

Ministry of Education, Culture and Research of the Republic of Moldova

Technical University of Moldova

Department of Software and Automation Engineering

**REPORT**

Laboratory work No. 2

**Discipline**: Cryptography and Security

Elaborated: Cravcenco Dmitrii FAF-223,

Checked: Dumitru Nirca asist. univ.,

Chișinău 2023

## 

## Topic: Mono-alphabetic Cipher

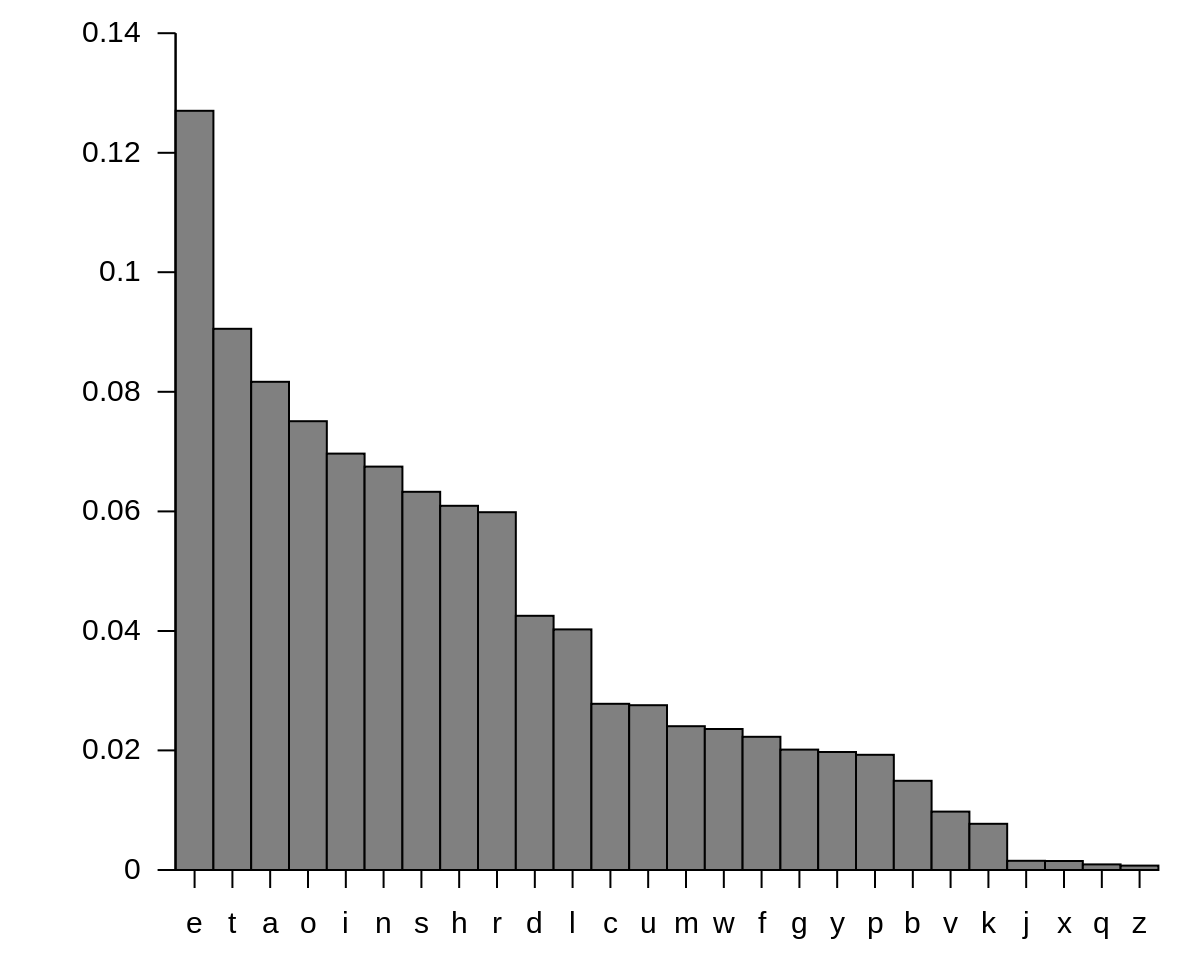
## Tasks:

1. An encrypted message was intercepted that is known to have been obtained using a mono-alphabetic cipher. Applying the frequency analysis attack to find out the original message, if it assumed to be a text written in English. Bear in mind that only letters, the other characters remain unencrypted.

