BLG 520E - Cryptography

1st Homework

Valentin L'HOMEL - 922110009

Note: All source code and the original report (as Markdown) are available on my personal Github.

1. Cryptanalysis of S_1

Method for Autokey decryption

Deciphering an autokey cipher requied some knowledge about the language used on the cipher. On our case, we will use exclusively the appearance rate of bigrams (combination of two letters) for English, which is partially available on my Github repository.

Checking the language of a text is actually perform by comparing two text. Rather than checking its language, we keep the text which is the most likely of the desired language. In that end, we give a score on each of them. This score using the appearance rate of bigrams, as mentionned previously. Since we know both text have the same length, the number of bigrams in them will be the same. We can simply sum the appearance rate of a given bigrams times its number of occurrence of the text to get our score. The highest this score is, the most likely is our text to be of the given language.

Autokey cipher is based on the usage of a key, the autokey, of a given length. The first step of deciphering it is to find the length of this key. Sadly, since this key is only used once for encryption, we can't rely on traditional mean, such as the Index of Coincidence to find its length. That means we have to test several possibilities, until one of them give us a text which seems of the desired language. On that end, we try generating a key of size 2 up to 64, and only keep the one giving us the highest score for the given language.

Once we know the length of the key, or rather for a given key length, we need to try finding it. By definition, autokey encryption encrypt the plain text, first using the key, and once every character of the key have been consumed, using the plain text itself, starting from its beginning. This means that after deciphering the first character of the cipher text, we can–have to–use it to decipher the n-th character, where n is the key length. The operation on characters is a simple mathematical addition, modulo 26.
Since we are using bigrams, we need at least two successives characters on our deciphered text. So to begin, we need to check all $26 \times 26 = 676$ possibilities for the first two characters of the key. With them, we can decipher the first two characters of the cipher text, and using them we can decipher two other characters, and so on. Finally, we can score our partial text, allowing us to find the most likely first two character.
After the first two letters, we can search all the other charachter one by one, by checking all of the 26 possibilities for the given character. Aditionnaly, we can restrict our scoring method to the newly constructed bigrams since the old ones will be the same for each of the 26 possibilities.

Application on C_1

Applying the method described above on the cipher text C_1 present at the end of this report, we can successfully find a key of size 6, corresponding to `OLIVER`. After comparison, it appears that the decrypted text is the same as given the plain text, with the exeption of an interrogation mark (`?`).

2. Cryptanalysis of $S_1 \times S_1 = S_2$

In order to check for the idempotency of autokey, we need to encrypt our cipher text another time. To that end, we have decided to reused the previously found key `OLIVER`. The second encryption, which have been performed by an external website results on the cipher text C_2 present at the end of this document.

When trying to apply the previously define cryptanalys method, we fail to find an adequate key. The resulting key is one of size 62, and do not produce any good text. Even forcing a key of size 6 failed to give us a proper result.

However this result is not unexpected. Let's take a very simple example. We will use number instead of letter for the ease of understanding. We will encrypt $[2, 5]$ with $[1]$ twice. The first one give us $[2+1, 5+2] = [3, 7]$ and the second $[3+1, 7+3] = [4, 10]$. Now we will try to find the corresponding key which will allow us to get the beginning of the plain text. In order to go from $[2]$ to $[4]$, we need the key $[2]$. So reversing the second cipher gives us first $4 - 2 = 2$ for the first character. Now, we need to use the first deciphered character: $10 - 2 = 8 \neq 5$. We can clearly see that it is not possible to retrieve the initial plain text from a twicely ciphered text in only one iteration.

We can say that autokey cipher is NOT idempotent.

3. Cryptanalysis of $S_1 \times S_3 = S_4$

Method for Autokey $\times$ Permutation decryption

Deciphering a combination of autokey and permutation is doable, with a slightly alternated version compared to previously. The first step is still to get the size of the key, supposing both key have the same size. Then we need to decipher the autokey encryption, before handling the permutation.

For handling the size of the key, the same method as explained previously can be applied. I will not talk any more about it.

Deciphering the autokey cipher is no longer possible by checking the bigrams since the text is shuffled. The only solution is to check for letter frequencies. Just like previously, we sum the probability of a letter and its number of occurrence to get a score. For each character of the key, we try every 26 possibilities and keep only the one scoring the highest. That way, we can get a text encrypted only with S_3 and the encryption key of S_1 itself encrypted using S_3.

In order to decipher S_3, we will once again use our bigrams. We will try to get the most likely following character for each character of the key. After trying every possibilities, we keep the one scoring the highest. We then choose the combination among the selected ones which scored the lowest and use it as the last character of the key. Then, we can reconstruct the whole key by combining every other pairs.

Application on C_4

The cipher text used on the first part (C_1), has been encrypted by an external website using once again the same key `OLIVER`, which has to be translated as `[3,2,1,5,0,4]`. This new cipher text (C_4) can be once again found at the end of the document.

Applying the previously described algorithm on C_4 can successfully give us a key of size 6. The key for S_1 first found, that is encrypted using S_3, is `EILORV`. After the second part, the original key for S_1 is found `OLIVER`, as well as the decryption key for the permutation `[3,2,1,5,0,4]`. This second key should be understood as the first element of the plain text is at position 3 on the cipher, the second at position 2, and so on. Using all that, we can successfully reconstruct the original text.

