1. **Letter frequency and deciphering of text**:
    a. Letter Frequency

Letter	**Relative Frequency (%)**
R	13
B	10.53
M	9.59
K	7.58
J	7.43
W	7.28
I	6.34
P	4.64
U	3.71
H	3.56
…	…

    b. Common bigrams and trigrams
        i. Bigrams (TH, HE, IN)
            1. Bigram frequency analysis

	Bigram	**Frequency**
7	BP	19
96	WK	15
36	MB	15
8	PR	14
46	MK	11
37	BM	10

18	JX	10
50	BR	10
…	…	…

ii. Trigrams (THE, AND, ING)
1. Trigram Frequency Analysis

	Trigram	**Frequency**
7	BPR	14
51	MKD	6
17	RJX	5
145	BWJ	4
69	RII	4
32	RKB	4
…	…	…

c. Decryption process
i. Initial substitution hypothesis
1. First step
a. Most frequent trigram (BPR) with 14 occurrences
i. Most likely common English trigram “THE”
ii. Hypothesis: B = T, P = H, R = E
b. Most frequent bigram which also includes parts of trigram (ex: BR or PR)
i. If BR aligns with HE, this supports trigram substitution hypothesis
2. Substitution Key Update
a. We’ll start replacing B, P, and R with their hypothesized mappings (T, H, E) in the ciphertext to see how it affects the text
b. After applying initial substitution, partially decrypted text is:

levmnie the sumvtwve jx the lmiwv yjeeyekti jx qmtm wi the xjvni mkd ymiteut jx iehx
wi the eiiekve jx ymtinlmtmihw utn qmumte dj w imhhtutt je hnvwdmte the yjeeyekti
jx the qmtm mvvjudwkot jt wkteusuetmtwjk lmi ed jk xjutttemui jx itndt
wt wi kjt mke mitt miqt je ashmwk emvh yjeeyek mkt wi iwokwxwvmkve mkd ijye ynit ueymwk nkeashmwked jt owee mvjysh ete ashmkmtwjkjk ecjnhd hmee jt le

fnmhwxwed mkd wkiswued jt invt mk etekt the vjnhd uemvh the eimte jx ekwhohteked
ywkd vmsmlhe jx uevjokwgwko ijnkdheii ijnkd mkd ihmseheiii hmse w dj
kjt deeyy tiehx the xwkmhmnt hjuwttlnt yte aseeuwekvecwth qmtm hmi hex jk djntl
the xjhhjcwko wi the sujseu msshwvmtwjk mkd wkteusuetmtwjk w jxxeu yt thejuweiwk the hjsethmt the eiiekve jx jqwkmcmk qmumte cwhh ueymwk wkmtv

c. From the decrypted text
    i. Spaces make it easier to identify possible English words like:
        - **"the"** (decoded correctly multiple times).
        - Two-letter sequences like **"wi"** might correspond to **"is"** or **"it"**.
    ii. Repeated patterns:
        - **"eii"** could hint at common sequences like **"ess"** or **"ell".**
        - **"yjeeyek"** and similar patterns suggest recurring bigrams/trigrams.
d. Refining some substitutions (common patterns and English words)
    i. **"wi"** occurs frequently and appears in places where a common two-letter word like "is" or "it" could fit.
        1. Hypothesis: `W = I`, `I = S`.
    ii. **"jx"** often occurs at the start of phrases. It might represent "of."
        1. Hypothesis: `J = O`, `X = F`.
    iii. **"lmiwv"** might correspond to a word like "which" or "there."
        1. Hypothesis: `L = T`, `M = H`.
e. This will take a very long time to decrypt hence I switched to using another tool online for this problem:
    i. [Online calculator: Substitution cipher decoder]
    ii. Key used to decrypt the message:
        1. XTWDVQZLSONBAUGHKEPYRCIFMJ
    iii. Details:
        1. Population size: 100
        2. Number of generations: 20
        3. Mutation chance: 0.01
        4. Initial text fitness: 5.3764
        5. Final text fitness: 1.1793
    iv. Table

