Exercise 1

Fredrik Kortetjarvi & Rohullah Khorami

February 10, 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.[2]

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 see figure 1. 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.[4]

Figure 1: Raytracing.

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.
$11 = (x - 84) mod 26 \Leftrightarrow T = 11 \rightarrow L, newkey = 19 \rightarrow T$
$0 = (x - 82) mod 26 \Leftrightarrow T = 25 \rightarrow Z, newkey = 16 \rightarrow Q$
$19 = (x - 84) mod 26 \Leftrightarrow T = 21 \rightarrow V, newkey = 20 \rightarrow U$
$4 = (x - 83) mod 26 \Leftrightarrow T = 3 \rightarrow D, newkey = 17 \rightarrow R$
$17 = (x - 72) mod 26 \Leftrightarrow T = 18 \rightarrow S, newkey = 8 \rightarrow I$

First attempt
Plain Text = LZVDS - 11 25 21 3 18
Key = TRTSH - 84 82 84 83 72
Cipher Text = EQNVZ - 4 16 13 21 25

Take out the key
Plain text = LATER - 11 0 19 4 17
Key = TQURI - 19 16 20 17 8
Cipher Text = EQNVZ - 4 16 13 21 25

$T = (x - k) mod 26 + 65$
$78 - 65 = 13 = (x - 84) mod 26 + 65 \Leftrightarrow T = 78 \rightarrow N, x = 71 \rightarrow G$
$69 - 65 = 4 = (x - 82) mod 26 + 65 \Leftrightarrow T = 69 \rightarrow E, x = 86 \rightarrow V$
$86 - 65 = 21 = (x - 84) mod 26 + 65 \Leftrightarrow T = 86 \rightarrow V, x = 79 \rightarrow O$
$69 - 65 = 4 = (x - 83) mod 26 + 65 \Leftrightarrow T = 69 \rightarrow E, x = 87 \rightarrow W$
$82 - 65 = 17 = (x - 72) mod 26 + 65 \Leftrightarrow T = 82 \rightarrow R, x = 89 \rightarrow Y$

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

4

Answer is a java program with name OTPInputStream.java

5

All steps to find public key and private key

1.
$p = 7, q = 11$

2.
$N = P * q = 77$

3.
$W = (p-1)(q-1) = 60$

4.
To decide an E value thoug we should know that E must be a prime number and GCD(E,W) = 1 and 1 < E <W we asume that E = 53 and GCD(53,60) = 1

5.
D = 1/E mod W => ED = 1 Mod W => D = ((W*i)+1)/E
We check i value step by step or we count the number of prime numbers from 1 to 53. The i Value must be an Integer. In this situation there are 15 prime number before 53 than the i value become 15.
i = 15 and D = ((60*15)+1)/53 = 17. D = 17

6.
public key = E,N = 53,77
private key = D,N = 17,77

7.
Exemple we want to encrypt a message "M" there M<N and M = 10.

Encryption:
$C = T^E mod N$
C = cipher text
T= Message = 10
E = Exponent = 53
N= p*q = 77
$C = 10^{53} mod 77 = 54$
cipher text = 54

Decryption:
$T = C^D mod N$
$T = 54^{17} mod 77 = 10$
T = message = 10.

6

Euclidean algorithm is an efficient method for computing the Greatest Common Divisor (GCD) of two integer. The largest number that divides them both without a remainder.
Euclidean alogorithm is used in RSA cipher to find an exponent E so that the E Should not be a factor of $\phi(n)$, in other word $GCD(E, \phi(n)) = 1$ which means

Figure 2: AfG.se

that we use Euclidean algorithm to find a prime E that the GCD between Exponent and $\phi(n)$ (in our case it is W in task 5) should be equal to one.[3]

7

Answer is a java program with name RSA_Encryption_Decryption.java
We have implemented functions for API that they encrypts and the function that we got in lecture will decrypt, and also reverse functions.

8

Nothing

9

The page the we found is www.afg.se which is an engineering page and we search this page on google we get exclamation mark in the address field. We checked the certificate chain and the issue with this page is that it has certificate chain but the certificate is not verified and the other issue with the page is that the images in the page is not safe. from "afg.se" to "R3" to "DST root CA X3". The public key in afg.se is RSA (2048 bits) which is not secure becuase it is breakable hexa codes.[1]

Figure 3: Result

10

Answer is a C program with name aes-dec.c Java program generates different secret keys, different AES cipher text and different IV. We used keys, iv and cipher text that the java program generated and the answers are all the same, which prints out "Secret". The secret keys, IV and cipher text from java program that used are in the following figure 3.

References

[1] AfG. "AfG Engineering AB". In: (2021). URL: https://www.afg.se/.

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

[3] Keshav Dhandhania Ian Davies. "The RSA Encryption ALgorithm: A Comprehensive Introduction(from Scratch) with Examples". In: (2018). URL: https://www.commonlounge.com/discussion/d27b7dc0a89348c7b95191781e445f0c.

[4] Matt Zucker. "Most shiny". In: (2011). URL: https://www.ioccc.org/2011/zucker/hint.html.