References

Plain text (Original)

```
TREATS OF THE PLACE WHERE OLIVER TWIST WAS BORN AND OF THE CIRCUMSTANCES ATTENDING HIS BIRTH.

Among other public buildings in a certain town, which for many reasons it will be prudent to refrain from mentioning, and to which I will assign no
fictitious name, there is one anciently common to most towns, great or small: to wit, a workhouse; and in this workhouse was born; on a day and
date which I need not trouble myself to repeat, inasmuch as it can be of no possible consequence to the reader, in this stage of the business at
all events; the item of mortality whose name is prefixed to the head of this chapter.

For a long time after it was ushered into this world of sorrow and trouble, by the parish surgeon, it remained a matter of considerable doubt
whether the child would survive to bear any name at all; in which case it is somewhat more than probable that these memoirs would never have
appeared; or, if they had, that being comprised within a couple of pages, they would have possessed the inestimable merit of being the most concise
and faithful specimen of biography, extant in the literature of any age or country.

Although I am not disposed to maintain that the being born in a workhouse, is in itself the most fortunate and enviable circumstance that can
possibly befall a human being, I do mean to say that in this particular instance, it was the best thing for Oliver Twist that could by possibility
have occurred. The fact is, that there was considerable difficulty in inducing Oliver to take upon himself the office of respiration,—a troublesome
practice, but one which custom has rendered necessary to our easy existence; and for some time he lay gasping on a little flock mattress, rather
unequally poised between this world and the next: the balance being decidedly in favour of the latter. Now, if, during this brief period, Oliver
had been surrounded by careful grandmothers, anxious aunts, experienced nurses, and doctors of profound wisdom, he would most inevitably and
indubitably have been killed in no time. There being nobody by, however, but a pauper old woman, who was rendered rather misty by an unwonted
allowance of beer; and a parish surgeon who did such matters by contract; Oliver and Nature fought out the point between them. The result was,
that, after a few struggles, Oliver breathed, sneezed, and proceeded to advertise to the inmates of the workhouse the fact of a new burden having
been imposed upon the parish, by setting up as loud a cry as could reasonably have been expected from a male infant who had not been possessed of
that very useful appendage, a voice, for a much longer space of time than three minutes and a quarter.

As Oliver gave this first proof of the free and proper action of his lungs, the patchwork coverlet which was carelessly flung over the iron
bedstead, rustled; the pale face of a young woman was raised feebly from the pillow; and a faint voice imperfectly articulated the words, 'Let me
see the child, and die.'

The surgeon had been sitting with his face turned towards the fire: giving the palms of his hands a warm and a rub alternately. As the young woman
spoke, he rose, and advancing to the bed's head, said, with more kindness than might have been expected of him:

'Oh, you must not talk about dying yet.'

'Lor bless her dear heart, no!' interposed the nurse, hastily depositing in her pocket a green glass bottle, the contents of which she had been
tasting in a corner with evident satisfaction.

'Lor bless her dear heart, when she has lived as long as I have, sir, and had thirteen children of her own, and all on 'em dead except two, and
them in the wurkus with me, she'll know better than to take on in that way, bless her dear heart! Think what it is to be a mother, there's a dear
young lamb do.'

Apparently this consolatory perspective of a mother's prospects failed in producing its due effect. The patient shook her head, and stretched out
her hand towards the child.

The surgeon deposited it in her arms. She imprinted her cold white lips passionately on its forehead; passed her hands over her face; gazed wildly
round; shuddered; fell back—and died. They chafed her breast, hands, and temples; but the blood had stopped forever. They talked of hope and
comfort. They had been strangers too long.

'It's all over, Mrs. Thingummy!' said the surgeon at last.

'Ah, poor dear, so it is!' said the nurse, picking up the cork of the green bottle, which had fallen out on the pillow, as she stooped to take up
the child. 'Poor dear!'

'You needn't mind sending up to me, if the child cries, nurse,' said the surgeon, putting on his gloves with great deliberation. 'It's very likely
it will be troublesome. Give it a little gruel if it is.' He put on his hat, and, pausing by the bed-side on his way to the door, added, 'She was a
good-looking girl, too; where did she come from?'

'She was brought here last night,' replied the old woman, 'by the overseer's order. She was found lying in the street. She had walked some
distance, for her shoes were worn to pieces; but where she came from, or where she was going to, nobody knows.'

The surgeon leaned over the body, and raised the left hand. 'The old story,' he said, shaking his head: 'no wedding-ring, I see. Ah! Good-night!'

The medical gentleman walked away to dinner; and the nurse, having once more applied herself to the green bottle, sat down on a low chair before
the fire, and proceeded to dress the infant.

What an excellent example of the power of dress, young Oliver Twist was! Wrapped in the blanket which had hitherto formed his only covering, he
might have been the child of a nobleman or a beggar; it would have been hard for the haughtiest stranger to have assigned him his proper station in
society. But now that he was enveloped in the old calico robes which had grown yellow in the same service, he was badged and ticketed, and fell
into his place at once—a parish child—the orphan of a workhouse—the humble, half-starved drudge—to be cuffed and buffeted through the world—
despised by all, and pitied by none.

Oliver cried lustily. If he could have known that he was an orphan, left to the tender mercies of church-wardens and overseers, perhaps he would
have cried the louder.
```

Chapter 1, Oliver Twist, by Charles Dickens (1838)

