MINISTRY OF EDUCATION, CULTURE AND RESEARCH OF THE REPUBLIC OF MOLDOVA

Technical University of Moldova Faculty of Computers, Informatics and Microelectronics Department of Software and Automation Engineering

Postoronca Dumitru FAF-233

Report

Laboratory work n.2

of CS

Checked by:
A. Zaica, *university assistant*
DISA, FCIM, UTM

Chișinău – 2025

1 Purpose of the Laboratory Work

The purpose of this laboratory was to study the concept of frequency analysis as a method of cryptanalysis. Frequency analysis is one of the oldest techniques for breaking classical ciphers and is based on the observation that letters in natural languages appear with characteristic frequencies. For example, in the English language, the letters `E`, `T`, `A`, and `O` occur most often, while letters such as `Z`, `Q`, and `X` are much less frequent. By comparing the distribution of characters in the ciphertext with the expected distribution in English, it is possible to make informed guesses about the substitutions and progressively decrypt the message.

2 Strategy Used

To carry out this task, I first analyzed the frequencies of the letters in the given encrypted text and compared them with the known frequency distribution of English letters. Based on this comparison, I made initial assumptions about which ciphertext letters corresponded to which plaintext letters.

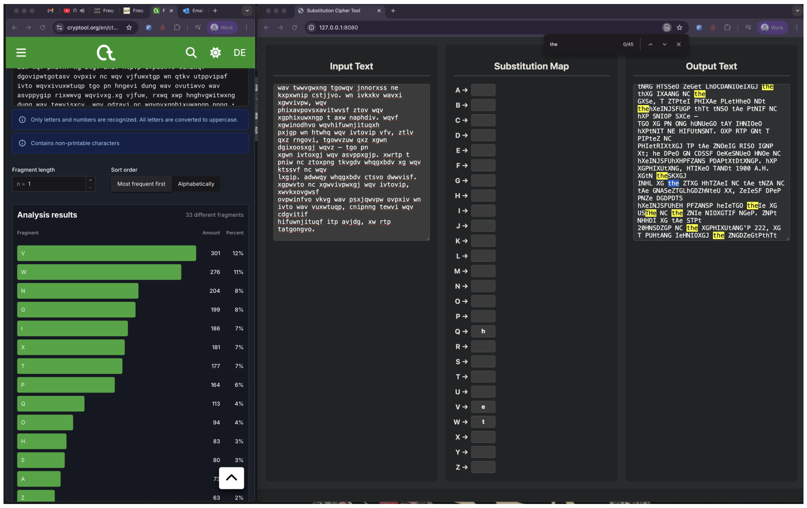
To simplify the decryption process, I developed a small interactive website. This tool allowed me to dynamically replace ciphertext letters with my assumptions, observe the updated text in real time, and iteratively refine the mapping. This approach significantly sped up the process of testing hypotheses and correcting mistakes.

3 Decryption Process

The decryption process was iterative and consisted of the following steps:

1. Calculate the frequency distribution of the ciphertext characters.
2. Match the most frequent symbols with the common English letters such as `E`, `T`, and `A`.
3. Dynamically replace characters using the developed website, checking if meaningful words begin to form.
4. Refine the mappings step by step until the majority of the text became readable and the intended plaintext was reconstructed.

The use of an interactive visualization tool proved to be highly effective, as it allowed quick adjustments and an intuitive workflow for breaking the cipher.



cryptool.org/en/ct...

```
dgovipwtgotasv ovpxiv nc wqv vjfuwxtgp wn qtkv utppvipaf
ivto wqvxivuxwtuqp tgo pn hngevi dung wav ovutiwvo wav
asvppygip rixwwvg wqvivxg.xg vjfuw, rxwq xwp hnghvgwitwxng
```

ⓘ Only letters and numbers are recognized. All letters are converted to uppercase.

