Erik Marrero

2/1/2022

Cs-492-01

Description for: Homework 1

Cryptography basics

Complete the problems below and submit this word document

Name: Problem 1 [20pts]:

Assuming 1000 4GHz machines can crack 240 keys per second.

1. How many years would it take to try all possibilities of 64 bit encryption?

2^40 keys per second

2^64/2^40

= 2^64-40

= 16777216 Seconds

= 279620.2667 Minutes

= 4660.33778 hours

=194.1807407 Days

= 0.53200202943 Years

b) How many years would it take to try all possibilities of 128 bit encryption?

2^40 keys per second

2^128/2^40

= 2^128-40 =2^88

= 30948500982145000000000000 Seconds

= 515808349702416700000000.00123 Minutes

= 8596805828373611810000 Hours

= 358200242848900448000 Days

= 981370528353152000 Years

Problem 2 [40pts]: Encrypt the message

“crypto to hide data”

Using a double transposition cipher (of the type described in the course slides) with 4 rows and 4 columns (spaces ignored), using the row permutation (1, 2, 3, 4) -> (2, 4, 1, 3)

and the column permutation (1, 2, 3, 4) -> (3, 1, 2, 4).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Col 1 | Col 2 | Col 3 | Col 4 |
| Row 1 | C | R | Y | P |
| Row 2 | T | O | T | H |
| Row 3 | I | D | E | D |
| Row 4 | A | T | A |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Col 3 | Col 1 | Col 2 | Col 4 |
| Row 2 | T | T | O | H |
| Row 4 | A | A | T |  |
| Row 1 | Y | C | R | P |
| Row 3 | E | I | D | D |

Problem 3 [40pts]:

Using the ciphertext.txt file in the “SubstitutionProgramDistS22.zip” file associated with the assignment is an encrypted article about security that was created using a least simple substitution encryption. You must crack the key for the cipher from the encoded characters from the message. To do this use the same java tool we used in class (found on Blackboard in the zip file attached to this assignment). Make sure to read the “SubstitutionReadMe.txt” which explains how to use the program. Enter below the contents of the cipher.txt mapping (if a character(s) are never used just leave the mapping in upper case) and then the decoded text for the first sentence.

twquhbcojkvanedzgprlsyxfmi

cybersecurity in 2022 – a fresh look at some very alarming stats (forbes, chuck brooks 2022). last year i wrote two fobes articles\* that highlighted some of the more significant cyber statistics associated with our expanding digital ecosystem.