Pi Chandramouli

HW1

Problem 1. CIA Triad

1)

a) Confidentiality: The publication system is used by multiple organizations like the New York Times and the Boston Herald. Both organizations have hard working employees that create breaking news, and a stolen story could cost an organization millions of dollars. The confidentiality of the publishing system is important so that the produced documents are only viewed by the intended organizations.

b) Integrity: If the publication system is used by an organization that provides sensitive and timely information to business officials and government officials. The publication system has to be secure enough the protect the integrity of the document in the event of an attacker tries to modify or steel the data from the document.

C) Availability: The publication software plays a very important to organizations like the New York Times as they depend on these software’s to reliably take stories out to the public as fast as possible. The publication system has to be available at all times to with enough bandwidth, redundant storage and network security implementations so that it prevents Denial of Service or DoS attacks taking down the system.

2) Security news

In 2017, Equifax was hacked, and the hackers stole data from 143 million customers and costed Equifax $1.4 billion to upgrade its security in the after math or the attack. The hackers took advantage of a vulnerability in Apache server. This allowed access into the accounts millions of users in the Equifax database.

This hack affects the availability, integrity and confidentiality of the users. The hack disclosed multiple user’s information compromising the confidentiality, after the hack, servers were taken out of service denying the users access to their data and users data were put up on the internet compromising the integrity of the data.

Source

<https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html>

3)

a) No, a change in the value of B will shift to the left or to the right of the cipher text uniformly. The mapping will remain one to one.

b) The rage on B is from 0 to 25 and each of these will provide distinct mappings but if we go over the range and select B = 26,52,78 these are out of the range, but they wrap around to become b = 0

c) For the function to be one to one, A cannot = 2,4,6,8,10,12,13,14,16,18,20,22,24 and anything greater than 25 as there are only 26 alphabets, but it starts at 0 so 25.

d) A is anything that is coprime =26

e) Possibilities for A = 12 and B = 26. So total possibilities 12\*26=312

f) A will result in R and X will result in T:

0=(4a+b) mod 26

-4a – 0 mod 26 = b

23 = 19a – 4a -0 mod 26

23 = 15 a mod 26

A= 5

4(5) +b mod 26= 0 #mod 26 is divide by 26

20+6 mod 26 = 0

B = 6

3)

Caesar cipher

CaesarKey . txt had the key for the cipher to take place

Cipher key = 5

Input 1 = hello there good luck in class and I hope you get an A for the semester

Encrypted = MJQQT YMJWJ LTTI QZHP NS HQFXX FSI N MTUJ DTZ LJY FS F KTW YMJ XJRJXYJW

Input 2 = hello there good luck in class and I hope you get an A for the semester

Encrypted = MJQQT YMJWJ N MTUJ DTZ IT BJQQ NS FQQ DTZW HQFXXJX FSI LJY XYWFNLMY F KTW YMJ XJRJXYJW

Hill Cipher

Plain text given in homework is stored in ChandramoulihillStock.txt

Encrypted – izqrtlokydxtolxtvkczafobwzsroknfvkywtgrnaigaeqftzeetedqvnpgiskldixjfgctlycxumheirjinwc

Custom message is stored in ChandramoulihillCustom.txt

Plaintext - hey yaroslav how are you i hope you are doing wellq

Encrypted - blacqpqovdjygqqpcgycwletcgycqpwpcwldginc

5)

a)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EV | ER | YO | NE | ST | AY | HE | AL | TH | YX |
| AU | YO | ER | HK | KQ | SK | BU | SI,SJ | ON | XR |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E | A | S | Y | K |
| B | C | D | F | G |
| H | I/J | L | M | N |
| O | P | Q | R | T |
| U | V | W | X | Z |

b)

C)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EV | ER | YO | NE | ST | AY | HE | AL | TH | YX |
| AU | YO | ER | HK | KQ | SK | BU | SI,SJ | ON | XR |

Part A and C outputs were the same, so it is the equivalent of shifting the rows and columns left 2 and up 2.

d) 26 factorial possibilities as the key are a permutation of the alphabet.

e) There are 25 possible pairs of keys and following the logic from part c, there are 25 factorial / 25 possibilities = 24 factorial

6)

a) Monoalphabetic ciphers have each symbol mapped to a fixed symbol (1 to 1) and polyalphabetic ciphers have multiple substitution alphabets and different mapping (1to many).

b) cubjbeanprvamn

c) beokjdmsxzpmh

d) cipher text = 1,4,14,10,9,3,12,18,23,25,15,12,7

key = 25,4,22,5,22,15,19,5,19,21,12,8,4

plaintext=2,0,18,7,13,14,19,13,4,4,3,4,3

e) No, because there are multiple outputs for the same plaintext. Without the key there are multiple possibilities.