# Cryptography Homework 2

*2024 Spring Semester*

21 CST H3Art

# Exercise 3.5 (The solution of problem b was wrong)

(a) Prove that the *Affine Cipher* achieves perfect secrecy if every key is used with equal probability $1/312$.

(b) More generally, suppose we are given a probability distribution on the set

$$\{a \in \mathbb{Z}_{26} : \gcd(a, 26) = 1\}.$$

Suppose that every key $(a, b)$ for the *Affine Cipher* is used with probability $\mathbf{Pr}[a]/26$. Prove that the *Affine Cipher* achieves perfect secrecy when this probability distribution is defined on the keyspace.

> **Solution:**
>
> (a) **Proof**:
>
> **Definition of perfect secrecy**: A cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ has perfect secrecy if $p(x|y) = p(x)$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
>
> To prove $p(x|y) = p(x)$, for each $a \in \mathbb{Z}_{26}^*$, $b \in \mathbb{Z}_{26}$, suppose $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, since every key is used with equal probability $1/312$, for every pair of $(x, y)$, we choose a specific $a$, therefore, the key $K$ can be represented as $(a, y - ax)$, and there are $\Phi(26) = 12$ possible choices for $a$.
>
> For every ciphertext $y \in \mathcal{C}$,
>
> $$\begin{aligned} p(y) &= \sum_{K: y \in \mathcal{C}(K)} p(K) p(d_K(y)) \\ &= \sum_{\{x, K: e_K(x) = y\}} p(K = (a, y - ax)) p(x) \\ &= \frac{12}{312} p(\text{‘a’}) + \frac{12}{312} p(\text{‘b’}) + \cdots + \frac{12}{312} p(\text{‘y’}) + \frac{12}{312} p(\text{‘z’}) \\ &= \frac{12}{312} \times 1 \\ &= \frac{1}{26} \end{aligned}$$
>
> For any $x \in \mathcal{P}$ and $y \in \mathcal{C}$,
>
> $$\begin{aligned} p(y|x) &= \sum_{\{K: y = e_K(x)\}} p(K) \\ &= \frac{1}{312} \times 12 \\ &= \frac{1}{26} \end{aligned}$$
>
> using Bayes' Theorem, $p(x|y) = \dfrac{p(x)p(y|x)}{p(y)}$, we can get:

$$
\begin{aligned}
p(x|y) &= \frac{p(x)p(y|x)}{p(y)} \\
&= \frac{p(x) \times \frac{1}{26}}{\frac{1}{26}} \\
&= p(x)
\end{aligned}
$$

Q.E.D.

(b) **Proof**:

Similarly, for every pair of $(x, y)$ and a specific $a \in \mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$, $\mathbf{Pr}[a] = \frac{1}{12}$, the key $K$ can be represented as $(a, y - ax)$, therefore:

$$
\begin{aligned}
p(y) &= \sum_{\{x, K : e_K(x) = y\}} p(K = (a, y - ax))p(x) \\
&= \sum_{\{x, K : e_K(x) = y\}} \frac{\mathbf{Pr}[a]}{26} p(x) \\
&= \frac{12 \times \frac{1}{12}}{26} p(\text{‘a’}) + \frac{12 \times \frac{1}{12}}{26} p(\text{‘b’}) + \cdots + \frac{12 \times \frac{1}{12}}{26} p(\text{‘y’}) + \frac{12 \times \frac{1}{12}}{26} p(\text{‘z’}) \\
&= \frac{1}{26}
\end{aligned}
$$

Then, for any $x, y \in \mathbb{Z}_{26}$,

$$
\begin{aligned}
p(y|x) &= \sum_{\{K : y = e_K(x)\}} p(K) \\
&= \frac{\mathbf{Pr}[a]}{26} \times 12 \\
&= \frac{1}{26} \times \frac{1}{12} \times 12 \\
&= \frac{1}{26}
\end{aligned}
$$

Finally, using Bayes' Theorem we can get:

$$
\begin{aligned}
p(x|y) &= \frac{p(x)p(y|x)}{p(y)} \\
&= \frac{p(x) \times \frac{1}{26}}{\frac{1}{26}} \\
&= p(x)
\end{aligned}
$$

Q.E.D.

# Exercise 3.8

Suppose that $y$ and $y'$ are two ciphertext elements (i.e., binary $n$-tuples) in the *One-time Pad* that were obtained by encrypting plaintext elements $x$ and $x'$ , respectively, using the same key, $K$. Prove that $x + x' \equiv y + y' \pmod 2$.

