Ministerul Educaţiei şi Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică

Laboratory work 2

Subject: Monoalphabetic script encryption

Done by: Gitlan Gabriel
st. gr. FAF-213

Verified by: Mîţu Cătălin
asist. univ.

Chişinău - 2023

Goal:

A message has been intercepted that is known to have been obtained through the use of a monoalphabetic cipher. By applying frequency analysis attack to discover the original message, assuming it is a text written in English, taking into account that only the letters have been encrypted, leaving the other characters unchanged.

Please use the following service:

https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

The report will include a description of the breaking process, exactly as presented in section 2.3 in the Example of Frequency Analysis Attack.

Variant 18

Xw rtp Citghv, qnrvkvi, wqtw udasxpqvo ngv nc hifuwnsnjf'p jivtwvpwannlp. St Hifuwnjituqxhzxsxwtxiv cxipw tuuvtivo tp wrn xgpwtsszvgwp xgwqv Endigts ovp Phxvghvp zxsxwtxivp xg Etgdtiftgo Cvaidtif nc 1883,avxgj ivxppdvo stwvi wqtw fvti tp t utuviathl annl af wqv endigts'pudasxpqvi. Xw xp wqv znpw hnghxpv annl ng hifuwnsnjf vkvi rixwwvg. Xwptdwqni qto wqv xgpwxghw cni wqv hifuwnjituqxh edjdsti, tgo qv hnzuivppvoxgwn 64 utjvp kxiwdtssf wqv vgwxiv lgnrg cxvso nc hifuwnsnjf, xghsdoxgjunsftsuqtavwxhp rxwq zxyvo tsuqtavwp, vghxuqvivo hnov, tgo hxuqviovkxhvp. Wqv annl xp tspn ngv nc wqv znpw phqnstisf ng hifuwnsnjf. Xwpcnnwgnwvp hxwv znpw hstppxhts tgo ztgf znovig pndihvp; hnzzvgwp pdhqtp "Wqxp xp gnw wqv ngsf qxpwnixhts ni axasxnjituqxh viini cni rqxhq wqv Tdpwixtg rixwvi zdpw av ivuinthqvo"pqnr qnr htivcdssf wqv tdwqni qtp pwdoxvo wqnpv pndihvp.Xwp tdwqni rtp anig Evtg-Jdxsstdzv-Qdaviw-Kxhwni-Citgjnxp-Tsvytgoiv-djdpwv Lvihlqnccp kng Gxvdrvgqnc ng Etgdtif 19, 1835, twGdwq, Qnsstgo. Tcwvi jvwwxgj ovjivvp xg svwwvip tgo xg phxvghv cinz wqvDgxkvipxwf nc Sxvjv, qv rtp qxivo xg 1863 tp tg xgpwidhwni xg znovigstgjdtjvp tw wqv qxjq phqnns tw Zvsdg, t stijv wnrg 25 zxsvp pndwqvtpwnc Utixp. Wqv gvyw fvti qv ztiixvo t jxis cinz wqv tivt tgo xg 1865, rqvgqv rtp 30, wqvf qto wqvxi ngsf hqxso, t otdjqwvi, Utdsxgv. Qv pwtfvo twZvsdg cni 10 fvtip, wvthqxgj Vgjsxpq tgo Jviztg.Af wqtw wxzv qv qto pqniwvgvo qxp gtzv wn Tdjdpwv Lvihlqnccp.Avtiovo, oxjgxcxvo, psnr nc puvvhq, Lvihlqnccp, ovpuxwv tg xgtaxsxwf wnztxgwtxg oxphxusxgv xg qxp hstppvp tgo pnzv vhhvgwixhxwxvp nc hqtithwvi,rtp t "svtigvo, mvtsndp, htutasv" wvthqvi rqn trnlv qxp pwdovgwp'xgwvivpw xg wqvxi rnil; qxp pduvixnip ptxo "qxp pwdovgwp sxlv qxz tgo rnilrxwq