Exercise 1

Fredrik Kortetjarvi & Rohullah Khorami

January 22, 2021

1

Citoday breach this contains 226,883,414 accounts. The breach used socail engineering to get the information they used mailinator to mail fake mails to users in a guitar forum there it could send out. This kind of breaches cant be stoped becasue this is using tricks to trick the brain of people so they give out the information for free. this can only be improved but not fixed.[1]

2

The program generate a picture with a name IOCCC in raytracing. We used cmake to make this into a ppm file then display it in gimp to see the picture that was created. We found the makefile on the internet which was a programming contest. The program use functions to make a program to draw graphics into a ppm file that is a picture.[2]

3

The Key that Eve guessed indeed decrypts the cipher text to "LATER". we checked the result in java program and on pen and paper. The program explaind in Task 4.
$T = (x - k) mod 26 + 65$
$78 - 65 = 13 = (x - 84) mod 26 + 65 \Leftrightarrow T = 78 \rightarrow N, x = 71 \rightarrow G$
$69 - 65 = 4 = (x - 82) mod 26 + 65 \Leftrightarrow T = 69 \rightarrow E, x = 86 \rightarrow V$
$86 - 65 = 21 = (x - 84) mod 26 + 65 \Leftrightarrow T = 86 \rightarrow V, x = 79 \rightarrow O$
$69 - 65 = 4 = (x - 83) mod 26 + 65 \Leftrightarrow T = 69 \rightarrow E, x = 87 \rightarrow W$
$82 - 65 = 17 = (x - 72) mod 26 + 65 \Leftrightarrow T = 82 \rightarrow R, x = 89 \rightarrow Y$

Plain text = NEVER - 78 69 86 69 82
Key = TRTSH - 84 82 84 83 72
Cipher text = GVOWY - 71 86 79 87 89

4

References

[1] Tony Hunt. “Inside the Cit0Day Breach Collection”. In: (2020). URL: `https://www.troyhunt.com/inside-the-cit0day-breach-collection/`.

[2] Matt Zucker. “Most shiny”. In: (2011). URL: `https://www.ioccc.org/2011/zucker/hint.html`.