Cipher text (C_1)

```
HCMVXJHWXHXHZFVLAWPRGSHPZVVHHQNXNTOJGKJAFECWGHRFWWVBQUBRPWQKTTGGRVIGZLVVJVXAPSNWEZVTTSEVIUSMTQOJWLKOAATQIPKJBNIPXFPNEUBQDSKYUCUDFVMSBLJMTOWYDJXLZFO
FRIKIUISKTWEJWFMURSKWAZMAZIBQBBCHVFAWSPTNHAOQRYNGXQIGVHNWWLVTUSNZRRQMLVRVEVUWRRTYAKSZFZLVCYAGGMCIBKZKSWGGXJQAEZKGIIELPCNSAOQGVKURCFXHVVEBKRPGQGVGHG
VGVJOFBRRLOADGAREJKLCAMJLMFUWGXVRHPEXDMMFWJFMJIAJTHZRPWMNKUAKUNEHNTMHHNBQSGXVPASUGVTPUWSAUIJIXUGVXOWLVZRTKMJAGTNMGXMHKFIXBUITMSBNPDWVXNEDXCIVMWFVJU
HVFOQUHPPHZAXLWTSAWCRQJQPTUXTBEIKXOWVJALIVQMTWBWTMOGTPFSUKIXSNLMMDMTBTWLAAARWXAUXFXKQFPCKSLGBGFCUCBSBUKFKUOOXSMNIPTBPBZLHUIOWVFCKXIANQGVHMMIGXHRAFV
HRJWIGFNTTHHFUCEAKSNIXNALXJLZEKAQBTOVQFPTYWNFWMVVTBZRADENRNLXMNPHTNPPWZMKAKSKSUXEZSHYSNLTAMBGVHIAOAVHIAUELXZEFXTSAVEAAITUFAJYCKNZZEGWEVVESDVIWXKSPP
FWALYABHBUGVPQXEOUSPLZBZMQWKHBXYEQTJPRIGYWEEAGNSHFWJYARZSZWHSVLLWARHLAMUNFDXUQRJESRFVQGUYIIUBYMJSZQALGOAFNSMTUIZLAILHCXWCSHJUSTFFQPMKOTPURMKMHREQGX
YEECKIFFTHPEUJOEAOARHIAOFGAFSGSBHAHUALIECCLHLLDASMQMOUNBUTTBUXIEBGNFPVVVTBKFESUOQGVSZWHAXAWTSBAWQZXMMSDHMGFHVTHQEGZINEPRXQRDFQUBRPWQLAAGEEGWOLUIOAM
TWNBWJBLZMLYBLCZGVESURGVWCEEYGAOLILMOILXNKAQUJLRKQPMEAEKRAMWNUXPXXEKMALJRYYHYWYOASIHHQNXKAWBUHNSDUADIDVJZXZALGIIGMHAJUMVSFVBVWEFMPWYHCMBZXYEPTZGFRO
IVGFNTTHHZFGTGXTYDQPCYWSKVVTRFKDRXHZBVOVNDHNRMGHSYMBTWSQKBJICKWMUTWWRXADVRTKWIOLXJCGFAVSQFMRVBWMWPIXBBQUGQZBQTJUKKSZKEJVHAHGVWVNVAXGGUICTGMYOMSLCRZ
MSGHSQVSBPJHZESTIEIKKHWAILMOFPTVZHYEQTHVVQFEHTOESKTKLWJLNXXYRFYCFIIDPBQSBOIHOXAEWABKSLSJRKSHNRAMALRFXETUGFBPIAIHFGQQKGPAQQJDGMCETFOVYCOYMLVYOPBJUHF
EVLWBZAOXBLNHFIQSIDPZDSUVLLWIVUSXSVSHFXVUPSPDVHGSNGIESXXUKHRUEOGEMFMSNRVHMWXJRKAIKRIUVYEUIVNHUVSUTBUVCHIFFXCZCUKNGXBPDMORIXKQKGNTQQJAMIOPTIGDJYBUOL
BNEFZPTVFMCLNFMMPIQSVYZXLURGVXZQFXPRXRPFWQEOMICZCWCYPQXVTRVJXRDLXLSDOYZDCIAFNLBZEJVHEDXYIUDILACSKIFNLXMNGYQWZYHADNNPCBBRGVOSEETRRVVHHUIOWVFQYUHWQOB
QKUDLNGYEBRVSELSYEHBEZVGKOYLIEKUEHSONAYXTINZOXDIBGAFTHERXOXAAQXUXYIENSXNEKNSTPAXMLRTFJPWKRZKCDXJIROGIJPCMVXYFUWNXLDHVNRHOVRCRHSVRVSEGZHKHIVZXFMPWMG
ATAIABRTAIOCWDOSQGVDOSZSGMVJFNGPPZRQIJIUMLRTIEZVVSQSWRLGECFXKYEOEBZLQYJMLAJLYYITAYUOSAUCMUVCQLJDJGOMZQRFLQVNVFMCLNZBQIGGIAUVQFEPFCSUNRAYXEUTHNWJVHI
EHADHTWIFHSVGJLZEWJJKFULZJLJUHTJHOAVTEIRIIIFJFIOYHVCOZAGYDDNIIFXIIOIHMTVFLKLEZBULXIEIAXTUMAEWEHUSFEMMEJULDZXYOSAMKZBHWWFXHUKVSKFJXHRIGVSPRUPTHXSEOH
AQGYISNALSYCGLVOADRDEVRSIVGHRLZNLPWZKCYALWUSCCQPMFRMAPLGNSDVFGIILJHRBHUMLXLHUNZXAEOXMEREZJFYQYBLWMAUACWGDAVOEVWEMTPBKVSNEFJGWXEVAPVOLTWIAWVTIKRBHDM
TJMOIPPFVVBNSLRMMFNSEPSUWZPAHDHKPIMTIULMEKEPKLTHTUHVCVZLSFBRJFSRUSLUXMAYEBMPUOONTJLBMWNGHMINNVGLHDEWLJXNMAQEKZPZXNRFZSUHTEZOSKASDAEPSNZAIGBNOTVLOAE