Number	Best Key In Generation	Decrypted text
1	KRUSAHPGOVLZNBWYFEXIQMJCDT	ZEMNBOE RYE XQNMRJME VC RYE ZNOJM DVAEDELRO VC FNRN JO RYE CVMBO NLS DNOREQI VC OEGC JO RYE EOOELME VC DNROBZNINOYJ QIB FNQNRE SV J OYNGG RQI RV EGBMJSNRE RYE DVAEDELRO VC RYE FNRN NMMVQSJLW RV DI JLREQXQERNRJVL ZNOES VL CVQRI IENQO VC ORBSI JR JO LVR NL ENOI RNOF RV EKXGNJL ENMY DVAEDELR NLS JRO OJWLJCJMNLME NLS OVDE DBOR QEDNJL BLEKXGNJLES RV WJAE N MVDXGERE EKXGNLNRJVL VLE UVBGS YNAE RV ZE HBNGJCJES NLS JLOXJQES RV OBMY NL EKRELR RYNR YE MVBGS QENMY RYE ORNRE VC ELGJWYRELES DJLS MNXNZGE VC QEMVWLJPJLW OVBLSGEOO OVBLS NLS OYNXEGEOO OYNXE J SV LVR SEED DIOEGC RYE CJLNG NBRYVQJRI ZBR DI EKXEQJELME UJRY FNRN YNO GECR LV SVBZR RYNR RYE CVGGVUJLW JO RYE XQVXEQ NXXGJMNRJVL NLS JLREQXQERNRJVL J VCCEQ DI RYEVQJEO JL RYE YVXE RYNR RYE EOOELME VC VFJLNUNL FNQNRE UJGG QEDNJL JLRNMR
2	VRIGLFZSKONBAPWYHETJDMUCQX	BEMAPKE RYE TDAMRUME OC RYE BAKUM QOLEQENRK OC HARA UK RYE COMPK ANG QAKREDJ OC KESC UK RYE EKKENME OC QARKPBAJAKYU DJP HADARE GO U KYASS RDJ RO ESPMUGARE RYE QOLEQENRK OC RYE HARA AMMODGUNW RO QJ UNREDTDERARUON BAKEG ON CODRJ JEADK OC KRPGJ UR UK NOR AN EAKJ RAKH RO EVTSAUN EAMY QOLEQENR ANG URK KUWNUCUMANME ANG KOQE QPKR

		DEQAUN PNEVTSAUNEG RO WULE A MOQTSERE EVTSANARUON ONE IOPSG YALE RO BE FPASUCUEG ANG UNKTUDEG RO KPMY AN EVRENR RYAR YE MOPSG DEAMY RYE KRARE OC ENSUWYRENEG QUNG MATABSE OC DEMOWNUZUNW KOPNGSEKK KOPNG ANG KYATESEKK KYATE U GO NOR GEEQ QJKESC RYE CUNAS APRYODURJ BPR QJ EVTEDUENME IURY HARA YAK SECR NO GOPBR RYAR RYE COSSOIUNW UK RYE TDOTED ATTSUMARUON ANG UNREDTDERARUON U OCCED QJ RYEODUEK UN RYE YOTE RYAR RYE EKKENME OC OHUNAIAN HADARE IUSS DEQAUN UNRAMR
3	WHGRQXJBTESVIDYUMANKFPOLCZ	VAPIDTA HUA NFIPHOPA EL HUA VITOP CEQACASHT EL MIHI OT HUA LEPDT ISR CITHAFK EL TABL OT HUA ATTASPA EL CIHTDVIKITUO FKD MIFIHA RE O TUIBB HFK HE ABDPORIHA HUA CEQACASHT EL HUA MIHI IPPEFROSY HE CK OSHAFNFAHIHOES VITAR ES LEFHK KAIFT EL THDRK OH OT SEH IS AITK HITM HE AWNBIOS AIPU CEQACASH ISR OHT TOYSOLOPISPA ISR TECA CDTH FACIOS DSAWNBIOSAR HE YOQA I PECNBAHA AWNBISIHOES ESA GEDBR UIQA HE VA XDIBOLOAR ISR OSTNOFAR HE TDPU IS AWHASH HUIH UA PEDBR FAIPU HUA THIHA EL ASBOYUHASAR COSR PINIVBA EL FAPEYSOJOSY TEDSRBATT TEDSR ISR TUINABATT TUINA O RE SEH RAAC CKTABL HUA LOSIB IDHUEFOHK VDH CK AWNAFOASPA GOHU MIHI UIT BALH SE REDVH HUIH HUA LEBBEGOSY OT HUA NFENAF INNBOPIHOES ISR OSHAFNFAHIHOES O ELLAF CK HUAEFOAT OS HUA UENA HUIH HUA ATTASPA EL EMOSIGIS

