



## 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" .

## Assignment 6

● GRADED

### GROUP

Jeet Sarangi

Alok Kumar Trivedi

Akshay Kumar Chittora

[View or edit group](#)

### TOTAL POINTS

**80 / 80 pts**

### QUESTION 1

Team Name

**0 / 0 pts**

### QUESTION 2

Commands

**10 / 10 pts**

### QUESTION 3

Analysis

**60 / 60 pts**

### QUESTION 4

Password

**10 / 10 pts**

### QUESTION 5

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

"n =

8436444373572503486440255453382627917470389343976334334386326034275  
667860921689509377926302880924650595564757217668266944527000881648  
17717014175547688712850204424030016492544050583034399062292019095993  
4866956569753433165201951640951480026588738853928338105393743349699  
4442146419682027649079704982600857517093

Goldfish: This door has RSA encryption with exponent 5 and the password is  
60278917802604119062164317348887608230355852573467939559623685511662  
664827094799119961975647948079028381561909992682799715331816075454441  
0081412682706706163320949292260330134198887287552376424480797853439  
95296657167212939406356487301422599540737091376110873706828441276659  
546878209779201560390761048657774255 "

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:

$(P + M)^{1/e} = C \bmod n$ , 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  $f \in \mathbb{Z}$  be a polynomial of degree d . for given n , we can find all  $x_0$  such that  $f(x_0) = 0 \bmod m$  where  $x_0 \leq N^{1/d-\epsilon}$  for  $1/d > \epsilon > 0$ .

we can use above equation to model our problem as  $f(x) = (P + x)^5 \bmod n$

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  $N^{1/a-\epsilon}$ , we treated 200 as the upper limit.  
Our final expression becomes  $((binary\_padding \ll password\_length) + x)^e - C$

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

1000011001110000101100101010000001101110110111101001100011011110011011001011001'

we later appended a zero to make it a multiple of 8 and the final expression becomes

0100001100111000010110010101000000110111011011110100110001101111001101100101100

1.


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](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

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