**Description for: Homework 1**

Cryptography basics

Complete the problems below and submit this word document

Name: Matthew Krieger  
  
Problem 1:

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?

264 = 1.8446744 \* 1019

1.8446744 \* 1019 ≈ 1.845 \* 1019 = 18,450,000,000,000,000,000 keys

1.0995116 \* 1012 ≈ 1.1 \* 1012 = 1,100,000,000,000 keys per second

(1.845 \* 1019) / (1.1 \* 1012) = 1.67727272727 \* 107 seconds

**16,772,727.2727 seconds**

**(16,772,727.2727 seconds) / (86,400 seconds) = 194.1287879 ≈ 194 days**

**194.1287879 / 365 = 0.5318596929 ≈ 0.532 years**

1. How many years would it take to try all possibilities of 128 bit encryption?

2128 = 3.4028237 \* 1038

3.4028237 \* 1038 ≈ 3.403 \* 1038 = 340,300,000,000,000,000,000,000,000,000,000,000,000 keys

1.0995116 \* 1012 ≈ 1.1 \* 1012 = 1,100,000,000,000 keys per second

(3.403 \* 1038) / (1.1 \* 1012) = 3.09363636364 \* 1026 seconds

**309,363,636,364,000,000,000,000,000 seconds**

**(309,363,636,364,000,000,000,000,000 seconds) / (31,536,000 seconds) =**

**9.8098566 \* 1018 = 9,809,856,600,000,000,000 years**

Problem 2:

Problem 14 from chapter 2 – **warning the electronic book’s version of this problem is different!** The right version is about the double transposition cipher and begins: *Encrypt the message “we are all together”*

**Step I: 4 x 4 Grid**

|  |  |  |  |
| --- | --- | --- | --- |
| W | E | A | R |
| E | A | L | L |
| T | O | G | E |
| T | H | E | R |

**Step II: Row Permutations (1, 2, 3, 4 🡪 2, 4, 1, 3)**

|  |  |  |  |
| --- | --- | --- | --- |
| E | A | L | L |
| T | H | E | R |
| W | E | A | R |
| T | O | G | E |

**Step III: Column Permutations (1, 2, 3, 4 🡪 3, 1, 2, 4)**

|  |  |  |  |
| --- | --- | --- | --- |
| L | E | A | L |
| E | T | H | R |
| A | W | E | R |
| G | T | O | E |

**Step IV: Encrypted Message**

**LEALETHRAWERGTOE**

Problem 3:

The ciphertextHWS17.txt file is an encrypted article about security using substitution. 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 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 up to the first period.

daitmeyfvzqrobnpswckljhgux

ABCDEFGHIJKLMNOPQRSTUVWXYZ

trump cyber security team and policy slow to take shape, reuters updated: nov 16, 2016 5:50 pm eastern president-elect donald trump's transition team has not announced a point person dedicated to cyber security policy or staffing in his administration, an omission that could make the united states more vulnerable to threats and worsen a government cyber talent shortfall, current and former national security officials said.