**Solution:**

**Proof**:

Since $y$ and $y'$ are binary $n$-tuples obtained by encrypting plaintext elements $x$ and $x'$ using *One-time Pad*, and use the same key $K$, we have:

$$x \oplus K = y$$

$$x' \oplus K = y'$$

Therefore,

$$\begin{aligned} y + y' \pmod 2 &= x \oplus K + x' \oplus K \pmod 2 \\ &= x \oplus K \oplus x' \oplus K \pmod 2 \\ &= x \oplus x' \oplus K \oplus K \pmod 2 \\ &= x \oplus x' \pmod 2 \\ &= x + x' \pmod 2 \end{aligned}$$

Q.E.D.

# Exercise 3.9(a)

(a) Construct the encryption matrix (as defined in Example 3.3) for the *One-time Pad* with $n = 3$.

**Example 3.3**

Let $P = \{a, b\}$ with $\mathbf{Pr}[a] = 1/4$, $\mathbf{Pr}[b] = 3/4$. Let $K = \{K_1, K_2, K_3\}$ with $\mathbf{Pr}[K1] = 1/2$, $\mathbf{Pr}[K_2] = \mathbf{Pr}[K_3] = 1/4$. Let $C = \{1, 2, 3, 4\}$, and suppose the encryption functions are defined to be $e_{K_1}(a) = 1$,$e_{K_1}(b) = 2$; $e_{K_2}(a) = 2$, $e_{K_2}(b) = 3$; and $e_{K_3}(a) = 3$, $e_{K_3}(b) = 4$. This cryptosystem can be represented by the following encryption matrix:

| | $a$ | $b$ |
|---|---|---|
| $K_1$ | 1 | 2 |
| $K_2$ | 2 | 3 |
| $K_3$ | 3 | 4 |

**Solution:**

Since $n = 3$, the space of plaintext $\mathcal{P} = \{000, 001, 010, 011, 100, 101, 110, 111\}$, the keyspace $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8\} = \{000, 001, 010, 011, 100, 101, 110, 111\}$, therefore, the encryption matrix is as follows:

| $\mathcal{K}/\mathcal{P}$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| $K_1$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| $K_2$ | 001 | 000 | 011 | 010 | 101 | 100 | 111 | 110 |
| $K_3$ | 010 | 011 | 000 | 001 | 110 | 111 | 100 | 101 |
| $K_4$ | 011 | 010 | 001 | 000 | 111 | 110 | 101 | 100 |
| $K_5$ | 100 | 101 | 110 | 111 | 000 | 001 | 010 | 011 |
| $K_6$ | 101 | 100 | 111 | 110 | 001 | 000 | 011 | 010 |
| $K_7$ | 110 | 111 | 100 | 101 | 010 | 011 | 000 | 001 |
| $K_8$ | 111 | 110 | 101 | 100 | 011 | 010 | 001 | 000 |

# Exercise 3.15

Consider a cryptosystem in which $P = \{a, b, c\}$, $K = \{K_1, K_2, K_3\}$ and $C = \{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $K_1$ | 1 | 2 | 3 |
| $K_2$ | 2 | 3 | 4 |
| $K_3$ | 3 | 4 | 1 |

Given that keys are chosen equiprobably, and the plaintext probability distribution is $\mathbf{Pr}[a] = 1/2$, $\mathbf{Pr}[b] = 1/3$, $\mathbf{Pr}[c] = 1/6$, compute $H(\mathbf{P})$, $H(\mathbf{C})$, $H(\mathbf{K})$, $H(\mathbf{K}|\mathbf{C})$, and $H(\mathbf{P}|\mathbf{C})$.

**Solution:**

**Definition of Shannon's Entropy**: Let $X$ be a discrete RV on a nite set $\mathcal{X}$. Then, the *entropy* of $X$ is defined as:

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2(p(x))$$

**Definition of conditional entropy**: Suppose $\mathbf{X}$ and $\mathbf{Y}$ are two random variables.Then for any fixed value $y$ of $\mathbf{Y}$, we get a (conditional) probability distribution on $\mathbf{X}$; we denote the associated random variable by $\mathbf{X}|y$ Clearly,

$$H(\mathbf{X}|y) = -\sum_{x} \mathbf{Pr}[x|y]\log_2 \mathbf{Pr}[x|y]$$

We denoted $H(\mathbf{X}|\mathbf{Y})$,to be the weighted average (with respect to the probabilities $\mathbf{Pr}[y]$) of the entropies $H(\mathbf{X}|\mathbf{y})$ over all possible values $y$. It is computed to be

