INFO2222: Homework 1

Instructions: read all the questions carefully and explain your answers with examples and figures where it is required. If you want to reuse a diagram from slides, it is always recommended to redraw and give reference. This assessment (HW1) has total of 100 points and weightage of 6%.

Q1. Confidentially, Integrity and availability are considered as three main components of the information security. Classify each of the element in following two scenarios and explain how they are implemented: (7.5*2=15 points)

1. Web server handling online sales for the computer hardware parts.
2. ATM machines

Q2. Technically, one time pad encryption looks perfect and it's hard to break it; however, one time pad has weak points and its hardly in the practice. Please state the reasons with an example that explain why it's not in practice. What are the streamciphers, why we need pseudorandom generators (PRG) with stream ciphers? Use diagrams where appropriate. (10+10=20 points)

Q3. What is the difference between hash functions and message authentication code (MAC)? Why HMAC looks more secure? Justify with an example. Highlight the shortcomings of both mechanisms. Please use figures where it is appropriate. (15 points)

Q4. What is 256 in SHA-256? Why SHA256 is better than the previous versions of SHA like SHA-1? Compare the performance of SHA256 with MD5. Please justify your answer with examples. (15 points)

Q5. Generating keys require the users to collect enough random data, it is well known that user generated secret keys are mostly with bad quality, i.e., easy to predict. Suppose USYD implements a secure communication system, and the university admin wishes to establish a secure channel for each of the student to Canvas, i.e., the university wishes to generate/share a secret key with each of the student. On the other hand, the university only wishes to store one single short secret msk, i.e., creating a different key for each student and store all of them in the server is NOT an option. What should the university do to produce a key for each student without the need to store all of them? Suppose there are in

total 50,000 students, and the university only wishes to store one 128-bit master secret. Briefly explain your solution. The above is actually a standard functionality of a key distribution center. (Hint: each student has a unique and public sid) (10 points)

Q.6 Suppose before the first lecture, you all received an email claiming “it is from the teacher, and please use the following public key pk for future communication with me, the lecturer". Since we never met, you guys naturally felt suspicious about the email. In order to convince you the public key is the correct one for me, what should I further provide, assuming you all have access to USYD VC's public key pk_{VC}, which is on the website of USYD, thus available to everyone. (10 points)

Q7. Consider the following application scenario: suppose you would like to backup your birthday party video in a cloud, say Google Cloud. During the party, you and some of the friends got drunk, so you don't want anyone you don't know to see the video, moreover, the video file is about 5 Gigabytes. Google's public key is pk_G and can be found easily online. We know that public key encryption is flexible, but it is computationally expensive, especially on large filles. While a symmetric key encryption is simple and efficient, however, Google won't be able to share a secret key with its clients. More concretely, a public key encryption on 1Kb data might use less than one second, but if on 5 Gigabytes data, it might take two hours; on the other hand, a symmetric key encryption on 5 Gigabytes still cost only a couple of, say 10 seconds. Describe a possible mechanism with detailed algorithm description, so that you can use it to upload the 5 Gigabytes video quickly and securely to Google Cloud, taking about only 12 seconds (ignoring the network latency)? (15 points)