Q1 Team Name
0 Points

Noobs

Q2 Commands
5 Points

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

The commands used are as follows:
1. go
2. wave
3. dive
4. go
5. read
6. password

Q3 Analysis
50 Points

Give a detailed description of the cryptanalysis used to figure out the password. (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 observed that the output ciphertext only contains characters in the range (f-u) and each byte of input block has a value between 0 to 127. So, we come to the conclusion that each input block consists of 16 characters, where 2 characters is equal to one byte.
Moreover since the maximum value of each byte is 127, the range of each byte comes out to be (ff — mu) where f f = 0 and mu = 127 i.e. val(ab) = (a —' f') * 16+ b—' f'. Basically, the odd positions contain [f-m] and even positions contain [f-u]. Also we observe following things while keeping only one byte non-zero:

i) If only the first byte is non-zero in input block, then no byte is zero in output block.

ii) If only the last byte is non-zero in input block, then only last byte is non-zero in output block.

iii) If only the i_{th} byte is non-zero, then j_{th} byte is also non-zero for $j >= i$.

So we conclude that A is a lower-triangular matrix.

Now we generate 1024 plaintexts(8 * 128) such that only one byte is non-zero in input block. We also fetched the 1024 ciphertexts corresponding to each plaintext using the code. So there comes a relation between the non-zero input byte and corresponding output byte. The relation is as follows:

Let i-th byte is non-zero in input-block, then the i^{th} output byte comes out to be: $O_j = (a_{i,i} * (a_{i,i} * {I_i}^{e_i})^{e_i})^{e_i}$ where e_i is the i^{th} byte of E and $a_{i,i}$ is the A[i][i] entry in A. So we bruteforce the relation for all values of e_i; and a_{ii};; and that gives us more than one pair of e_i and a_{ii}. To eliminate the pairs, we started finding the remaining values of matrix. For example, if i^{th} byte is non-zero in input-block, then the $(i+1)^{th}$ output byte comes out to be: $O_{i+1} = (a_{i+1,i} * (a_{i,i} * I_i^{e_i})^{e_i} + a_{i+1,i+1} * (a_{i+1,i} * {I_i}^{e_i})^{e_{i+1}})^{e_{i+1}}$.

$Block$	$Final a_{i,i}$	$Final e_i$
$Block0$	84	21
$Block1$	70	112
$Block2$	43	43
$Block3$	12	72
$Block4$	112	91
$Block5$	11	54
$Block6$	27	25
$Block7$	38	29

Now we bruteforce for all values of $a_{i+1,i}$ and (e, a) pairs we got before. This eliminates the wrong pairs. Doing so for the remaining bytes of output block we found the E and A matrix to be as follows :

E :

[21, 112, 43, 72, 91, 54, 25, 29]

A :

$$\begin{bmatrix} 84 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 113 & 70 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 27 & 43 & 0 & 0 & 0 & 0 & 0 \\ 101 & 23 & 30 & 12 & 0 & 0 & 0 & 0 \\ 100 & 57 & 0 & 117 & 112 & 0 & 0 & 0 \\ 29 & 41 & 19 & 46 & 96 & 11 & 0 & 0 \\ 23 & 122 & 10 & 98 & 26 & 95 & 27 & 0 \\ 94 & 8 & 77 & 26 & 23 & 70 & 5 & 38 \end{bmatrix}$$

Using final A and E, we decrypted the encrypted password "lhlikkgllmkqimlhmmhkmfffhpffjifr" (code to generate A and E and decrypt is in answer.py). We divided the encrypted password into 2 blocks(becasue 16 was the maximum block length) and finally we applied the following transformations on each block of encrypted password:

$$E^{-1}(A^{-1}(E^{-1}(A^{-1}(E^{-1}(encrypted\_password)))))$$

We mapped the numerical values obtained after applying our transformation using However, because this text did not contain our password, we assumed the numerical values were ASCII codes. We get the decrypted password as uqtncarzeb000000 after converting these numerical numbers to ASCII values, where '0' is used for padding. Hence the command(final password) used to clear the level is 'uqtncarzeb'.

Note: As stated on the game's panel, the matrix A was guaranteed to be invertible.

Please refer to the readme of the code to learn about how the code works.

No files uploaded

Q4 Password
5 Points

What was the final commands used to clear this level?

uqtncarzeb

Q5 Codes
0 Points

It is mandatory that you upload the codes used in the cryptanalysis. If you fails to do so, you will be given 0 for the entire assignment.

▾ Noobs.zip Download

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

Assignment 5 ● GRADED

GROUP
Divyansh Bisht
Manu Shukla
Rishabh Lakhwani
View or edit group

TOTAL POINTS
35 / 60 pts

QUESTION 1 Team Name	**0** / 0 pts
QUESTION 2 Commands	**5** / 5 pts
QUESTION 3 Analysis	**45** / 50 pts
QUESTION 4 Password	**5** / 5 pts
QUESTION 5 Codes	R **-20** / 0 pts