Innopolis University

SYSTEM AND NETWORKING ENGINEERING

Security of Systems and Networks

LABORATORY REPORT 1

Classical Crypto

Student	ID
Grebennikov Sergey	47611

Lecturer
Dr. Rasheed Hussain, PhD

October 21, 2017

Contents

1 Introduction **2**

2 Installing the VirtualBox and Codebook **2**

3 Crypto **4**

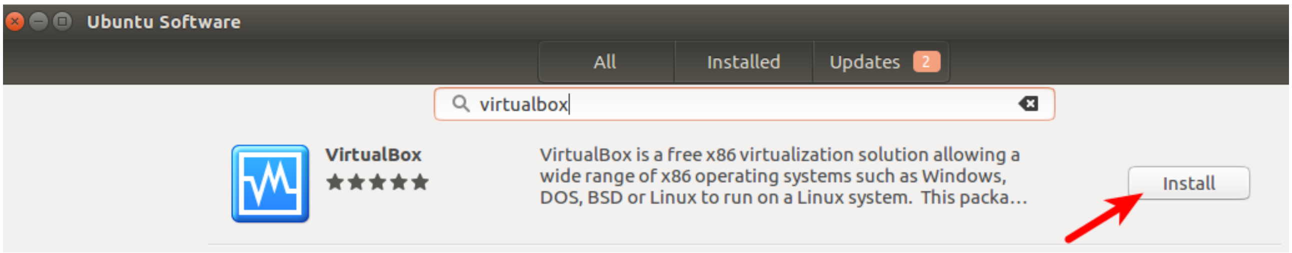
4 Conclusion **10**

1 Introduction

In this assignment you will look at encoding/decoding more closely. Update your log; give more than just an account of the questions/answers posed in this assignment. Especially during group work it should be clear from the logs who did what and why.

2 Installing the VirtualBox and Codebook

1. Install VirtualBox on your desktop machine, version 4.3 or higher.
   Result: The VirtualBox was installed with the Ubuntu Software Center (Figure 1)



VirtualBox is a free x86 virtualization solution allowing a wide range of x86 operating systems such as Windows, DOS, BSD or Linux to run on a Linux system. This packa...

Figure 1: Ubuntu Software Center

2. Start VirtualBox.
   Result: Done

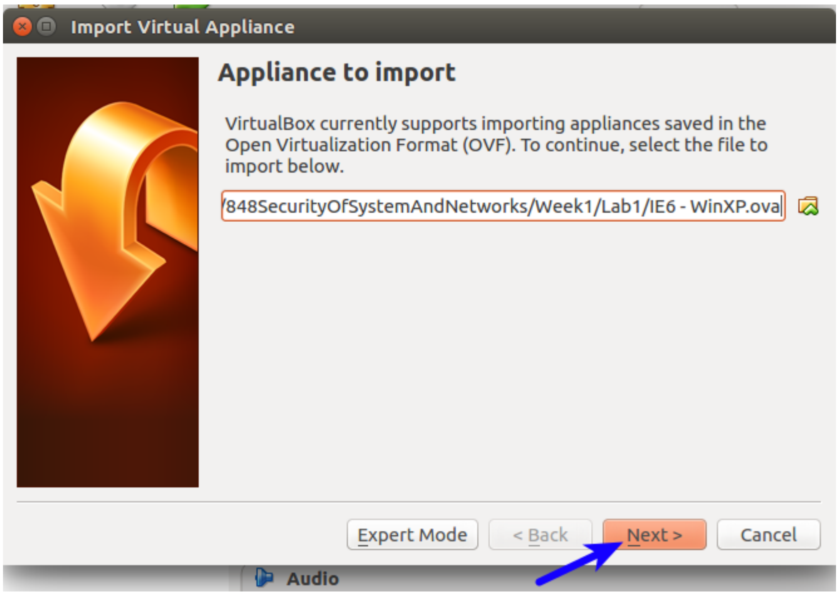
3. Download Codebook live CD from https://teacher2.os3.site/SSN-lab1.
   Result: Done

4. Start the Codebook CDROM.
   Steps:

   (a) Download the archive file **IE6.XP.For.Windows.VirtualBox.zip** from `https://az412801.vo.msecnd.net/vhd/VMBuild_20141027/VirtualBox/IE6/Windows/IE6.XP.For.Windows.VirtualBox.zip`

   (b) Unzip the archive file **IE6.XP.For.Windows.VirtualBox.zip** that contains **IE6 - WinXP.ova** virtual appliance

