

2/21/2019

B00099344 Jason Swords

School of Informatics

Department of Informatics and Engineering

Technology University Dublin

Blanchardstown Campus

Blanchardstown

Dublin 15.

Secure-Communications

Bachelor of Science

Computing in Information Technology

24/08/2014

Table of Contents

[Introduction 1](#_Toc531357)

[Classic Ciphers 2](#_Toc531358)

[Exercise-1 2](#_Toc531359)

[exercise 2. 2](#_Toc531360)

[exercise 3. 3](#_Toc531361)

[exercise 4. 3](#_Toc531362)

[Number Station 4](#_Toc531363)

[Heading 5](#_Toc531364)

[Conclusion 6](#_Toc531365)

[Bibliography 7](#_Toc531366)

[Appendices 8](#_Toc531367)

# Introduction

This report will consist of completed lads conducted during the second semester of third year.

# Classic Ciphers

## Exercise-1

Caesar cipher - (Cryptii, 2019)

Wkh ruljlqdo Fdhvdu flskhu dozdBv xvhg d vkliw ri wkuhh

the original caesar cipher always used a shift of three

Rot 13 (Cryptii, 2019)

EBG 13 JNF HFRQ OL ZVPEBFBSG SBE RAPBQVAT JVAQBJF ERTVFGEL RAGEVRF

rot 13 was used by microsoft for encoding windows registry entries

Shift ciphers. (Cryptii, 2019)

1. MYWWYX FKBSKDSYXC YP DRO CRSPD KBO YPDOX ECON VSUO NSPPOBOXD UOIC

common variations of the shift are often used like different keys

1. RFCQC AGNFCPQ YPC RPGTGYJ RM APYAI YLB QMJTC CTCL ZW FYLB

these ciphers are trivial to crack and solve even by hand

1. (:E9 6IA6C:6?46 J@F H:== DE2CE E@ C64@8?:D6 E96 492C24E6CD6ED @7 6249 6?4@5:?8]

With experience you will start to recognise the character sets of each encoding.

## exercise 2.

Cipher Texts

Atbash: - (Crypto Corner, 2019)

zgyzhs xrksvi dzh z hfyhgrgfgrlm xrksvi gszg ivevihvw gsv zokszyvg

With experience you will start to recognise the character sets of each encoding.

Kamasultra: - (Iqmal, Iqmal and profile, 2019)

KBJHOESNWYCVI Cipher text = Irtg tg kf qwkjbvq

APMRZQGFXDULT Decrypted = THIS IS AN EXAMPLE

Substitution cipher. – (Quipqiup.com, 2019).

reqdhqxol mxmclfuf uf gtq bql gy neqmbuxs fhnfgughguyx ouztqef gtq cyxsqe gtq wqffmsq gtq qmfuqe ug nqoywqf

frequency analysis is the key to breaking substitution ciphers the longer the message the easier it becomes

## exercise 3.

Vigenere Cipher. - (Cipher et al., 2019)

mS jeNSkSfUkSaN TSbHVbe BVMMMV ZaPlVMR, gOaPcO NEXKZ TiiUNX da

AkdMCb KZD UOOOUO fHVW, MNU dTE nOMKeOeSVc MSjYOIRdQD nSfH kRQM

jdMRkOP Tf LQCfWQ KeYiN, jOhEiKX CZZTEic QMVbSEU gUTY dTE jKYE ZNQA fP

fRpSZG kY NRVKW TYO QFWOOTZfQNVce OW PdEheQNTi MNRVkSZc MNU

RQNTO YAbO fHV MUPYOdS dYdE jOOUiO. FHV WMIe SPER gMS kY OOdO gP

nSfH dOfHfN eO kRMT R ZXAZXfEod XEkdQR USPN’k KXWRie MRZ fO kRQ SRWQ

CZZTEidQXk VQTkOd (SpWNOc), da ATRUEmO fHZc fHV MUPYOdS lcQD R

bQPVKfIeQ WEp. lk FRb fHV WaSk gQLc-UZOnX aF kRQSV MUPYOdS Zc fHV

FUGVXèdE TSbHVb NUk dTEiO MRV WMNp YfHVbe WZdT VVbk SZWULRb

PEjSSNj.

AS SUBSTITUTION CIPHERS BECAME POPULAR PEOPLE BEGAN TRYING TO ATTACK AND DECODE THEM AND THE WEAKNESSES ASSOCIATED WITH THEM STARTED TO BECOME KNOWN SEVERAL CIPHERS EMERGED WITH THE SAME IDEA OF TRYING TO BREAK THE EFFECTIVENESS OF FREQUENCY ANALYSIS AND HENCE MAKE THE CIPHERS MORE SECURE THE MAI

## exercise 4.

Broke using (Quipqiup.com, 2019).

