CS4236 Individual Assignment 1

August 19, 2022

1 The rules...

You can use any result stated in the book and lecture. However, suppose you are asked to prove, say, Theorem x.y, typically you should not use a result that appears after the occurrence of Theorem x.y in the book. (i.e. you cannot use a more *powerful* theorem that appears later). You are not allowed to use *sophisticated* notions not (yet)taught in class. It is hard to precisely indicate what can, and what cannot be used, and common sense applies.

This assignment should take only 2 or so pages if using 12 point fonts. Neatly handwritten, and then scanned will be accepted. However, if illegible, the grader might just skip it. If handwriting is large, the submitted solution can be longer.

A longer solution doesn't mean better. Unnecessary arguments, wrong statements, wrong notations, wrong choice of wordings (e.g. writing something like "from theorem X I think it should be perfectly secure" would be penalised).

Assignment deadline is 5pm, 2nd Sept 2022. Uploaded to the Luminus assignment submission folder in pdf format. The file name should be like e00XXXXXX.A1.pdf (Your student id and ".A1.pdf") .

2 Questions - 5 assignment questions, due 2nd Sept.

1. Provide a formal definition of the Gen, Enc, and Dec algorithms for a (poorly constructed) Vigenere poly-alphabetic cipher over the alphabet $A \dots Z$, which does not allow any of the corresponding characters in the message and plaintext to be the same. The repeated key length of the cipher is t. (3 marks)

2. Prove the correctness of the cipher in question 1. (2 marks)

3. Explain why the cipher in question 1 is a poorly constructed cipher. (2 marks)

4. In the lecture on perfect secrecy (Topic2), there was a brief discussion about a specific (bad) crypto scheme: a shift cipher that operates in the domain $\mathbb{Z}$. The key and the message were integers uniformly and randomly chosen from $\{0, 1, 2, 3, 4, 5\}$. The encryption is $\text{Enc}_k(x) = x + k$ (note, no modulo). Find the following, clearly stating *why* for each answer: (4 marks)

1. $\Pr[X = 1, K = 2|C = 5]$, $\Pr[X = 1|C = 5, K = 2]$.
2. $\Pr[K = 3|X = 2]$.
3. $\Pr[X = 0|C = 5]$, $\Pr[X = 1|C = 5]$,... (i.e. the distribution $X|C = 5$).
4. $\Pr[X = 0|C = 1]$, $\Pr[X = 1|C = 1]$,...

5. Prove or refute: For every perfectly secret encryption scheme it holds that for every distribution on the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$: (4 marks)

$$\Pr[M = m | C = c] = \Pr[M = m' | C = c]$$

probability of M=m given C=c is the probability of M=m' given C=cidea is to prove that perfect