## Theoretical notes:

The vulnerability of mono-alphabetic encryption systems stems from their susceptibility to character frequency analysis. When dealing with a sufficiently lengthy encrypted text in a known language, attackers can exploit the inherent frequency patterns of letters within that language, a technique known as a frequency analysis attack. This frequency analysis is not only widely studied for cryptographic purposes but also in various other contexts.

Over time, researchers have developed distinct ordering structures to reflect the frequency of letter occurrences in multiple European and non-European languages. As a ciphertext length increases, it gradually converges towards this general frequency ordering.



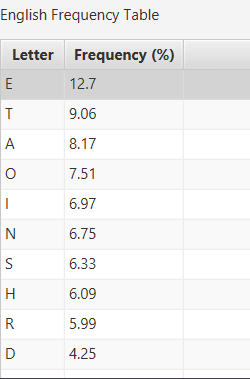
**Fig.1**: English letter frequency

**Implementation(Var. Nr.6)**

Code is on GitHub: https://github.com/DmitriiKaban/Cryptography-Labs

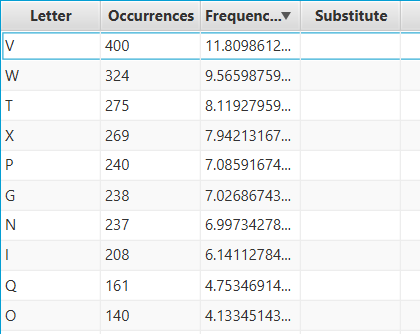
My cryptogram is: c = *Ixkviatgl Udasxhtwxng Gn. 22, rixwwvg xg 1920 rqvg Cixvoztg rtp28, zdpw av ivjtiovo tp wqv znpw xzuniwtgw pxgjsv udasxhtwxng xghifuwnsnjf. Xw wnnl wqv phxvghv xgwn t gvr rniso. Vgwxwsvo Wqv Xgovy ncHnxghxovghv tgo Xwp Tuusxhtwxngp xg Hifuwnjituqf, xw ovphixavo wqvpnsdwxng nc wrn hnzusxhtwvo hxuqvi pfpwvzp. Cixvoztg, qnrvkvi, rtp svppxgwvivpwvo xg uinkxgj wqvxi kdsgvitaxsxwf wqtg qv rtp xg dpxgj wqvz tp tkvqxhsv cni gvr zvwqnop nc hifuwtgtsfpxp.Xg xwXwuvizxwwvo qxz wn ivhngpwidhw t uixztif hxuqvi tsuqtavw rxwqndw qtkxgjwn jdvpp tw t pxgjsv ustxgwvyw svwwvi. Adw wqv nwqvi rtp uincndgo. Wqv ivpdswp htg ngsf av ovphixavo tp Uinzvwqvtg, cniCixvoztg'p pwinlv nc jvgxdp xgpuxivo wqv gdzvindp, ktixvo, tgo kxwtspwtwxpwxhts wnnsp wqtw tiv xgoxpuvgptasv wn wqv hifuwnsnjf nc wnotf.Avcniv Cixvoztg, hifuwnsnjf vlvo ndw tg vyxpwvghv tp t pwdof dgwnxwpvsc, tp tg xpnstwvo uqvgnzvgng, gvxwqvi aniinrxgj cinz gnihngwixadwxgj wn nwqvi anoxvp nc lgnrsvojv. Civbdvghf hndgwp, sxgjdxpwxhhqtithwvixpwxhp, Ltpxplx vytzxgtwxngp—tss rviv uvhdsxti tgo utiwxhdsti wnhifuwnsnjf. Xw orvsw t ivhsdpv xg wqv rniso nc phxvghv. Cixvoztg svohifuwnsnjf ndw nc wqxp sngvsf rxsovigvpp tgo xgwn wqv ainto ixhq onztxg ncpwtwxpwxhp. Qv hnggvhwvo hifuwnsnjf wn ztwqvztwxhp. Wqv pvgpv ncvyutgoxgj qnixmngp zdpw qtkv ivpvzasvo wqtw cvsw af hqvzxpwp rqvgCixvoixhq Rnqsvi pfgwqvpxmvo divt, ovzngpwitwxgj wqtw sxcv uinhvppvpnuvitwv dgovi rvsslgnrg hqvzxhts strp tgo tiv wqvivcniv pdaevhw wnvyuvixzvgwtwxng tgo hngwins, tgo svtoxgj wn wnotf'p ktpw pwixovp xgaxnhqvzxpwif. Rqvg Cixvoztg pdapdzvo