MATH 323: Cryptography
Homework 1

Sepehr Akbari | August 26, 2025

1 Caesar Cipher

Problem 1.1

Encrypt the message:
"For duty, duty must be done; the rule applies to everyone."
using a Caesar cipher with a shift of six letters. (Don't worry about encrypting the punctuation.)

Solution to Problem 1.1

LUXJA ZEJAZ ESAYZ HKJUT KZNKX ARKGV VROKY ZUKBK XEUTK

Problem 1.2

The message: ESTYRD LCP DPWOZX LD ESPJ DPPX. is a cipher text encrypted using a Caesar cipher (the shift amount is not provided). What is the plaintext message?

Solution to Problem 1.2

THINGS ARE SELDOM AS THEY SEEM

(Solution found with K = 11)

Problem 1.3

Can you find two English words other than sleep and bunny, with at least four letters, that encrypt to each other under a Caesar cipher? What are the longest such words you can find?

Solution to Problem 1.3

For this question, I wrote a program to take a list of about 400,000 words and find all pairs of words that encrypt to each other under a Caesar cipher. (cipherMatched.py)

Found 1705 unique pairs.
Number of pairs with the longest length (7 characters): 4 pairs

- ABJURER and NOWHERE (Shift: 13)
- BUMPILY and UNFIBER (Shift: 19)
- CHECHEN and PURPURA (Shift: 13)
- PRIMERO and SULPHUR (Shift: 3)

Problem 1.4

Alice sends Bob a ciphertext encrypted using a Caesar cipher. Bob knows the shift amount, but being a beginner in cryptography at this stage, he accidentally encrypts it rather than decrypting it. Fortunately, by doing so, he still recovers the original plaintext. What was the shift amount?

Solution to Problem 1.4

Assuming the message is in English, for a text to be encrypted and remain unchanged, the shift amount must be 0 or 26, or a mod of it, for example 52. In this case a shift is applied twice and then the original text is recovered, so the shift1 + shift2 = 26, which means **shift = 13** or a mod of it, for example 39.

Problem 1.6

Suppose Alice starts with a plaintext message and encrypts it using a Caesar cipher with a shift of k letters. Since she is also just learning about cryptography at the moment, she explores what happens when she encrypts the encrypted ciphertext, using the same shift of k. She does this repeatedly, and eventually she finds that she has decrypted the message. In terms of k, how many times did Alice have to encrypt the message before it became decrypted? (You may assume that the message is in English this time, so that the alphabet has 26 letters.)

Solution to Problem 1.6

Each encryption applies a shift of k, and the message is decrypted when the total shift is a multiple of 26. Therefore, Alice must encrypt the message n times such that $nk \equiv 0 \mod 26$.

Furthermore, since we want to find the smallest positive integer n where nk is a multiple of 26, we can divide by the factors n and 26 have in common, which is $\gcd(k, 26)$. So the solution with the smallest n is:

$$nk \equiv 0 \mod 26, \text{ where, } n = \frac{26}{\gcd(k, 26)}$$

2 Substitution Ciphers

Problem 2.1

One issue with substitution ciphers is the difficulty of remembering the key. There is a version of the substitution cipher that uses a key word that makes it easier to remember. To set this up, pick a key word that has no repeated letters (or else delete the repeated letters). Then, append to the key word all the unused letters in the alphabet, starting from the last letter in the keyword. This is a permutation of the letters in the alphabet, and it serves as the key. For example, if the keyword is LIME, then the full key would be LIMEFGHJKNOPQRSTUVWXYZABCD. That means that we encrypt a as L, b as I, and so forth. The message

VOQDK MABJJ DZAXC ABAEE YCEVC OGDZH RGAJR
UQDKZ KHJOV GHJRG CAJCJ UCKBV LCGHC

was encrypted in this way using the key word APRICOT. What is the plaintext message?

Solution to Problem 2.1

Key: "APRICOTUVWXYZBDEFGHJKLMNQS"

Decrypted Message: "IFYOU WANTT OMAKE ANAPP LEPIE FROMS CRATC HYOUM USTFI RSTCR EATET HEUNI VERSE"

Message: "If you want to make an apple pie from scratch you must first create the universe"

Problem 2.2

What are the advantages and disadvantages of using a permutation as in problem 1 over an arbitrary permutation?

Solution to Problem 2.2

Advantages:

- Easier to remember the password, than the entire key.
- The key is reproducible, as long as the password is remembered. So it can be easily shared.
- Although not very relevant, a password takes less space to store than the entire key.

Disadvantages:

- The key is less secure, as it is based on a memorable password rather than a random key.
- If the password is weak or easily guessable, the security of the entire system is compromised.
- The key space is reduced from $26!$ to a smaller number, making it more vulnerable to brute-force attacks.

Problem 2.3

The message

WBJGW RBGRC BRKHW RJKCK RZZDR CDZRW BJLGV
TNTPT JKCIR LBERH JKCCE IPRMR HPCBR JCARK
VWBUK VTKBC CBRRM RHYBR NIRSC HRILK WBDCR
KHPWK JKVRR OTGKC DDCJW KR

is a ciphertext encrypted using the mechanism in problem 1. What is the plaintext message?