

# Introduction to Cryptography

TEK 4500 (Fall 2022)

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 kilxvhrlmh, gsv hkvvxsvh, gsv hslfgrmt, gsv hrmtrmt, gsv yzmmvih, gsv klhgvi, gsv uronh, gsv dzcdliph, gsv iloormt lu wifnh zmw hjfvzormt lu gifnkvg, 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 ylvovw fk rmgl hfxs wvorirfn gszg ru gsv xildw xlfow szez tlg gsvri szmwh lm gsv 2,000 Vfizhrzm dzi-xirnmzoh dsl div gl yv kfyorxob szmtvw lm gsv ozhg wzb lu gsv kilxvvrmt, gsvb dlfow fmjfvhgrlmzyob szez glim gsvn gl krxxvh—zg qfhg gsrh nlnvmg rg szw yvvm zmmfmxxvw gszg Lxvzmrz dzh mlg zugvi zoo zg dzi drgs Vfizhrz. Lxvzmrz dzh zg dzi drgs Vzhgzhz. 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) 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

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

with the Vigenère cipher, define a keyword

$$K = \text{dice}$$

and encrypt as follows:

$$\begin{array}{r}
M = \text{thisisaniceday} \\
+K = \text{dicedicedi} \\
\text{-----} \\
C \equiv \text{wpkwlacrlkghdg} \pmod{26}
\end{array}$$

where each letter  $\{a, b, \dots, z\}$  is mapped to  $\{0, 1, \dots, 25\}$  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, punctuations, 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 uxuyfzhztc lkg-gumcq vwoe  
ziu tdaui g ntsp pcrq bq ldvf eql, ymwp vlh nqvpncne, "1 ltmqs vs pg crqj-  
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.** [An equivalent definition of perfect privacy]

*This exercise is optional, but might be useful in answering Problem 5, 6, 7 and 8 below.*

There are a number of different formulations of one-time perfect privacy that turns out to be equivalent to the game-based definition we gave in class. Here is one of the most common ones (also used in [BR]):

**Definition.** An encryption scheme  $\Sigma = (\text{Enc}, \text{Dec})$  defined over  $(\mathcal{K}, \mathcal{M}, \mathcal{C})$  has *one-time perfect privacy* if for every  $M, M' \in \mathcal{M}$  and every  $C \in \mathcal{C}$

$$\Pr[\text{Enc}(K, M) = C] = \Pr[\text{Enc}(K, M') = C].$$

In both cases the probability is taken over the random choice  $K \xleftarrow{\$} \mathcal{K}$  and the coins tossed by Enc (if any).

- a) Show that the substitution cipher does not achieve perfect privacy using the above definition.

**Hint:** If you get stuck, look at the proof of Claim 2.4 in [BR].

- b) Prove that the one-time pad has perfect privacy using the above definition.

**Hint:** Calculate  $\Pr[K \oplus M = C]$  and  $\Pr[K \oplus M' = C]$  directly.

**Hint:** If you get stuck, look at the proof of Claim 2.5 in [BR].

- c) [Hard] Prove that the above definition is equivalent to the game-based definition given in class. In other words, you need to show that if  $\Sigma$  satisfies the above definition then it also satisfies the game-based definition, and vice-versa.

**Hint:** Above def.  $\implies$  game-based def.: This is basically just a generalization of the argument given in class: given that  $\Pr[\text{Enc}_K(M) = C] = \Pr[\text{Enc}_K(M') = C]$  for *any*  $M, M' \in \mathcal{M}, C \in \mathcal{C}$ , is there any difference in what the adversary sees in World 1 and World 0 in experiment 1-priv? What does this imply about what the adversary learns about  $b$  by observing  $C$ ?

**Hint:** Above def.  $\Leftarrow$  game-based def.: Prove the **contrapositive**: show that if  $\Sigma$  does *not* have perfect privacy according to the above definition, then it also does *not* have perfect privacy according to the game-based definition. In particular, show that if  $\Pr[\text{Enc}_K(M) = C] \neq \Pr[\text{Enc}_K(M') = C]$  for *some*  $M, M', C$ , then you can create an adversary that is able to distinguish World 1 and World 0 with probability other than  $1/2$ , i.e.,  $\Pr[b' = b] \neq 1/2$ .

### Problem 5.

Alice is using the one-time pad and notices that when her key is the all-zero string  $K = 0^n$ , then  $\text{Enc}(K, M) = M$  and her message is sent in the clear! To avoid this problem, she decides to modify the scheme to exclude the all-zero 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 6.** [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 7.** [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 8.** [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).

- a) 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:** Find an explicit enumeration of all the possible ways of dealing the 52 cards. That is, find a way of associating every possible deal with an integer in the range  $0, 1, \dots, \binom{52}{26} - 1$ . Once this is done, encryption can be defined using the idea of Problem 7. For the enumeration it might be helpful to look up the concept of a [combinatorial number system](#).

- b) 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 9.**

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 10.** [Problem 0.1 in [Ros]]

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

- 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 11.**

- 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?<sup>1</sup>
- 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 there is a great prize (say a million dollars); behind the other two doors there is nothing. You're 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 your 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>.

---

<sup>1</sup>Assume that boys and girls are born with equal probability.