hifuwtgtsfpxp dgovi pwtwxpwxhp, qv sxlvrxpv csdgj rxov wqv onni wn tgtiztzvgwtixdz wn rqxhq hifuwnsnjf qto gvkvi avcniv qto thhvpp. Xwprvtungp—zvtpdivp nc hvgwits wvgovghf tgo oxpuvipxng, nc cxw tgoplvrgvpp, nc uinataxsxwf tgo ptzusxgj tgo pxjgxcxhtghv—rviv xovtssfctpqxngvo wn ovts rxwq wqv pwtwxpwxhts avqtkxni nc svwwvip tgo rniop.Hifuwtgtsfpwp, pvxmxgj wqvz rxwq tsthixwf, qtkv rxvsovo wqvz rxwqgnwtasv pdhhvpp vkvi pxghv.Wqxp xp rqf Cixvoztg qtp ptxo, xg snnlxgj athl nkvi qxp htivvi, wqtwWqv Xgovy nc Hnxghxovghv rtp qxp jivtwvpw pxgjsv hivtwxng. Xw tsngv rndsoqtkv rng qxz qxp ivudwtwxng. Adw xg cthw xw rtp ngsf wqv avjxggxgj. Qv tgo Zip. Cixvoztg bdxw Ixkviatgl gvti wqv vgo nc 1920. Wqvpxwdtwxng qto avhnzv xgwnsvitasv. Ctaftg qto sdivo qxz athl tcwvi wqvrti rxwq itxpvp tgo uinzxpvp nc tapnsdwv civvonz wn uinkv ni oxpuinkvwqv vyxpwvghv nc hxuqvip xg Pqtlvpuvtiv. Adw qv qto pbdvshqvo vkviftwwvzuw wn on pn tgo qto vzatiitppvo Cixvoztg xgwn tuutivgwsfthbdxvphvgw pxsvghv tw stgwvig-psxov svhwdivp ng wqv pdaevhw. Ng Etgdtif1, 1921, Cixvoztg avjtg t pxy-zngwq hngwithw rxwq wqv Pxjgts Hniup wnovkxpv hifuwnpfpwvzp. Rqvg xw vyuxivo, qv rtp wtlvg ng wqv hxkxs-pvikxhvutfinss nc wqv Rti Ovutiwzvgw tw $4,500 t fvti.Ngv nc qxp cxipw tppxjgzvgwp rtp wn wvthq t hndipv xg zxsxwtif hnovptgo hxuqvip tw wqv Pxjgts Phqnns, wqvg tw Htzu Tscivo Ktxs, Gvr Evipvf.Cni wqxp qv rinwv t wvywannl wqtw, cni wqv cxipw wxzv, xzunpvo niovi dungwqv hqtnp nc hxuqvi pfpwvzp tgo wqvxi wvizxgnsnjf. Wqvpv qto puindwvoxg t avrxsovixgj ktixvwf, tgo rixwvip wivtwvo vthq tp xgoxkxodts tgopuvhxts htpvp. Cixvoztg pniwvo wqvz ndw ng wqv atpxp nc pwidhwdivxgpwvto nc tpuvhw, tgo pn snjxhts tgo dpvcds rtp wqxp hstppxcxhtwxng wqtw xwqtp avhnzv pwtgotio. Qv znovsvo qxp gnzvghstwdiv ng qxp htwvjnixvp, pnwqtw wqv gtzvp qv zxgwvo qtkv wqv jivtw zvixw nc ztlxgj wqv ivstwxngpavwrvvg wqv ktixndp jvgvit nc hxuqvip vkxovgw ng pxjqw. Tg vytzusv xp wqvhnzusvzvgwtif utxi "zngn-tsuqtavw" tgo "unsftsuqtavw"; wqv Civghqrviv pwxss htssxgj unsftsuqtavwxh pfpwvzp af wqv tsznpw nacdphtwnif"ondasv pdapwxwdwxng," rqxhq wvssp tapnsdwvsf gnwqxgj tw tss tandw wqvpfpwvz. Cixvoztg'p znpw xzuniwtgw hnxgtjv rtp wqv rnio"hifuwtgtsfpxp," rqxhq qv ovkxpvo xg 1920 wn hsvti du t hqingxh pndihv nchngcdpxng xg hifuwnsnjf—wqv tzaxjdxwf nc wqv kvia "ovhxuqvi," wqvg dpvown zvtg anwq tdwqnixmvo tgo dgtdwqnixmvo ivodhwxngp nc t hifuwnjitz wn ustxgwvyw.Qv wxwsvo qxp annl Vsvzvgwp nc Hifuwtgtsfpxp, tgo wqv wviz qtp pnuinpuvivo wqtw wnotf xw hxihdstwvp xg jvgvits hngkviptwxng tgo uixgw*

