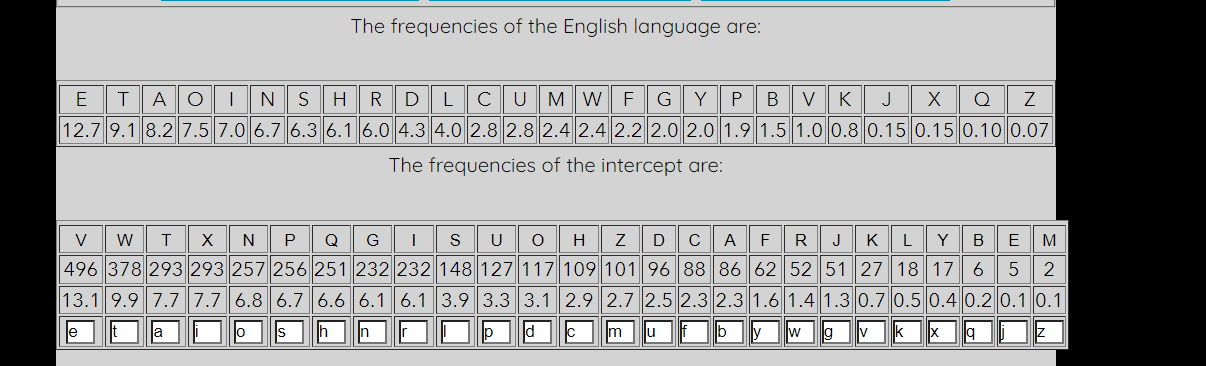
**Lucrare de laborator nr.2**

**Executat:** Frasiniuc Ilona, IS31Z

**Criptanaliza cifrurilor monoalfabetice**

**Varianta nr.9**

VTHQ GVR PVWWXGJ NC TSAVIWX'P OXPL AINDJQW XGWN USTF T GVR HXUQVITSUQTAVW, XG RQXHQ ANWQ WQV USTXGWVYW TGO WQV HXUQVIWVYW VBDXKTSVGWP TIVHQTGJVO XG IVJTIO WN NGV TGNWQVI. WQVIV TIV TP ZTGF NC WQVPV TSUQTAVWPTP WQVIV TIV UNPXWXNGP NC QXP OXPL, TGO WQXP ZDSWXUSXHXWF ZVTGP WQTW TSAVIWXQVIV OVKXPVO WQV CXIPW UNSFTSUQTAVWXH HXUQVI.WQXP THQXVKVZVGW—HIXWXHTS XG WQV QXPWNIF NC HIFUWNSNJF —TSAVIWX WQVGTONIGVO AF TGNWQVI IVZTILTASV XGKVGWXNG: VGHXUQVIVO HNOV.XW RTP CNIWQXP WQTW QV QTO UDW GDZAVIP XG WQV NDWVI IXGJ. XG T WTASV QV UVIZDWVOWQV GDZAVIP 1 WN 4 XG WRN-, WQIVV-, TGO CNDI-OXJXW JINDUP, CINZ 11 WN4444, TGO DPVO WQVPV TP 336 HNOVJINDUP CNI T PZTSS HNOV. "XG WQXP WTASV,THHNIOXGJ WN TJIVVZVGW, RV PQTSS VGWVI XG WQV KTIXNDP SXGVP TW WQVGDZAVIP RQTWVKVI HNZUSVWV UQITPVP RV USVTPV, CNI VYTZUSV,HNIIVPUNGOXGJ WN 12, 'RV QTKV ZTOV IVTOF WQV PQXUP RQXHQ RV UINZXPVOTGO PDUUSXVO WQVZ RXWQ WINNUP TGO JITXG.' " WQVPV HNOV KTSDVP OXO GNWHQTGJV, TGF ZNIV WQTG WQV ZXYVO TSUQTAVW NC WQV OXPL OXO. ADW WQV OXJXWPIVPDSWXGJ CINZ TG VGHNOXGJ RVIV WQVG VGHXUQVIVO RXWQ WQV OXPL EDPW TP XCWQVF RVIV USTXGWVYW SVWWVIP.XG TSAVIWX'P RNIOP, "WQVPV GDZAVIP X WQVGXGPVIW XG ZF ZVPPTJV THHNIOXGJ WN WQV CNIZDST NC WQV HXUQVI, IVUIVPVGWXGJWQVZ AF WQV SVWWVIP WQTW OVGNWV WQVPV GDZAVIP." WQVPV GDZAVIP WQDPHQTGJVO WQVXI HXUQVIWVYW VBDXKTSVGWP TP WQV OXPL WDIGVO. QVGHV 341,UVIQTUP ZVTGXGJ "UNUV," ZXJQW AVHNZV ZIU TW NGV UNPXWXNG TGO CHN TWTGNWQVI. WQXP