ⓘ Contains non-printable characters

Fragment length: n = 1

Sort order: Most frequent first | Alphabetically

Analysis results — 33 different fragments

Fragment	Amount	Percent
V	301	12%
W	276	11%
N	204	8%
G	199	8%
I	186	7%
X	181	7%
T	177	7%
P	164	6%
Q	113	4%
O	94	4%
H	83	3%
S	80	3%
A	73	
Z	63	2%

Substitution Cipher Tool — 127.0.0.1:8080

the 0/45

Input Text

```
wav twwvgwxng tgowqv jnnorxss ne
kxpxwnip cstjjvo. wn ivkxkv wavxi
xgwvivpw, wqv
phixavpovsxavitwvsf ztov wqv
xgphixuwxngp t axw naphdiv. wqvf
xgwinodhvo wqvhifuwnjituqxh
pxjgp wn htwhq wqv ivtovip vfv, ztlv
qxz rngovi, tgowvzuw qxz xgwn
dgixoosxgj wqvz — tgo pn
xgwn ivtoxgj wqv asvppxgjp. xwrtp t
pniw nc ztoxpng tkvgdv whqgxbdv xg wqv
ktssvf nc wqv
lxgip. adwwqy whqgxbdv ctsvo dwwvisf.
xgpwvto nc xgwvivpwxgj wqv ivtovip,
xwvkxovgwsf
ovpwinfvo vkvg wav psxjqwvpw ovpxiv wn
ivto wav vuxwtuqp, cnipnng tewvi wqv
cdgvitif
hifuwnjituqf itp avjdg, xw rtp
tatgongvo.
```

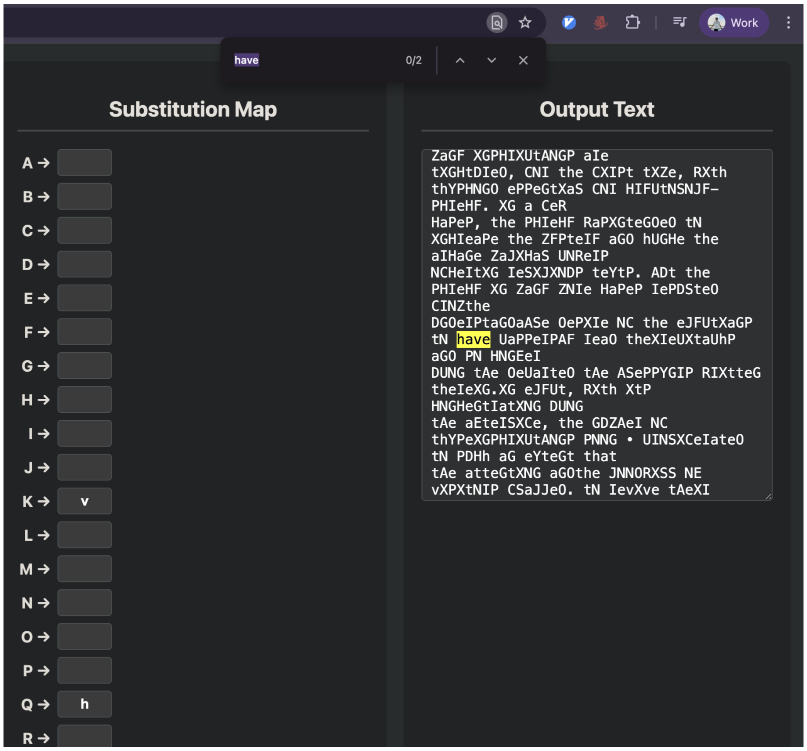
Substitution Map

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

Output Text

```
tNRG HTSSeO ZeGet LhDCDANIOeIXGJ the
thXG IXAANG NC the
GXSe, T ZTPteI PHIXAe PLetHheO NDt
thehXeINJSFUGP thTt tNSO tAe PtNIF NC
hXP SNIOP SXCe —
TGO XG PN ONG hUNUeGO tAY IHNIOeO
hXPtNIT NE HIFUtNSNT. OXP RTP GNt T
PIPteZ NC
PHIetRIXtXGJ TP tAe ZNOeIG RISO IGNP
Xt; he DPeO GN CDSSF OeKeSNUeO HNOe NC
hXeINJSFUhXHPFZANS PDAPtXtDtXNGP. hXP
XGPHIXUtXNG, HTIKeO TANDt 1900 A.H.
XGtN theSKXGJ
INHL XG the ZTXG HhTZAeI NC tAe tNZA NC
tAe GNASeZTGLhGDZhNteU XX, ZeIeSF DPeP
PNZe DGDPDTS
hXeINJSFUhEH PFZANSP heIeTGO theIe XG
USTHe NC the ZNIe NIOXGTIF NGeP. ZNPt
NHHDI XG tAe STPt
20HNSDZGP NC the XGPHIXUtANG'P 222, XG
T PUHtANG IeHNIOXGJ the ZNGDZeGtPthTt
```