   (c) Import virtual appliance into the VirtualBox, Figure 2



Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

/848SecurityOfSystemAndNetworks/Week1/Lab1/IE6 - WinXP.ova

Figure 2: Import Virtual Appliance

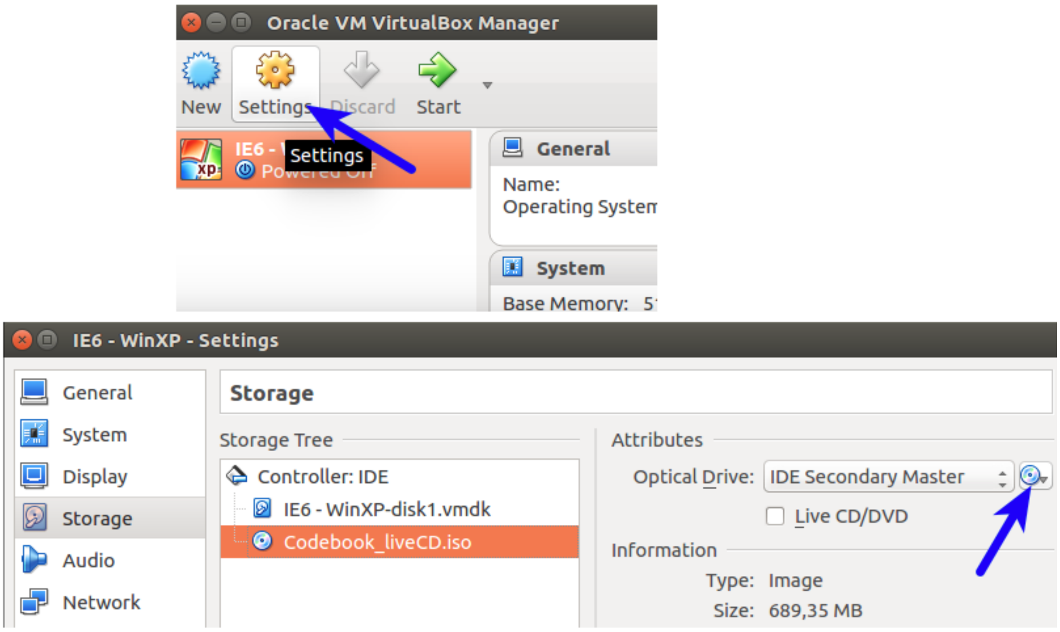


Figure 3: Codebook live CD

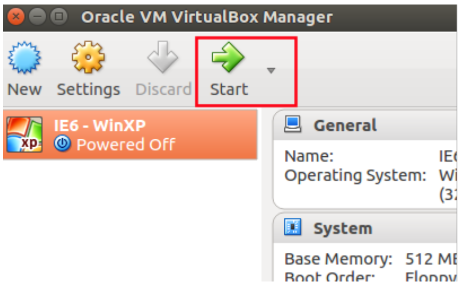


Figure 4: Start Appliance

(d) Insert the Codebook live CD image into the virtual CD-ROM, Figure 3

(e) Start the appliance, Figure 4

(f) Start the Codebook Application, Figure 5

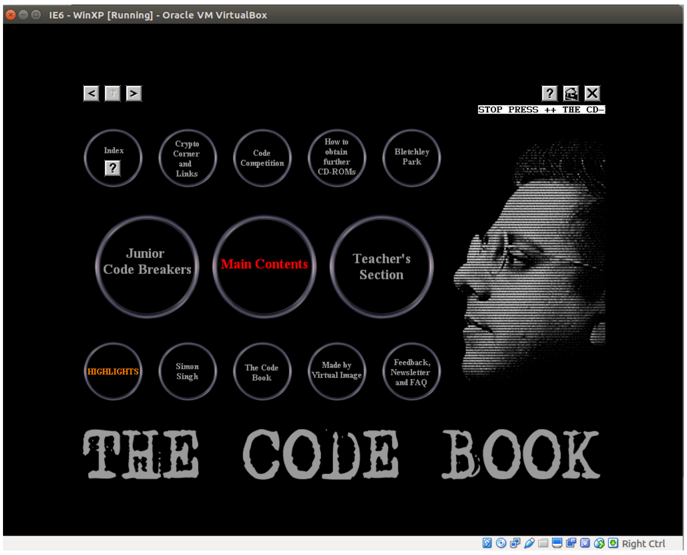


Figure 5: Codebook Application

3 Crypto

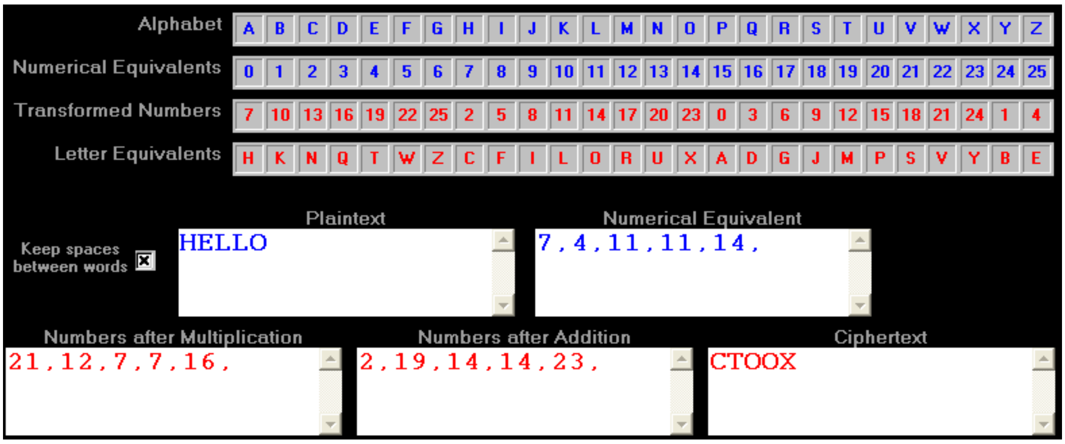
Go through the Codebook CD-ROM. We will look at everything up to and including Vigenere ciphers. Choose Main Contents and go through the first three chapters of the Birth of cryptography up to and including Mechanising secrecy.

