CS4236 Assignment 1 feedback

September 14, 2022

1 Questions with feedback

1. Provide a formal definition of the Gen, Enc, and Dec algorithms for a (poorly constructed) Vigenere polyalphabetic cipher over the alphabet $A \ldots Z$, 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)

Feedback: *Your definition had to*

- ***(a)*** *identify the symbols A..Z encoding to 0..25.*
- ***(b)*** *clearly show that the individual subkeys were drawn from 1..25, not 0..25.*
- ***(c)*** *be for a rotation type polyalphabetic cipher, not some other kind of substitution. It had to include the repeated key length for example. No model answer here, but a possibe Enc might be:*

  Enc: *Given plaintext encoding $P = p_0, \ldots, p_n$ and key $K = k_0, \ldots, k_{t-1}$, then for each p_i in the plaintext, set $c_i := ((p_i + k_{[i \bmod t]}) \bmod 26)$. The full ciphertext output is $C = c_o, \ldots, c_n$.*

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

Feedback: *Your proof had to*

- ***(a)*** *show clear understanding of the question, that is you were being asked to prove in detail: the correctness requirement for a symmetric cipher. This was expressed in the first lecture as "For correctness, we see that for all k, m, $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$".*
- ***(b)*** *give the reasons for each step of the proof - i.e. follow the style of proof that was asked for.*

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

Feedback: *Your explanation had to*

- ***(a)*** *show clearly that you understood that not allowing individual plaintext elements to encode to the same ciphertext was the "poor construction".*
- ***(b)*** *some clarity, for example that the resulting system has a smaller keyspace, OR that if the message length n is less than or equal to the repeated key length t this is not an OTP, but would be if you allowed all possible encodings, OR an example of an attack - for example if you knew a plaintext, you might be able to see where it is not.*

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. $\Pr[X = 0 | C = 1]$, $\Pr[X = 1 | C = 1]$,...

Feedback: *You only got full marks if there was an explanation (however brief) attached to each part of the question.:*

1. *0 and 0. It is not possible that C could be 5 with the given values.*

2. *Also a bit of a trick - the key and the message are integers uniformly chosen, and as such they are independent, so can remove X=2, and the remaining probability is* $\frac{1}{6}$.

3. *Each value will be* $\frac{1}{6}$. *This could be done by applying Bayes theorem.*

4. *First two are* $\frac{1}{2}$ *(show working), but all the others are 0.*

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)

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

Feedback: *Your proof should*

(a) *argue that it is false*

(b) *be clear in the explanation. Note that there was no requirement for a message space to be uniformly distributed in perfect secrecy, and so we cannot equate the two equations - in fact since there may be a pair* $m, m' \in \mathcal{M}$ *where* $\Pr[M = m] \neq \Pr[M = m']$, *then we have a case where* $\Pr[M = m | C = c] \neq \Pr[M = m' | C = c]$. *Therefore it is not true that it MUST be the case that* $\Pr[M = m | C = c] = \Pr[M = m' | C = c]$.