Problem Set 1

Andrew Kaufman
SID: 998048873

April 22, 2016

PROBLEM 5

(a) Alice shuffles a deck of cards and deals it out to herself and Bob so that each gets half of the 52 cards. Alice now wishes to send a secret message *M* to Bob. Eavesdropper Eve is watching and sees the transmissions.

Suppose Alice's message M $\epsilon\{0, 1\}^{48}$ is a string of 48 bits. Describe how Alice can communicate M to Bob in a way that achieves perfect privacy.

PROBLEM 6

```
# Andrew Kaufman
# 998048873

# run using Python3

import math
import random
import string


def keygen():
    key = []
    for i in range(16):
        byte = random.randint(0, 255)
        key.append(byte)

    return key

def init(key):
    length = len(key)
    S = list(range(256))

    j = 0
    for i in range(256):
        j = (j + S[i] + key[i % length]) % 256
        S[i], S[j] = S[j], S[i]

    return S

def stream(S):
    i = 0
    j = 0

    K = []

    for _ in range(2):
        i = (i + 1) % 256
        j = (j + S[i]) % 256

        S[i], S[j] = S[j], S[i]
        K.append(S[(S[i] + S[j]) % 256])

    return K


def main():
    table = [0 for i in range(10)]

    for i in range(100000):
        key = keygen()
        S = init(key)
        K = stream(S)

        if 0 <= K[1] <= 9:
            table[K[1]] += 1

    for j in range(10):
        table[j] /= 10000
        print(str(j) + ": " + str(table[j]))
```

```
if __name__ == '__main__': main()
```