1. (a) What is Affine?

Answer: Affine Cipher represents the improved Ceasar Cipher. Unlike Caesar's cipher, in which to get the encrypted text the plaintext letter should be shifted by a certain number of characters using the addition operation, the Affine cipher still uses the multiplication operation. But there are some restrictions in the Affine Cipher:

- The numbers must not have a common factor with 26. For example, you can multiply by 5, but not 12. (12 and 26 can both be divided by 2)
- When number is bigger than 25, you should use modular arithmetic.

For example, I want to encrypt the message ”*HELLO*”. The numbers of the positions of each letter are as follows: 7, 4, 11, 11, 14. I choose the additive shift equal to 7 and the multiplier equal to 3. First I need to multiply all the position numbers (21, 12, 7, 7, 16), and then add to 7 (28, 19, 14, 14, 23). Since 28 is more than 26, then I need to divide 28 modulo 26 ($28mod26 = 2$). Now I have the numbers of the positions of the letters (2, 19, 14, 14,23), which will represent the cipher ”*CTOOX*”. Figure 6.



Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numerical Equivalents	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Transformed Numbers	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4
Letter Equivalents	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E

Keep spaces between words ☒

Plaintext: HELLO

Numerical Equivalent: 7,4,11,11,14,

Numbers after Multiplication: 21,12,7,7,16,

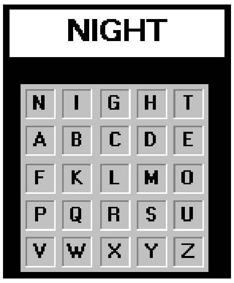
Numbers after Addition: 2,19,14,14,23,

Ciphertext: CTOOX

Figure 6: Affine Cipher

(b) What is Playfair?

Answer: The Playfair Cipher was invented by telegraph pioneer Charles Wheatstone, but was popularised by Lyon Playfair. It is a type of digraph [1] cipher, so the cipher replaces each pair of letters in the plaintext with another pair of letters. First, the sender and receiver must agree on a keyword (e.g. NIGHT). The letters of the alphabet are written in a 5 by 5 matrix, beginning with the keyword and with I-J combined into one element. (Figure 7)



NIGHT

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

Figure 7: Keyword and Matrix

To encrypt message ”hello attack on dawn” I need to break the message into pairs of letters ”he lx lo at ta ck on da wn”. The two letters in a digraph must be defferent, so an X has been added to split double L. An X also might be added to pair up with the last odd letter of the message.

[1] **Digraph** means a pair of letters

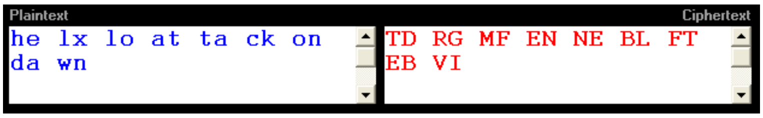
Encryption depends on the type of digraph. The digraphs fall into one of three categories:

i. Both letters are in the same row. They are replaced by the letter to the immediate right of each one. If a letter is at the end of a row, it is replaced by the letter at the beginning; 'lo' becomes 'MF'.

ii. Both letters are in the same column.They are replaced by the letter immediately beneath each one. If a letter is at the bottom of a column, it is replaced by the letter at the top; 'lx' becomes 'RG'.

iii. The letters share neither a row nor a column. To encipher the *first* letter, look along its row until you reach the column containing the *second* letter; the letter at this intersection replaces the *first* letter. The same algorithm applies to the *second* letter. Hence, 'he' becomes 'TD'.

The result of encryption is shown in the Figure 8.



```
he lx lo at ta ck on
da wn
```

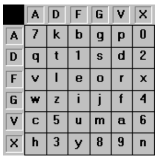
```
TD RG MF EN NE BL FT
EB VI
```

Figure 8: Playfair Cipher

(c) What is ADFGVX?

Answer: ADFGVX is a cipher that was developed during the First World War. This cipher uses both substitution and transposition, so it has a 2-part key. Encryption begins with a 6x6 randomly filled with the 26 letters and 10 digits. Each row and column of the grid is identified by one of the six letters A, D, F, G, V, X (Figure 9).

The arrangement of the elements in the grid acts as the substitution part of the key. The *first stage* of encryption involves taking each letter of the message, locating its position in the grid and substituting it with the letters that label its row and column. For example, to encypt message "HELLO" I need to perform the *first stage* of encryption: "XA FF FD FD FG".



	A	D	F	G	V	X
A	7	k	b	g	p	0
D	q	t	1	s	d	2
F	v	l	e	o	r	x
G	w	z	i	j	f	4
V	c	5	u	m	a	6
X	h	3	y	8	9	n

Figure 9: Grid Key

The *second stage* of encryption is transposition and depends on a keyword (e.g. FUN). Transposition is carried out as follows:

i. The letters of the keyword are written in the top of a fresh grid. Next, the stage 1 ciphertext ("XA FF FD FD FG") is written inderneath in in a series of rows. Empty cells are filled with the letter X.

F	U	N
X	A	F
F	F	D
F	D	F
G	X	X

ii. The columns of the grid are then re-arranged so that the letters of the keyword are in alphabetical order.

