Shashank Karthikeyan
A50703012

CSE 201 Homework #7

1. The focus of chapter 5 was error detection and correction. The first method of error detection and correction is called the repletion trick. Here a message transmitted repeatedly such that it is possible to detect errors. Let's say you transmit the numerical value 5213.75 1000 times. Due to an unreliable connection, some digits do get changed but across the 1000 transmissions, a computer can figure out what are the most commonly occurring digits. The next method is called the redundancy trick where the information is encoded in such a way that it has a higher tolerance to data corruption. For example, the above message of 5213.75 would be encoded in English to get "five two one three point seven five". Even if some of the letters got changed, it would still be possible to understand what the message so a computer can decode it. The next method is called the check sum trick where the values are summed up and the last digit of the sum is used as the checksum value. It is then transmitted along with the message. On the receiving end, the checksum value set aside, the check sum is recalculated using the remaining digits and compared to the received check sum. This method served only as an error detection method. The last method is called the pin point trick. Here the message is split into 4 rows and 4 columns. The check sums for the rows are calculated and added as a new column to right of the array. The check sums for the columns are calculated and added as new row to the bottom of the array. Then you create the final message by reading from left to right, top to bottom.
2.
    a. Malware is an umbrella term that refers to any hostile and unwanted piece of software that run on a user's computer without consent. It includes viruses, worms, ransomware, spyware, adware and others.
    b. Viruses are a type of malware that have the unique ability to replicate or grow larger through "infected" files. They can be transferred over the internet, a network or any form of transferable media. They are usually reliant on some sort of user action such as clicking on suspicious links or advertisements.
    c. Like a virus, a worm can replicate but it is not reliant on other files. It can spread without the need for the user to do anything.
    d. Phishing is the use of fake links, fake websites or even fake emails that look legitimate. They often contain key loggers that can aid in the theft of login credentials, payment information and other types of sensitive data.
    e. A botnet is a network of private computers that are infected with malicious software and are controlled as a group to perform things like sending spam messages or host a web server. Often, it is done without the knowledge of the users.

3. The International Standard Book Number is unique numerical identifier for books. ISBN 13 contains 13 digits. The check digit calculation for an ISBN-13 number is as follows. The last digit (check digit) must range between 0 and 9. The sum of all 13 digits each multiplied by its weight (alternates between 1 and 3) should be a multiple of 10. Converting from ISBN 10 to ISBN 13 works as follows. Remove the ISBN check digit (last digit), prefix 978 to the front of the number, then calculate the 13th check digit using the following formula: x13=(10-(x1+3x2+x3…+3x12)mod10)mod10. Ex. Given the ISBN 10 number 0735611319, if we follow the above steps we get 978073561131.
4. A bank routing number or ABA routing transit number is a 9-digit code used by banks in the USA. The first 4 digits are the federal reserve routing symbol. The next four digits identify the bank. The 9th digit is the check digit. To check if it's valid, you multiply the first digit by 3, second by 7 and third by 1. Repeat for 4th,5th,6th, then 7th, 8th, 9th. Sum all the values if the sum is a multiple of 10 then it is valid. Given 072000805, the check sum is 80 which is a multiple of 10. Therefore the account number is valid.