XPPNSMLPWOMGNAMAUAYLCWEUWGCCIHRUOVZAAFIQBTBVPRHXRLOIBHVSPHWLLHURNMDPZREICAGKNREAZOTUMDKIXLNZBQIGGIADJJBQRVDVCYIZRBIFNSEXOUHUENYJBARHRTBXZPXDGYFCHWS
YLVDVTEVMNKXEDWFXHKWSFYULLLNMKAPFDWIWDGWMCUAVAMEVWPRIKPUTOIGGRRWWOUETDWUVXVZRMLRVGBYAUBUVXDLPCKTLIUTDTXMAZIFTKBXVRRYWKUIMELXUXNIWMFYSCMQGSLQKJZRDGY
FCHWSYLVDVTNOINJAAOEFDPZLDSDTJRJAKTVNBEKQYAIHZIUTULYTHXUKYBPHEGUWQKVVBKSHRUOHYOAHMOPOQIJFIPWXTQECWMDSMVQMOIICEDBWSCKRGWOPXSXOFVAMPDGSNULTGXFMHKRHBB
NDLOGENRILXOSFFCHWSYLVDVTKOMNBPAHBVDEZTHJXIEHHIIRFVXYIJTKIRVQOXRGCYAVQULPBBUSNIAYKLVLNMGZWDCHBJMAEKGGCRXZNTSHTUJXVJREDKVWGWRKGXPMNXVNNXCSGCPXEULNUL
HKMYXHWXXMJTCMBLRISAWSXAWYVSKKEEKWTUEGFZXUSNVOIUVUGKXFDAEGLHDETKAEKXJLAFUZLSFXVVSGVWISWLQGLHZTZZZWYEZYHJPRBQSYMEVSOKAYKHPOEWAIEDAXGCALWTMBNBXDDCEMA
WFRGEZWEGWEJZEQKWFCEEKWFAETLKREEFAOLCPBNWFQOQYIXQHJLXIHPCFDHOLYEDKODGKHGGKTMIBJLRGVHHWKIRRDKTUDGHEPYHLFGIELWCFHHKLBOGHRWPHVYCGTZHWHYITXRERIBHFSYTHO
SKQDQFBUVHTJMYTWIICUSWSERTWKJTBUPFFZWHDOYRWOWRXCGOLZZXMFTGFGCPFFWSCUZLSFUKREGGAAAOGKDLPFGFLXIJKOQWBZWNCULLTVWBARVCRDPRIIGDVJVVVQFJXUFUKXPRXVBVSLWKN
CSSEQTUEZRGVYIWYEVAPADSSOTGGWIVMCHPOHNDMHOGBXEKTQVZOHPFMFXREVBBNZMRGFXZLVQYYCWWZKCUMVQGPNEKGTPMDQWIAIKNCULLWSCUZLSFJLZXWAVIGAQFMZBCMKCTHCKJAIMKKCMB
XUEEQPRZTLDSEGEAFICWTBGMWJJXPZZFCPXJCGFRMNSUXGTDXBEERZNXWMLZNMDPJXNBGULXMAOGHVVWANSVQVBSLPRHFBLPHFSQZQVAOLAWLDEBHCKHHGSRJHHZEVSNSKDDOUYWQRUWBTGUUEY
PKSREKWYIFWPWMVQAELJNOETYSQGZUYSLKSTZXEMRHLKRXRPXUXWPWPGPVQOYEUHTEBWCKZISMWFJHIIKVVZEJXVYJDDDWHTLYRPRYBEXLXKAVLEWOHPREGOOXOHLKHMRFMXHRUGVXVFLWNWYSA
GNRKSLWVPXGQCXYLWSYLDLGRQWMVQMAVBYSDSJDLARWYVMJGLUBWOUWMXBPKVRRRGQJZLSFFVGRSQZZEEXKSWSURHREFDGSRGKHMDIIMOEYHYALOYGLASFJKWLOZBZLSKQQYOICPRGKVGDIDGVB
CVLQOVYVMMNNOGSHNPMVHWUMSLWBJEXKHVVLPSEAPLPWEQWWLIXRDENLXFDVQGLVNHULLLNPZFKVNXMZUFRCTBZZIDWTCAIOMXFLLPLKSXUFUKXPRTOMWZAFOGDZKJQUATFXGMOZVULJTZVXHRIX
ISCRHSVRVSHUIVLHKVMFXTUXEUFTNGAECXLYIKVIILQCEILFFWPTCBXYSURNIJGDRLRYGJWPRXHHQNXNTOEJTLPWZZNIWIETNGRIUHHVMLAWKPKAOEUAWYVVDXRMWJAROFKGJRCGPUCIDQTNALM
DKIXLNOLFGLVEKSHHVZEZJMNBPCENETURRJXCUUCLAWJYMHLNCESHJBYTYHMOLZOXPEMZZMZEFZWKKOUGZVTGZIBREVZQSUMVWZAWMJHKOIMFFBNLWQVMGQPWBRHUUBTGVAPHSXUZALGTRYMYHW
IRTQVHPWNRTOMMUKYWDLZWKOTVDNBKCZKJGRESSOIZXZIJVUGWLVRIUFHHCEVBNGZMFKRWXLCXHYIOLVQYSSTACEOJMSIZNEIAIOEKWHRHZTVAJLWCSAHRCWPDOEYMOQGVDOSBMQUSIOUXGDXHR
GJVWRLYKHWFVHIYYTFHCHIGYIFRWFXYMVHYJAAYSQUYEKHAGGTVHHTNIDPDOBPTEIRGQGGWRHPJVJRVQCQZHCWJBMOJCXAMNMCQKLCJYVQVWIXRNHDRPHSTUSNPZAAZVUATBELJMXBWLVFIEFMV
ESWEPYJQMYHLUGUOAEGSIWRFHSMWGWVLRHHLVDOJDKLWJYNUPEYXJVTSXWLV
```