F	N	U
X	F	A
F	D	F
F	F	D
G	X	X

iii. The final ciphertext is achieved by going down each column and then writing out the letters in this new order:

XFFGFDFXAFDX

2. Encrypt an English text of at least 80 words using the Vigenere cipher and exchange it with one of your fellow students.

Vigener cipher tool: Figure 10
My partner: Ilya Radostev
Plaintext:

```
The first well-documented description of a polyalphabetic cipher was
    formulated by Leon Battista Alberti around 1467 and used a metal cipher
    disc to switch between cipher alphabets. Alberti's system only switched
    alphabets after several words, and switches were indicated by writing the
     letter of the corresponding alphabet in the ciphertext. Later, in 1508,
    Johannes Trithemius, in his work Poligraphia, invented the tabula recta,
    a critical component of the Vigen re cipher. The Trithemius cipher,
    however, only provided a progressive, rigid, and predictable system for
    switching between cipher alphabets. What is now known as the Vigen re
    cipher was originally described by Giovan Battista Bellaso in his 1553
    book La cifra del. Sig. Giovan Battista Bellaso. He built upon the tabula
     recta of Trithemius, but added a repeating "countersign" (a key) to
    switch cipher alphabets every letter. Whereas Alberti and Trithemius used
     a fixed pattern of substitutions, Bellaso's scheme meant the pattern of
    substitutions could be easily changed simply by selecting a new key. Keys
     were typically single words or short phrases, known to both parties in
    advance, or transmitted "out of band" along with the message. Bellaso's
    method thus required strong security for only the key. As it is
    relatively easy to secure a short key phrase, say by a previous private
    conversation, Bellaso's system was considerably more secure.
```

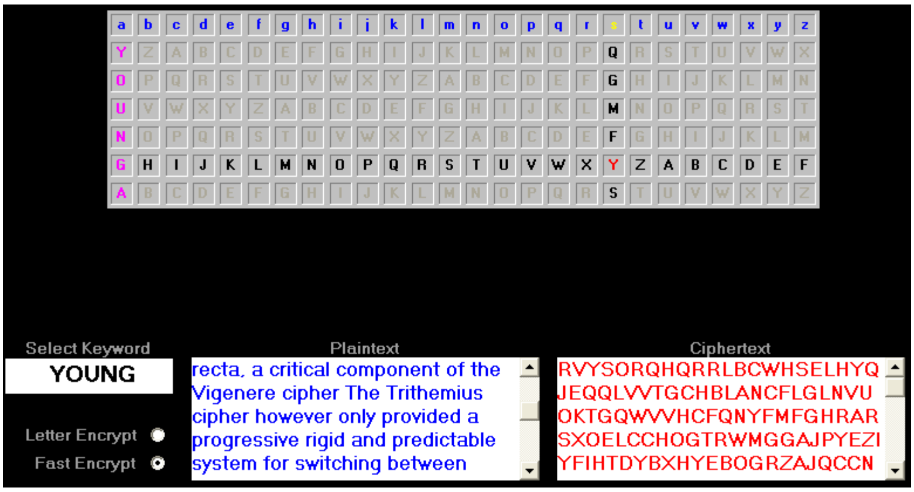
Keyword: YOUNG
Ciphertext:

```
RVYSOPGNJKJZXBISAYAZCRXRYAFCCZGCHBLYDIYEYZJUGZSNVIAWJUKPKUFLMFGHRYHYQHWZYBTZ
ONGOQHUNRZSLGOYFIHTBOHQAQSXNSCHUYIGDBRXBWMPZMGQVZAVVRZUSYAIGDBRXYZJUGZSNFGJP
YEZGGMLYRSGBTJMMJORQBRJYZJUGZSNFGDHYEYCJYEGJKIEJQOHQYUWNPNCGQRXCWHQOAONRJZMQ
EORWHTZFSFRZRSLBLRVYPUPFYFVMBXVTEOFCNYPYGOLHBRIGDBRXRSRGRYHYEOLXIUGLBYFZPWNU
KKWOFOLVCFCMFECUJWAEGNVCNOLJYAZCRNUKROVHRYFYPZYOWEORWWNRACGCULSHGUDHBRBGUYAX
CQCCNCFNUKRFCGNCACHYAWJUKPVIJKTSLBTJMJEUTWXRJYDLBMPSMFOTSLVMGRUAJNFYQOAHUORC
GSFZCAZBXQKCGIFWHTHCHQRKLQCCNCFUYVFOVRZQKBNZGGHBCIBIJTYGNUKTWARTPSWVVFSLJGQC
LVMGBUYRWRYFIPWVRJZMAVUTOHOGRHCFZYPYYRYGIVTFWMOUMYFNIGTLNJCZMVMEWIIGLPUGZGGN
NHCZFNYMVYOAGZNHVMBNUKROVHRYFYPZYCZGXGHBRSGIMOAROXQKBOLRVCONVTEQIHTRSLFOEBUX
KWHIFCGHWUIGDBRXYZJUGZSNFKTSLLRCHNRXUVYEKYGUYHCFNVGLRNEORVYZOSGOFKBOZVDCRJNZ
RSLAUDGOOYRWNHZGCHFHCZFNYMGMPNCAYZKYBNGNCDUGZCFHBLQIVFZGHOGOMBMPUSZXOKCOMVRW
QBNTESXFOKDFLHWGYYKAHCAMYBYJQCMEREQKYEKRMJVIYZFLYGBAYKUCLQYMFMUUPHJUXYGYFQLC
QAZMPIGNNOLGOCGCAGBJUAICCLGXYBMZORHYQUSHISHYBXNRMBAJORVNUKKSMFGESVRRJOMBYKSN
UUBHBHYPSKHOPSXFZPCHTYCQOEORMZBXMBFLZFSEREYGCGOQFYYGRWPRRWSUFERCMRISFYNYFCLG
QCMJUXYGYFGWPSNVPSPVUSGJEOTONRIMBPRXQONVULPYYRYGIFYWGNRSUOMPULGCQKPOVYEKCLRY
CQOEK
```