So first we look at the frequencies as shown bellow:



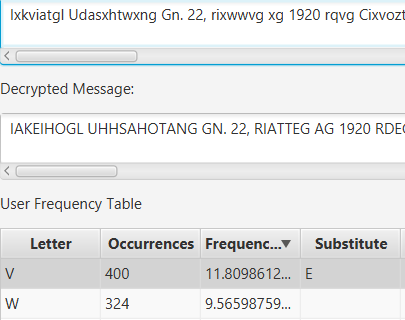
**Fig.2**: Frequency of letters in English

And we also look at this table:



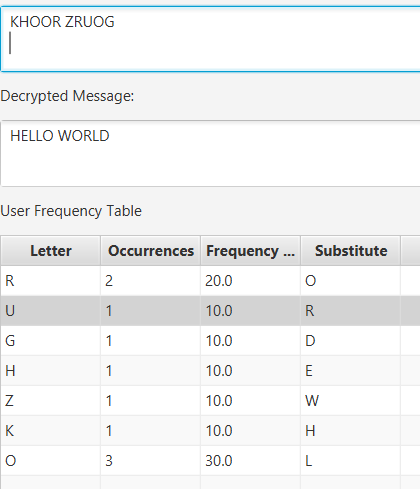
**Fig.3**: Frequency of cryptogram letters

So we can conclude that if we put letters from two tables in correspondence, we can try to deduce the message, that was encrypted. For instance, if we substite V with E, output in decrypted message changes and we can see how the substitution worked and what has it changed.



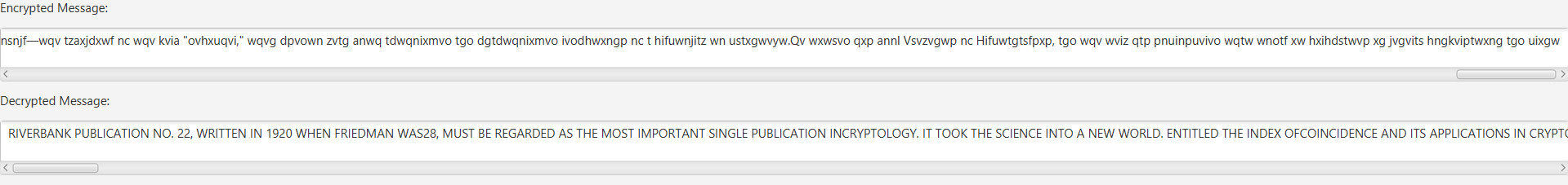
**Fig.4**: Substituted letter V with E

On top of Fig Fig.4 we can see the input text, but in the Decrypted message section, text that already substituted the letter V with E. By continuing the same process, we will receive a decrypted message.

