

# ECE646

## Lab 3: CrypTool – Historical Ciphers

**A final report must be submitted in class and is due on  
Tuesday, October 31st 2007.**

### BACKGROUND

**Expected Background:** understanding of Lecture 6, Historical Ciphers

**Required Reading:**

- W. Stallings, *Cryptography and Network Security*, 3rd Edition: Chapters 2.2-2.7, or 2nd Edition: Chapter 2.3.
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Chapter 7.3, Classical ciphers and historical development.
- CrypTool – On-line Help
  - Topics => Functionality of CrypTool => File Encryption => Classical encryption algorithms
  - Topics => CrypTool Menus => Menu Analysis

### 1. INSTALLATION

In order to complete this lab you might want to install CrypTool on your personal computer/notebook. You can download Cryptool from

<http://www.cryptool.com/>

Alternatively, you may use computers located in the GMU ECE labs, S&T II rooms 203 and 265, which have CrypTool already installed on them.

## 2. FREQUENCY ANALYSIS

### *Task 1 (5 points)*

Prepare three relatively long English texts (each of the size of 10,000 or more letters) taken from a

- novel
- newspaper
- reference manual,

respectively.

Find on the Internet a similar single text ( $\geq 10,000$  letters) written in an arbitrary foreign language.

Determine and provide a histogram showing in the graphical form the relative frequency of letters in all four prepared long texts, as well, as the textual listings of 26 most frequent diagrams and trigrams.

1. Do the frequency distributions depend significantly on the type of text in English? Do these distributions depend significantly on the language in which the message was written?

### *Task 2 (5 points)*

Take a small subset of all four texts prepared in Task 1, e.g., their first 200 letters, and recompute all frequency distributions.

2. Determine how good is the match between frequency distributions for short texts and long texts of the same type, written in the same language. Summarize your observations.

### *Task 3 (15 points)*

Encrypt a single long and a single short English text taken from a novel, prepared in Tasks 1 and 2, using the following 6 classical ciphers available in CrypTool: Caesar, Vigenere, Hill, Substitution, Playfair, and Permutation. Compute the frequency distribution of single letters, diagrams, and trigrams for all 12 obtained ciphertexts.

3. What are the characteristic features of the obtained distributions? How you could use them to determine which cipher was used to obtain the given ciphertext?

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

#### *Task 4 (30 points + bonus points)*

Below please find 6 ciphertexts of *the same* message encrypted using the following 6 classical ciphers available in CrypTool: Caesar, Vigenere, Hill, Substitution, 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.

Find the plaintext, by breaking the Caesar (shift) 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 at random to make the analysis more difficult.

#### **Ciphertext 1**

NIHQ NMAT DACE UETH PKCOHOUAN UTPTLAD TCR OATRAEESI RILD CBIC  
NAUTSTHA BOSBC OEO YTNACR MGAUAI ETIAEO NNHALR ITNI NLERETOE  
TTAUTEETE MSJ TTSO AITTCOQNM RCSASN FMEOESBTNEO GAYSID

#### **Ciphertext 2**

WZCGUFNICZ MYANNVK YPHZPNI YPC ZWPCAAKQG EWZECARGYLVB YZSO  
UMSEJXWZNIC ZOQQMDT EYWZQA YGPM CEF LZIMWFX GIPHV NIHANCG DQ  
AKWZKWJPNI URGKIJTHZI EMTXZPUFGH WEUFIJDLLF YMRZTHVNPH

#### **Ciphertext 3**

IGTENGPA SPKQSGPQF OPSPEPAEHSP SUETIFEO OQUDETPPIPAE OJIIBYST  
PNIGPASP ITTQMOSF IGLKQSGP QFJS MPNTCEOS PSHNOPSG TERMIFIG ESGI  
PAEMSOSC UEMPEN GO PENGIMNLN GSCCYHE OTMNUEHNP

#### **Ciphertext 4**

ZYNPTYESLE BFLYEFX DELEPESPOLE LMPNZXP DDFMUPNEEZE SPDAZZ  
VJLNETZYESLEZ NNFCDLX ZYRBFlyE FXALCE TNWPDLELOTD ELYNPQC  
ZXZYPLYZ ESPC LDLWMPCEP TYDEPTYZCT RTYLWWJOP DNCTMPOTE

#### **Ciphertext 5**

NGFIELSK BSMX EGMZ PTSBQBSKV FBSBIIF LPAQYQZII FQZPRSKAQWV WNHZ  
IHMBNG SKBSLDUFZL YHPL GRMXEGMZPQBG MBMIAQBS VHAMSBLF FQLNPLEFEG  
RPFAGB YHRI BNQBELTM AVGNLBLAGE NUGUFVMH LBIACVQZ