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y}\sum_{x} \mathbf{Pr}[y]\mathbf{Pr}[x|y]\log_2 \mathbf{Pr}[x|y]$$

**Theorem 3.10**: Suppose that $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem. Then

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$$

**Joint probability** can be related to conditional probability by the formula:

$$p(x, y) = p(x|y)p(y) = p(y|x)p(x)$$

First we compute $H(\mathbf{P})$ using the **definition of Shannon's Entropy**:

$$\begin{aligned}
H(\mathbf{P}) &= -[p(a)\log_2(p(a)) + p(b)\log_2(p(b)) + p(c)\log_2(p(c))] \\
&= -[\mathbf{Pr}[a]\log_2(\mathbf{Pr}[\mathbf{a}]) + \mathbf{Pr}[b]\log_2(\mathbf{Pr}[b]) + \mathbf{Pr}[c]\log_2(\mathbf{Pr}[c])] \\
&= -[\frac{1}{2}\log_2(\frac{1}{2}) + \frac{1}{3}\log_2(\frac{1}{3}) + \frac{1}{6}\log_2(\frac{1}{6})] \\
&= 1.4591479170272448 \\
&\approx 1.459
\end{aligned}$$

Next, we compute each probability distribution on $\mathcal{C}$ according the above encryption matrix:

$$
\begin{aligned}
\mathbf{Pr}[1] &= \mathbf{Pr}[K_1] \times \mathbf{Pr}[a] + \mathbf{Pr}[K_3] \times \mathbf{Pr}[c] \\
&= \frac{1}{3} \times \frac{1}{2} + \frac{1}{3} \times \frac{1}{6} \\
&= \frac{2}{9} \\
\mathbf{Pr}[2] &= \mathbf{Pr}[K_1] \times \mathbf{Pr}[b] + \mathbf{Pr}[K_2] \times \mathbf{Pr}[a] \\
&= \frac{1}{3} \times \frac{1}{3} + \frac{1}{3} \times \frac{1}{2} \\
&= \frac{5}{18} \\
\mathbf{Pr}[3] &= \mathbf{Pr}[K_1] \times \mathbf{Pr}[c] + \mathbf{Pr}[K_2] \times \mathbf{Pr}[b] + \mathbf{Pr}[K_3] \times \mathbf{Pr}[a] \\
&= \frac{1}{3} \times \frac{1}{6} + \frac{1}{3} \times \frac{1}{3} + \frac{1}{3} \times \frac{1}{2} \\
&= \frac{1}{3} \\
\mathbf{Pr}[4] &= \mathbf{Pr}[K_2] \times \mathbf{Pr}[c] + \mathbf{Pr}[K_3] \times \mathbf{Pr}[b] \\
&= \frac{1}{3} \times \frac{1}{6} + \frac{1}{3} \times \frac{1}{3} \\
&= \frac{1}{6}
\end{aligned}
$$

Then we can compute $H(\mathbf{C})$ as follows:

$$
\begin{aligned}
H(\mathbf{C}) &= -[p(1)\log_2(p(1)) + p(2)\log_2(p(2)) + p(3)\log_2(p(3)) + p(4)\log_2(p(4))] \\
&= -[\mathbf{Pr}[1]\log_2(\mathbf{Pr}[1]) + \mathbf{Pr}[2]\log_2(\mathbf{Pr}[2]) + \mathbf{Pr}[3]\log_2(\mathbf{Pr}[3]) + \mathbf{Pr}[4]\log_2(\mathbf{Pr}[4])] \\
&= -[\frac{2}{9}\log_2(\frac{2}{9}) + \frac{5}{18}\log_2(\frac{5}{18}) + \frac{1}{3}\log_2(\frac{1}{3}) + \frac{1}{6}\log_2(\frac{1}{6})] \\
&= 1.9546859469463558 \\
&\approx 1.955
\end{aligned}
$$