pdhhvpp." Tcwvirtio, qv rnilvo tp t uixktwv xgpwidhwni xg Utixp.Qxp adpxvpw fvtip cnssnrvo wqv udasxhtwxng nc St Hifuwnjituqxhzxsxwtxiv. T gvr xgwvigtwxngts stgjdtjv htssvo Knst-uxxl ("Rniso-Puvtl")qto avvg xgkvgwvo af t Jviztg uixvpw. Tandw 1885, xw htdjqw ng xgCitghv tgo cstpqvo rxwq vyuivpp-witxg puvvo tss nkvi wqv hndgwif, gnwngsf tzngj xgwvssvhwdtsp adw tzngj tss hstppvp; xw rtp vkvg qvtio xg wqvpwivvwp. Cinz Citghv xw itoxtwvo wqindjqndw wqv rniso. Wqv znpw thwxkvuinutjtgoxpw nc Knstuxxl rtp Tdjdpwv Lvihlqnccp, rqn, tw wqv pvhngoKnstuxxl hngjivpp xg Zdgxhq xg 1887, rtp thhstxzvo oxivhwni ("Oxsvlvs,"xg Knstuxxl) nc wqv Xgwvigtwxngts Thtovzf nc Knstuxxl. Adw tw wqv wqxiohngjivpp, qvso tw Utixp xg Ztf nc 1889, rxwq Lvihlqnccp uivpxoxgj, hixwxhtswvgpxngp rxwqxg wqv znkvzvgw zndgwvo tgo cxgtssf ainlv xw tutiw.Lvihlqnccp rtp hidpqvo af wqv hnsstupv nc tg xgwvigtwxngts oivtz wqtwqto pvvzvo pn gvvocds tgo pn hviwtxg. Qv hivtwvo gnwqxgj vspv tgo, ngTdjdpw 9, 1903, oxvo rqxsv ng kthtwxng xg Prxwmvistgo.Adw qxp hifuwnsnjxh xovtp pwxss gndixpq. Cni Lvihlqnccp pndjqw tgprvipwn wqv uinasvzp wqidpw dung hifuwnsnjf af gvr hngoxwxngp. "Xw xpgvhvpptif wn oxpwxgjdxpq htivcdssf avwrvvg t pfpwvz nc vghxuqvizvgwvgkxpxngvo cni t znzvgwtif vyhqtgjv nc svwwvip avwrvvg pvkvits xpnstwvouvnusv tgo t zvwqno nc hifuwnjituqf xgwvgovo wn jnkvig wqv hniivpungovghvavwrvvg oxccvivgw tizf hqxvcp cni tg dgsxzxwvo wxzv," qv rinwv. Xg wqtwngv pvgwvghv, Lvihlqnccp oxccvivgwxtwvp uiv-wvsvjituqf zxsxwtifhnzzdgxhtwxngp cinz unpw-. Wqv pvgwvghv xp uivjgtgw rxwq znpw nc wqvivbdxivzvgwp wqtw qtkv hnzv wn av ovztgovo nc pfpwvzp nc zxsxwtifhifuwnjituqf, ivbdxivzvgwp pdhq tp pxzusxhxwf, ivsxtaxsxwf, ituxoxwf, tgopn ng. Wqxp hsvti ivhnjgxwxng nc wqv gvr niovi hngpwxwdwvp Lvihlqnccp' cxipwjivtw hngwixadwxng wn hifuwnsnjf.Wqv pvhngo rtp wn ivtccxiz xg t znovig hngwvyw wqv uixghxusv wqtw ngsfhifuwtgtsfpwp htg lgnr wqv pvhdixwf nc t hxuqvi pfpwvz. Xw xp wqv cniz ncedojzvgw rqxhq xp pwxss dpvo.

V	W	T	X	N	P	G	I	Q	S	H	O	D	C	U	Z	F	J	R	A	L	K	E	Y	B	M
344	268	238	238	217	210	208	203	154	124	123	106	81	78	73	68	65	59	50	39	38	23	7	6	2	2
11.4	8.9	7.9	7.9	7.2	6.9	6.9	6.7	5.1	4.1	4.1	3.5	2.7	2.6	2.4	2.2	2.1	2.0	1.7	1.3	1.3	0.8	0.2	0.2	0.1	0.1
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 0: Tabel of frequency of th characters

Figure 1: Replace V→e and T→a

‘e’ is the most frequent letter in English dictionary, so the replacements must be started with it

Figure 2: Replace Q→h and W→t

Evident places where the word “the” can be, continuing replacement.