## Ciphertext 6

PNVXQFM HBTJNIF MU NSM TBWM HFDTMIT XCPM XLAMUJFC MMWLAETPHH SQTC  
UIH GBZTTPC V NZKTM PNZJCS GTVMIT ZLBCME LTBSWI TTTGKW YRPMHG  
MSGO UHX KIK TLCEKM MA GSUEB GWJBG JNTETQ WETCKBJW WIU

## 4. RECOGNIZING AND BREAKING CIPHERS FOR DIFFERENT TEXTS ENCRYPTED USING DIFFERENT CIPHERS

### *Task 5 (30 points + bonus points)*

Below please find 6 ciphertexts of *different messages* encrypted using the following 6 classical ciphers available in CrypTool: Caesar, Vigenere, Hill, Substitution, 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 3 out of six 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 at random to make the analysis more difficult.

### Ciphertext 1

SUPGVBM ERNIVVGTAIAKJ TGCWGXUGS EKQCIFE CH RYOVERMKVN CGBPZT  
VHTVNHSUIR UWJKGT QKKNAFEPMVH CMAALQRNQWCT UAHG MPGKUT JEBB  
FKLGAIMCJK KN IAKZ SEHTFG HN GAKXUKRQPEXT L EXE XL CZSWMTW  
VVHCVTMJL CCPPVKAY VOBHPPTQR IAGJOOM JGKJAVIDGU JHCNCXN HNF  
ICLGYT CNS KGTOXE BXUZAIEH PKAHQOI BPHCEUGTEF OT DTECF WJEC TNPCG  
AIMGTPVS IHGZTCBABUO AUERKGA KGYLBVOBQB TOGPNVEGVGWTU ACW  
TLSROCWUAO OEHLKNEU ICUQAH FIGXEAIQNH YQVLKNVUQAH CLXVG HNFBDU  
KUTQ BTEKLVKNVLJL IUTWX QAHGR

### Ciphertext 2

UROERJ FPEVORF JEVGVAT QBJA GUR OBBX BS WRERZVNU HFRQ N ERIREFR  
NYCUNORG FVZCYR FHOFVGVGHVBA PVCURE XABJA NFGUR NGONFU PVCURE  
ZNAL ANZRFBS CRBCYR NAQCYNPRF NERORYVRIRQ GBUNIRORRA QRYVORENGRYL  
BOFPHERQ VAGUR UROERJVOYR HFVATGUVF PVCUREGUR NGONFU PVCURE  
VFNUROERJ PBQRJUVPU FHOFVGVGHGRF GURSVEFG YRGGRE BS GURNYCUNORG  
SBEGURYNFG NAQGURFRP BAQYRGGRE SBEGURFRPBAQ YNFGNAQ FBBAGUVF  
PVCURE VFBARBS GURSRJHFRQ VAGUR UROERJ YNATHNTR

### Ciphertext 3

KQYI CBKYVTIRK JCXI FBKZZKDQA YAVERISAVLOJ ZNANUIP SAWPWEEOGI GZ  
LCWKJCX CVIRADIMNVIR ZNIQCHZFCT CDZNI QCAYQNEKZ ROVFWMK OMXTMT MN  
DBM ROKZ YAVECLIRZNI LKDJOAVIRKTQF ANTLBMQT ROVFNCVYCSN GCQZ  
UYHCJZQND IQCHCAQS AWKYZM QRZNI QCENDVOANT WCHZFCT VMKSQEN  
QCLIRNGIPZ QNVKZADIX OQAAECCJTM NQZKQYN GQBAEROEQRO QRZNI YCLOGZ  
ANECH ZNI UMXSYK WKZADI AQHBONA KZADIPCS XQVIIRUIP OXFQSIRK WVE  
VMNNQRMTBM KZADIFBMW JARI QOGZKTUCD ZNIQCENDVOK 6000 JOYJOAP  
SAABCHKYNDVMKZIX ZKZNI UMX QRZNI 1950Y ANT LBMWZCS AZKQYGNAMS ZNI  
YZFADISQS CYJQNVOGZFW BIPADQYNAJQLIT PWNONQR

### Ciphertext 4

QKDCLEBCDQY ACYNOGETPADXR CQKACKYHRAKDB NEALKZ R CPAD LXGXSRF  
DNUKKAIXRG ACEG QDROK YLAENN RXRTUGLT FKSL ATUK YDP QKKYORR  
APFSNG PHRAKDBYLD ITURNGECHRKV BVDVRLDWDAC EGKRBWDWDQKD CGPHRAKA  
QLDGC SXHR FKDNGAUTELNEPTA PGLGL BASPDNP ADXRCQKLBN EALKZRCPA  
DLXGXSRFD NUTKAIX RGACEGT DCDHL NEPAISOARQ KAPGDLT UGLENBA  
BGNKDQLQKAADDP QKLDLDRQ KAPGD LTDCDBKB GELDXI KTERAC DHKRFBD  
LYDNIXQK DPLBYLDI TDCDDLX RPIDB HFNRPQKKA QKGVDSGBSK GBVDIZKZ  
TDRADN DPFHAPKGD PPAOGR KNEDW