Cipher text (C_2)

```
SJAHBUOYJCUQGBSSXDOWBDHLOMBZOFMSIAVZTHWTTNIGPHWJYSBIHZXNKXGEUKVCHFBZFRMQRBWLKNWRBZKLGOIUDNLEXLWDOXDEOJPBSDKJUDQEHOQAMJYVSFOSVSXVPTGUVOOHFGXJMVQZVDR
OOTJNINJSDEYROPFQVBGBMTDSJEBPNBBPWVBXUWOSHWGFKLUGLGZEINKMERQAHOJKMKKEYUIMUHFRIMXTUGJQYXLFUXFFRHEGBQFWUEHQWTIWKFHPYIIKZIVAEZFIICUFSLSRPMGGHYKBUHFXWM
LMQPVLWXMUCFEXRCSJNRCRQSVXHUIPIHWBLKUYDTUAGIYVNWSYTIZPFFUJLPGGAOBNDGULUOJENEIQQKADQIPMQYVNXDEPUADGWTFBUOHGXEZXMXYPXSAXROUNBSYUPCHXWINYATGTXFIQZCXRP
TRKJZOOKUVPUEALARATNNJBQLVLNCRTBEUHXZRKIWRLVTHJRJYHCULYEIQBMXFFWUAEGMFIOMTBKSIAUXWTHQZMHHCBLQIPUFICYGWEHLMPIHXWHWDQTBOHAAVXPVGMWSLEVSSQSPMZYMSODMNB
EYAWNBMECPPNKHVXHRXHKBNKDKRIMEVXZMSSFQVQMMRDKLFTRGGVDVYXOQELAQAGUEKBCLGFXPZOJEEXORCZSPRKLHKTTGAIMPGQOQAIEGEHEZBEPZZJXTATPJAJGVESZICIGRUUIYZZDRBCVKX
BTKDNPGDBFEVQXYYUPHFIDPTEFHJIAJOAAAKMPMWRFTVIMLOLJWPLSYEOIUHJUDKSHJCWLIUEMOXGKEOHPLVMZKMPNDKHSKRATRYXPGZVNDSHUNMDMBFPBIWKDOLROVXMZJEDTYFJDWYFWLVCQJ
FVISQFDJXJZMZOHLPSUAVMACFXHNSUXHHFZASMPEJWLSTPFCDTBXRUFNKFHVHYCXUHHCXZWBGGZAZNNPALZKTKXGSSVPZBXWMSPNMOTGJSRZYATWJNUBUUTXWYEHUHRRISBGFBRVAURWORYMUWA
EQVPWVUHMNHHCWBLRTFDWQMQAUYVEBWQPMJSOWWFYWOYFGYBKGJVPROAGMQWREOPJTREJPIGVIKHJFPMYZGDFENPSHDRHEXSZVUKVVYDZAHDGPHFFMSGRCSHZFEVHRWKHQRULHYQVVFGBUYDDVD
BUMKEHBCNESZMNESDJJVZRUVAKXRNXUYMQYELYFSUCIIFHTKZLDNZDKOWCCEUAGNDBYGNJUWRNKHWLJCQTYOTLSBSLRRQTMRIGDYXNMJONACGNPKJLISTYTFZZRKERCNCGSCBHDCQMSSWOLROPN
YKRJJPHKHWBXUWTIRLHOCAEEQVWVBPBGLVDTJOGCTUVXOOJUXOADZABVGHIUAQLZCGZINDVAJRXIEPBSEHPHSPOJSUKSFARWSSEWXQTFXKYTBUOMGVYQSNUGGGTJVMSUCIUHAGHDAGTACNNUPFT
TWUQIEEJIXMMHTFRDVKUHTKCYAKZAPPDIODNBXUNPHZUAQBVKCJDLYPKASLJRBIQLDZQGTVHMYOKAMRMEHAZEVGOLQPIFYPAPGIOQUBBGZSEGKZPKIWDJNZUOJMNCYXVQAGTGZBEFCISLXNUCUO
KLFZNAUIJRBAGARYRTDXHKOFBMMEUUKKWDKOWHUCLHBFBNYPGKOGRPZRVPKZUMWCSUPURJWOULODMODHEOISFCBHDBHLIYKMNQQNNPWVLLBTLLNYTJMNJBEETKQTFVZMFNZLALZJRCMKGIDRVEZ
KRQTZOWIYECIYCPTPZZFPRTKRPCKDKUICSASXUCELWAZMUWQOFOCWPFXXTQHEHUIUYIUKMULMOAKQCEHZDKIFGBHBKETRZHAHBQJFSXTABFHUWIIUJIBRAOSRCMPIOGQIXJLYUYFZMBYEPTXRLD
FFPEMHRMAQODNWOAEIRGCKPYBPJBEFMBKIWDOYXTDBZCQYLGMLYWVMGYUUBOVEIQJYJJUMNNKLZJHKTTJJSMATUAGINCKNVXEIEXITALZCUDMKXSGAUGCKRTHBKDWLMPZXIZRGFAPYHKHLTNPAP
RDJYOBAPFKZOCRQGWRPSVEYHISVOOSSSSXUCMNPFIDBJRWQWGMEHWNYNTFRMIODALVWQMJBDTTRXXUGFVIMDJUIQCQIETXBGSJAQTYBZPPLBHIDDLHXPZWIPWIBGRXHMDHCJSLEPWICVOZMJYDA
HNYCWZNQRQGUTLGGYFXOZJRVZYKCIDHIRWNKJPJPHVEUACBLGXTOQEXLEEDKQMVAOEMXJPFVSOMOOZKULLIKLBRINGRCHCAUBKQSBNSSDUVQABZEHHTWGZEGTGTBOKIAJVRLPOWXVKGMESRXCWU
DANVLBIOHJJCHQMHNSFDVBEZJRTPZXDJEITWPEAUQDMJVXXRXJRGVCSFZADMIQKWVJUZPDUQPVJBUMSOFYFPAJGPSNUJABNXPQRRRUEQQWBNHMBZNRBEORRUKJYGMRTWCOWZSFCAMVTANTDRPNS
