โครงงานย่อยภาษาไพธอน "การเข้าและถอดรหัสแบบ Monoalphabetic Substitution"

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

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

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

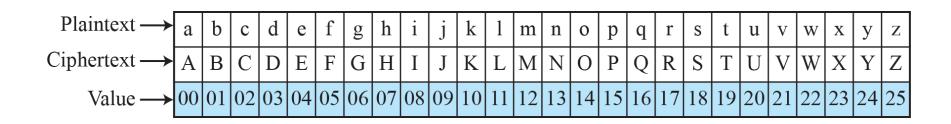
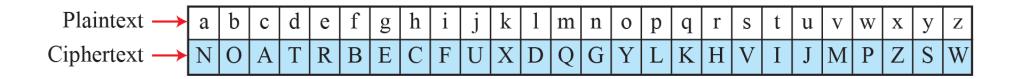


Figure 31.5: An example key for a monoalphabetic substitution cipher



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: $1 \rightarrow 11$	Encryption: $(11 + 15) \mod 26$	Ciphertext: $00 \rightarrow A$
Plaintext: $1 \rightarrow 11$	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).

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: $11 \rightarrow 1$
Ciphertext: A \rightarrow 00	Decryption: $(00 - 15) \mod 26$	Plaintext: $11 \rightarrow 1$
Ciphertext: D \rightarrow 03	Decryption: $(03 - 15) \mod 26$	Plaintext: $14 \rightarrow 0$

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 สำหรับ โครงงานนี้

	А	В	С	D	Е
1	1	а	L	Α	h
2	2	b	\	В	0
3	3	С	0	С	j
4	4	d	Z	D	crlf
5	5	е	Y	E	r
6	6	f	V	F	g
7	7	g	F	G	m
8	8	h	Α	Н	n
9	9	i	U		sp
10	10	j	С	J	1
11	11	k	N	K	W
12	12	I	J	L	а
13	13	m	G	M	р
14	14	n	Н	N	k
15	15	0	В	0	С
16	16	р	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	у	[Y	е
26	26	Z	R	Z	d
27	27	•]	[У
28	28	sp	l	\	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()
```

• การอ่านข้อมูลจาก keyboard

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

• การเขียนข้อมูลลงไฟล์

```
file1 = open('file_to_write.txt', 'w')

file1.write(...) # write a string

file1.writelines(...) # write a list of strings

file1.close()
```

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 ตรวจสอบ ความถูกต้อง