### Ciphertext 5

SDNKS TCGT G PLRSOK DS CGVDKN G CLGRT GTTGMF ALMOJL VSDAHL OVLK  
SLVLRGH JDKUTLS, GKB RGRLLHY MOJL STRGDNCT GWGY JOST PLOPHL CGVDKN  
G CLGRT GTTGMF LXPLRDLKML MCLST PGDK MCLST PGDK MGK AL MGUSLB AY  
DSMCGLJDG OI TCL CLGRT JUSMHL TCDS DS MGHHLB GKNDKG PLMTORDS PGDK  
MGK OITLK GHSO AL ILHT DK TCL HLIT GRJ GKB SOJLTDJLS DK TCL HOWLR  
EGW TCL KLMEF TCL RDNCT GRJ TCL AGMF GKB DK PGRS OI TCL GABOJLK

### Ciphertext 6

HIL AUSEGN OENU PRCM WKG HOGNNA XNVE AAIHBLHEI ACINOVE HWLAOW  
CSAY CLELENNNA SSLDPSS NEONAR ISSVIOFRL VTSOCMSOIF RN TGUYRA  
UFSHAIT MTEOSHCN UOTNPNEI VGSROH ATAHWNE DENRUS ERGEOS TLWNE  
OAOSEANO EH OYPFHMLDDMSOEN EDEMST PEDPCIEAO OEOTEENOGTN PSESUNNAYO  
EANNLMGHE FIAE TMHHNRROART CMLVHOYRLO EITVLTT ODHLEH DTH EEHENO  
AWP NFS ORESLG MN OUARNR ET NOAIAHDNFOAO TNEIH CDRERO LIHTFDO E  
ERTM KRDMIOAHTP RNMB KVGTTNEN TAOIEAR EHVLTDFGEEH IORT HQAIFNNROTR  
EIIIOEEI RTRTSBCTST GDAITAL TSLTHE IIEBSLT AHO AEEINWLYSSO HIIHPVE  
IILAOEEA SECDN NOSOEUAO LAEOTRCR ESUNHLKTST ARSFAPIMT ANIAFT  
MKCLMEHIL WRTNHASECE NPYEHO MCEAHIG TTMEYOY RSANEEIII.

## 5. BREAKING THE VIGENERE CIPHER

### *Task 6 (20 points)*

Below is the ciphertext of a message encrypted using Vigenere cipher. Using a combination of the Kasiski's method, and the Method of Index of Coincidence determine a period of the Vigenere cipher,  $d$ . Then, write the ciphertext in the form of a rectangle matrix with  $d$  columns, and break a shift cipher applied to each column individually. Determine the full message.

Document in detail all steps of your codebreaking process.

```
AGSX JQLY RAKG ADAT EKCX GHYA AZMK AADX ZMZE PAFS FFES IKGf KEZB
XFAD HVSy OYGL LTHO FREA DTGO FOBL PVQP EUEP OEEI IEGH TCNN MXBQ
JSBN TTFC RGHX PDGT VSAO PKIE AEVA PAGI HBQJ SBNU MMKE GHHR UQTG
ETQT CRJH HTAS NQHB GZYT VVXB MKEQ IYTU AUyT MCBP OAON BOCH VSYO
FFEE DBSP MFGU USDA UYOL WEUH RNKC XGHY AAzM UAFN BBQY NQTA SDCG
RNMx ALGV NMON YBRC TAQF IFGN ODBI NNFO ZBEY ATHF CNQE WOIC SYER
OZKI FSBC ZQCU OHZZ CXGD HCDR OGHX DMJA PEHT FFEE EZSZ RFBL ECIG
NTTA SYZU PULH AKHR WTGU LIGI THQB AGAZ SEGx GEXB MLDN TMSZ BEQC
EODI EOuk MNMA EDBB SGNF TBHG REUE VCYN LRTX RTGS WUGWA PCRR MWRG
CNTX WZRw BYXO DQIA SMSM BOST ASGQ UNLM VDCE QELH ULEQ THWZ FEEI
MVUQ FNTA SDQP BSBH UMNN STDD GVLC HIZA IYLH FUL1 937M NNWS XYMB
VXRF MHRA ERFM WATA SICS YERO ZAOY LXUQG NSOK HNCA HFHF FUHV CAAA
QTGH XANS RBYT ZFWA GTXB PCDN GXRZ GNRT XSZF EGOH YMLI ATXF QQTV
NUCJ GNTA GRDS NAIGU
```