First homework

1 Important notices:

- **If you have any questions regarding the tasks, please do not hesitate to contact instructors.**
- This assignment gives you 15% of the final grade.
- **Provide an explicit explanation to your solutions**. Providing answers to the task with no explanation will give you 0 points.
- Your solution must be in the PDF format. You may either scan a handwritten solution or type your solution in Latex (LaTeX) or MS Word. Then export it into PDF. **Solutions submitted in a non-PDF format will receive 0 points**.
- You may write the programming code to solve any task. However, you have to explain explicitly the code logic in your submission and how it helped you solving the task. **Providing the code with no explanations will give you 0 points for the task.** You must submit your code either in the appendix of your submission or to a public repository (Github or Gitlab).
- You may use any online or installed tools to solve a task. However, you must explain how exactly tool helped you solve the task and your personal contribution. The tool must be properly referenced.
- **Plagiarism is prohibited.** Any used sources of information must be referenced. If you are suspected of plagiarism, then you will receive 0 for the task and will be reported to the Dean's office and Program Manager.
- This assignment is due **9th of March, 23:59**.

Tasks

Task 1. Assume that the Affine cipher is implemented in $\mathbb{Z}_{97}$, not in $\mathbb{Z}_{26}$. (Imagine that we just extended alphabet, added a set of special symbols. But the first 26 letters stay the same as in English alphabet.)

1. Write down encryption and decryption functions for this modification of Affine cipher.
2. What is the number of possible keys?
3. Suppose that modulus $p = 97$ is public. Malicious Eve intercepts 3-letter ciphertext $c = 28 \quad 83 \quad 43$. Assume that Eve also knows corresponding plaintext $m = D \quad O \quad G$. Find out the encryption key, decryption key and use it to decrypt message $c^{'} = 78 \quad 23 \quad 33$ (The result should be 3-letter airport code).

Task 2. This task is on constructing frequency diagrams:

- Find and write down paragraph of English plaintext. It should be at most 600 letters long.
- Construct frequency diagram for the chosen plaintext.
- Encrypt your plaintext with **shift cipher, permutation cipher, Vigenère cipher** and construct frequency diagrams for the corresponding ciphertexts. You may choose any suitable keys for the ciphers.
- Analyse constructed diagrams and explain which properties help you to identify which encryption scheme was used.

To construct frequency diagrams for this task, we recommend to use online tools or write a code. Do not forget about referencing rules.

Task 3. Assume you have used a time machine and you are back at Julius Caesar's era. Now, you need to help Julius Caesar in selecting better ways for sending secret messages to his military units. You may select among the ones that have been discussed during this course up to Week 3 included (shift cipher, substitution cipher, permutation cipher, affine cipher, Vigenère cipher, OTP). Provide an explanation for your choice.

Task 4. Suppose you intercepted the following ciphertext $c = 00010010 \quad 00000111 \quad 11101010$. You know that a 3-letter word was encrypted using one-time pad (to convert letters to binary strings ASCII table was used). Can you bruteforce possible keys and learn the message that was encrypted?

Task 5. You have intercepted the following ciphertext encrypted using Vigenere cipher. You have a crypto-analyst friend who can help you break the cipher, but they asked you to **find key length**.

$ctx =$
FHKOJASZAFUDTBJQLVMKFHKZKFWGACXWGGUMNGAVKSNWEWWNMPANKWHFHKUIXI
JMFEUJLGZLEBJDOAOJMDUWTKOAEGDEZZAUNMBQAPKVPQAXTATEGLNQSYVKOKCIUM
LCIAEHGXRKTUXQUNZVGIGXGHRITLQDSOVVTEXQITTJQTQCZQQZBABRQEBMUFHKXQX
TKZIQIYBYMSCWTFHZEQXOISGPDUWTEATLCFROKMETGQTOAYMKRYUCOQTNQOIHKVA
AUCMTQLGBGROXKNMSYPGIOATFPRUXYMSZMRMPKZDMSQMVEOTGQGRNMCPPATN
DUMAHDOSCPPEXGQGRLMGFPKTVKOAEKFHHQVEOLKJMLQWTENKIMGPHMJUNJGQGIT
DKEIHTGSRGJAAUXVQEEGVFECXMGOHMWVKOAZEANQ

Once you figured out possible key length, use additional material from Appendix A to **confirm your solution using index of coincidence**. For this part of the task you are recommended to use online resources (or your own code) for frequency analysis and you must reference it properly.
HINT: To solve this task, use explanations from "Historical Ciphers" lecture slides.

Bonus Task 1 Suppose you encrypt m using an Vigenere cipher of keylength 3 and then encrypt the result using Vigenere cipher with different key of length 5. Is there any advantage of doing this, rather than using a single encryption function? Why or why not?

Bonus Task 2 Assuming that the rate of English language is 1.8, find unicity distance of affine cipher.

