Q1 Team Name

0 Points

Goldfish

Q2 Commands

10 Points

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

exit1, exit3, exit4, exit4, exit1, exit3, exit4, exit1, exit3, exit2, read

Q3 Analysis

60 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.)

First to reach the last level we had to find right combination of exit commands after which we reached the last screen on which the final text was there.
We obtained a series of hexadecimal number. we examined the pattern and decided to convert those number to decimal number system. We further changed those decimal numbers to there corresponding charcter using ASCII code system. Upon changing those numbers to charcters , we got message as " You see a Gold-bug in one corner. It is the key to a treasure found by" .

Upon reaching to the last exit , we got the following message.

"n =
84364443735725034864402554533826279174703893439763343343863260342756678609216895093779263028809246505955647572176682669445270008816481771701417554768871285020442403001649254405058303439906229201909599348669565697534331652019516409514800265887388539283381053937433496994442146419682027649079704982600857517093

Goldfish: This door has RSA encryption with exponent 5 and the password is
6027891780260411906216431734888760823035585257346793955962368551166266482709479911996197564794807902838156190999268279971533181607545444100814126827067061633209492922603301341988872875523764244807978534399529665716721293940635 64

873014225995407370913761108737068284412766595468782097792
01560390761048657774255 "

Since as we know that RSA is being used for encryption and exponent is 5. Here d is unknown . To crack the password we need to either factorise n or find d.As n is too large to factorise , we will use different method to solve the above problem.

We decided to use coppersmith algorithm and LLL Lattice reduction technique to solve the problem. we first decided to ensure if any padding has been used . we calculated $C^{1/e}$ value, which turned out to be a non integral value, which indicates that padding has been used .
so the new equation becomes as:
$(P+M)^{1/e} = C\, mod\, n$, here P is the padding and M is the original message.
First we tried " You see a Gold-bug in one corner. It is the key to a treasure found by" as padding , but it did not work , then we tried "Goldfish: This door has RSA encryption with exponent 5 and the password is " sentence as padding and it gave away the solution .

Following is the introduction to coppersmith algorithm
Let n be a integer and $f \epsilon Z$ be a polynomial of degree d . for given n , we can find all x_0 such that $f(x_0) = 0$ mod m where $x_0 <= N^{1/d-\epsilon}$ for $1/d > \epsilon > 0$.
we can use above equation to model our problem as $f(x) = (P + x)^5$ mod n
we need find roots of f(x) to get the password.

we programmed our algorithm in code_1.ipynb file to get the password.
1. we first converted padding messages to their corresponding ASCII number. later we converted those numbers to 8 bit binary .
2. As length of x cannot exceed $N^{1/d-\epsilon}$. we treated 200 as the upper limit.
Our final expression becomes $((binary\_padding << password\_length) + x)^e - C$
where password length ranges from 1 to 200 in multiple of 4

With the help of above described algorithm , with assumed password length as 80, we obtained following password
100001100111000010110010101000000110111011011110100110001101111001
1011001011001'
we later appended a zero to make it a multiple of 8 and the final expression becomes
0100001100111000010110010101000000110111011011110100110001101111 00
11011001011001.
Upon considering 8 bit at once and converting them to decimal number ,later we converted those decimal to ascii charcters we got "C8YP7oLo6Y" as password.

Ref:
1. https://en.wikipedia.org/wiki/Coppersmith%27s_attack
2. https://www.youtube.com/watch?v=3cicTG3zeVQ
3. https://github.com/mimoo/RSA-and-LLL-attacks/

No files uploaded

Q4 Password

10 Points

What was the final command used to clear this level?

C8YP7oLo6Y

Q5 Codes

0 Points

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

▾ codefile.zip

Download

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

Assignment 6

● GRADED