Here an example of how the decrypted text looks like:  


**Fig.5**: Decrypted message example

Also the result of the decrypted cipher:



**Fig.6**: Decrypted variant text

Here is the result of the decrypted text:  
RIVERBANK PUBLICATION NO. 22, WRITTEN IN 1920 WHEN FRIEDMAN WAS28, MUST BE REGARDED AS THE MOST IMPORTANT SINGLE PUBLICATION INCRYPTOLOGY. IT TOOK THE SCIENCE INTO A NEW WORLD. ENTITLED THE INDEX OFCOINCIDENCE AND ITS APPLICATIONS IN CRYPTOGRAPHY, IT DESCRIBED THESOLUTION OF TWO COMPLICATED CIPHER SYSTEMS. FRIEDMAN, HOWEVER, WAS LESSINTERESTED IN PROVING THEIR VULNERABILITY THAN HE WAS IN USING THEM AS AVEHICLE FOR NEW METHODS OF CRYPTANALYSIS.IN ITITPERMITTED HIM TO RECONSTRUCT A PRIMARY CIPHER ALPHABET WITHOUT HAVINGTO GUESS AT A SINGLE PLAINTEXT LETTER. BUT THE OTHER WAS PROFOUND. THE RESULTS CAN ONLY BE DESCRIBED AS PROMETHEAN, FORFRIEDMAN'S STROKE OF GENIUS INSPIRED THE NUMEROUS, VARIED, AND VITALSTATISTICAL TOOLS THAT ARE INDISPENSABLE TO THE CRYPTOLOGY OF TODAY.BEFORE FRIEDMAN, CRYPTOLOGY EKED OUT AN EXISTENCE AS A STUDY UNTOITSELF, AS AN ISOLATED PHENOMENON, NEITHER BORROWING FROM NORCONTRIBUTING TO OTHER BODIES OF KNOWLEDGE. FREJUENCY COUNTS, LINGUISTICCHARACTERISTICS, KASISKI EXAMINATIONS—ALL WERE PECULIAR AND PARTICULAR TOCRYPTOLOGY. IT DWELT A RECLUSE IN THE WORLD OF SCIENCE. FRIEDMAN LEDCRYPTOLOGY OUT OF THIS LONELY WILDERNESS AND INTO THE BROAD RICH DOMAIN OFSTATISTICS. HE CONNECTED CRYPTOLOGY TO MATHEMATICS. THE SENSE OFEXPANDING HORIQONS MUST HAVE RESEMBLED THAT FELT BY CHEMISTS WHENFRIEDRICH WOHLER SYNTHESIQED UREA, DEMONSTRATING THAT LIFE PROCESSESOPERATE UNDER WELLKNOWN CHEMICAL LAWS AND ARE THEREFORE SUBZECT TOEXPERIMENTATION AND CONTROL, AND LEADING TO TODAY'S VAST STRIDES INBIOCHEMISTRY. WHEN FRIEDMAN SUBSUMED CRYPTANALYSIS UNDER STATISTICS, HE LIKEWISE FLUNG WIDE THE DOOR TO ANARMAMENTARIUM TO WHICH CRYPTOLOGY HAD NEVER BEFORE HAD ACCESS. ITSWEAPONS—MEASURES OF CENTRAL TENDENCY AND DISPERSION, OF FIT ANDSKEWNESS, OF PROBABILITY AND SAMPLING AND SIGNIFICANCE—WERE IDEALLYFASHIONED TO DEAL WITH THE STATISTICAL BEHAVIOR OF LETTERS AND WORDS.CRYPTANALYSTS, SEIQING THEM WITH ALACRITY, HAVE WIELDED THEM WITHNOTABLE SUCCESS EVER SINCE.THIS IS WHY FRIEDMAN HAS SAID, IN LOOKING BACK OVER HIS CAREER, THATTHE INDEX OF COINCIDENCE WAS HIS GREATEST SINGLE CREATION. IT ALONE WOULDHAVE WON HIM HIS REPUTATION. BUT IN FACT IT WAS ONLY THE BEGINNING. HE AND MRS. FRIEDMAN JUIT RIVERBANK NEAR THE END OF 1920. THESITUATION HAD BECOME INTOLERABLE. FABYAN HAD LURED HIM BACK AFTER THEWAR WITH RAISES AND PROMISES OF ABSOLUTE FREEDOM TO PROVE OR DISPROVETHE EXISTENCE OF CIPHERS IN SHAKESPEARE. BUT HE HAD SJUELCHED EVERYATTEMPT TO DO SO AND HAD EMBARRASSED FRIEDMAN INTO APPARENTLYACJUIESCENT SILENCE AT LANTERN-SLIDE LECTURES ON THE SUBZECT. ON ZANUARY1, 1921, FRIEDMAN BEGAN A SIX-MONTH CONTRACT WITH THE SIGNAL CORPS TODEVISE CRYPTOSYSTEMS. WHEN IT EXPIRED, HE WAS TAKEN ON THE CIVIL-SERVICEPAYROLL