Introduction to Cryptography

TEK 4500 (Fall 2021)
Problem Set 1

Problem 1.

Read Chapter 1 and Chapter 2 in [BR].

Problem 2.

The ciphertext below was encrypted using a substitution cipher (punctuation, cases, and numbers maintained for readability).

> Lm gsv hrcgs wzb lu Szgv Dvvp, zugvi gsv kilxvhhrlmh, gsv hkvvxsvh, gsv hslfgrmt, gsv hrmtrmt, gsv yzmmvih, gsv klhgvih, gsv uronh, gsv dzcdliph, gsv iloormt lu wifnh zmw hjfvzormt lu gifnkvgh, gsv giznk lu nzixsrmt uvvg, gsv tirmwrmt lu gsv xzgvikroozih lu gzmph, gsv ilzi lu nzhhvw kozmvh, gsv yllnrmt lu tfmh—zugvi hrc wzbh lu gsrh, dsvm gsv tivzg litzhn dzh jfrevirmt gl rgh xornzc zmw gsv tvmvizo szgivw lu Vfizhrz szw ylrovw fk rmgl hfxs wvorirfn gszg ru gsv xildw xlfow szev tlg gsvri szmwh lm gsv 2,000 Vfizhrzm dzi-xirnrmzoh dsl dviv gl yv kfyorxob szmtvw lm gsv ozhg wzb lu gsv kilxvvwrmth, gsvb dlfow fmjfvhgrlmzyob szev glim gsvn gl krvxvh—zg qfhg gsrh nlnvmg rg szw yvvm zmmlfmxvw gszg Lxvzmrz dzh mlg zugvi zoo zg dzi drgs Vfizhrz. Lxvzmrz dzh zg dzi drgs Vzhgzhrz. Vfizhrz dzh zm zoob.

a) Compute the relative frequency of all letters in the ciphertext. Compare with the relative frequency of letters found in the English alphabet.

Hint: 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.

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:

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

where each letter $\{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ 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-zero 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-zeroe 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, the 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. [Problem 0.1 in [Ros]]
Consider rolling several fair 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?

Problem 10.

a) Suppose a family, having two children, tells you that their oldest child is a girl. What is the probability that the *other* child is a girl?[1]

b) Suppose a family, having two children, tells you that one of their children is a girl. What is the probability that the *other* child is a girl?

c) Suppose you're the contestant on a game show where you are presented with three doors. Behind one of them there is a great prize (say a million dollars). Behind the other two doors there is nothing. You are then asked to choose a door. After you make your choice, the game host opens one of the doors you did *not* pick and which does *not* contain the prize. Before opening the remaining two doors, the game host offers you the choice of switching to the other (unopened) door. However, you can also decide to stay with you original choice. What should you do? Switch, or stay? (And why?)

References

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

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

[1] Assume that boys and girls are born with equal probability.