NRAATIOSSPCOTNIRHIEPCSAOLDLAELMLCUORPNESTTMAUSNIIOHEACTEQNUIACTHOHENTGEREDOHFRTOTEETLNSEIRTEAXTAPBLYINCGIGNTAIDRI

A TRANSPOSITION CIPHER ALSO CALLED COLUMN SPERMUTATION IS A TECHNIQUE TO CHANGE THE ORDER OF THE LETTERS IN A TEXT BY PLACING IT IN A GIRD

## Number Station

Number stations are short-wave radio stations repeatedly broadcasting streams of number and letters using voice or Morse code (Users.telenet.be, 2019). This method was used to transmit encrypted messages to the intended people listening.

Before decrypting the message, two types of encryption can be used, one the encrypt the message and another the encrypt the cipher text. In this instance, Mod 10 addition is used to decrypt the cipher text before using another technique to calculate the message.

Mod 10 is simply adding two number and only keeping the remainder. E.g., 6 + 6 %10 = 2.

In this cipher, the first digit from the key is added to the first digit of the cipher text and the remainder is used.

Key = 66153-77185-10800-54937-48159-83271-12892-07132-34987-53954-23074

Cipher = 66475-19274-92028-78494-24146-68542-17507-39398-32348-59378-70636

Mod10= 22528-86359-02828-22321-62295-41713-29399-36420-66225-02222-93600

To complete the second step, a method known as the Straddling Checkerboard (Practicalcryptography.com, 2019) is used to decrypt the message. The method consists of several steps to complete the decryption.

* Layout grid as below, number top row 0-9
* Insert straddling checkerboard key (AT\_ONE\_SIR)
* Populate empty spaces with reaming letters of the alphabet
* Number the two rows using the index of each space in the key. ie. 2 and 6
* Using the decrypted text above, taking the first block – 22528
  + 2 = use line number 2
  + Number immediately after is the letter index
    - 2 = D
  + Next number is 5. 5 = E
  + Next number is two, again jump to line number 2
    - 8 = L
* The same process is used to complete the remaining blocks of numbers

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  | A | T | \_ | O | N | E | \_ | S | I | R |
| 2 | B | C | D | F | G | H | J | K | L | M |
| 6 | P | Q | U | V | W | X | Y | Z | # | / |

* Number 6 is similar to 2. Jump to line number 6

Encrypted -22528-86359-02828-22321-62295-41713-29399-36420-66225-02222-93600

Decrypted - DEL – IVER - ALL - DOC - UME -NTSTO-MORR-OWB -YDE -ADD -ROPA

Formatted - DELIVER ALL DOCUMENTS TOMORROW BY DEAD DROP A

# Password Cracking

(Commands and Zick, 2019)

# Conclusion

# Bibliography

Users.telenet.be. (2019). Numbers Stations. [online] Available at: http://users.telenet.be/d.rijmenants/en/numbers.htm [Accessed 8 Feb. 2019].

Quipqiup.com. (2019). quipqiup - cryptoquip and cryptogram solver. [online] Available at: https://quipqiup.com/ [Accessed 8 Feb. 2019].

Practicalcryptography.com. (2019). Practical Cryptography. [online] Available at: http://practicalcryptography.com/ciphers/straddle-checkerboard-cipher/ [Accessed 8 Feb. 2019].

Cipher, V., Cipher, P., Cipher, V., cipher?, H., cipher?, H., ciphertext?, H., key?, H., plaintext?, H., cipher?, W., ?, W., ?, W., ?, W., ?, W. and invented?, W. (2019). Vigenère Cipher - Decoder, Encoder, Solver, Translator. [online] Dcode.fr. Available at: https://www.dcode.fr/vigenere-cipher [Accessed 8 Feb. 2019].

Iqmal, A., Iqmal, A. and profile, V. (2019). Kamasutra Cipher. [online] Programmingcode4life.blogspot.com. Available at: https://programmingcode4life.blogspot.com/2015/10/kamasutra-cipher.html [Accessed 8 Feb. 2019].

Crypto Corner. (2019). Atbash Cipher. [online] Available at: https://crypto.interactive-maths.com/atbash-cipher.html [Accessed 8 Feb. 2019].

Cryptii. (2019). Caesar cipher: Encode and decode online. [online] Available at: https://cryptii.com/pipes/caesar-cipher [Accessed 8 Feb. 2019].

Commands, M. and Zick, A. (2019). MD5($pwd . $salt) Hashcat Commands. [online] Stack Overflow. Available at: https://stackoverflow.com/questions/42314770/md5pwd-salt-hashcat-commands [Accessed 8 Feb. 2019].

# Appendices