3. Crack the crypted text of your fellow student using the Vigenere cipher tool.
   My partner: Ilya Radostev
   Vigener cipher tool: Figure 11
   Ciphertext:

```
DSSQABAJTVSEOKFVKGAUGJWGFXSUZXNIUFUBVXIXGABTKHFCKTSYAURXPTKRUBZNSAXTGKFZKEXW
GHPGVSSVBRORQHNTOYRQOKMCNEUFEFWYFARBFWISXIFOEXPQULBRJPMFZFWODQOWVPZWMJXSEMIW
UECETHWUECJUVYOEFWGRPTXNERIEFXTTKGFWOFPEQMYBOKZLQAMIIREDUXTXYTQQBFWUJXOGEQGQ
YOEBJZIDHAFXNVQSLQIIMQGHGIRIBVTOXGRPHAFANMFSTOHORPWTOVNMZCVFVUWPSLQMZIUHLTXU
GWMLIEVIMBWTLUVFZXHWOXUGVBTGFXSHGVARZWGHOSLYDAPZKVEVHSXJMEHTOGKWFVXIMVTADHUE
SYEWLBLOKTZRBKMVQGLJZKEZRNOTXIPWVUEHPQOGJQGPMBWJWXEZYXEESSZUMIISSEHWBRMIDCNT
ETMYOETMTXTSPPVRHZSOFVZLQZXTWZLQMTSIYXUZEULXIMHXOIJFKVTCMZEFZHTWGRPDHBGNMZUY
PVZLQWKNIGXMBWJZUVKQTOMTIFSXUL
```

   Keyword: BEGEMOT
   Plaintext:



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Select Keyword: YOUNG

Letter Encrypt ○

Fast Encrypt ●

Plaintext:

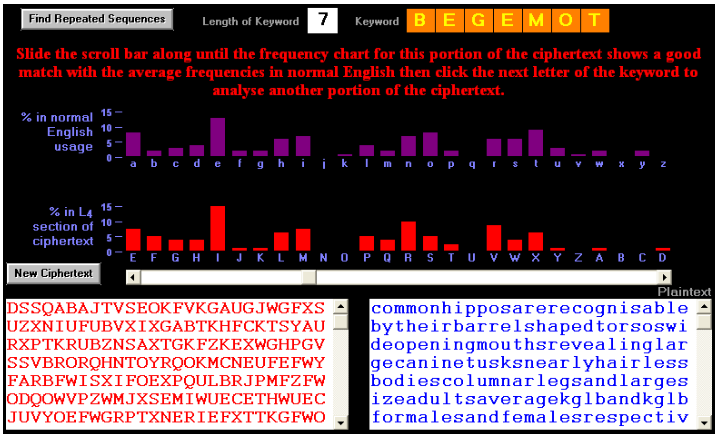
recta, a critical component of the
Vigenere cipher The Trithemius
cipher however only provided a
progressive rigid and predictable
system for switching between

Ciphertext:

RVYSORQHQRRLBCWHSELHYQ
JEQQLVVTGCHBLANCFLGLNVU
OKTGQWVVHCFQNYFMFGHRAR
SXOELCCHOGTRWMGGAJPYEZI
YFIHTDYBXHYEBOGRZAJQCCN

Figure 10: The Vigenere cipher tool

```
common hippos are recognisable by their barrel shaped torsos wide opening
    mouths revealing large canine tusks nearly hairless bodies columnar legs
    and large size adults average kg lb and kg lb for males and females
    respectively making them the largest species of land mammal after the
    three species of elephant and the white and indian rhinoceros despite its
     stocky shape and short legs it is capable of running km h mph over short
     distances the hippopotamus is a highly aggressive and unpredictable
    animal and is ranked among the most dangerous animals in the world
    nevertheless they are still threatened by habitat loss and poaching for
    their meat and ivory canine teeth vxqw
```



Find Repeated Sequences

Length of Keyword: 7

Keyword: B E G E M O T

Slide the scroll bar along until the frequency chart for this portion of the ciphertext shows a good match with the average frequencies in normal English then click the next letter of the keyword to analyse another portion of the ciphertext.