QKABSQIELBESYPIOGGLLOWYUUREYMBNAQXHHRZWLATBAXHIQSGDZIEMDDPXSGZJYJXOWTIRUFPFBRZGAFYGLQDJWQFZCLYFRTHBTRPHYRYMEDOZUUWKDVRVYWZUMIKMDIUVUPCCXQWOWHVEREZY
WQXKRLCGHQFQIYISHEOZOKVBVHDSKELAQQISWSLZIKQDBWYGPWKRUOKQIFQQVLKKEUAVKZSIPBOCNGGOQFSKLLWAWVDFQWFQOTJVNMIUUSLYQWBWDWKIXHPZDCHHOFZMHJZVFKICLQDSWZFJOWI
OBYZYWQXKRLLZDQETNCMSMPZZHXGIICMSNMEEKEUJTNJLJYSTCSXBBQOVWUWEYQSXFRZBVGIRMPPRQVRBAVNCQPVTXDMFCVMRSJWIQXMYRAUXUPPEAEOUHSGRHJDKTKXEMRLNNGAWMPSGSDXEGN
UNCVHFAUTZDSFWNNEKKDQXKRLIZHQWIKVNIETZAIEAMDAORFZJCEGQAYFFPDZHHZXXOOSHANNBWKMYXBZEDITNKQKROPTHIIDGRHPORBJTZUYQTWQNQKYMHQFXAUUBTVIEHBKCJPPBPCUGMRPJI
LEXLRSDHJKGAYJYXABUMXDOIOYRKHKACFODEIKPVQOWTANFONHBYFZYUKQIMGEXQLLNBCVAJEWUDFCPUDYATDNORLCTZVEPFKDXXYXGFNVAOZHBVWIGIMCFZDYEUKPTRETGKEOWQSDNMTWPDRNX
ZITKQZSJXCIIVIWGAOBIUUSKCIXVGWEIYLYCGTGNKQSDRLECGVZJFFXWLQAPVAAJGRCOEOKQUNZWPHPVKSDIQHBOMYKGDCUXKOISKRMKXCSHHLPLVHDTNOBHQVBFTCIGCUJEBSENLPQUEWWPBIV
XCOWXTTELKJONSODBROSLSAMTNOGBXSNLPOSXBSTDQSVZFVTCCHQWZSTEFEDOUYLBYEJEQOXWEQPYLUKRSMQDLPTMPOIXOQTBTJIGBSQMKPIYVLCOXNEPIDKXGKADDBTASSPAKPGMLCPLSHCTFO
XKDAAGWWRVWOSMVPKQYXWBWNOIGJOAJFINLWCZFTWCNOAQRHWWWSRIVHELYTANGKQQMHGKYXMWDVBHRPIAWIRPQRHQFWZEZHACBPUNDYCLTGFEOKWOXLFYIOFETFXMFHHHCCPOSIEWTCBTMULMJ
JEOGCQOTXPTHVFXLIAGCXBLUYFCYVLVOLMMIBLHGJWUACXFQPVBKKCKYAQCYAJZBUWANJJUUZBUASSHWOTZQLRBFDKHCGTWEYMXRKFCFGBZMGDSMHYVKLHZTTOOFWMBUZJHYGHQGTUIQZPWLOAZ
IQMLIILIAWAZSKDVWTHVIEEXJBDUDNWKBQRNXPPWJAKHVJIWIEOTGLMAMRFKNKJCJSZAWRSMTIYPIPAUGAEGMRHQTIHMARFCOBULYRMCOAOIBZIPTYHKCICCVMFLRYVJFMXHODLLHUCWFCITTXL
CANIKLCIGHYBYSNICIAIBWCJOHPGWDQRNTIPSEEJSUOHYXJXHSWIXAHGYXDERDOSVAEQCJLVEFCKVEUKVPARVWYORJAXXXZIKPKSVZOWVQBPGMZSWNJADTHQHLGEKJHDYPRXZAMFHEYDISZJQQH
FDOWJWAQXDBJENTACABZDHBEGDXDQPVDWEPMCLVKWEOIQLHAEBHZAYTUWGZDRIAQCKRWGAWTQVGAMLEEAEZFATEZFPUBZQRIQHLTDXHXIFUFUPMLYIWTORYCSZYKOEADSPGWGOSARRVHYQRSABW
DPJIPPDJXJOMDMGZRPUAIAESQZCMHDEYHQYEIOXFTJYMZQTQVYTBNGCUHNTOFHYXIYZHMMNAIVNQMCOKAVUWQYIKDIGTLEDSAONQYAUBDTUDRKWLOAEPGYJZXXNKREDOFRGPJIQLZALZFWIHCTP
TDVXWZRVNDWISVXNSQDORQTIATBNZRUJTVWBVOLTUXYDSOSLJLCEOUOAXQOVPJSMEBSXYNJOIRYVWJSZFVFDUTOAMXBYYTLQQVPSQYEDJOEYOMLBTIVANTBLMWDNKJXUXCUJILDPZPSYQLXMJNP
ZPFOCDXNGHOVBIHBRKPXTGIKWGCJLYVUNWHBGRCXOQBRAXDTDVTEMCABSCTMPGUNBQALECWXHHYUFZNSXWAGEVSCGBFSKDBNUSQNROEHZVDDRHASVVNAQCYYHDVVAIDTUZBAGRSLXGAPGNAVFVL
DPYTYCETCSWGFSFUYAOKFGZDPHYELVGRMDDGYMTZODYEIZQAEXFOHZTBYWKHOXWTLFHFZKEINFPBFICFLLIYXMLRLVLYGBYBVENKXPVALAGYRVMDCZZMYFAXJCWRTURIJZTBDGDMQCAWERFFBXQ
JAAJBTNIICWJDWGMHPAYCKRJNKUSXBCDDDNHQOFQKVGZXHQEAAHVWPIWVTUQ
```

