Assignment 3

Graded

Group

ANANYAE KUMAR BHARTARI
ABHAYA PRATAP SINGH
NAVEEN KUMAR MATHUR
View or edit group

Total Points

65 / 70 pts

Question 1

Team name

0 / 0 pts

✓ **+ 0 pts** Correct

+ 0 pts Incorrect

Question 2

Commands

10 / 10 pts

✓ **+ 10 pts** go/enter, climb/enter, pluck/pick,back/climb,give,back,back, thrnxxtzy, read or correct combination of the above ("c" and "put" can be ignored).

+ 0 pts Incorrect

Question 3

Analysis

45 / 50 pts

✓ **+ 15 pts** Finding at least two distinct powers of g.

✓ **+ 25 pts** Finding the values of g by repeated division or Extended Euclid's algorithm or any other method.

✓ **+ 5 pts** The value of g is 192847283928500239481729

✓ **+ 5 pts** Finding $password$ using the information of g.

+ 0 pts Wrong answer or NA.

+ 50 pts Solving the assignment using an entirely different approach.

− 5 pts you should have compiled it carefully, it is not readable

Question 4

Password

10 / 10 pts

+ 0 pts Incorrect

✓ **+ 10 pts** 360852885036840078603672 5

Question 5

Codes

0 / 0 pts

✔ **+ 0 pts** Correct

Q1 Team name

0 Points

NAA

Q2 Commands

10 Points

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

enter - enter - pluck -climb - give - (take magic words thrnxxtzy) - back - back - (thrnxxtzy) - read

