**Solutions for Assignment 1**

Rahul Chowdary Garigipati

Chapter-1:

1. Consider the definitions of confidentiality, integrity, and availability.
2. When might each of these aspects of information security be more important than the others?

Ans.) **Confidentiality** can be defined as a way to prevent unauthorized ‘reading’ of information.

**Integrity** can be defined as a way to prevent unauthorized ‘writing’ of information.

**Availability** can be defined as a way to prevent ‘Distribution of Denial of Service(DDoS)’. In other words, it can be defined as data is available in a timely manner when needed.

Each aspect has importance than the other aspects in different cases. For ex: information Confidentiality is more important than the Integrity and Availability in the case of proprietary of a company or in case of people’s personal information.

Integrity is more important than the Confidentiality and Availability in the case of financial information, as any changes in the financial records leads to the issues like instability, consistency, and the value of the information. Note that Confidentiality and Integrity are not the same.

Availability is more important than the Confidentiality and Integrity in the case of information availability to the public from the government announcements.

1. Describe a few situations, where strengthening one of these might weaken another.

Ans.) Based on the above question, we can say that there is no such thing as a weak aspect as each aspect has an utmost importance based on the different situation in the real life. For ex: let`s take the same above example to define the importance of the three aspects. As the example states the importance of one aspect than the others doesn`t mean that the least important aspect is a weak aspect.

Confidentiality is more important than the Integrity and Availability in the case of proprietary of a company or in case of people’s personal information. Here the ‘Availability’ has the least importance than that of ‘Confidentiality’ followed by ‘Integrity’. This doesn`t mean that ‘Availability’ is a weak aspect, as it also helps in maintaining the information security.

Integrity is more important than the Confidentiality and Availability in the case of financial information, as any changes in the financial records leads to the issues like instability, consistency, and the value of the information. Note that Confidentiality and Integrity are not the same. Here the ‘Availability’ has the least importance than that of ‘Integrity’ followed by ‘Confidentiality’. This doesn`t mean that ‘Availability’ is a weak aspect, as it also helps in maintaining the information security.

Availability is more important than the Integrity and Confidentiality in the case of information availability to the public from the government announcements. Here the ‘Confidentiality’ has the least importance than that of ‘Availability’ followed by ‘Integrity’. This doesn`t mean that ‘Confidentiality’ is a weak aspect, as it also helps in maintaining the information security.

Chapter-2:

1. Using the letter encodings in Table 2.1, the following ciphertext message was encrypted with a one-time pad:

KITLKE.

1. If the plaintext is "thrill," what is the key?

Ans.) We know that to find the key we need to XOR the plaintext and the ciphertext.

From the Table 2.1 we know that,



We know that the Plaintext is: T H R I L L

We know the binary from the table above, hence: 111 001 101 010 100 100

We know that the Ciphertext is: K I T L K E

We know the binary from the table above, hence: 011 010 111 100 011 000

Hence the binary for Key is (by doing XOR operation): 100 011 010 110 111 100

Hence the Key is:  **L K I S T L**

1. If the plaintext is "tiller," what is the key?

Ans.) We know that to find the key we need to XOR the plaintext and the ciphertext.

From the above table we know the binaries of the plaintexts, ciphertexts and keys,

We know that the Plaintext is: T I L L E R

We know the binary from the table above, hence: 111 010 100 100 000 101

We know that the Ciphertext is: K I T L K E

We know the binary from the table above, hence: 011 010 111 100 011 000

Hence the binary for Key is (by doing XOR operation): 100 000 011 000 011 101

Hence the Key is:  **L E K E K R**

1. Suppose that Alice encrypted a message with a secure cipher that uses a 40-bit key. Trudy knows the ciphertext and Trudy knows the algorithm, but she does not know the plaintext or the key. Trudy plans to do an exhaustive search attack, that is, she will try each possible key until she finds the correct key.
2. How many keys, on average, must Trudy try before she finds the correct one?

Ans.) The total number of keys in total that Trudy has to find are (since it is a 40-bit key). And the total number of keys that Trudy has to try before finding the right one is = .

1. How will Trudy know when she has found the correct key? Note that there are too many solutions for Trudy to manually examine each one she must have some automated approach to determining whether a putative key is correct or not.

Ans.) As keys is a bit much to go through manually, so what Trudy can do is write a program to decrypt the cipher text using all the possible keys and return the plaintexts.

1. How much work is your automated test in part b?

Ans.) Our work is to return a meaningful plaintext to Trudy.

1. How many false alarms do you expect from your test in part b? That is, how often will an incorrect key produce a putative decrypt that will pass your test?

Ans.) False Alarms are said to be plaintexts that generate after the decryption but doesn`t contain the exact plaintext that is needed. Since we have only one key that gives us the exact plaintext even though they are meaningful plaintexts, the rest are all False Alarms. So, the maximum number of False Alarms are ‘- 1.’

1. Suppose a cipher uses an 8-character mixed-case alphanumeric key (0-9, a-z, and A-Z).
2. What is the size of the keyspace (i.e., how many unique keys are possible)?

Ans.) The alphanumeric key consists of 10 characters from (0-9) and 26 characters from (a-z) and 26 characters from (A-Z). So, the keyspace would be 10 \* 26 \* 26 = 6760.

Therefore, 6760 unique keys are possible.

1. What is the approximate strength of the key, measured in bits? (Hint: rewrite the size of the keyspace as a power of two.)

Ans.) The approximate strength of the key would be between .

1. If a particular computer can test keys per second, how long will it take (on average) to guess the key of this cipher?

Ans.) The time taken is calculated by dividing the total number of keys with the 40-bit key. i.e., seconds.

1. Consider that the 8-character key from the previous problem would take up 64 bits if stored as an ASCII string. However, in this scenario, not every bit would contribute to the strength of the key. Assume the cipher is upgraded to use all 64 bits.
2. What is the new size of the keyspace?

Ans.) The new size of the keyspace is .

1. How much time would it take to crack the new version of the cipher (if able to test keys per second)?

Ans.) The time it takes to crack the new version of the cipher if