		MIFIHA GOBB FACIOS OSHIPH
4	CRXLJKYFSIDBEUZHVAWGNPOTMQ	BAPEUSA RHA WNEPROPA IT RHA BESOP MIJAMADRS IT VERE OS RHA TIPUS EDL MESRANG IT SAFT OS RHA ASSADPA IT MERSUBEGESHO NGU VENERA LI O SHEFF RNG RI AFUPOLERA RHA MIJAMADRS IT RHA VERE EPPINLODZ RI MG ODRANWNAREROID BESAL ID TINRG GAENS IT SRULG OR OS DIR ED AESG RESV RI ACWFEOD AEPH MIJAMADR EDL ORS SOZDOTOPEDPA EDL SIMA MUSR NAMEOD UDACWFEODAL RI ZOJA E PIMWFARA ACWFEDEROID IDA XIUFL HEJA RI BA KUEFOTOAL EDL ODSWONAL RI SUPH ED ACRADR RHER HA PIUFL NAEPH RHA SRERA IT ADFOZHRADAL MODL PEWEBFA IT NAPIZDOYODZ SIUDLFASS SIUDL EDL SHEWAFASS SHEWA O LI DIR LAAM MGSAFT RHA TODEF EURHINORG BUR MG ACWANOADPA XORH VERE HES FATR DI LIUBR RHER RHA TIFFIXODZ OS RHA WNIWAN EWWFOPEROID EDL ODRANWNAREROID O ITTAN MG RHAINOAS OD RHA HIWA RHER RHA ASSADPA IT IVODEXED VENERA XOFF NAMEOD ODREPR
5	PSKTJXZFRADBEUYHVIWGNCOLMQ	BICEURI SHI WNECSOCI AL SHI BEROC MAJIMIDSR AL VESE OR SHI LACUR EDT MERSING AL RIFL OR SHI IRRIDCI AL MESRUBEGERHO NGU VENESI TA O RHEFF SNG SA IFUCOTESI SHI MAJIMIDSR AL SHI VESE ECCANTODY SA MG ODSINWNISESOAD BERIT AD LANSG GIENR AL RSUTG OS OR DAS ED IERG SERV SA IPWFEOD IECH MAJIMIDS EDT OSR ROYDOLOCEDCI EDT RAMI MURS NIMEOD UDIPWFEODIT SA YOJI E CAMWFISI IPWFEDESOAD ADI

		KAUFT HEJI SA BI XUEFOLOIT EDT ODRWONIT SA RUCH ED IPSIDS SHES HI CAUFT NIECH SHI RSESI AL IDFOYHSIDIT MODT CEWEBFI AL NICAYDOZODY RAUDTFIRR RAUDT EDT RHEWIFIRR RHEWI O TA DAS TIIM MGRIFL SHI LODEF EUSHANOSG BUS MG IPWINOIDCI KOSH VESE HER FILS DA TAUBS SHES SHI LAFFAKODY OR SHI WNAWIN EWWFOCESOAD EDT ODSINWNISESOAD O ALLIN MG SHIANOIR OD SHI HAWI SHES SHI IRRIDCI AL AVODEKED VENESI KOFF NIMEOD ODSECS
6	GTJFKXWDLORBAUZHVEPYNCISMQ	BECAULE THE PNACTICE OS THE BALIC MOKEMERTL OS VATA IL THE SOCUL ARF MALTENY OS LEDS IL THE ELLERCE OS MATLUBAYALHI NYU VANATE FO I LHADD TNY TO EDUCIFATE THE MOKEMERTL OS THE VATA ACCONFIRZ TO MY IRTENPNETATIOR BALEF OR SONTY YEANL OS LTUFY IT IL ROT AR EALY TALV TO EGPDAIR EACH MOKEMERT ARF ITL LIZRISICARCE ARF LOME MULT NEMAIR UREGPDAIREF TO ZIKE A COMPDETE EGPDARATIOR ORE JOUDF HAKE TO BE XUADISIEF ARF IRLPINEF TO LUCH AR EGTERT THAT HE COUDF NEACH THE LTATE OS ERDIZHTEREF MIRF CAPABDE OS NECOZRIWIRZ LOURFDELL LOURF ARF LHAPEDELL LHAPE I FO ROT FEEM MYLEDS THE SIRAD AUTHONITY BUT MY EGPENIERCE JITH VATA HAL DEST RO FOUBT THAT THE SODDOJIRZ IL THE PNOPEN APPDICATIOR ARF IRTENPNETATIOR I OSSEN MY THEONIEL IR THE HOPE THAT THE ELLERCE OS OVIRAJAR VANATE JIDD NEMAIR IRTACT

