Homework 1

Introduction to Cryptography

1. The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key.

Dro rewkx xkdsyx yp Cdybwgsxn rkn pkvvox lopybo dro Rybno. Uxsqrd Mrkwzsyx Kxnesx Vydrkb qkdrobon dro cmkddobon bowxkxdc yp dro rewkx kbwi kxn von dro bopeqooc xybdr kmbycc dro Qbokd Cok dy dro usxqnyw yp Vybnkobyx. Li oxvscdsxq dro ksn yp ydrob xkdsyxc - rewkxc, qxywoc, ovfoc, kxn ngkbfoc - Vydrkb rovzon pybw k qbokd Kvvskxmo dy cdkxn kqksxcd dro ybmc kxn drosb bedrvocc xog voknob, Ybqbsw Nyywrkwwob. Dro coowsxqvi excdyzzklvo Rybno myxdsxeon sdc bkwzkqo, bosxpybmsxq sdc qbygsxq kbwi gsdr ckfkqo dbyvvc kxn lbedscr yqboc. Led, yx dro ofo yp fsmdybi, Qev'nkx kxn rsc pyvvygobc covpscrvi klkxnyxon drosb kvvsoc dy coou yed zygobpev kbdspkmdc, pybmsxq dro gokuoxon Rybno dy bodbokd. Nyywrkwwob wywoxdkbsvi bkvvson dro ybmc grox ro cvog Vydrkb sx k rkbbygsxq lkddvo, led dro roby'c nokdr nsn xyd lboku dro Kvvskxmo'c bocyvfo. Debkviyx, Vydrkb'c vyikv vsoedoxkxd, aesmuvi dyyu ez voknobcrsz yp Kjobydr'c nopoxnobc kxn psxkvvi nopokdon dro Rybno.

a) Compute the relative frequency of all letters A...Z in the ciphertext. You may want to use a tool such as the open-source program CrypTool [50] for this task. However, a paper and pencil approach is also still doable.
b) Decrypt the ciphertext with the help of the relative letter frequency of the English language (see Table 1.1 in Sect. 1.2.2). Note that the text is relatively short and that the letter frequencies in it might not perfectly align with that of general English language from the table.

2. We consider the long-term security of the Advanced Encryption Standard (AES) with a key length of 128-bit with respect to exhaustive key-search attacks. AES is perhaps the most widely used symmetric cipher at this time.

a) Assume that an attacker has a special purpose application specific integrated circuit (ASIC) which checks $5 \cdot 10^8$ keys per second, and she has a budget of $1 million. One ASIC costs $100 (including manufacturing the printed circuit boards, power supply, cooling, etc.). How many ASICs can we run in parallel with the given budget? How long does an average key search take? Relate this time to the age of the Universe, which is about 10^{10} years.

b) We try now to take advances in computer technology into account. Predicting the future tends to be tricky but the estimate usually applied is Moore's Law, which states that the computer power doubles every 18 months while the costs of integrated circuits stay constant. How many years do we have to wait until a key-search machine can be built for breaking AES with 128 bit with an average search time of 24 hours? Again, assume a budget of $1 million (do not take inflation into account).

2. We now consider the relation between passwords and key size. For this purpose, we consider a cryptosystem where the user enters a key in the form of a password.

a) Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?
b) What is the corresponding key length in bits?
c) Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?
d) At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of
   i. 7-bit characters?
   ii. 26 lowercase letters from the alphabet?

4. Compute the result without a calculator.
a) $15 \cdot 29 \bmod 13$
b) $2 \cdot 39 \bmod 13$
c) $2 \cdot 8 \bmod 13$
d) $-11 \cdot 4 \bmod 13$

5. Compute without a calculator:
a) $1/5 \bmod 13$
b) $1/5 \bmod 7$
c) $4 \cdot 2/5 \bmod 7$
d) $9^{2021} \bmod 80$

6. We consider the rings Z_5 and Z_6.
a) Construct the addition and multiplication tables for Z_5.
b) Construct the addition and multiplication tables for Z_6.
c) There are elements in Z_6 without a multiplicative inverse. Which elements are these?
d) Why does a multiplicative inverse exist for all nonzero elements in Z_5?