A Additional material for Task 5 (part 2)

For key length 2

FKJSAUTJLMFKKWAXGUNAKNEWMAKHHUXJFULZEJOOMUTOEDZANBAKPATTGNSVOCUL
IEGRTXUZGGGRTQSVTXITQQZQBBQBUHXXKIIBMCTHEXIGDWETCRKEGTAMRUOTQIKAU
Y_0 = MQGGOKMYGOTPUYSMMKDSMETQRMPANUADSPEGGLGPTKAKHQELJLWEKMPMUJQID
EHGRJAXQEVEXGHWKAEN

HOAZFDBQVKHZFGCWGMGVSWWNPNWFKIIMEJGLBDAJDWKAGEZUMQPVQXAELQYKKI
MCAHXKUQNVIXHILDOVEQTJTCQZAREMFKQTZQYYSWFZQOSPUTALFOMTQOYKYCQNO
Y_1 = HVACTLBRXNSPIAFRXMZRPZMQVOGGNCPTDMHOCPXQRMFKVOEFHVOKMQTNIGHJNG
GTKITSGAUVEGFCMOMVOZAQ

For key length 3

FOSFTQMHKGXGNVNWMNHKXMUGEDODTADZNQKQTENYOILAGKXNGXRLSVXTQCQAQ
Y_0 = MHQKQBSTZXSDTTFKTTYRCTOKAMLGXMPOFUMMPDQEGRCADAOPXGMPVAFQOJQEIPJ
JGDIGGAVEFXOWOEQ

HJZUBLKKFAWUGKWWPKFUIFJZBOJUKEEAMAVAAGQVKUCEXTQZIGIQOTQTTZZBEUKXZI
Y_1 = YCFEOGUELRMGOMYONIVUTGRKSGAPXSRKMMOQNPTUHSPGRGKKEHVLMWNMHUGIK
HSJUQGEMHVAA

KAADJVFZWCGMASENAWHIJELLJAMWOGZUBPPXTLSKCMIHRUUVGHTDVEIJQQBRBFXTIY
Y_2 = MWHQIPWACOEQAKUQQHACQBONYITRYZMZSVTGMPNMDCEQLFTOKHEKLTKGMNQTE
TRAXEVCGMKZN