HNGPWXWDWVP TG VYHVSSVGW CNIZ NC VGHXUQVIVO HNOV, TGO EDPWQNR UIVHNHXNDP TSAVIWX RTP ZTF AV PVVG AF WQV CTHW WQTW WQV ZTENIUNRVIP NC WQV VTIWQ OXO GNW AVJXG WN VGHXUQVI WQVXI HNOV ZVPPTJVP DGWXS400 FVTIP STWVI, GVTI WQV VGO NC WQV 19WQ HVGWDIF, TGO VKVG WQVG WQVXIPFPWVZP RVIV ZDHQ PXZUSVI WQTG WQXP.TSAVIWX'P WQIVV IVZTILTASV CXIPWP—WQV VTISXVPW RVPWVIG VYUNPXWXNG NCHIFUWTGTSFPXP, WQV XGKVGWXNG NC UNSFTSUQTAVWXV PDAPWXWDWXNG, TGO WQVXGKVGWXNG NC VGHXUQVIVO HNOV—ZTLV QXZ WQV CTWQVI NC RVPWVIGHIFUWNSNJF. ADW TSWQNDJQ QXP WIVTWXPV RTP UDASXPQVO XG XWTSXTG XG THNSSVHWXNG NC QXP RNILP XG 1568, TGO TSWQNDJQ QXP XOVTP RVIV TAPNIAVO AFUTUTS HIFUWNSNJXPWP TGO UVIQTUP XGCSDVGHVO WQV PHXVGHV'P OVKVSNUZVGW,WQVF GVKVI QTO WQV OFGTZXH XZUTHW WQTW PDHQ UINOXJXNDPTHHNZUSXPQZVGWP NDJQW WN QTKV UINODHVO. PFZNGOP' VKTSDTWXNG NC QXPRNIL XG JVGVITS ZTF ANWQ VYUSTXG RQF TGO PDZZTIXMV WQV ZNOVIG KXVR NC QXP HIFUWNSNJXHTS HNGWIXADWXNGP:"WQXP ZTG NC ZTGF-PXOVO JVGXDP HTZV XGWN WQV RNISO WNN PNNG CNI WQVUVICVHW VYVIHXPV NC QXP PXGJDSTI CTHDSWXVP. RQVWQVI RV IVJTIO QXZ CINZ WQVUNXGW NC KXVR NC TIW, NC PHXVGHV, NI NC SXWVITWDIV, QV NHHDUXVP XG VTHQOVUTIWZVGW WQV UNPXWXNG NC UIVHDIPNI, UXNGVVI, TGO XGOXHTWNI. TSRTFPNIXJXGTS TGO TSRTFP CVIWXSV, QV UINUQVPXVO NC STGOP QV RTP GNW UIXKXSVJVOWN VGWVI, SVTKXGJ WQV ZVZNIF NC OXZ TGO KTIXVO JIVTWGVPP ITWQVI WQTG TGFPNSXO ZNGDZVGW AVQXGO QXZ."UNSFTSUQTAVWXHXWF WNNL TGNWQVI PWVU CNIRTIO XG 1518, RXWQ WQVTUUVTITGHV NC WQV CXIPW UIXGWVO ANNL NG HIFUWNSNJF, RIXWWVG AF NGV NC WQVZNPW CTZNDP XGWVSSVHWDTSP NC QXP OTF. WQXP RTP ENQTGGVP WIXWQVZXDP, TAVGVOXHWXGV ZNGL RQNPV OTAASXGJ XG TSHQVZF TGO NWQVI ZFPWXH UNRVIPZTOV QXZ NGV NC WQV ZNPW IVKVIVO CXJDIVP XG NHHDSW PHXVGHV, RQXSV QXPZNIV PNSXO PHQNSTIPQXU RNG QXZ WQV WXWSV NC "CTWQVI NC AXAXSXNJITUQF." XG1518, T FVTI TGO T QTSC TCWVI QXP OVTWQ, QXP UNSFJITUQXTV SXAIX PVY, SNTGGXPWIXWQVZXX TAATWXP UVTUNSXWTGX, BDNGOTZ PUTGQVXZVGPXP, TO ZTYXZXSXTGDZHTVPTIVZ ("PXY ANNLP NC UNSFJITUQF, AF ENQTGGVP WIXWQVZXDP, TAANW TWRDIMADIJ, CNIZVISF TW PUTGQVXZ, CNI WQV VZUVINI ZTYXZXSXTG") RTPUDASXPQVO. AF CTI WQV ADSL NC WQV KNSDZV HNGPXPWP NC WQV HNSDZGP NCRNIOP UIXGWVO XG STIJV JNWQXH WFUV WQTW WIXWQVZXDP DPVO XG QXP PFPWVZP NCHIFUWNJITUQF. ADW XG WQV RNIL'P ANNL K TUUVTIP, CNI WQV CXIPW WXZV, WQVPBDTIV WTASV, NI WTASVTD. WQXP XP WQV VSVZVGWTS CNIZ NC UNSFTSUQTAVWXHPDAPWXWDWXNG, CNI XW VYQXAXWP TSS TW NGHV TSS WQV HXUQVI TSUQTAVWP XG TUTIWXHDSTI PFPWVZ. WQVPV TIV DPDTSSF TSS WQV PTZV PVBDVGHV NC SVWWVIP, ADWPQXCWVO WN OXCCVIVGW UNPXWXNGP XG IVSTWXNG WN WQV USTXGWVYW TSUQTAVW, TP XGTSAVIWX'P OXPL WQV XGGVI TSUQTAVW TPPDZVO OXCCVIVGW UNPXWXNGP XG IVJTIO WNWQV NDWVI TSUQTAVW. WQV WTASVTD PVWP WQVZ NDW XG NIOVISF CTPQXNG—WQVTSUQTAVWP NC WQV PDHHVPPXKV UNPXWXNGP STXO NDW XG INRP NGV AVSNR WQVNWQVI, VTHQ TSUQTAVW PQXCWVO NGV USTHV WN WQV SVCW NC WQV NGV TANKV. VTHQINR WQDP NCCVIP T OXCCVIVGW PVW NC HXUQVI PDAPWXWDWVP WN WQV SVWWVIP NC WQVUSTXGWVYW TSUQTAVW TW WQV WNU. PXGHV WQVIV HTG AV NGSF TP ZTGF INRP TPWQVIV TIV SVWWVIP XG WQV TSUQTAVW, WQV WTASVTD XP PBDTIV.WQV PXZUSVPW WTASVTD XP NGV WQTW DPVP WQV GNIZTS TSUQTAVW XG KTIXNDPUNPXWXNGP TP WQV HXUQVI TSUQTAVWP. VTHQ HXUQVI TSUQTAVW UINODHVP, XGNWQVI RNIOP, T HTVPTI PDAPWXWDWXNG.