Q3 Analysis

50 Points

Give a detailed analysis of how you figured out the password? (Explain in less than 500 words)

```
\documentclass[a4paper]{article}

\usepackage[english]{babel}
\usepackage[utf8]{inputenc}
\usepackage{algorithm}
\usepackage[noend]{algpseudocode}

\title{Assignment 3}

\author{NAA}

\date{\today}
\def\changemargin#1#2{\list{}{\rightmargin#2\leftmargin#1}\item[]}
\let\endchangemargin=\endlist
\begin{document}
\maketitle
\section{ Theory}
\begin{itemize}
   \item Z$p^*$ is a multiplicative group as p is an prime number.
   \item the group action on Z$p^*$ is denoted by $*_p$ which is defined by:
   \begin{center}
      \hspace{0cm} $*_p$ \colon G $x$ G \rightarrow G \\
     \hspace{4cm}(x,y) \rightarrow x*y\bmod p
   \end{center}
   \item We are going to use the fact that every element in the group has a
\textbf{unique} inverse.
   \item Also as Z$p^*$ is a group $*_p$ is \textbf{associative} .
   \item We use \textbf{Fermat's little theorem} to calculate the inverse which
states that  if p is a prime number, then for any integer a, the number $a^p - a$
is an integer multiple of p. If a is not divisible by p, Fermat’s little theorem is
equivalent to the statement that $a^{p-1}-1$ is an integer multiple of p.
   \begin{center}
       $a^{p-1} \equiv 1$ (mod p)\\
        $a*a^{p-2} \equiv 1 (\bmod p)$
```

```
    \end{center}
    therefore $a^{-1}=a^{p-2} \bmod p$
    \item Next we are going to use an recursive method to find g.
\end{itemize}
\section{ Initial calculation}

    \begin{center}
     \begin{tabular}{||c c||}
 \hline
 a & password $*_p$ $g^a$ \\ [0.5ex]
 \hline\hline
  324 & 11226815350263531814963336315\\
 \hline
 2345&9190548667900274300830391220 \\
 \hline
  9513& 4138652629655613570819000497\\[1ex] \hline
 \end{tabular}\vspace{.5cm}
 \end{center}
 \newline Let password $*_p$ $g^3^2^4$=$x_1$
 \newline Therefore we can substitute this variable in other two equation. (We
know the inverse of $(x_1)^-^1$=11676372716222599136085566753)
 \begin{enumerate}
     \item $(x_1)$ $*_p$ $g^2^0^2^1$= 7021284369301638640577066679
     \item $(x_1)$ $*_p$ $g^9^1^8^9$=9190548667900274300830391220
 \end{enumerate}
 \newline Multiplying by inverse of $(x_1)$ both sides give:
 \begin{enumerate}
     \item  $g^2^0^2^1$=3426347385144995225825016781
     \item  $g^9^1^8^9$=4138652629655613570819000497
 \end{enumerate}
\section{ Algorithm}
\heading Used this algorithm while solving the equation $g^a$=$x_1$ and
$g^b=x_2$ st $a>b$
\begin{itemize}
\item Both x$_1$,x$_2$ $\epsilon$ G where G is the multiplicative group.
\item $*_p$ is the group operation that is $*_p$(x$_1$,x$_2$) \rightarrow
$x$_1$*x$_2$  \bmod$ p
\newline If a $\epsilon $ G  then $a^x$ implies a$*_p$a$*_p$a.... x times a also
$a^x$ $\epsilon$ G
\end{itemize}
```

```
\begin{algorithm}
\caption{Algorithm}
\begin{algorithmic}
\Procedure{}{$a,b$}\Comment{Use recursive method to solve }
\State $rem\gets a\bmod b$
\State $Q\gets [$a/b$]$\Comment{[x] the greatest integer less than x}
\While{$ rem\not=0$}\Comment{Check if remainder is not zero}
\State $g^r^e^m\gets g^a*_p((g^b)^-^1)^Q$ \Comment{ $*_p$ is the group operation  }
\State $a\gets b$
\State $b\gets rem$
\State $rem\gets a\bmod b$
\State $Q\gets [$a/b$]$
\EndWhile\label{euclidendwhile}
\State \textbf{return} $(b,g^b)$\Comment{the function will return (rem,$g^r^e^m$)}
\EndProcedure
\end{algorithmic}
\end{algorithm}

Let's do the first step of this algorithm explicitly to get the idea
\begin{center}
\hspace{-4.7cm}We have:\newline
$g^9^1^8^9=3426347385144995225825016781$
\newline$g^2^0^2^1=3426347385144995225825016781$
\newline
\newline We can write {9189= 4*2021 +  1105} [the rem $\gets$ 9189 $\bmod$ 2021 = 1105]
\begin{center}
   \item $\rightarrow g^9^1^8^9=(g^2^0^2^1)^4*_pg^1^1^0^5$\\
   \item$\rightarrow ((g^2^0^2^1)^4)^-^1*_pg^9^1^8^9=g^1^1^0^5$
\end{center}

\end{center}
\hspace{.5cm}Therefore we will be able to get the value of $g^1^1^0^5$
\section{ Important notes on algorithm}
\begin{itemize}
   \item The multiplication used in the above algorithm is the Group operation ($*_p$)
   \item If we know any element the group we can easily take out it's inverse.
```

```
   Hence all the values can be computed for the steps of the algorithm (We know $x_1$,$x_2$)
\end{itemize}

\section{ Implementing the Algorithm in our case }
\begin{center}
    \begin{tabular}{||c c c c||}
 \hline
 a & b & Q & rem \\ [0.5ex]
 \hline\hline
 9189 & 2021 & 4 & 1105 \\
 \hline
 2021 & 1105 & 1 & 916  \\
 \hline
 1105 & 916 & 1 & 189  \\
 \hline
 916 & 189 & 4 & 160  \\
 \hline
 189 & 160 & 1 & 29 \\
 \hline
  160 & 29 & 5 & 15 \\
   \hline
 29 & 15 & 1 & 14\\
   \hline
  15 & 14 & 1 & 1\\ [1ex]
 \hline
\end{tabular} \hspace{-3.5cm}
\newline
\begin{tabular}{||c c||}
 \hline
 a & $g^a$  \\
 \hline\hline
 9189 & 34263473851449952258250167 81  \\
 \hline
 2021 &  70212843693016386405770666 79  \\
 \hline
 1105 &  13325243597151936924936026 50   \\
 \hline
 916 & 16928329349929603757418032 233  \\
 \hline
```

```
 189 & 7233340894988383169873081319 \\
 \hline
 160  & 15480832131739101784049259744 \\
   \hline
29 & 14409628835368808838382787765\\
   \hline
15 & 9862566087568179051837025782\\
\hline
14 & 11662011900497299711580345247\\
\hline
1 & 192847283928500239481729\\
[1ex]
 \hline
\end{tabular}

\end{center}

\section{ Finally solving the equation }
 We have got the value of g now we will use : \vspace{.125cm}
\newline
    password $*_p$ $ g^3^2^4$=11226815350263531814963336315
\vspace{.125cm}
    \newline password= 11226815350263531814963336315 $*_p$ $ (g^3^2^4)^-^1$ \vspace{.125cm}
   \newline  password= 11226815350263531814963336315 $*_p$
726117032386935245054894092 \vspace{.125cm}
   \newline  password= 3608528850368400786036725




\end{document}
```

Q4 Password

10 Points

What was the final command used to clear this level?

3608528850368400786036725

Q5 Codes
0 Points

Upload any code that you have used to solve this level.

assignment_3.py

Download

```python
def M(a,b,mod):
    res=1
    while(b>0):
        if(b%2==1):
            res=(res*a)%mod
        a=((a%mod) *(a%mod))
        b=b//2
    return res

def I(a,mod):
    return M(a, mod-2, mod)


# print(I(324,19807040628566084398385987581))
ans = 324*I(324,19807040628566084398385987581)
# print(ans//19807040628566084398385987581 , ans%19807040628566084398385987581)


mod=19807040628566084398385987581
print()


# 11226815350263531814963336315
g9189=4138652629655613570819000497*I(11226815350263531814963336315,1980704
print("g9189        : ",g9189%mod)
print()


g2021=I(11226815350263531814963336315, mod)*9190548667900274300830391220
print("g2021        : ",g2021%mod)
print()

g2021_4_num = ((I(((g2021)**4),mod)) * (g9189))%mod
# print("g2021_4_num : ",g2021_4_num%mod)
# print()

g1105=g2021_4_num
print("g1105        : ",g1105%mod)
print()

g916= (g2021*(I(g1105,mod)))%mod
print("g916        : ",g916%mod)
print()


```

```
g189 = ((g1105)*(I(g916,mod)))%mod
print("g189        : ",g189)
print()


g160= (I((g189**4),mod) * g916 )%mod
print("g160        : ",g160%mod)
print()


g29= (I(g160, mod) * g189 )%mod
print("g29         : ",g29%mod)
print()


g15 = (I(g29**5, mod)*g160) %mod
print("g15         : ",g15%mod)
print()


g14 = (I(g15, mod)*g29) %mod
print("g14         : ",g14%mod)
print()


g1 = (I(g14, mod)*g15) % mod
print( "g1          : ",g1%mod)
print()

inverse_g = I(g1, mod)
print("g : " ,inverse_g)
print()

# password =11226815350263531814963336315//(I(g1**324,mod))

tmp= inverse_g


for i in range(1,324):
    inverse_g = (inverse_g * tmp) % mod

password = (inverse_g * 11226815350263531814963336315 )% mod


print("password   : ",password)
```

```
# enter - enter - pluck -climb - give - (take magic words ) - back - back - (magic word ) - read - pasword ( 3608528850368400786036725)

# (324, 11226815350263531814963336315)
# (2345,9190548667900274300830391220)
# (9513, 4138652629655613570819000497)
```

Assignment_3 (2).pdf Download

Your browser does not support PDF previews. You can [download the file instead.]