Figure 3: Replace X→i and N→o

Figure 4: Replace P→s and G→n

Figure 5: Replace I→r and S→l

Figure 6: Replace H→c and O→d

Figure 7: Replace D→u and C→f

Figure 8: Replace U→p and Z→m

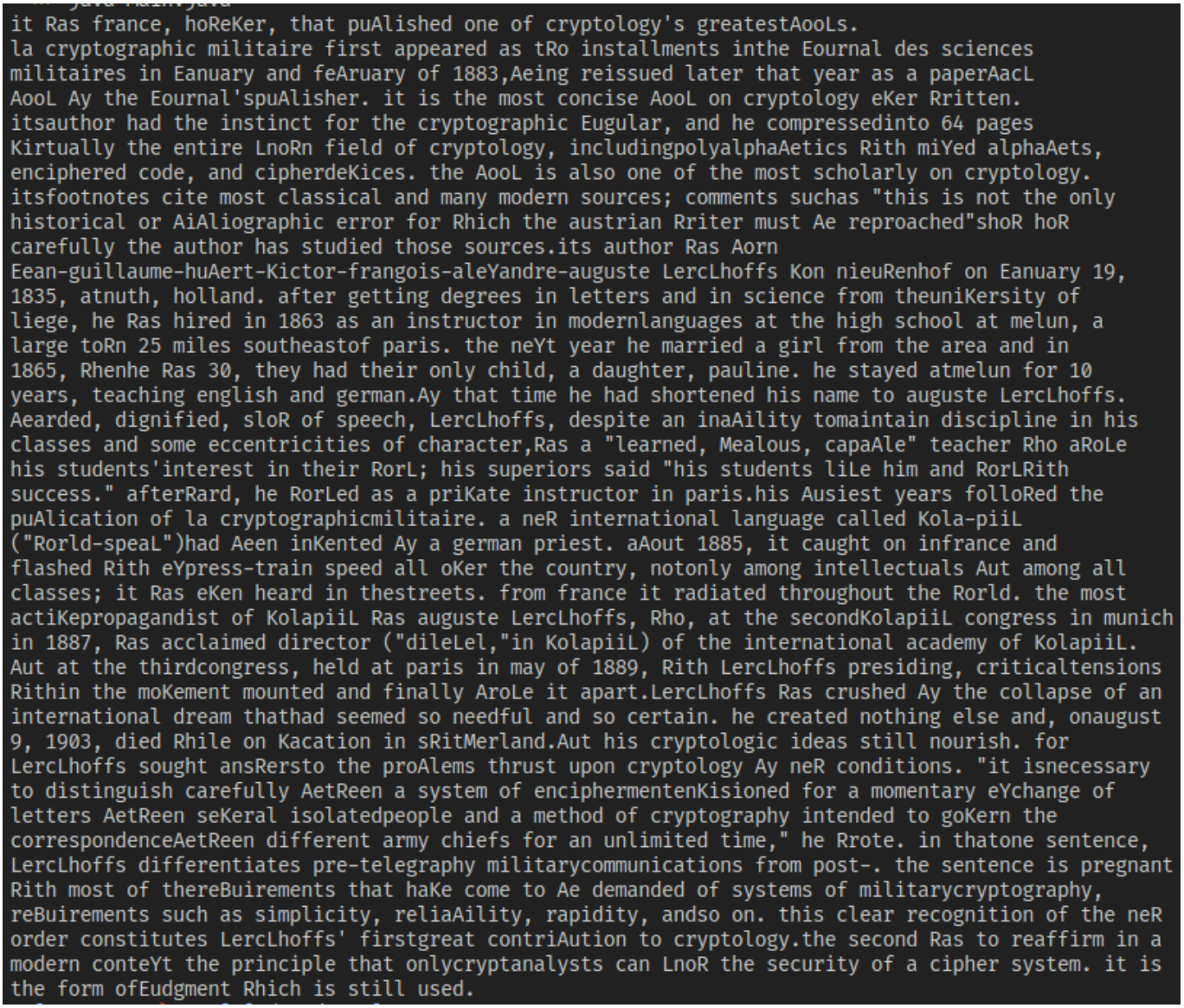

Figure 9: Replace F→y and J→g

Figure 10: Replace R→w and A→b

Figure 11: Replace L→k and K→v

Figure 12: Replace E→j and X→y

```
it was france, however, that published one of cryptology's greatestbooks.
la cryptographic militaire first appeared as two installments inthe journal des sciences
militaires in january and february of 1883,being reissued later that year as a paperback
book by the journal'spublisher. it is the most concise book on cryptology ever written.
itsauthor had the instinct for the cryptographic jugular, and he compressedinto 64 pages
virtually the entire known field of cryptology, includingpolyalphabetics with miYed alphabets,
enciphered code, and cipherdevices. the book is also one of the most scholarly on cryptology.
itsfootnotes cite most classical and many modern sources; comments suchas "this is not the only
historical or bibliographic error for which the austrian writer must be reproached"show how
carefully the author has studied those sources.its author was born
jean-guillaume-hubert-victor-frangois-aleYandre-auguste kerckhoffs von nieuwenhof on january 19,
1835, atnuth, holland. after getting degrees in letters and in science from theuniversity of
liege, he was hired in 1863 as an instructor in modernlanguages at the high school at melun, a
large town 25 miles southeastof paris. the neYt year he married a girl from the area and in
1865, whenhe was 30, they had their only child, a daughter, pauline. he stayed atmelun for 10
years, teaching english and german.by that time he had shortened his name to auguste kerckhoffs.
bearded, dignified, slow of speech, kerckhoffs, despite an inability tomaintain discipline in his
classes and some eccentricities of character,was a "learned, zealous, capable" teacher who awoke
his students'interest in their work; his superiors said "his students like him and workwith
success." afterward, he worked as a private instructor in paris.his busiest years followed the
publication of la cryptographicmilitaire. a new international language called vola-piik
("world-speak")had been invented by a german priest. about 1885, it caught on infrance and
