Security & Cryptography Assignment 1

Anna Visman 6351115

01/12/2025

1 Historical Ciphers

a)

b)

c)

2 Number Theory and Elliptic Curve

3 Information Theoretic Security

a) To avoid hand calculations, I coded the formulas required for this exercise. My code can be found in the appendix.

First we calculate the probability of each cipher text occuring usings the formula:

$$p(C = c) = p(P = m) \cdot p(C = c|P = m)$$

$P(C = 1) = p(K = k_1) \cdot p(P = b) + p(K = k_2) \cdot p(P = c) + p(K = k_3) \cdot p(P = d) + p(K = k_4) \cdot p(P = a) = \frac{1}{5} \cdot \frac{4}{15} + \frac{3}{10} \cdot \frac{1}{5} + \frac{1}{5} \cdot \frac{1}{5} + \frac{3}{10} \cdot \frac{1}{3} = 0.25\bar{3}$

Repeating this for the other ciphertexts gives:

$P(C = 2) = 0.25\bar{3}$

$P(C = 3) = 0.24\bar{6}$

$P(C = 4) = 0.24\bar{6}$

Then, we calculate the probability of each cipher text occuring given the plaintext and key distributions using the encryption schema:

$$p(C = c) = \sum_{k:c \in \mathbb{C}(k)} p(K = k) \cdot p(P = d_k(c))$$

$$
\begin{aligned}
&P(C=1 \mid P=a)=0.3, \quad P(C=2 \mid P=a)=0.3, \quad P(C=3 \mid P=a)=0.2, \quad P(C=4 \mid P=a)=0.2,\\
&P(C=1 \mid P=b)=0.2, \quad P(C=2 \mid P=b)=0.2, \quad P(C=3 \mid P=b)=0.3, \quad P(C=4 \mid P=b)=0.3,\\
&P(C=1 \mid P=c)=0.3, \quad P(C=2 \mid P=c)=0.3, \quad P(C=3 \mid P=c)=0.2, \quad P(C=4 \mid P=c)=0.2,\\
&P(C=1 \mid P=d)=0.2, \quad P(C=2 \mid P=d)=0.2, \quad P(C=3 \mid P=d)=0.3, \quad P(C=4 \mid P=d)=0.3.
\end{aligned}
$$

Finally, we can calculate the probability of each plaintext conditioned on each ciphertext occurrence (see code in appendix):

$$p(P=m|C=c)=\frac{p(P=m)\cdot p(C=c|P=m)}{p(C=c)}$$

$$
\begin{aligned}
&P(P=a \mid C=1)=0.395, \quad P(P=a \mid C=2)=0.395, \quad P(P=a \mid C=3)=0.270, \quad P(P=a \mid C=4)=0.270,\\
&P(P=b \mid C=1)=0.211, \quad P(P=b \mid C=2)=0.211, \quad P(P=b \mid C=3)=0.324, \quad P(P=b \mid C=4)=0.324,\\
&P(P=c \mid C=1)=0.237, \quad P(P=c \mid C=2)=0.237, \quad P(P=c \mid C=3)=0.162, \quad P(P=c \mid C=4)=0.162,\\
&P(P=d \mid C=1)=0.158, \quad P(P=d \mid C=2)=0.158, \quad P(P=d \mid C=3)=0.243, \quad P(P=d \mid C=4)=0.243.
\end{aligned}
$$

b)

c) A cryptosystem has perfect secrecy if

$$p(P=m|C=c)=p(P=m)$$

for all plain texts m and ciphertexts c.

A Code

Code used for exercise 3a:

```
M = [1/3, 4/15, 1/5, 1/5]
K = [1/5, 3/10, 1/5, 3/10]

m = ['a', 'b', 'c', 'd']

scheme = [
    [3, 1, 4, 2],
    [2, 4, 1, 3],
    [4, 2, 3, 1],
    [1, 3, 2, 4]
]

def prob_ciper(cipher, M, K, scheme):
    rows, cols = len(scheme), len(scheme[0])
```

```
    total = 0
    for i in range(rows):
        for j in range(cols):
            if scheme[i][j] == cipher:
                total+= M[i] * K[j]

    return total


for i in range(4):
    print(f"P(C={i+1}) =", prob_ciper(i+1, M, K, scheme))

def prob_cipher_given_plain(cipher, plain, K, scheme):
    rows, cols = len(scheme), len(scheme[0])

    total = 0

    col = ord(plain) - ord('a')

    # get only the column col
    col = [scheme[i][col] for i in range(rows)]

    for c in col:
        if c == cipher:
            total+= K[col.index(c)]

    return total

for char in m:
    for i in range(4):
        print(f"P(C={i+1}|P={char}) =",
            prob_cipher_given_plain(i+1, char, K, scheme))

def prob_plain_given_cipher(plain, cipher, M, scheme):
    rows, cols = len(scheme), len(scheme[0])

    total = 0

    p = ord(plain) - ord('a')

    prob = M[p]*prob_cipher_given_plain(cipher, plain, K, scheme)/
        prob_ciper(cipher, M, K, scheme)

    return prob

for char in m:
```

```python
for i in range(4):
    print(f"P(P={char}|C={i+1}) =",
        prob_plain_given_cipher(char, i+1, M, scheme))
```