Cipher text (C_4)

```
XMCHJVXXWHHHAVFZWLHGRPPSHVVZQHONXNJTFJKGEARGWCFHQVWWUBQPRBKWRGTTVGVZGIVLPXVJSAVEWNTZIESTUVOTMSJQAKLWAOKIQTJPXINBFPBENPQUUKSDCYMFDUSVTJLBOMXDYWLJROF
ZIFSUIKKIWEWTFJKRUMWSZMZAIACBQBHBSAFVPWOHNTQAXNYRQGNVGIWHUVLWSTQRZNMRERVLVVTRWUYRFSKAZZACVLGYBCMGKIGSKZGWEQJXZAEIGKLIANCPOSUVGQRKVXFCVHPKBEGRHVGQGG
OVGVFJORRBALEAGDJRMCLKJAWFMLGUPRVXEHFMDXWMIMFJAJRHTJPZUNMWAKHNUKNENHMTBHVGSQPXVUSATGAWUPUSUIJIGXLOXVVWMTRZJKMTGAGNFHMXIKTUBXMIDNBSWPDNXVXEWVICFMVUJ
VFHPUQOPHLAZHWXCASTRWTQJQUPIBTXKEJWOXAVMVILTQMWBWOTSPTGUFNXIKLSTDMMBMALWTAAUXWRXAFKXFPQGSKCBLCCFGBUFUBSKKSOOUMXBPINPTULZBIHCVWOKFQAIXGNIMHVGMFRHXVA
IJRHGWHTNFHTACUFKENINSAXZJXLELTQAKOBTFQVYPMFNWVWRBTVAZNNEDLRHNMXTPZPPNMWKKAKSSSEXUHZTNSYALHGBMIVHAOAIVXEUAZLSXFEATIAEVTAYAFUCJEZNKGZEVEWSVXIVDKWWPP
SAFHAYLBBQVGUXPPUOELSQZBZWMYBHKEXRJTQIPEWYGAEFSNGWHZAYJSRVHWZLSHAWLLRFUMADNJQUXERQFRSGVUIYUBIZJMYQSAGLAFOUMSNITLALZHISWXCHCFSUJFTOMPQTKKRUPMMGERHXQ
KEEYICPTFFEHAOJUOEAHRAOISAGFGFHHBSUACILACEDLHLALOQMSUMTUBNBTBIXUGEVPFNVVEKBTSFVQOUSGXHWZAAASTWWBMXZQSMFMHDHGEHTVGQPNIZREFRQXQDWRBUQPEAALEGUOWGILWMA
ONTLJWBZBLYLMCBSVGZUECVGREWOGYELAIMLILOQKNXUAQRLJPKKAEMREUWMAXNKXXPMEYJLAYROWYHAYQHISNHBAKXUWUSNHADJDIDZVGAZXILAMGIJHFVMUVSFWVBMECYWPMHEXZBPYRGZTOF
NGVITFFHHTGZYXGTDTWCPQSYRVVKFTHRDKZXNOVBDVGRNHHMTMYSWBJKQSIBUWKCTMARWWDXWTRVIKCXLOGJQVAFFSWVRMMBBIPWBXZGUQBQKJTQKUJKZSVEVHAHWGXVNVGATIUGGCSOYMLMSZR
CGMSQSHBVEHJPSZKEITKILAWHMIVPFOZTTEYHHQEQVVHFKEOTTSLWLKNJFYXXYRDIFCPIOSQBIBEXOHWALKBASSHKRJNSLMARRAUEXFGTAPBFIIQGFHKQQAPGJQEMGDTCCVOFOYYLMYOVHJBPFU
BLVEZWLXOANBSIFHIQSZPDUDILLVVWVXSUSSUXFHPVHDPSGVEGNSSIHUXXRKEOEUMGRSMFVNJWMHRXRIAKIKUYVUIEVHNVSUVBTUCUXFIHCFNUCZGKMPBXODQXIRKKQTNGJQPIMATOYDGIBJNLO
UEBVPZFFTFLCMMNSIPMVQUXZYRLQXVGFZRRPXPXOQWFMEWZCICCVQPYTXRJVRDXDLXLOSIDZYACZLNFEBDHVJXEIUIYLDISCAFKNXLNGMYWQYHZPNDACNVRBBOGREESRTUHVVIHQVWOYFOWHUBQ
LUKQNDREYGVBYLESESVEBHGZIYOKELSEUKOHTYANIXDOZNIXTAGBHFXXREAOXXQAYUXNEINSTNKEPSRMXATLKPJFRWXCKZJDIORIJGXMCPYVXWUFLNRVHDHNRRVOHCSRVSEVHHZGIKMXZVPFTGM
WAATBAIARDCOIOWDGQSOVMSZSVGPNFJPGJQRZIITLMUIRSVZEQVGRWSELYXFCEKLBEOQZAMJYJLTYYLAIAOUYUSCUMCQVGDJLOJFQZMLRFNVQMVBNLCQZAGGIUIPFQVFERUSCANTEXYHUHJWNIV
HAHETDSFIWVHELJGWZUKJJLFULJZHJAHJTVOIIETIRIJFIOFOVHYZCDYGANDIFIIIXTHIOVMEKLFZLILUBEXUXAIMTHWEAUEMEFSEMZLUJXDMSOYKAWHBZFWVUHXSKHJFKRXPVGIRSXTPUSHQHO
EGAASIYLNLCYSVGDDAOERVSRVGINLRHLZCZWPYKSWLACUFPQCRMGPAMNLGVDSIFRJLIBHXMUHLLXNUHAZEXOERMYJZEQFMLBYAWGCAUDWVOVAWEBTMEKPFNSVJEVXWGAETOVPWLTWAIIVDBRKMH
IMJTPOBVFPNVMRLSFMSESNUPHPZWDAMPKHTIELUIKMTKPEHLCHUTVVBSLZRFUSFJSRAXULYMUMBEOPLTNOBJHNWMMGGNNILVLEDHJWQMNXEAXPZKNZUZFRHSSZETKOEDSAPAIZNSGAVONBLTPEA