Figure 1: Progress of the decryption process using the interactive replacement tool.



have 0/2

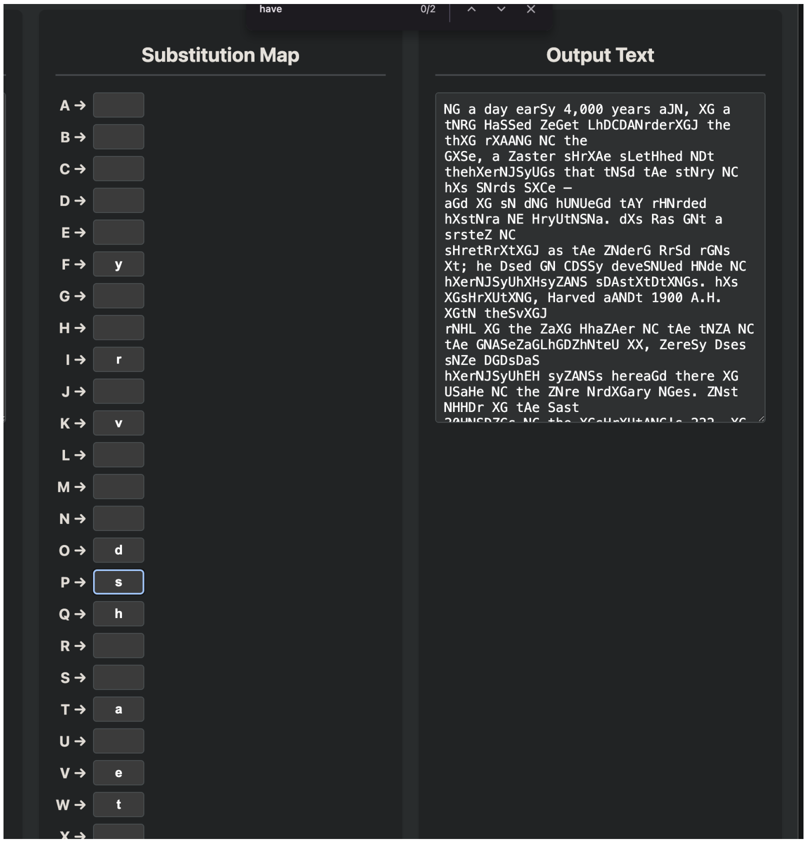
Substitution Map

A →	
B →	
C →	
D →	
E →	
F →	
G →	
H →	
I →	
J →	
K →	v
L →	
M →	
N →	
O →	
P →	
Q →	h
R →	

Output Text

```
ZaGF XGPHIXUtANGP aIe
tXGHtDIeO, CNI the CXIPt tXZe, RXth
thYPHNGO ePPeGtXaS CNI HIFUtNSNJF—
PHIeHF. XG a CeR
HaPeP, the PHIeHF RaPXGteGOeO tN
XGHIeaPe the ZFPteIF aGO hUGHe the
aIHaGe ZaJXHaS UNReIP
NCHeItXG IeSXJXNDP teYtP. ADt the
PHIeHF XG ZaGF ZNIe HaPeP IePDSteO
CINZthe
DGOeIPtaGOaASe OePXIe NC the eJFUtXaGP
tN have UaPPeIPAF IeaO theXIeUXtaUhP
aGO PN HNGEeI
DUNG tAe OeUaIteO tAe ASePPYGIP RIXtteG
theIeXG.XG eJFUt, RXth XtP
HNGHeGtIatXNG DUNG
tAe aEteISXCe, the GDZAeI NC
thYPeXGPHIXUtANGP PNNG • UINSXCeIateO
tN PDHh aG eYteGt that
tAe atteGtXNG aGOthe JNNORXSS NE
vXPXtNIP CSaJJeO. tN IevXve tAeXI
```

