Problem Set 3 Cryptography, 6CCS3CIS
Eamonn W. Postlethwaite October 9, 2025

Let HISTORICAL-CIPHERS = {Caesar, monoalphabetic substitution, Vigenère}.[1] In each question below you may assume sk for Vigenère has length n, a positive integer.

Problem 1. *On the insufficient security of historical ciphers.*

In this question we will examine ways in which historical examples of SKE fail to achieve security definitions demanded of contemporary cryptography *without* requiring sometimes tedious cryptanalysis.

i. For each cipher in HISTORICAL-CIPHERS define it in the framework of $\mathsf{SKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. In particular define the message, ciphertext and key spaces; $\mathcal{M}$, $\mathcal{C}$ and $\mathcal{K}$. Then define Enc and Dec. (If the historical description does not specify KGen you may assume a key is uniformly sampled from $\mathcal{K}$.)

ii. For each cipher in HISTORICAL-CIPHERS describe how to recover sk given access to $\mathsf{Enc}(sk, \cdot)$.

iii. For each cipher in HISTORICAL-CIPHERS suppose sk is chosen according to KGen and $b \in \{0,1\}$ is chosen uniformly. Give two messages $m_0, m_1 \in \mathcal{M}$ of the same length such that if you are given $c = \mathsf{Enc}(sk, m_b)$ you can determine b.

Problem 2. *On the one time pad.*

In this question assume the message, ciphertext and key alphabet are binary, i.e. $\alpha_{\mathcal{M}} = \alpha_{\mathcal{C}} = \alpha_{\mathcal{K}} = \{0,1\}$. This means $\mathcal{M}, \mathcal{C}, \mathcal{K} \subseteq \{0,1\}^*$.

i. Define the one time pad in the framework of $\mathsf{SKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ for messages of length at most n bits. Here n is an arbitrary positive integer.

ii. An adversary with access to $\mathsf{Enc}(sk, \cdot)$ can recover sk for the one time pad. How?

iii. Why does (*ii.*) not contradict the perfect secrecy of the one time pad? (Hint: what conditions on sk does the proper operation of the one time pad demand?)

iv. Let KGen sample uniformly from $\mathcal{K} = \{0,1\}^n$. With what probability does KGen sample $sk = 00\cdots0$, i.e. the all zeros secret key?

v. The one time pad is perfectly secure even though the all zeros secret key of (*iv.*) exists and is sampled with positive probability. Why?

vi. Let $n = 1$ so messages are a single bit. Assume messages are equal to 0 with probability 1/3 and equal to 1 with probability 2/3. If the same $sk \in \{0,1\}$ is mistakenly used to encrypt many such one bit messages $m_1, m_2, \ldots, m_\ell$ to $c_1, c_2, \ldots, c_\ell$, how should we guess sk? (Hint: each $c_i = m_i \oplus sk$ will be either 0 or 1, if there are e.g. many more c_i equal to one than zero then which sk do we expect?).

vii. Should you use the same key to encrypt many messages via the one time pad?

viii. Which of Kerckhoffs' principles does the one time pad satisfy? Which does it not?

ix. Research and describe a historical use of the one time pad.

Problem 3. *On practical use and cryptanalysis of historical ciphers.*

i. For each cipher in HISTORICAL-CIPHERS use it to encrypt and decrypt a message of your choice.

For each of the following three questions decrypt the ciphertext. They are produced using the Caesar, monoalphabetic and Vigenère ciphers respectively. They are all film quotes, and I have left the spaces in for your convenience. The key for the Vigenère cipher has length three.

ii. w jtcm kwum nwzbp w jtcm izqam w jtcm iakmvl w jtcm kwum qv

iii. itqr qfr iqfrl fttr q dtroqzgk zit dtroqzgk wtzvttf itqr qfr iqfrl dxlz wt zit itqkz

iv. zjc jsce hfzbej mml dcfdjv kmlzbeh zvzgvjc rhrrqi jvggg me tgis mwt rys qycscrci cd ffgfb g nortvcu q zvokj ujzhrvf ge hfv ryiy lvop kvc kolevylgci uyks ycz rycqv amdslkg uzzj ss jfgr zb rzac cwiv hcrfq zb prwl kwkv hm uwc

[1] We use 'cipher' here for historical reasons.