โครงงานย่อยภาษาไพธอน “การเข้าและถอดรหัสแบบ Monoalphabetic Substitution”

- คอนเซ็ปการเข้าและถอดรหัสแบบ Monoalphabetic Substitution
- การอ่านและเขียนไฟล์โดยใช้ภาษาไพธอน
- การรับค่า User Input โดยใช้ฟังก์ชัน input()
- การนิยามโมดูล simple_codec.py
- การนิยามฟังก์ชันหลัก (“__main__”)

https://kmutt.me/skeic-python-2022

Figure 31.4: Representation of plaintext and ciphertext characters in modulo 26

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 31.5: An example key for a monoalphabetic substitution cipher

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

Example 31.1

Use the additive cipher with key = 15 to encrypt the message “hello”.

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h $\rightarrow$ 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 $\rightarrow$ W
Plaintext: e $\rightarrow$ 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 $\rightarrow$ T
Plaintext: l $\rightarrow$ 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 $\rightarrow$ A
Plaintext: l $\rightarrow$ 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 $\rightarrow$ A
Plaintext: o $\rightarrow$ 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 $\rightarrow$ D

The result is “WTAAD”. Note that the cipher is monoalphabetic because two instances of the same plaintext character (l) are encrypted as the same character (A).

Example 31.2

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution

We apply the decryption algorithm to the plaintext character by character:

Ciphertext: W $\rightarrow$ 22	Decryption: (22 – 15) mod 26	Plaintext: 07 $\rightarrow$ h
Ciphertext: T $\rightarrow$ 19	Decryption: (19 – 15) mod 26	Plaintext: 04 $\rightarrow$ e
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: A $\rightarrow$ 00	Decryption: (00 – 15) mod 26	Plaintext: 11 $\rightarrow$ l
Ciphertext: D $\rightarrow$ 03	Decryption: (03 – 15) mod 26	Plaintext: 14 $\rightarrow$ o

The result is "hello". Note that the operation is in modulo 26, which means that we need to add 26 to a negative result (for example −15 becomes 11).

ตัวอย่าง Monoalphabetic Substitution Code Table สำหรับโครงงานนี้

	A	B	C	D	E
1	1	a	L	A	h
2	2	b	\	B	o
3	3	c	O	C	j
4	4	d	Z	D	crlf
5	5	e	Y	E	r
6	6	f	V	F	g
7	7	g	F	G	m
8	8	h	A	H	n
9	9	i	U	I	sp
10	10	j	C	J	l
11	11	k	N	K	w
12	12	l	J	L	a
13	13	m	G	M	p
14	14	n	H	N	k
15	15	o	B	O	c
16	16	p	M	P	q
17	17	q	P	Q	u
18	18	r	E	R	z
19	19	s	T	S	x
20	20	t	X	T	s
21	21	u	Q	U	i
22	22	v	W	V	f
23	23	w	K	W	v
24	24	x	S	X	t
25	25	y	[	Y	e
26	26	z	R	Z	d
27	27	.	]	[	y
28	28	sp	I	\	b
29	29	crlf	D	]	.

การอ่านข้อมูลและเขียนกลับข้อมูลลงไฟล์

- การอ่านข้อมูลจากไฟล์

```
file1 = open('file_to_read.txt', 'r')
file1.read(...)          # read bytes
file1.readline(...)      # read one line
file1.readlines(...)     # read all lines
file1.close()
```

- การเขียนข้อมูลลงไฟล์

```
file1 = open('file_to_write.txt', 'w')
file1.write(...)         # write a string
file1.writelines(...)    # write a list of strings
file1.close()
```

- การอ่านข้อมูลจาก keyboard

```
usr_name = input("Enter user name: ")
```

ไฟล์โมดูล simple_codec.py (ทำโดยสมาชิก 1 คน)

- กำหนดนิยาม Codec Table โดยอาจใช้
  - List 2 list … List หนึ่งสำหรับ Code Table และอีก List สำหรับ Decode Table หรือ
  - Python dictionary หรือ
  - นิยายฟังก์ชันเพื่ออ่านค่าจากไฟล์ CSV เช่น

    code_list = read_code(“codec_table.csv”)

    decode_list = read_decode(“codec_table.csv”) หรือ

    codec_dict = read_codec(“codec_table.csv”)
- กำหนดนิยามฟังก์ชัน ดังต่อไปนี้

  code(plaintext_string, key, code_table_info) returns coded_text_string

  decode(coded_text_string, key, decode_table_info) returns plaintext_string

ฟังก์ชัน “__main__” ไฟล์ codec_main.py (ทำโดยสมาชิก 1 คน)

- นำเข้าโมดูล simple_codec.py เพื่อใช้งาน
- ถ้ายังไม่ได้กำหนดนิยาม codec_table ในไฟล์โมดูล simple_codec.py ให้เรียกฟังก์ชันที่ได้นิยามไว้ในโมดูล simple_codec.py เพื่ออ่านค่า codec_table ตามที่ได้นิยามไว้ (เช่น เป็น list หรือเป็น dictionary)
- ถาม user ให้ระบุกุญแจเพื่อใช้ในการเข้ารหัส
  - ตัวอย่างของ Built-in Module ก็เช่น random

- อ่าน plaintext จากไฟล์ plaintext.txt
- เรียก code(plaintext, key, code_table) เพื่อทำการเข้ารหัส จากนั้นจึงแสดงผล
- เรียก decode(coded_text, key, decode_table) เพื่อทำการถอดรหัส จากนั้นจึงแสดงผล ตรวจสอบความถูกต้อง