Figure 2: Breaking down the first words



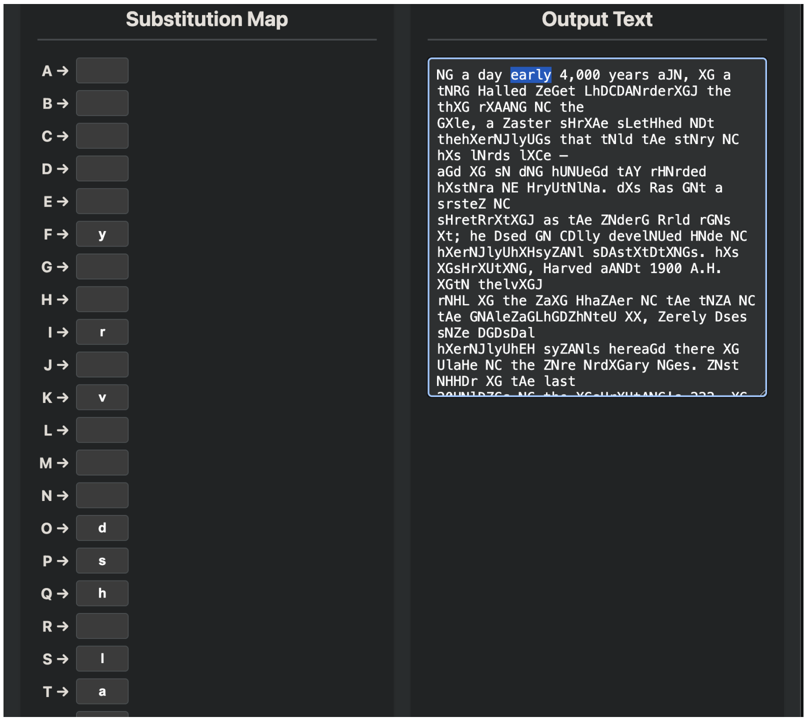
Substitution Map

A →	
B →	
C →	
D →	
E →	
F →	y
G →	
H →	
I →	r
J →	
K →	v
L →	
M →	
N →	
O →	d
P →	s
Q →	h
R →	
S →	
T →	a
U →	
V →	e
W →	t

Output Text

```
NG a day earSy 4,000 years aJN, XG a
tNRG HaSSed ZeGet LhDCDANrderXGJ the
thXG rXAANG NC the
GXSe, a Zaster sHrXAe sLetHhed NDt
thehXerNJSyUGs that tNSd tAe stNry NC
hXs SNrds SXCe —
aGd XG sN dNG hUNUeGd tAY rHNrded
hXstNra NE HryUtNSNa. dXs Ras GNt a
srsteZ NC
sHretRrXtXGJ as tAe ZNderG RrSd rGNs
Xt; he Dsed GN CDSSy deveSNUed HNde NC
hXerNJSyUhXHsyZANS sDAstXtDtXNGs. hXs
XGsHrXUtXNG, Harved aANDt 1900 A.H.
XGtN theSvXGJ
rNHL XG the ZaXG HhaZAer NC tAe tNZA NC
tAe GNASeZaGLhGDZhNteU XX, ZereSy Dses
sNZe DGDsDaS
hXerNJSyUhEH syZANSs hereaGd there XG
USaHe NC the ZNre NrdXGary NGes. ZNst
NHHDr XG tAe Sast
```