**Rezultatul**

Each new setting of alberti's disk brought into play a new cipheralphabet, in which both the plaintext and the ciphertext equivalents arechanged in regard to one another. There are as many of these alphabetsas there are positions of his disk, and this multiplicity means that albertihere devised the first polyalphabetic cipher.this achievement—critical in the history of cryptology —alberti thenadorned by another remarkable invention: enciphered code. It was forthis that he had put numbers in the outer ring. In a table he permutedthe numbers 1 to 4 in two-, three-, and four-digit groups, from 11 to4444, and used these as 336 codegroups for a small code. "in this table,according to agreement, we shall enter in the various lines at thenumbers whatever complete phrases we please, for example,corresponding to 12, 'we have made ready the ships which we promisedand supplied them with troops and grain.' " these code values did notchange, any more than the mixed alphabet of the disk did. But the digitsresulting from an encoding were then enciphered with the disk just as ifthey were plaintext letters. In alberti's words, "these numbers i theninsert in my message according to the formula of the cipher, representingthem by the letters that denote these numbers." these numbers thuschanged their ciphertext equivalents as the disk turned. Hence 341,perhaps meaning "pope," might become mrp at one position and fco atanother. This constitutes an excellent form of enciphered code, and justhow precocious alberti was may be seen by the fact that the majorpowers of the earth did not begin to encipher their code messages until400 years later, near the end of the 19th century, and even then theirsystems were much simpler than this.alberti's three remarkable firsts—the earliest western exposition ofcryptanalysis, the invention of polyalphabetie substitution, and theinvention of enciphered code—make him the father of westerncryptology. But although his treatise was published in italian in acollection of his works in 1568, and although his ideas were absorbed bypapal cryptologists and perhaps influenced the science's development,they never had the dynamic impact that such prodigiousaccomplishments ought to have produced. Symonds' evaluation of hiswork in general may both explain why and summarize the modern view of his cryptological contributions:"this man of many-sided genius came into the world too soon for theperfect exercise of his singular faculties. Whether we regard him from thepoint of view of art, of science, or of literature, he occupies in eachdepartment the position of precursor, pioneer, and indicator. Always original and always fertile, he prophesied of lands he was not privilegedto enter, leaving the memory of dim and varied greatness rather than anysolid monument behind him."polyalphabeticity tookanother step forward in 1518, with theappearance of the first printed book on cryptology,written by one of themost famous intellectuals of his day. This was johannes trithemius, abenedictine monk whose dabbling in alchemy and other mystic powersmade him one of the most revered figures in occult science, while hismore solid scholarship won him the title of "father of bibiliography." in1518, a year and a half after his death, his polygraphiae libri sex, loannistrithemii abbatis peapolitani, quondam spanheimensis, ad maximilianumcaesarem ("six books of polygraphy, by johannes trithemius, abbot atwurzburg, formerly at spanheim, for the emperor maximilian") waspublished. By far the bulk of the volume consists of the columns ofwords printed in large gothic type that trithemius used in his systems ofcryptography. But in the work's book v appears, for the first time, thesquare table, or tableau. This is the elemental form of polyalphabeticsubstitution, for it exhibits all at once all the cipher alphabets in aparticular system. These are usually all the same sequence of letters, butshifted to different positions in relation to the plaintext alphabet, as inalberti's disk the inner alphabet assumed different positions in regard tothe outer alphabet. The tableau sets them out in orderly fashion—thealphabets of the successive positions laid out in rows one below theother, each alphabet shifted one place to the left of the one above. Eachrow thus offers a different set of cipher substitutes to the letters of theplaintext alphabet at the top. Since there can be only as many rows asthere are letters in the alphabet, the tableau is square.the simplest tableau is one that uses the normalalphabet in variouspositions as the cipher alphabets. Each cipher alphabet produces, inother words, a caesar substitution.