% in normal English usage
15
10
5
0
a b c d e f g h i j k l m n o p q r s t u v w x y z
% in L4 section of ciphertext
15
10
5
0
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
New Ciphertext
Plaintext

DSSQABAJTVSEOKFVKGAUGJWGFXS
UZXNIUFUBVXIXGABTKHFCKTSYAU
RXPTKRUBZNSAXTGKFZKEXWGHPGV
SSVBRORQHNTOYRQOKMCNEUFEFWY
FARBFWISXIFOEXPQULBRJPMFZFW
ODQOWVPZWMJXSEMIWUECETHWUEC
JUVYOEFWGRPTXNERIEFXTTKGFWO

commonhipposarerecognisable
bytheirbarrelshapedtorsoswi
deopeningmouthsrevealinglar
gecaninetusksnearlyhairless
bodiescolumnarlegsandlarges
izeadultsaveragekglbandkglb
formalesandfemalesrespectiv

Figure 11: The Vigenere cipher tool

4. Go through the previous two steps again, this time using a cipher of your own choosing. Do not tell your fellow student what cipher you used!

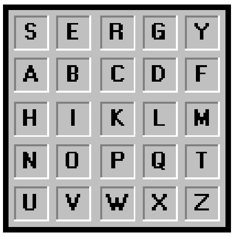
ENCRYPTION

Cipher: Playfair
Plaintext:

```
In academia, various proposals for a DES-cracking machine were advanced. In
    1977, Diffie and Hellman proposed a machine costing an estimated US$20
    million which could find a DES key in a single day. By 1993, Wiener had
```

proposed a key-search machine costing US$1 million which would find a key within 7 hours. However, none of these early proposals were ever implemented or , at least , no implementations were publicly acknowledged . The vulnerability of DES was practically demonstrated in the late 1990s . In 1997, RSA Security sponsored a series of contests , offering a $10 ,000 prize to the first team that broke a message encrypted with DES for the contest. That contest was won by the DESCHALL Project , led by Rocke Verser , Matt Curtin , and Justin Dolske , using idle cycles of thousands of computers across the Internet. The feasibility of cracking DES quickly was demonstrated in 1998 when a custom DES-cracker was built by the Electronic Frontier Foundation (EFF) , a cyberspace civil rights group , at the cost of approximately US$250,000 (see EFF DES cracker). Their motivation was to show that DES was breakable in practice as well as in theory: "There are many people who will not believe a truth until they can see it with their own eyes. Showing them a physical machine that can crack DES in a few days is the only way to convince some people that they really cannot trust their security to DES." The machine brute-forced a key in a little more than 2 days search.

Keyword: SERGEY
Key Square: Figure 12



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

Figure 12: Key Square

Ciphertext:

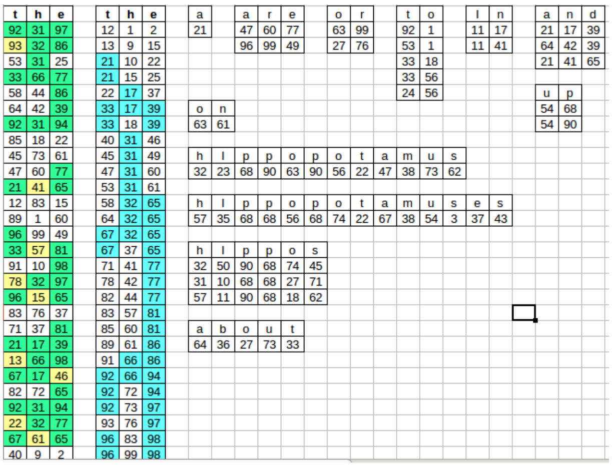
```
HO BD BF YI HB UB EK NV RN EP QP AH HG BT SC BG RA SC KP HO YL BD IK OS VR
    GR BF UB PA GB HO BL DZ BM SB QA IS QG MH HU WC PQ NE GB FH BD IK OS BP
    YN HO SD OS YN KH FN GB SA HK QG MK PO UK KB KA NV QL BM QA BF RE IR EM
    UH EH QS IG FB EF RZ OB OS SK BF WC PQ NE GB CH RS ER CS AK HF AK HO RB
    NE OM QS SA HK QG MK PO UK KB KU NV QL BM QA CH RS VK NM HO IN WS AN PV
    BE RG OP OS TB NM RE GV SB GK RT EP QP AH HG VR GR BE RG KH QK YI SO OY
    BQ SC QM SB YN OP KH QK YI SO NF OM PO RU RG RO VA MK DK SF KP OP XK GB
    YR FQ IS WV HQ RG BC KM MO ET AF RE UC RN SC FP KB DH MG BG IT UA PY FN
    GB HO NM GI FN RE HO GE HA RB WS MO SE QP UA PE GB HA RG OB EN AD PO OY
    YN EN DZ BY EK QS CN EK VY NP NM YB KE YN OY FH NM FN CE PI SB IY GU AH
    YR SO KC RT OY CX MO LA RE BT YP IS BP ON RE QZ NM FN BP ON RE PZ HA VP
    OA FZ IS BG RA NH QG KQ EP OB FP IG FC SG PB IR EB GE RG HF QZ PF WS OM
    UH QA HV YN HO BQ HG IR SA HO EL LQ RB RF IG EN MZ IN SA HU AG TB BP KT
    ZN RG AH KC NE YN IS HO OY SP YO NM YB SB EH IO MK ZF TB KC BD LK QS BG
    GN VH KP MG UC GA YI PO YN SC OY BL PU IS UH AW YN TI BG RA SC KP RG UC
    EA VH MQ FE NM GV GI RB PY PO KB CY PO OM RG BT SU FB OM PO YB AB FR IB
    GE NC BR BK EO KG LE MN EY EP WN FN NM RB NE NP AB QW WC QV KH FN GI SZ
    GU ER GV YB AF RE KC BD IR YP IS KE IT OM UB OM PO UC YN NE IN ZP NH QF
    RE UC EA GR CH BC IG HO WC BD OM BR HA VR QG HD EH ON IS PE FZ IS GR CS
    YI HU RT BV QK RV IN VK QG HQ PN IB MK BE SB PY ZN NS ON KM NM RS DB UA
    GV BO PZ MO MN IS KE PV OS SR GU AN PV HO YQ IS HF NK SE KB DH HF AK HO
    YO NH PF HU KC BD LC RE HO BA RV FB SE HE NM BV QH RZ FS NP BP OU HO BR
    EN IY OR PQ IG NM FN NM RS GR DH MG DB QU OP QZ PY SA QZ NM BO GE RB WS
    MO FZ QB RE NM YI BD IK OS CE ZN YB PE BR FB IR EM UH MK QZ QM YI PE YO
    NH QA FS GU ER CS AK
```

