

Introduction to Cryptography

TEK 4500 (Fall 2024)

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). Recall that the substitution cipher works by selecting a random *permutation*¹ of the message alphabet $\Sigma = \{A, B, \dots, Z\}$ and applying this permutation to each letter in the message.

Lm gsv hrcgs wzb lu Szgv Dvvp, zugvi gsv kilxvhhrmlh, gsv hkvvxsvh, gsv
hslfgrmt, gsv hrmtrmt, gsv yzmmvih, gsv klhgvi, gsv uronh, gsv dzedliph,
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 ylvow fk rmgl hfxs
wvorirfn gszg ru gsv xildw xlfow szew tlg gsvri szmwh lm gsv 2,000 Vfizhrzm
dzi-xirnmzoh dsl dviv gl yv kfyorxob szmtvw lm gsv ozhg wzb lu gsv kilxvvrmt,
gsbv dlfov fmjfvhgrlmzyob szew glim gsvn gl krxxvh—zg qfhg gsrh nlnvmg rg
szw yvvm zmmlfmxxw 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.

¹A function $\pi: \Sigma \rightarrow \Sigma$ that maps each letter in Σ to a unique letter in Σ .

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:

```
M = thisisaniceday
+K = dicedicedicedi
-----
C ≡ wpkwlacrlkghdg (mod 26)
```

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 whzxmfj 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 prcg bq ldvf eql, ymwp vlh nqvpcne, "l ltmqs vs pg crqqj-
moivmr," 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 $\text{Enc}(K, M) = M$ 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 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.

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

Problem 7.

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) Find x such that $5 \cdot x \equiv 1 \pmod{19}$

Hint: it is *not* $\frac{1}{5}$

Problem 8. [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 9.

- 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?²
- 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) A drawer contains red socks and black socks. When two socks are drawn at random the probability that both are red is $1/2$. How small can the number of socks in the drawer be? What if the number of black socks is required to be even?
- d) You have 3 coins. Two of them are fair; one is rigged so that it always lands on heads. You choose a coin at random and flip it; it lands on heads. The coin is probably:
- Fair
 - Rigged
 - Equally likely

Hint: Use [Bayes' Theorem](#).

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 Jan 3, 2021). <https://web.engr.oregonstate.edu/~rosulekm/crypto/crypto.pdf>.

²Assume that boys and girls are born with equal probability.