Introduction to Cryptography

TEK 4500 (Fall 2020)
Problem Set 1

Problem 1.
Read Chapter 1 and Chapter 2 in [BR].

Problem 2. [Problem 1.1 in [PP]]
The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key.

> lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt
>
> wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

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 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.

c) Who wrote the text?

Problem 3.

A problem with the substitution cipher is that it leaks the letter frequency of the encrypted message. The reason is that it uses the same permutation (substitution table) for each letter of the message. One solution is to use the Vigenère Cipher, which uses multiple permutations to encrypt a message. It is defined as follows. To encrypt a message

$$M = \texttt{this is a nice day}$$

with the Vigenère cipher, define a keyword

$$K = \texttt{dice}$$

and encrypt as follows:

$$\begin{aligned} M &= \texttt{thisisaniceday} \\ +K &= \texttt{dicedicedicedi} \\ \hline C &\equiv \texttt{wpkwlacrlkghdg} \pmod{26} \end{aligned}$$

where each letter $\{\texttt{a}, \texttt{b}, \ldots, \texttt{z}\}$ is mapped to $\{0, 1, \ldots, 25\}$ as usual.

a) What is the key space, message space, and ciphertext space for the Vigenère cipher?

b) With the same key as above (`dice`), decrypt the following ciphertext (spaces, punctiations, and quotes are mapped to themselves):

> wpg whzxmfm jeg jgkxv. vlh lghlkcxhl uspi veetgxv egvh xnefmf mq bji fmpxum qj wpg xdjni. wpg prdkrj kwt rn uxuiyfhztc lkg-gumcq vwoe ziu tdauig ntsp pcrg bq ldvf eql, ymwp vlh nqvpcne, "l ltmqs vs pg crqqj-moivmrv," vahtxi wqoiv yweingh.

c) Suppose a really long message (say 1 GB in size) of english text has been encrypted with the Vigenère cipher using a key of length 6. Explain how you would break it.

d) Same as above, but now you don't know the length of the key. Explain how you nevertheless can break the scheme.

Problem 4.

Alice is using the one-time pad and notices that when her key is the all-zeroes string $K = 0^n$, then $\mathsf{Enc}(K, M) = M$ and her message is sent in the clear! To avoid this problem, she decides to modify the scheme to exclude the all-zeroes key. That is, the key is now chosen uniformly from $\{0,1\}^n \setminus \{0^n\}$, the set of all n-bit strings except 0^n. In this way, she guarantees that her plaintext is never sent in the clear. Is this variant still one-time perfectly secure? Justify your answer.

Problem 5. [Problem 2.1 in [BR]]

Suppose that you want to encrypt a single message $M \in \{0, 1, 2\}$ using a random shared key $K \in \{0, 1, 2\}$. Suppose you do this by representing K and M using two bits (00, 01, or 10), and then XOR-ing the two representations. Does this seem like a good protocol to you? Explain.

Problem 6. [Problem 2.2 in [BR]]

Suppose that you want to encrypt a single message $M \in \{0, 1, 2\}$ using a random shared key $K \in \{0, 1, 2\}$. Explain a good way to do this.

Problem 7. [Problem 2.3 in [BR]] *Hard* (*optional*)*:*

Symmetric encryption with a deck of cards. Alice shuffles a deck of cards and deals it all out to herself and Bob (each of them gets half of the 52 cards). Alice now wishes to send a secret message M to Bob by saying something aloud. Eavesdropper Eve is listening in: she hears everything Alice says (but Eve can't see the cards).

1. Suppose Alice's message M is a string of 48-bits. Describe how Alice can communicate M to Bob in such a way that Eve will have no information about what is M.

   Hint: Try to define an explicit enumeration of all the possible ways of dealing the 52 cards. That is, for each possible shuffle, assign it an integer value in the range $0, 1, \ldots, \binom{52}{26} - 1$. For this it might be helpful to look up the concept of a combinatorial number system. How can you use this enumeration to create an encryption scheme?

2. Now suppose Alice's message M is 49 bits. Prove that there exists no protocol which allows Alice to communicate M to Bob in such a way that Eve will have no information about M.

The remaining problems give some simple practice with the concept of modular arithmetic, as well as a refresher on some basic probability techniques.

Problem 8.

Compute the following without the use of a calculator:

a) $23 + 28 \pmod{29}$

b) $3 - 11 \pmod{9}$

c) $15 \cdot 29 \pmod{13}$

d) $16 \cdot 13 \pmod{26}$

e) $2^5 \pmod{31}$

f) $2^{103} \pmod{31}$

g) $5^{-1} \pmod{19}$ // i.e., find x such that $5 \cdot x \equiv 1 \pmod{19}$

Problem 9.

Generate a table of $2^x \bmod 11$ for $x = 0, 1, 2, ...10$. Which pattern do you discover? Use your table to solve the modular equation $2^x \equiv 3 \pmod{11}$.

Problem 10. [Problem 0.1 in [Ros]]

Consider rolling several d-sided dice, where the sides are labeled $\{1, 2, \ldots, d\}$.

(a) When rolling two of these dice, what is the probability of rolling snake-eyes (a pair of 1s)?

(b) When rolling two of these dice, what is the probability that they don't match?

(c) When rolling **three** of these dice, what is the probability that they all match?

(d) When rolling three of these dice, what is the probability that at least two of them match? This includes the case where all three match.

(e) When rolling three of these dice, what is the probability of seeing at least one 1?

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[PP] Christof Paar and Jan Pelzl. *Understanding Cryptography - A Textbook for Students and Practitioners*. Springer, 2010.

[Ros] Mike Rosulek. *The Joy of Cryptography*, (draft Feb 6, 2020). https://web.engr.oregonstate.edu/~rosulekm/crypto/crypto.pdf.