DECRYPTION

Ciphertext:

```
64 36 27 73 33 −1 92 31 97 −1 32 23 68 90 63 90 56 22 47 38 73 62 −1 −1 57
   35 68 68 56 68 74 22 67 38 54 03 37 43 −1 91 51 16 29 −1 93 67 22 77 60
   −1 −1 93 32 35 12 79 −1 35 45 −1 93 32 86 −1 53 31 25 −1 84 82 29 81 34
   45 −1 17 67 40 98 39 −1 22 32 72 40 −1 33 66 77 −1 −1 −1 −1 −1 48 35 16
   20 48 −1 85 27 99 45 81 −1 −1 −1 −1 −1 32 50 90 68 74 45 −1 43 90 20 61
   65 −1 54 68 −1 33 18 −1 −1 −1 −1 57 56 54 48 08 −1 21 −1 58 44 86 −1 71
   73 36 38 29 48 84 37 46 −1 11 17 −1 −1 48 10 16 77 82 62 −1 64 42 39 −1
   05 83 34 94 62 −1 33 56 −1 34 98 72 68 −1 78 57 94 50 06 −1 40 44 03 62
   35 16 97 −1 87 27 46 11 94 08 −1 88 74 74 05 −1 73 04 39 77 76 −1 92 31
   94 −1 85 18 22 −1 −1 64 19 76 50 70 21 42 −1 45 73 61 −1 −1 31 10 68 68
   27 71 −1 47 60 77 −1 14 99 44 70 72 19 54 05 −1 11 41 −1 93 83 24 37 82
   −1 −1 84 27 18 65 −1 03 75 50 38 38 94 48 03 −1 −1 21 41 65 −1 12 83 15
   −1 −1 79 18 05 46 −1 24 85 94 52 76 −1 36 60 29 47 24 85 −1 73 17 39 81
   82 93 83 53 72 99 −1 89 01 60 −1 54 90 −1 92 01 −1 89 10 16 69 −1 40 50
   04 54 53 72 45 −1 −1 57 18 93 97 16 81 82 −1 −1 78 66 72 02 −1 −1 96 99
   49 −1 56 89 53 94 17 −1 00 21 48 84 72 −1 69 42 27 73 14 66 −1 24 56 −1
   62 35 40 68 59 02 −1 75 83 59 34 −1 63 99 −1 43 22 09 15 39 −1 63 61 −1
   33 57 81 −1 91 96 34 77 −1 19 59 63 74 06 −1 −1 −1 27 76 −1 91 10 98 −1
   10 17 −1 78 32 97 −1 45 57 83 59 05 18 75 03 −1 −1 33 32 25 50 60 −1 72
   02 37 71 −1 96 15 65 −1 15 56 08 24 99 50 05 62 −1 83 76 37 −1 59 51 70
   67 53 72 65 −1 66 50 14 57 −1 51 04 −1 −1 24 66 72 11 60 −1 32 49 09 58
   62 −1 −1 75 66 52 70 57 −1 21 05 05 18 93 71 −1 22 85 29 40 −1 07 63 −1
   71 37 81 −1 21 17 39 −1 36 99 94 83 30 79 97 −1 93 66 52 00 72 −1 38 01
   45 30 59 86 −1 −1 08 54 87 40 98 06 84 77 65 −1 −1 −1 57 11 90 68 18 62
   −1 21 00 08 56 −1 87 83 71 34 −1 56 61 −1 13 66 98 −1 62 32 01 99 20 59
   23 41 25 −1 67 17 46 −1 03 81 12 76 29 22 97 −1 96 15 −1 27 35 59 86 −1
   82 72 65 −1 −1 71 95 87 43 24 64 61 12 69 −1 −1 93 57 52 12 79 −1 14 83
   16 25 −1 82 35 45 49 −1 53 01 −1 92 31 94 −1 38 86 78 31 −1 22 66 47 22
   −1 22 66 94 86 −1 43 75 25 96 22 −1 87 00 01 74 58 −1 −1 22 32 77 −1 −1
   59 23 80 95 23 46 −1 10 45 −1 47 70 13 95 64 05 05 02 −1 83 −1 08 34 35
   41 −1 38 51 11 43 30 20 04 20 48 −1 67 61 65 −1 71 95 61 87 05 74 88 34
   −1 30 79 44 13 −1 40 09 02 −1 44 59 08 74 −1 −1 90 06 63 16 23 46 20 −1
   68 60 27 13 29 12 30 23 63 15 −1 67 84 67 50 04 08 07 −1 84 94 60 40 08
   −1 −1
```