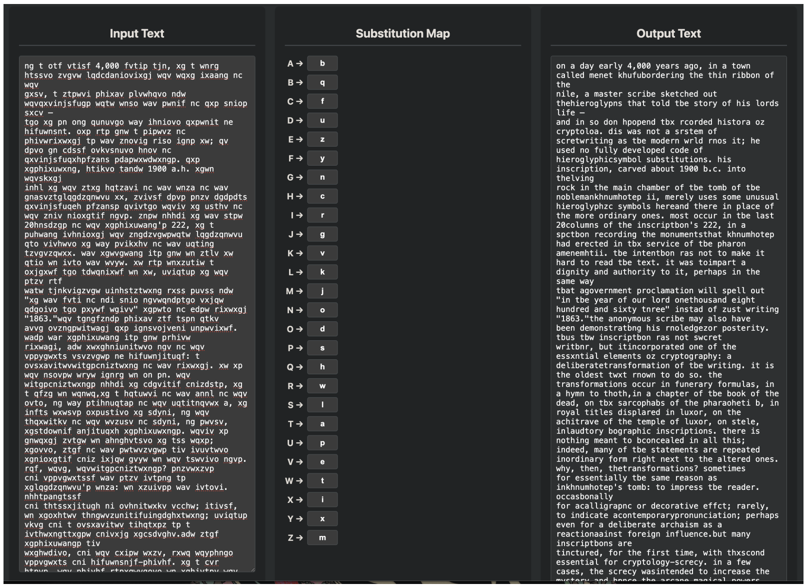
Figure 3: Third of the letters are known



```
A →
B →
C →
D →
E →
F → y
G →
H →
I → r
J →
K → v
L →
M →
N →
O → d
P → s
Q → h
R →
S → l
T → a
```

```
NG a day early 4,000 years aJN, XG a
tNRG Halled ZeGet LhDCDANrderXGJ the
thXG rXAANG NC the
GXle, a Zaster sHrXAe sLetHhed NDt
thehXerNJlyUGs that tNld tAe stNry NC
hXs lNrds lXCe —
aGd XG sN dNG hUNUeGd tAY rHNrded
hXstNra NE HryUtNlNa. dXs Ras GNt a
srsteZ NC
sHretRrXtXGJ as tAe ZNderG Rrld rGNs
Xt; he Dsed GN CDlly develNUed HNde NC
hXerNJlyUhXHsyZANl sDAstXtDtXNGs. hXs
XGsHrXUtXNG, Harved aANDt 1900 A.H.
XGtN thelvXGJ
rNHL XG the ZaXG HhaZAer NC tAe tNZA NC
tAe GNAleZaGLhGDZhNteU XX, Zerely Dses
sNZe DGDsDal
hXerNJlyUhEH syZANls hereaGd there XG
UlaHe NC the ZNre NrdXGary NGes. ZNst
NHHDr XG tAe last
```

Figure 4



```
ng t otf vtisf 4,000 fvtip tjn, xg t wnrg
htssvo zvgvw lqdcdaniovixgj wqv wqxg ixaang nc
wqv
gxsv, t ztpwvi phixav plvwhqvo ndw
wqvqxvinjsfugp wqtw wnso wav pwnif nc qxp sniop
sxcv —
tgo xg pn ong qunuvgo way ihniovo qxpwnit ne
hifuwnsnt. oxp rtp gnw t pipwvz nc
phivwrixwxgj tp wav znovig riso ignp xw; qv
dpvo gn cdssf ovkvsnuvo hnov nc
qxvinjsfuqxhpfzans pdapwxwdwxngp. qxp
xgphixuwxng, htikvo tandw 1900 a.h. xgwn
wqvskxgj
inhl xg wqv ztxg hqtzavi nc wav wnza nc wav
gnasvztglqgdzqnwvu xx, zvivsf dpvp pnzv dgdpdts
qxvinjsfuqeh pfzansp qvivtgo wqviv xg usthv nc
wqv zniv nioxgtif ngvp. znpw nhhdi xg wav stpw
20hnsdzgp nc wqv xgphixuwang'p 222, xg t
puhwang ivhnioxgj wqv zngdzvgwpwqtw lqgdzqnwvu
qto vivhwvo xg way pvikxhv nc wav uqting
tzvgvzqwxx. wav xgwvgwang itp gnw wn ztlv xw
qtio wn ivto wav wvyw. xw rtp wnxzutiw t
oxjgxwf tgo tdwqnixwf wn xw, uviqtup xg wqv
ptzv rtf
watw tjnkvigzvgw uinhstztwxng rxss puvss ndw
"xg wav fvti nc ndi snio ngvwqndptgo vxjqw
qdgoivo tgo pxywf wgivv" xgpwto nc edpw rixwxgj
"1863."wqv tgngfzndp phixav ztf tspn qtkv
avvg ovzngpwitwagj qxp ignsvojveni unpwvixwf.
wadp war xgphixuwang itp gnw prhivw
rixwagi, adw xwxghniunitwvo ngv nc wqv
vppygwxts vsvzvgwp ne hifuwnjituqf: t
ovsxavitwvwitgpcniztwxng nc wav rixwxgj. xw xp
wqv nsovpw wryw ignrg wn on pn. wqv
witgpcniztwxngp nhhdi xg cdgvitif cnizdstp, xg
t qfzg wn wqnwq,xg t hqtuwvi nc wav annl nc wqv
ovto, ng way ptihnuqtap nc wqv uqtitnqvwx a, xg
infts wxwsvp oxpustivo xg sdyni, ng wqv
thqxwitkv nc wqv wvzusv nc sdyni, ng pwvsv,
xgstdownif anjituqxh xgphixuwxngp. wqviv xp
gnwqxgj zvtgw wn ahnghvtsvo xg tss wqxp;
xgovvo, ztgf nc wav pwtwvzvgwp tiv ivuvtwvo
xgnioxgtif cniz ixjqw gvyw wn wqv tswvivo ngvp.
rqf, wqvg, wqvwitgpcniztwxngp? pnzvwxzvp
cni vppvgwxtssf wav ptzv ivtpng tp
xglqgdzqnwvu'p wnza: wn xzuivpp wav ivtovi.
nhhtpangtssf
cni thtssxjitugh ni ovhnitwxkv vcchw; itivsf,
wn xgoxhtwv thngwvzunitifuingdghxtwxng; uviqtup
vkvg cni t ovsxavitwv tihqtxpz tp t
ivthwxngttxgpw cnivxjg xgcsdvghv.adw ztgf
xgphixuwangp tiv
wxghwdivo, cni wqv cxipw wxzv, rxwq wqyphngo
vppvgwxts cni hifuwnsnjf-phivhf. xg t cvr
```