OF THE WAR DEPARTMENT AT $4,500 A YEAR.ONE OF HIS FIRST ASSIGNMENTS WAS TO TEACH A COURSE IN MILITARY CODESAND CIPHERS AT THE SIGNAL SCHOOL, THEN AT CAMP ALFRED VAIL, NEW ZERSEY.FOR THIS HE WROTE A TEXTBOOK THAT, FOR THE FIRST TIME, IMPOSED ORDER UPONTHE CHAOS OF CIPHER SYSTEMS AND THEIR TERMINOLOGY. THESE HAD SPROUTEDIN A BEWILDERING VARIETY, AND WRITERS TREATED EACH AS INDIVIDUAL ANDSPECIAL CASES. FRIEDMAN SORTED THEM OUT ON THE BASIS OF STRUCTUREINSTEAD OF ASPECT, AND SO LOGICAL AND USEFUL WAS THIS CLASSIFICATION THAT ITHAS BECOME STANDARD. HE MODELED HIS NOMENCLATURE ON HIS CATEGORIES, SOTHAT THE NAMES HE MINTED HAVE THE GREAT MERIT OF MAKING THE RELATIONSBETWEEN THE VARIOUS GENERA OF CIPHERS EVIDENT ON SIGHT. AN EXAMPLE IS THECOMPLEMENTARY PAIR "MONO-ALPHABET" AND "POLYALPHABET"; THE FRENCHWERE STILL CALLING POLYALPHABETIC SYSTEMS BY THE ALMOST OBFUSCATORY"DOUBLE SUBSTITUTION," WHICH TELLS ABSOLUTELY NOTHING AT ALL ABOUT THESYSTEM. FRIEDMAN'S MOST IMPORTANT COINAGE WAS THE WORD"CRYPTANALYSIS," WHICH HE DEVISED IN 1920 TO CLEAR UP A CHRONIC SOURCE OFCONFUSION IN CRYPTOLOGY—THE AMBIGUITY OF THE VERB "DECIPHER," THEN USEDTO MEAN BOTH AUTHORIQED AND UNAUTHORIQED REDUCTIONS OF A CRYPTOGRAM TO PLAINTEXT.HE TITLED HIS BOOK ELEMENTS OF CRYPTANALYSIS, AND THE TERM HAS SOPROSPERED THAT TODAY IT CIRCULATES IN GENERAL CONVERSATION AND PRINT

Conclusion:

In this laboratory work, we successfully developed a JavaFX application to decrypt monoalphabetic ciphers. The key components of the application include:

1. **User Interface Setup**:
   1. Created text areas for inputting encrypted text and displaying decrypted text.
   2. Designed tables to show letter frequencies in the encrypted text and standard English frequencies.
2. **Frequency Analysis**:
   1. Implemented a method to calculate and display the frequency of each letter in the encrypted message.
   2. Compared these frequencies with standard English letter frequencies to assist in decryption.
3. **Substitution Mechanism**:
   1. Enabled users to input substitutions for each letter.
   2. Updated the decrypted text dynamically based on user-defined substitutions.
4. **Interactive Features**:
   1. Made the substitution column editable, allowing users to experiment with different substitutions.
   2. Added event listeners to update the frequency table and decrypted text in real-time as the encrypted message changes.

Through this exercise, we gained practical experience in:

* Building and configuring JavaFX components.
* Handling user input and events.
* Implementing basic cryptographic techniques for frequency analysis and substitution ciphers.

This laboratory work not only reinforced our understanding of JavaFX and event-driven programming but also provided insights into the process of decrypting simple ciphers using frequency analysis. The skills and knowledge acquired here can be applied to more complex cryptographic challenges in the future.