Prospective Cipher: Homophonic Cipher
Assumption: I suppose that number **-1** is a non alphabetic symbol
Cryptanalysis: Figure 13



t	h	e
92	31	97
93	32	86
53	31	25
33	66	77
58	44	86
64	42	39
92	31	94
85	18	22
45	73	61
47	60	77
21	41	65
12	83	15
89	1	60
96	99	49
33	57	81
91	10	98
78	32	97
96	15	65
83	76	37
71	37	81
21	17	39
13	66	98
67	17	46
82	72	65
92	31	94
22	32	77
67	61	65
40	9	2

t	h	e
12	1	2
13	9	15
21	10	22
21	15	25
22	17	37
33	17	39
33	18	39
40	31	46
45	31	49
47	31	60
53	31	61
58	32	65
64	32	65
67	32	65
67	37	65
71	41	77
78	42	77
82	44	77
83	57	81
85	60	81
89	61	86
91	66	86
92	66	94
92	72	94
92	73	97
93	76	97
96	83	98
96	99	98

a
21

a	r	e
47	60	77
96	99	49

o	r
63	99
27	76

t	o
92	1
53	1
33	18
33	56
24	56

l	n
11	17
11	41

a	n	d
21	17	39
64	42	39
21	41	65

u	p
54	68
54	90

o	n
63	61

h	l	p	p	o	p	o	t	a	m	u	s
32	23	68	90	63	90	56	22	47	38	73	62

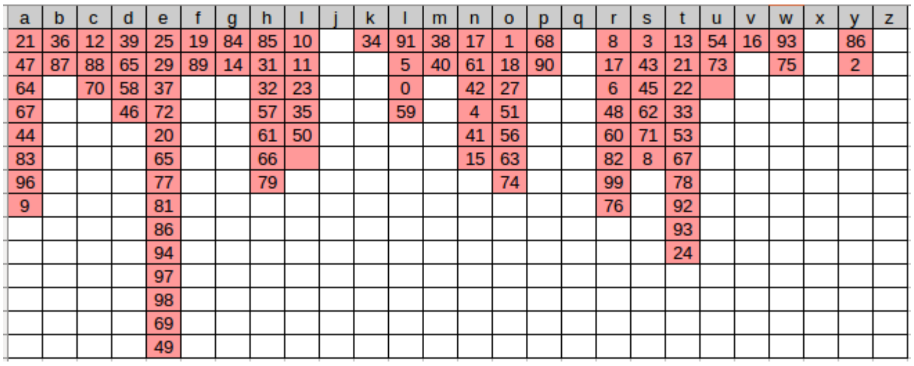
h	l	p	p	o	p	o	t	a	m	u	s	e	s
57	35	68	68	56	68	74	22	67	38	54	3	37	43

h	l	p	p	o	s
32	50	90	68	74	45
31	10	68	68	27	71
57	11	90	68	18	62

a	b	o	u	t
64	36	27	73	33

Figure 13: Cryptanalysis

The distribution of letters: Figure 14



a	b	c	d	e	f	g	h	l	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
21	36	12	39	25	19	84	85	10		34	91	38	17	1	68		8	3	13	54	16	93		86	
47	87	88	65	29	89	14	31	11			5	40	61	18	90		17	43	21	73		75		2	
64		70	58	37			32	23			0		42	27			6	45	22						
67			46	72			57	35			59		4	51			48	62	33						
44				20			61	50					41	56			60	71	53						
83				65			66						15	63			82	8	67						
96				77			79							74			99		78						
9				81													76		92						
				86															93						
				94															24						
				97																					
				98																					
				69																					
				49																					

Figure 14: Cryptanalysis

Plaintext:

```
about the hippopotamus hippopotamuses love water which is why the greeks
    named them the river horse  hippos spend up to hours a day submerged in
    rivers and lakes to keep their massive bodies cool under the hot african
    sun hippos are graceful in water good swimmers and can hold their breath
    underwater for up to five minutes however they are often large enough to
    simply walk or stand on the lake floor or lie in the shallows their eyes
    and nostrils are located high on their heads which allows them to see and
     breathe while mostly submerged hippos also bask on the shoreline and
    secrete an oily red substance which gave rise to the myth that they sweat
     blood the liquid is actually a skin moistener and sunblock that may also
     provide protection against germs
```

4 Conclusion

Cryptography is the practice and the study of methods of secure communication in the presence of third parties called opponents. Generally, cryptography consists of the construction and analysis of protocols that do not allow third parties or the public to read private messages; various aspects of information security, such as data confidentiality, data integrity, authentication, and non-repudiation, are key to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering and communication science. Cryptographic applications include e-commerce, chip-payment cards, digital currencies, computer passwords and military communications.

References

[1] M. Stamp, Information Security: Principles and Practice, Second Edition, 2011, 606 pages.

[2] Wikipedia: DES https://en.wikipedia.org/wiki/DES.