For key length 4

FJATLFKAGNKEMKHXFLEOMTEZNAPTGSOUIGTUGGTSTIQZBQUXKIMTEIDECKGAROQKU
Y_0 = QGKYOPYMKSEQMAUDPGLPKKQLLEMMJIEGJXEEGWAN

HAFBVHFCGGSWPWKIEGBADKGZMPQALYKMAXUNIHLOETTQAEFQZYSFQSUAFMQYYQO
Y_1 = VCLRNPARMRZQOGCTMOPQMKOFVKQNGJGTISAVGCOVZQ

KSUJMKWXUANWAHUJUZJOUODABKATNVCLERXZGRQVXTQQBBHXIBCHXGWTRETMUTI
Y_2 = AMGOMGTUSMDMTRPNASEGGTAHEJWKPUQDHRAQVXHKE

OZDQKZGWMVWNNFIMJLDJWAEUQVXEQKICHKQVXIDVQJCZRMKTQYWZOPTLOTOKCNH
Y_3 = ATBXSIFXZPMVGNPDHCXRFVEHOMTIHNGKTGUEFMMOA

For key length 5

FAUQFFXMKWAFXEZDMKDUAQTQOMEKUIRDTTQZQFXQMFXPEFEORQIAQRMIPMMMEG
Y_0 = PDDPGFKFEMEGUGESAEEOKA

HSDLHWWNSWNHIULODOENPAESKLHTNGISETCBEHTISHODARTAYTHULOSORSPSOR
Y_1 = PUOERPOHOLNPNIIRUECHON

KZTVKGGGNNKKJJEAUAZMKXGYCCGUZXTOXJZABKKYCZIUTOGYUNKCGXYAUZKQTNAMSX
Y_2 = LKAHLQKHJTHGXGXMAQ

OABMZAGAWMWUMLBOWEZBVTLVIIXXVGLVQQQBMXZBWESWLKQMCQVMBKPTXMZM
Y_3 = GMTACGMTEQKWIMGDTJVVMWZ

JFJKKCUVEPHIFGJJTGAQPANKUARQGHQVITQRUQIYTQGTCMTKOOATGNGFYRDVQCNHP
Y_4 = QGVKVJTMJQKGAQFGVE

For key length 6

Y_0 = FSTMKXNNMHXUEOTDNKTNOLGXGRSXQQQHKBTXDTKTRTKMGMOUMDERAAPGPAQJEPJDGAEXWE

Y_1 = HZBKFWGWPFIJBJKEMVAQKCXQIIOQTZEKZYFOULMOYNVTRSAXRMONTHPRKEVMNHGKSUGMVA

Y_2 = KAJFWGAEAHJLJMOZBPTSCIRUGTVIQBBXIMHIWCEAUQAQOYTYMSTMNDELTKELKMQERXVGKN

Y_3 = OFQHGGVWNKMGDDAZQQEYIAKNXLVTCAMQQSZSTFTYCOALXPFMPQGCDOXMVFOQIJGIGVFOOQ

Y_4 = JULKAUKWKUFZOUEAAAGVUETZGQTTZBUXICEGERGMOIUGKGPSKMQPUSGGKHLWMUIHJQEHA

Y_5 = ADVZCMSNWIELAWGUPXLKMHUVHDEJQRFTYWQPAOQKQHCBNIRZZVGPMCQFOHKTGNTTAECMZ

For key length 7

Y_0 = FZJHAMNPHMZATEBQGKLXUXQEQZBQIWXUCTMQKTOPPZDOMDSQPEEQMNDSXFHZ
Y_1 = HAQKCNWAKFLOKZQALOCRNGDXTBMXYTOWFGKTVQXGRMMTCUCGKKOWGJKRVEME
Y_2 = KFLZXGENUEEJOZAXNKIKZHSQQAUTBFITRQRNALKIURSGPMPRTFLTPGEGQCWA
Y_3 = OUVKWAWKIUBMAAPTQCATVROICBFKYHSEOTYQAGNOXMQQPAPLVHKEHQIJEXVN
Y_4 = JDMFGVWWXJJDEUKASIEUGIVTZRHZMZGAKOUOUBMAYPMGAHEMKHJNMGHAEMKQ
Y_5 = ATKWGKNHILDUGNVTYUHXITVTQQKISEPTMACICGSTMKVRTDXGOQMKJITAGGO
Y_6 = SBFGUSMFJGOWDMPEVMGQGLTJQEXQCQDLEYOHMRYFSZENNOGFAVLIUTGUVOA

For key length 8

Y_0 = FALKGKMHFEMENPGOITGTTQBUKMEDCGRQUGYPMSQADGPKLEMIGXEWN
Y_1 = HFVFGSPKEBDGMQLKAUILETAFZSQUFQYOCRPRRQGTOQKFKNJTSVCVQ
Y_2 = KUMWUNAUUJUDBANCEXGQXQBHICXWRTUIMOGUMMRNSGTHJKUDRQXK
Y_3 = ODKGMWNIJDWEQXQIHQXDQCRKQWOTOOCHTXIXPVNDCRVHMINKGEMO
Y_4 = JTFANEKXLOTZATSUGUGSIZQXITIEKAOKQKOYKEMUPLKQLMJEJEGA
Y_5 = ABHCGWWIGAKZPAYMXNHOTQEQYFSAMYQVLNAMZOCMPMOVQGGIAGOZ
Y_6 = SJKXAWHJZOOAKTVLRZRVTQBXBHGTEMTAGMTSDTPAEGAEWPQHAVHE
Y_7 = ZQZWVNFMLJAUVEKCKVIVJZMTYZPLTKNABSFZMGPHXFEOTHGTUFMA

For key length 9

Y_0 = FFMGNWHMEDDQTYLKGLXCQQBZDFTCKLMFMQRDPMAOEJDGEOE
Y_1 = HUKAGWFFBUEAAVCTIQQZEXYEUROOVGSPRMNUPGELNUKJGHA
Y_2 = KDFCANHEJWZPTKIUGDIQBTMQWOAQABYRMVMMEFKKKNEAVMN
Y_3 = OTHXVMKUDTZKEOAXXSTQMKSXTKYTAGPUPECAXPFJIJIAFWQ
Y_4 = JBKWKPUJOKAVGKEQGOTZUZCOEMMNURGXKOPHGKHMMGHUEV
Y_5 = AJZGSAILAOUPLCHUHVJBFIWIAEKQCOIYZTPDQTHLGQTXCK
Y_6 = SQKGNNXGOANQNIGNRVQAHQTSTTROMXOMDGAOGVQQPGGVXO
Y_7 = ZLFUWKIZJEMAQUXZITTBKIFGLGYITKASMQTSRKVWHISQMA
Y_8 = AVWMEWJLMGBXSMRVTEQRXYHPCQUHQNTZSGNCLOETMTREGZ

For key length 10

Y_0 = FUFXKAXZMDATOEURTQQXMXEERIQMPMEPDGKEEUEAEK
Y_1 = HDHWSNILDEPEKHNIECETSOATYHLSRPOPOROONNIUCO
Y_2 = KTKGNKJEUZKGCGZTXZBKCITGUKGYUKTASLALKJHXXA
Y_3 = OBZGWWMBWZVLIXVLQQMZWSLQCVBPXZGTCMEKIGTVMZ
Y_4 = JJKUEHFJTAPNURGQIQUITGCTOAGGYDQNPGKJMQGQGE
Y_5 = AQFMWFEDKUQQMKIDTZFQFPFOQARIMMGDPFFMGGSEOA
Y_6 = SLWNWHUOONASLTGSTBHIHDRATUOOSSRUEPHLPIREHN
Y_7 = ZVGGNKJAAMXYCUXOJAKYZUOYNCXAZQNMXKHQHTGGMQ

Y_8 = AMAAMULOEBTVIXGVQBXBEWKMQMKTMMMAGTQWMDJVW
Y_9 = FKCVPIGJGQAKAQHVTRQYQTMKOTNFRVCHQVVTJKAFV