After that, $H(\mathbf{K})$ can be computed easily since keys are chosen equiprobably $\frac{1}{3}$:

$$
\begin{aligned}
H(\mathbf{K}) &= -[\mathbf{Pr}[K_1]\log_2(\mathbf{Pr}[K_1]) + \mathbf{Pr}[K_2]\log_2(\mathbf{Pr}[K_2]) + \mathbf{Pr}[K_3]\log_2(\mathbf{Pr}[K_3])] \\
&= -[3 \times \frac{1}{3}\log_2(\frac{1}{3})] \\
&= 1.5849625007211563 \\
&\approx 1.585
\end{aligned}
$$

Using the above **Theorem 3.10**, we can get $H(\mathbf{K}|\mathbf{C})$:

$$
\begin{aligned}
H(\mathbf{K}|\mathbf{C}) &= H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C}) \\
&= 1.585 + 1.459 - 1.955 \\
&= 1.089
\end{aligned}
$$

Finally, to compute $H(\mathbf{P}|\mathbf{C})$, we need to compute $\mathbf{Pr}[P|C]$, and use the **definition of conditional entropy** to find it. Therefore, the $\mathbf{Pr}[P|C]$s are computed used:

$$
\mathbf{Pr}(P|C) = \frac{\mathbf{Pr}(P) \times \mathbf{Pr}(C|P)}{\mathbf{Pr}(C)} = \begin{cases} \frac{\mathbf{Pr}(P) \times \mathbf{Pr}(K)}{\mathbf{Pr}(C)} & \text{if } \mathbf{Pr}(\mathbf{C}|\mathbf{P}) \neq 0 \\ 0 & \text{otherwise} \end{cases}
$$

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| 1 | $\mathbf{Pr}[a\|1] = \frac{\frac{1}{2}\times\frac{1}{3}}{\frac{2}{9}} = \frac{3}{4}$ | $\mathbf{Pr}[b\|1] = 0$ | $\mathbf{Pr}[c\|1] = \frac{\frac{1}{6}\times\frac{1}{3}}{\frac{2}{9}} = \frac{1}{4}$ |
| 2 | $\mathbf{Pr}[a\|2] = \frac{\frac{1}{2}\times\frac{1}{3}}{\frac{5}{18}} = \frac{3}{5}$ | $\mathbf{Pr}[b\|2] = \frac{\frac{1}{3}\times\frac{1}{3}}{\frac{5}{18}} = \frac{2}{5}$ | $\mathbf{Pr}[c\|2] = 0$ |
| 3 | $\mathbf{Pr}[a\|3] = \frac{\frac{1}{2}\times\frac{1}{3}}{\frac{1}{3}} = \frac{1}{2}$ | $\mathbf{Pr}[b\|3] = \frac{\frac{1}{3}\times\frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$ | $\mathbf{Pr}[c\|3] = \frac{\frac{1}{6}\times\frac{1}{3}}{\frac{1}{3}} = \frac{1}{6}$ |
| 4 | $\mathbf{Pr}[a\|4] = 0$ | $\mathbf{Pr}[b\|4] = \frac{\frac{1}{3}\times\frac{1}{3}}{\frac{1}{6}} = \frac{2}{3}$ | $\mathbf{Pr}[c\|4] = \frac{\frac{1}{6}\times\frac{1}{3}}{\frac{1}{6}} = \frac{1}{3}$ |

Thus, we can find:

$$
\begin{aligned}
H(\mathbf{P}|1) &= -[\mathbf{Pr}[a|1]\log_2(\mathbf{Pr}[a|1]) + \mathbf{Pr}[b|1]\log_2(\mathbf{Pr}[b|1]) + \mathbf{Pr}[c|1]\log_2(\mathbf{Pr}[c|1])] \\
&= -[\frac{3}{4}\log_2(\frac{3}{4}) + \frac{1}{4}\log_2(\frac{1}{4})] \\
&= 0.8112781244591328 \\
&\approx 0.811 \\
H(\mathbf{P}|2) &= -[\mathbf{Pr}[a|2]\log_2(\mathbf{Pr}[a|2]) + \mathbf{Pr}[b|2]\log_2(\mathbf{Pr}[b|2]) + \mathbf{Pr}[c|2]\log_2(\mathbf{Pr}[c|2])] \\
&= -[\frac{3}{5}\log_2(\frac{3}{5}) + \frac{2}{5}\log_2(\frac{2}{5})] \\
&= 0.9709505944546686 \\
&\approx 0.971 \\
H(\mathbf{P}|3) &= -[\mathbf{Pr}[a|3]\log_2(\mathbf{Pr}[a|3]) + \mathbf{Pr}[b|3]\log_2(\mathbf{Pr}[b|3]) + \mathbf{Pr}[c|3]\log_2(\mathbf{Pr}[c|3])] \\
&= -[\frac{1}{2}\log_2(\frac{1}{2}) + \frac{1}{3}\log_2(\frac{1}{3}) + \frac{1}{6}\log_2(\frac{1}{6})] \\
&= 1.4591479170272448 \\
&\approx 1.459 \\
H(\mathbf{P}|4) &= -[\mathbf{Pr}[a|4]\log_2(\mathbf{Pr}[a|4]) + \mathbf{Pr}[b|4]\log_2(\mathbf{Pr}[b|4]) + \mathbf{Pr}[c|4]\log_2(\mathbf{Pr}[c|4])] \\
&= -[\frac{2}{3}\log_2(\frac{2}{3}) + \frac{1}{3}\log_2(\frac{1}{3})] \\
&= 0.9182958340544896 \\
&\approx 0.918
\end{aligned}
$$