OPXPMSNWLAGMOMNLAUACYGUEWCWUHICORFAZVIAVTBQPBLXHRORSHBIPVHLWHULPMNRZDAIERGCARNKZEDUTOKMZLXIBNIGIQAGQJJDRBYVDVICFBRZNIUXESHOJNEUBYTHRABRDPZXGXWCFYSH
VVLYTDKMVEXNXWDEHFYSWKUFMLLLKNWFPAIDMGDWCWMVAUEAIPWVKRITUPGOWRRGOWWTEUUDRVXVMZBVRLYGVBUAXUKPLDTCDUILTTIAMXFZVBKTRXUWYRIKULEMXXFWINYMGMCSSQZKQLRJCYG
DHFVYSWDLINTVNOEAAJFODZPDSLJJTDARBVTKENIYQKHAUUIZLTUHTYKXEPBYGHVQWUVKRSKBUHAYHOHOQPOMIOWIFJXPWEQTMCQMSDMVEIIODCKSWBRCXOWGSPAFOXMVNGDPUSFGTLMXBRKHBH
GLDNEOXIRNOLHFFSWCDLYSVVNOKTBMVHAPDBJTZEXHIHEIIHYVFRIXRKTJVIGXOQCRUVAYLQSBBPNULYAIVKZMNLWGJHCDMBGKEACGTZXRSNXUTHVJKERJVDKWGWGRXMPXVNSXNNGCUXPCLEKLU
NMHXHXYXWMTJMBCAIRLWSYAXSVWEKKSKEGUTWFENUXZVSUUIOGVAFXKEDEHLGTDXEAKJKZFALLUVXFSSVSWVGWIHGQLZLWZZTYZJYZEPHYQBRMSKSVEAOOHKYEPDIAWAELCGXWABBMTXNMCDDAE
ERFWZGEGEWJWWQEZFKWEECFKKTEARLOFEELAWBPCFNIQOQXYXJHQILDCPHHFDYLOKEHGDOGKITKGBMVRLJHGRKWHRIDTKDGUHPEHLYLIGFWEKHFCLHRGOBWHCVHPGYHHZTYWEXTIRRSHBIYFKOH
TQSUFQDVBYJTHTMUIIWSCTESWWRUTJKPBHZFFDWORYOWWOCXRLGFXZZTMPGFGFCUSWFZCKFSLRUAGGEAALKGOPDXFGFILWOKJBQUNWZLCBVTLAWDCVRPRDIIRVGQVVJFVUUXJKFVRPXBXKLSVNW
QSSCTEGZEUVREWIYVYSAPASDWGTOIGPCMVOHHDNHOMKXBGTEHZVQPORFMFEXZBBVMNZFGRLXCYQVWYUKZWMCNGQVEPMTGKDPIIWQKALUCNWLLUCSSZXLJFWZAIVAQGCZMFMBCTCKKHKIAJKMUBM
CEXZPQETRGSDLEEWIFATCJMGBJWFZPXCZGJXPFCUNMRXSBDTGEXXZREWNMZLMDNBXJPGNAXLUOMWVHGAVVVSNBQHPLSFRFPLBSHAQZQOVDWALELHCHBHKHRSGHJNVEZSSUDDKYOWRQWBUEUGTYU
ESKPKRWIYWPFAVMWEQENJLTOZQSYUGSLSYTKREXZHMRRKLPXPXUXWWQPGPOVTUEYEHZCWBIKJWMSHFVKIIZVYXJEJVHDDDTWRRYLYPXXEBKLWLVAOEGRPHOELOXOKHMRMHXFVURHXGNLFVWWNAS
YRGVLSKPWXQGXYCLSWLDYWRGLMQVMQVBAJDSYDSYRALVWUGJMBLMUOWXWRKPBRVZQGRLJGFFSRVEZQSEZSSKXUWFRHRDEKRSGHGMIDMOIAHYELYAGYOSLLKJFOWSZBZKLIYQQCOVGRPGKVDIDBG
OLVCVQNMVYONPHSGMNMWHVSUEBWLXJLVHKPVLAESPPWQEWLWERXINDVFXLQDHVLGUNPLLLZNXVKFMNCFUZTRDZZBWIOACTMIPLFXLLFXSKUUTPXKORFZWMOAJZDGQKXTAUGFUZOMLVXZTJHVSXI
RCIRSHRVVVUHSLIFVKHXMUXUTFEEGNTCAKYLXVICLIIEQWFLIPFYBCTSXJNRUGIYLRDGRXPWJHRNNQHTXLJEOPTIZZWWNGTEIRNVHUIMHPWALKKAEOAWUXVVYRDRJWMOARGKFCJIUPGDCLNTQMA
LIKDNXLFLOVGHSKEVHMZEZNJNCPBEEJRUTXRLUUCACHYJWLMHECNJSHTYBMYXZLOPOMZMEZZKZFEKWVGUOTZRIZGEBUQZVMSWZWVMAIKHJMOLBFFWNQMVQPGURBWUHAGTBPVZXSHAUYTGLMRRWH
YTIWHVQNPMOTRUMLWYKZDVOKWDTZKBNKCSRGJSEZZIOIXWUVJLGFIRVHUBECHNVKMZGRFXLXWHCVOIYQLASSYCTSJOEIMAENZIIHKEORWATZHJVACWLHSDWCROPQMYEGOBODVMSOSUQUIHDGXRX
RVJGLWFHKYVWTYIHFYGHCHYIFRFIXWYVMYJHQYAAUSAKEYGHHVTGTHDDINOPITPBREWGQGRGJJPHRVZCQVHQMJWCOBMXCJNALQCMCKVVYJWQHRXIDNTHPRUSAPNSAZTUVZBAXJLEBMIVLWEFSVM
FWEQYPEMJGLHYUUSEAOIGSFRWMHLWGWRVDLHHOVWKDJJLEUNYYPSVJXXTVLW
```