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

```
on a day early 4,000 years ago, in a town
called menet khufubordering the thin ribbon of
the
nile, a master scribe sketched out
thehieroglypns that told tbe story of his lords
life —
and in so don hpopend tbx rcorded histora oz
cryptoloa. dis was not a srstem of
scretwriting as tbe modern wrld rnos it; he
used no fully developed code of
hieroglyphicsymbol substitutions. his
inscription, carved about 1900 b.c. into
thelving
rock in the main chamber of tbe tomb of tbe
noblemankhnumhotep ii, merely uses some unusual
hieroglyphzc symbols hereand there in place of
the more ordinary ones. most occur in tbe last
20columns of the inscriptbon's 222, in a
spctbon recording the monumentsthat khnumhotep
had erected in tbx service of tbe pharon
amenemhtii. tbe intentbon ras not to make it
hard to read tbe text. it was toimpart a
dignity and authority to it, perhaps in the
same way
tbat agovernment proclamation will spell out
"in tbe year of our lord onethousand eight
hundred and sixty tnree" instad of zust writing
"1863."the anonymous scribe may also have
been demonstratbng his rnoledgezor posterity.
tbus tbw inscriptbon ras not swcret
writbnr, but itincorporated one of the
essxntial elements oz cryptography: a
deliberatetransformation of tbe writing. it is
the oldest twxt rnown to do so. the
transformations occur in funerary formulas, in
a hymn to thoth,in a chapter of tbe book of the
dead, on tbx sarcophabs of the pharaoheti b, in
royal titles displared in luxor, on the
achitrave of the temple of luxor, on stele,
inlaudtory bographic inscriptions. there is
nothing meant to bconcealed in all this;
indeed, many of tbe statements are repeated
inordinary form right next to the altered ones.
why, then, thetransformations? sometimes
for essentially tbe same reason as
inkhnumhotep's tomb: to impress tbe reader.
occasbonally
for acalligrapnc or decorative effct; rarely,
to indicate acontemporarypronunciation; perhaps
even for a deliberate archaism as a
reactionaainst foreign influence.but many
inscriptbons are
tinctured, for the first time, with thxscond
essential for cryptology-screcy. in a few
cases, the screcy wasintended to increase the
```

Figure 5: text is fully cracked

4 Conclusion

This laboratory work provided practical experience with one of the fundamental techniques of classical cryptanalysis — frequency analysis. By comparing the distribution of letters in the ciphertext with the expected frequencies of letters in the English language, I was able to gradually reconstruct the original message.

The use of an interactive website for testing assumptions greatly simplified the process, making it possible to quickly validate or discard hypotheses and progressively refine the decryption. Through this exercise, I gained a deeper understanding of the weaknesses of substitution ciphers and why they are considered insecure by modern standards. At the same time, the laboratory highlighted the power of statistical methods in cryptanalysis and their historical importance in the development of cryptography.