...	...	...
19	XTWDVQZLSONBAUGHKEPYRCIFMJ	BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION BASED ON FORTY YEARS OF STUDY IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A COMPLETE EXPLANATION ONE WOULD HAVE TO BE QUALIFIED AND INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE PROPER APPLICATION AND INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT
20	XTWDVQZLSONBAUGHKEPYRCIFMJ	BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION BASED ON FORTY YEARS OF STUDY IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A COMPLETE EXPLANATION

		ONE WOULD HAVE TO BE QUALIFIED AND INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE PROPER APPLICATION AND INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT

Decrypted text result:

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION BASED ON FORTY YEARS OF STUDY IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A COMPLETE EXPLANATION ONE WOULD HAVE TO BE QUALIFIED AND INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE PROPER APPLICATION AND INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT

2. Modular arithmetic
    a. 6/5 mod 11
        i. Inverse of 5 mod 11 is 9 (5 * 9 = 1 mod 11)
        ii. 6 * 9 = 54 = 10 mod 11
        iii. Answer = 10
    b. 3^20 mod 19
        i. By Fermat's Little Theorem, 3^18 = 1 mod 19
        ii. 3^20 = 3^18 * 3^2 = 1 * 9 = 9 mod 19
        iii. Answer = 9

c. 7x = 11 mod 17
    i. Inverse of 7 mod 17 is 5 (7 * 5 = 1 mod 17)
    ii. x = 11 * 5 = 55 = 4 mod 17
    iii. Answer: 4

3. Multiplicative inverse

a. In Zn:
    i. The inverse of 7 exists if gcd(7, n) = 1
    ii. It is 7^(-1) mod n
b. In Z16:
    i. Solving 7x = 1 mod 16
    ii. 7 * 7 = 49 = 1 mod 16
    iii. Answer: **7**

4. Affine Cipher

a. Affine Cipher equation: C = (aP+b) mod m
    i. C -> Ciphertext Letter Index
    ii. P -> Plaintext Letter Index
    iii. a and b are keys, with a being coprime to m
    iv. m = 30 (total characters in extended German alphabet)
b. Decryption function: P = a^(-1) (C - b) mod m
    i. a^-1 is the modular inverse of a modulo m
c. Key Space Size
    i. The key space consists of all valid values for a and b.
    ii. A must be coprime to m = 30
        1. Condition satisfying gcd(a, 30) = 1 in the range 1 <= a <= 30 are:
            a. 1,7,11,13,17,19,23,29 (**8 choices**)
        2. b can be any integer from 0 to 29 (**30 choices**).
        3. Total key space
            a. a * b = 8 * 30 = **240**
d. Decrypting Ciphertext
    i. "Ä Ü ß W ß" with a = 13, b = 5
        1. Ciphertext to numbers
            a. Ä → 26
            b. Ü → 28
            c. ß → 29
            d. W → 22
            e. ß → 29
        2. Modular inverse of a = 13 mod 30
            a. 13^(-1) mod 30 = 7 (13 * 7 = 1 mod 30)
        3. Decryption Formula
            a. P = 7(C - 5) mod 30
                i. P1 = 7(26 - 5) mod 30 = 27 → O umlaut
                ii. P2 = 7(28−5) mod 30 = 11 → L
                iii. P3 = 7(29−5) mod 30 = 18 → S

iv. P4 = 7(22−5) mod 30 = 29 → ß
v. P5 = 7(29−5) mod 30 = 18 → S

4. Plaintext output: "Ö L S ß S"