Assignment 1

Security and Cryptography (CS4520)

(Total number of achievable points: 24)

Issue date: November 26th, 2024.
Due date: December 6th, 2024, 23:59 CET *(hand in via Brightspace)*

- In this assignment, you will answer questions related to Historical Ciphers, Number Theory, and Information Theoretic Security.
- This is an individual assignment. Please mention your name and student number in the submission. You have to hand in a **SINGLE** document (PDF) with your answers and your source code (if any). **Also be aware that any form of plagiarism will not be condoned. If you took this course in previous years and used your old assignments and/or model answers, you need to provide an explanation and give a clear reference.**
- You are supposed to work on this assignment on your own, without any AI tool. In case you use a tool for grammatical purposes, give a reference to that tool and include a short description how you used it for your report.
- Please direct your questions to the teaching assistants. However, this document alone is sufficient to complete the assignment.
- **Please explain and motivate all your answers with your own words.**
- You have unlimited attempts to upload your report. Only the last one is kept. No submission via e-mail will be accepted.
- Do not use pencil, handwriting, or scanned figures. If so, your assignment will not be graded. Use formal language, provide references for your sources, and explain your solutions.

1. Historical Ciphers

In this exercise, you are given several ciphertexts originating from historical ciphers. (Ciphers that are explained in Chapter 7 from the textbook.) For each ciphertext, you need to answer the following questions:

- Which encryption scheme is used?
- What is the original plaintext message?
- What is the encryption key?

Or explain why it is not possible to decipher it.

Note that the plaintext- and the ciphertext-space consist only of the letters ‘a’ to ‘z’. Before encrypting, all capitalized letters are replaced by lowercase, and all spaces and punctuation are removed. Afterward, the capitalization, spaces, and punctuation are reintroduced in accordance with the plaintext.

(a) (2 points) Consider the ciphertext:
“Yt gj, tw sty yt gj, ymfy nx ymj vzjxynts: Bmjymjw ’ynx stgqjw ns ymj rnsi yt xzkkjw Ymj xqnslx fsi fwwtbx tk tzywfljtzx ktwyzsj, Tw yt yfpj fwrx flfnsxy f xjf tk ywtzgqjx Fsi gd tuutxnsl jsi ymjr. Yt inj—yt xqjju, St rtwj; fsi gd f xqjju yt xfd bj jsi Ymj mjfwy-fhmj fsi ymj ymtzxfsi sfyzwfq xmthpx Ymfy kqjxm nx mjnw yt: ’ynx f htsxzrrfynts Ijatzyqd yt gj bnxm’i.”

(b) (2 points) Consider the ciphertext:
“Ftkins Xpk Wvzu; llna eeryc Tdgq nyx Btsl? W ldvfomx Flvs! Wpzr tizoc, Xcs hycyiuq! Xywct mauiz Nizbv X ez meqz xf ycda; Goma Flp tdgxu-zxzqedwcv Pvmi jqazzstvf ti.

Buqv ob X, pnfmvs hvgdaegl xpq affas, Qnki umrztthx bu iidxy hd hpnf qizozbs! Csg vrm aj rza ilrzi emviwdgw ehroqh wcg hxepjm Qwtoetxu kiifl; kvdj wuhpb mpfbt hyecmdq.

Xysgtjbyi afeer je! avu jwd xymhtps yivaae, Qdcuhlv btc wcth, iaqsg flv ktppgo jqxpvr gteyt, Fg Yi kvtn eel etdirrn dzrygwyi, Ss iwsh alm aykkpgh phyaq, pvti-weakil arv. Rgdrn hrl Nlîjvbp eak Nikeufpiln, Rezze, rbs ppy alm axysg leeymwdw ysgt, Eel wtmme pn Bi. Qlwbdsp hwtq slezxijgan. Jvnlb! flfi hweya gzgwy hwn vvcete me hwt jvlpl.

Eeexpne fhml: Temwcv lrhvl flvgt lsekw wr Ovgwpzn, oi ets nspgigo e lueusb, lmgo nwurvr eppzz, ucmozbv prq wvwexioixrt omueict, heexl eomme hd Zvvzlvm, wkobbiepro imkv utee, jeafmeu sdaa oma rets. ”

(c) (4 points) Write your own code to solve (a) and (b) in C, C++, Java or Python. The input to your program is the ciphertext, and the output is the corresponding plaintext (showing the key is optional). Your code should decrypt any ciphertext of that type, not only the specific ones given in (a) and (b). Provide proofs, such as source code and screenshots of the output, in the appendix of your report.

Note: For (a) and (b), if you do not write your own code, provide the reference for the online tool you used.

2. Number Theory and Elliptic Curve

(a) (5 points) Find the 7^{th} root of 13 in modulo 119, i.e., find x such that $x \equiv 13^{\frac{1}{7}} \mod 119$. Show your steps.

Note: Using the techniques taught in the lectures, it is possible to calculate the end result without the need for a calculator (all calculations are done on numbers between -118 and 119). Brute forcing for all x values will not receive any points. (The marks are for the method, not the final result only.)

(b) (3 points) Consider an elliptic curve $F : y^2 = x^3 - 2x + 2 \mod 71$. We have $P = (1, 1)$ and $Q = (4, 49)$. Show the result of $2P$, and the result of adding P and Q. Show the process for your calculation.

3. Information Theoretic Security

We have the following sets of possible plaintexts, keys and ciphertexts:

$$\mathbb{M} = \{a, b, c, d\}$$
$$\mathbb{K} = \{k_1, k_2, k_3, k_4\}$$
$$\mathbb{C} = \{1, 2, 3, 4\}$$

The plaintexts and keys have the following probabilities:

$$Pr(\cdot) = \{a = \frac{1}{3}, b = \frac{4}{15}, c = \frac{1}{5}, d = \frac{1}{5}\}$$
$$Pr(\cdot) = \{k_1 = \frac{1}{5}, k_2 = \frac{3}{10}, k_3 = \frac{1}{5}, k_4 = \frac{3}{10}\}$$

Consider the encryption scheme listed in Table 1.

Table 1: Encryption Scheme

	a	b	c	d
k_1	3	1	4	2
k_2	2	4	1	3
k_3	4	2	3	1
k_4	1	3	2	4

(a) (3 points) Calculate the probability of each plaintext conditioned on each ciphertext occurrence.

(b) (3 points) Compute the entropy value for $H(M|C)$.

(c) (2 points) Is this scheme perfectly secure? Explain briefly.