Introduction to Cryptography

TEK 4500 (Fall 2023)
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 $\Sigma = \{\mathsf{A}, \mathsf{B}, \ldots, \mathsf{Z}\}$ and applying this permutation to each letter in the message.

> 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?

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

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

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

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.

The following problems give you some practice with the notion of one-time perfect privacy. In answering these you can either use the game-based definition presented in class, or any of the many formulations equivalent[2] to it. For example the following definition is probably the most common version of perfect privacy (also used in [BR]).

[2] See this note for a proof that the definition given in class is equivalent to Definition 1.

Definition 1. An encryption scheme $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has *one-time perfect privacy* if for every $M, M' \in \mathcal{M}$ and every $C \in \mathcal{C}$

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

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

For reference, here's the definition of one-time perfect privacy we used in class.

Definition 2. An encryption scheme $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has (*game-based*) *one-time perfect privacy* if any adversary $\mathcal{A}$ has *zero* advantage in the following game

$\underline{\mathbf{Exp}^{\text{1-priv}}_{\Pi}(\mathcal{A})}$

1: $b \xleftarrow{\$} \{0,1\}$
2: $K \xleftarrow{\$} \Pi.\mathsf{KeyGen}$
3: $M \leftarrow \mathcal{A}$ // $\mathcal{A}$ picks message it wants to see encrypted
4: $R \xleftarrow{\$} \{0,1\}^{|M|}$ // Challenger draws random msg. of equal length
5: $C_0 \leftarrow \Pi.\mathsf{Enc}(K, M)$ // "World 0": encrypt M
6: $C_1 \leftarrow \Pi.\mathsf{Enc}(K, R)$ // "World 1": encrypt R
7: $b' \leftarrow \mathcal{A}(C_b)$ // $\mathcal{A}$ tries to guess which world it's in based on C_b
8: **return** $b' \stackrel{?}{=} b$

where the *advantage* of $\mathcal{A}$ is defined as

$$\mathbf{Adv}^{\text{1-priv}}_{\Pi}(\mathcal{A}) \stackrel{\text{def}}{=} \left| \Pr[\mathbf{Exp}^{\text{1-priv}}_{\Pi}(\mathcal{A}) \Rightarrow \mathsf{true}] - \frac{1}{2} \right|.$$

Problem 4.

a) Show that the substitution cipher does not achieve one-time perfect privacy. For concreteness, suppose the message space consists of all four letter messages, i.e., $\mathcal{M} = \Sigma^4$ where $\Sigma = \{\mathsf{A}, \mathsf{B}, \ldots, \mathsf{Z}\}$.

Hint: If you're using the game-based one-time perfect privacy definition: which message should you (as the adversary $\mathcal{A}$) send to the challenger in order to maximize your chances of distinguishing between World 0 ($b = 0$) and World 1 ($b = 1$)?

Hint: If you're using Definition 1 you need to come up with two messages M, M and a ciphertext C such that $\Pr[\mathsf{Enc}_\pi(M) = C] \neq \Pr[\mathsf{Enc}_\pi(M') = C]$. Note here that the probability is taken over all possible keys, which for the substitution cipher is all possible permutations π of the alphabet Σ.

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

Hint: If you're using Definition 1, calculate $\Pr[K \oplus M = C]$ and $\Pr[K \oplus M' = C]$ directly.

Problem 5.
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-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 $0, 1, \ldots, \binom{52}{26} - 1$. 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 $\{1, 2, \ldots, d\}$.

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 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?[3]

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?

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

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.