing 0s)

Q5 Password
10 Points

What was the password used to clear this level?

vroodolwao

Q6 Code
0 Points

Please add your code here. It is MANDATORY.

fpc.zip Download