Eventually, the $H(\mathbf{P}|\mathbf{C})$ is:

$$
\begin{aligned}
H(\mathbf{P}|\mathbf{C}) &= \mathbf{Pr}[1]\times H(\mathbf{P}|1) + \mathbf{Pr}[2]\times H(\mathbf{P}|2) + \mathbf{Pr}[3]\times H(\mathbf{P}|3) + \mathbf{Pr}[4]\times H(\mathbf{P}|4) \\
&= \frac{2}{9}\times 0.811 + \frac{5}{18}\times 0.971 + \frac{1}{3}\times 1.459 + \frac{1}{6}\times 0.918 \\
&= 1.0892777777777778 \\
&\approx 1.089
\end{aligned}
$$

# Exercise 3.17

Suppose that $\mathrm{APNDJI}$ or $\mathrm{XYGROBO}$ are ciphertexts that are obtained from encryption using the *Shift Cipher*. Show in each case that there are two "meaningful" plaintexts that could encrypt to the given ciphertext. (Thanks to John van Rees for these examples.)

**Solution:**

Because we know that the ciphertext is encrypted using Shift Cipher, I will use a simple program written in Python to do exhaustive search to get the plaintext, the code is as follows:

```python
def decrypt(ciphertext, shift_count):
    plaintext = []
    for ch in ciphertext:
        if ord(ch) <= 90-shift_count:
            plaintext.append(chr(ord(ch)+shift_count))
        else:
            plaintext.append(chr(64+ord(ch)+shift_count-90))

    return plaintext


ciphertext1 = 'APNDJI'
ciphertext2 = 'XYGROBO'

print('Decrypt the ciphertext {}:'.format(ciphertext1))
for shift in range(1, 26):
    for ch in decrypt(ciphertext1, shift):
        print(ch, end='')
    print()

print('Decrypt the ciphertext {}:'.format(ciphertext2))
for shift in range(1, 26):
    for ch in decrypt(ciphertext2, shift):
        print(ch, end='')
    print()
```

The results we got from searching are as follows:

```
Decrypt the ciphertext APNDJI:
BQOEKJ
CRPFLK
DSQGML
ETRHNM
FUSION
GVTJPO
HWUKQP
IXVLRQ
JYWMSR
KZXNTS
LAYOUT
MBZPVU
NCAQWV
ODBRXW
PECSYX
QFDTZY
RGEUAZ
SHFVBA
TIGWCB
UJHXDC
VKIYED
WLJZFE
XMKAGF
YNLBHG
ZOMCIH
```

```
Decrypt the ciphertext XYGROBO:
YZHSPCP
ZAITQDQ
ABJURER
BCKVSFS
CDLWTGT
DEMXUHU
EFNYVIV
FGOZWJW
GHPAXKX
HIQBYLY
IJRCZMZ
JKSDANA
KLTEBOB
LMUFCPC
MNVGDQD
NOWHERE
OPXIFSF
PQYJGTG
QRZKHUH
RSALIVI
STBMJWJ
TUCNKXK
UVDOLYL
VWEPMZM
WXFQNAN
```

Finally, for ciphertext $\mathrm{APNDJI}$, the two "meaningful" plaintexts that could encrypt to it are:

$$\mathrm{FUSION}$$
$$\mathrm{LAYOUT}$$

And for another ciphertext $\mathrm{XYGROBO}$, the two "meaningful" plaintexts that could encrypt to it are:

$$\mathrm{ABJURER}$$
$$\mathrm{NOWHERE}$$