George Mason University — Prof. Foteini Baldimtsi
CS 487/587: Cryptography — Homework 1: Probabilities, Perfect Secrecy and OTP

Homework 1: Probabilities, Perfect Secrecy and OTP

Submission policy. Submit your answers on Blackboard by 11:79pm Friday, **Sept. 3**, 2021. Your submission should include a .PDF file with all the answers to the theoretical problems. You should try to typeset your homeworks. Latex is especially recommended. No late submissions will be accepted. Your writeup MUST include the following information:

1. Your name and whether you take the class at **487** or **587** level.
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

The homework will be graded by the class TA Anuj Pokhrel (apokhre@gmu.edu).

Exercise 1. Probabilities [20 points] Let s be a binary string of size n bits (where n is an even number). Compute the following probabilities:

- What is the probability that the nth bit of s is equal to 0?
- What is the probability that the last $n/2$ bits are equal to 0?
- What is the probability that the first and the last bit are equal?
- What is the probability that the first $n/2$ bits are equal to the last $n/2$ bits i.e. if $s = x||y$ (where $||$ denotes string concatenation), what is the probability that $x = y$?

Exercise 2. Shift Cipher [15 points] Consider the shift cipher as we discussed it in class.
Key space $\mathcal{K} = \{0, 1, \ldots, 25\}$.

Suppose that we are given the following message space distribution, M:
$\Pr[M = \text{‘bye’}] = 0.2$
$\Pr[M = \text{‘yes’}] = 0.3$
$\Pr[M = \text{‘now’}] = 0.5$

Answer the following questions and make sure that you show your work.

(a) **(5 Points)** Compute the probability:
$\Pr[M =$ ‘now’$|C =$ ‘baa’$]$

(b) **(10 Points)** Compute the probability:
$\Pr[M =$ ‘yes’$|C =$ ‘zft’$]$

Exercise 3. OTP [30 points] Recall the One Time Pad encryption system we saw in class:

Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

$\mathsf{Gen} : k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\mathsf{Enc}(k, m) : c_i = m_i \oplus k_i$
$\mathsf{Dec}(k, c) : m_i = c_i \oplus k_i$

Assume that an adversary knows that $\Pr[m = 010] = 0.5$ and $\Pr[m = 011] = 0.5$. The adversary then observes a ciphertext $c = 010$. Compute the following probabilities:

(a) **(10 Points)** What is $\Pr[m = 010 \mid c = 010]$? (Show your work.)

(b) **(10 Points)** What is $\Pr[m = 011 \mid c = 010]$? (Show your work.)

Alice is using one-time pad and notices that when her key is the all-zeroes string $k = 0^\lambda$, then $Enc(k, m) = m$ and her message is sent in the clear! To avoid this problem, she decides to modify Gen to exclude the all-zeroes key, i.e. choose a key uniformly from $\{0,1\}^\ell \backslash \{0\}^\ell$. In this way, she guarantees that her plaintext is never sent in the clear.

(c) **(10 Points)** Is the modified cryptosystem still perfectly secret? Prove or disprove (informally).