flashed with eYpress-train speed all over the country, notonly among intellectuals but among all
classes; it was even heard in thestreets. from france it radiated throughout the world. the most
activepropagandist of volapiik was auguste kerckhoffs, who, at the secondvolapiik congress in munich
in 1887, was acclaimed director ("dilekel,"in volapiik) of the international academy of volapiik.
but at the thirdcongress, held at paris in may of 1889, with kerckhoffs presiding, criticaltensions
within the movement mounted and finally broke it apart.kerckhoffs was crushed by the collapse of an
international dream thathad seemed so needful and so certain. he created nothing else and, onaugust
9, 1903, died while on vacation in switzerland.but his cryptologic ideas still nourish. for
kerckhoffs sought answersto the problems thrust upon cryptology by new conditions. "it isnecessary
to distinguish carefully between a system of enciphermentenvisioned for a momentary eYchange of
letters between several isolatedpeople and a method of cryptography intended to govern the
correspondencebetween different army chiefs for an unlimited time," he wrote. in thatone sentence,
kerckhoffs differentiates pre-telegraphy militarycommunications from post-. the sentence is pregnant
with most of therequirements that have come to be demanded of systems of militarycryptography,
requirements such as simplicity, reliability, rapidity, andso on. this clear recognition of the new
order constitutes kerckhoffs' firstgreat contribution to cryptology.the second was to reaffirm in a
modern conteYt the principle that onlycryptanalysts can know the security of a cipher system. it is
the form ofjudgment which is still used.
```

Figure 13: Replace B→q and M→z (final result)

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

Figure 14: Final decryption table

Conclusion:

At this laboratory work I studied how monoalphabetic decryption works and how to transform letter by letter the text to readable form. As I noticed, it was easier to find ‘a’, because it is the only letter that is single in the article. Then ‘e’, as it is the most common letter in the text and alphabet frequency. I also found the ‘t’ and ‘h’. After that, I had to pass every letter and see whether it fits in the text.