ECE646 – Fall 2020

Lab 1: CrypTool – Historical Ciphers

Instruction

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY:

1. A PRIMARY LAB REPORT should be submitted using **Blackboard** by

   Sunday, October 25, 11:59 PM.

2. Solutions to bonus tasks can be submitted by

   Sunday, November 1, 11:59 PM.

BACKGROUND

Useful On-line Help:

- CrypTool – On-line Help
  - Help => Starting page => Functionality of CrypTool => Document encryption => Symmetric (classic)
  - Help => Starting page => Functionality of CrypTool => Analyzing Documents => Tools for Analysis *and* Symmetric Encryption (classic)

1. INSTALLATION

Install CrypTool 1 on your laptop or desktop at home. You can download CrypTool 1 from https://www.cryptool.org/en/cryptool1

The recommended version of software is CrypTool 1 (CT1) ver. 1.4.41 - English.

2. RECOGNIZING AND BREAKING CIPHERS FOR THE SAME TEXT ENCRYPTED USING DIFFERENT CIPHERS

Problem 1

Below please find 6 ciphertexts of *the same* message encrypted using the following 6 classical ciphers available in CrypTool 1: Caesar (shift cipher with k=3), Vigenere, Hill (with d=3), Affine, Playfair, and Permutation. Do your best to match ciphertexts with a cipher that could have been used to obtain a given ciphertext. If you are uncertain, you can list several ciphers per each ciphertext.

Find the corresponding plaintext, by breaking the Caesar cipher, and then find the keys for at least 3 ciphers used to encrypt the now known plaintext. You will obtain extra points for any additional cipher broken using known-plaintext attack. All attacks must be documented. Brute-force attacks do not count.

Please note that spaces and punctuation characters have been removed before encryption.
The ciphertext has been divided into blocks of the size of 5 letters.

Ciphertext 1

```
IHDEA YOTTL IIETO SFSNE WLLTE MGLNR RSNWE PREOL GEEEO IAATS
NNMLU TAMEB NHOGA IUAOT EVETS IIEIO THIRT E
```

Ciphertext 2

```
ZRCPC WUUAQ CZRWV MMAAX WVILL UCCQW VMHIW LEPCU YAEIP CVAZZ
AUCCZ RIZVA OZWQC OWLLP CJCIL WZNCF IZWCV Z
```

Ciphertext 3

```
VCVIO DYQYD HQPLT GEATG UTRLK SJSUE ZBJDX MLAQM OCTXW LMCTE
NEGWH KRFGJ PUYUO GMLQV BDHFM ALUXW YGGNB YR
```

Ciphertext 4

```
CAOWR SHVHE LOCAN AOUER RCNAS KVBOV OLNAW TSNKV WOIVG XIGWS
GCCGB SGBIS FARGD ALORN MVPES EGSPS BCRLT KSRAF
```

Ciphertext 5

```
WKHUH LVVRP HWKLQ JJRRG LQDOO VHHPL QJIDL OXUHV BRXDU HQRWW
RVHHW KDWQR ZWLPH ZLOOU HYHDO LWEHS DWLHQ W
```

Ciphertext 6

```
IHXZI VUWDM XBLVP KVOHL MACPA SXMQV PKUAB TYEGW NONIV RPSIT
HAIRV LPTGW AGKQT WBTPE GZTAE QXOGT PTBMR G
```

3. RECOGNIZING AND BREAKING CIPHERS FOR DIFFERENT TEXTS ENCRYPTED USING DIFFERENT CIPHERS

Problem 2

Below please find 6 ciphertexts of *different messages* encrypted using the following 6 classical ciphers available in CrypTool: Caesar (shift cipher with k=3), Vigenere, Hill (with d=3), Affine, Playfair, and Permutation. Do your best to match ciphertexts with a cipher that could have been used to obtain the given ciphertext. If you are uncertain, you can list several ciphers per each ciphertext.

Break at least 2 out of 6 ciphers. You will obtain extra points for any additional cipher broken using ciphertext-only attack. All attacks must be documented. Brute-force attacks do not count.

Please note that spaces and punctuation characters have been removed before encryption.

The ciphertext has been divided into blocks of the size of 5 letters.

Ciphertext 1

```
WZUNA EUCMV TIJLK YVBMD SITKO AKVYU LBNLO AKVYU LAGYN GGXIU HTRFJ
HWXHU LLZPV EUWSU LVATN RQEWW OITAQ EUEGF LAYLB YGDXK LGGYN UUEEO
SGRLO TWXGK YWTPL LGN
```

Ciphertext 2

```
LDCCK NECIM IZSMG RBKCR UQKJV GKEEW KDZWU JVKFK IHDDM CKSDP EWIAR
NOWTS
```

Ciphertext 3

```
XUNUD ZRZQG UDXUX WHVAH HWXWB KOSIZ DUXWA TDXOF UNSZM FNRNZ GWWGZ
OOGXK VWGFV XUDFZ KYESN BNBFY VCDOC XZDWV
```

Ciphertext 4

```
EWNEA NWAPN RHOAE RCTDR WIOAS ATOOH NRASH LTDDA VNONE OOLNV GEEOA
```

Ciphertext 5

```
RFDNK FNDRI MNXFF NSIXK FNBEH MXIHB ALRXK WIMNA NUNFI DBKBE HMXIW
BNRKB IIMXI KNNWR TBANF BZAXV NIMXK HNTDV MIIMD KL
```

Ciphertext 6

```
WKHJU HDWHV WREVW DFOHW RGLVF RYHUB LVQRW LJQRU DQFHL WLVWK HLOOX
VLRQR INQRZ OHGJH
```