Repetition & Reinforcement

Andey Robins & Dr Borowczak

April 4-6, 2023

Outline

Outline

- Schedule
- Dictionaries Reinforcement
- Example Problems
- Applications for Dictionaries
- Game Modification

Class Schedule

Week	Tuesday	Thursday	Assignments
Apr 3	Reinforcement	Reinforcement	Quest Redo
Apr 10	No Class	No Class	Quest D
Apr 17	Lecture	Lecture	Lab
Apr 24	AMA	AMA	Lab
May 1	No Class	No Class	
May 11	Final Quest A	Comprehensive	10:15 AM

Dictionaries

Syntax

Declaration: `dictionary = {}`

Access: `dictionary[key]`

Membership: `if "string" in dictionary:`

Syntax

Looping:

```
for key, val in dictionary.items():
  print(key)
  print(val)
```

Syntax

Removal: `del dictionary[key]`

What does it do?

```
dictionary = {
  'key1': 1,
  'key2': 2,
  'key3': 3
}

del dictionary['key4']
```

Syntax

Smart Removal:

```
if key in dictionary:
  del dictionary[key]
```

Example Problems

Caesar Cipher Decoder

Given some text encrypted with the Caesar cipher, can we decode it?

Aside: The Caesar Cipher

How do I send secret messages?

How do I send this message in secret to Alicia?

“What time is the Wicys meeting?”

Encryption

Encryption is a methodology for obscuring the true meaning of data. The message from the previous slide might look like this: “Zkdw wlph lv wkh Zlfbv phhwlqj?”

Caesar Cipher

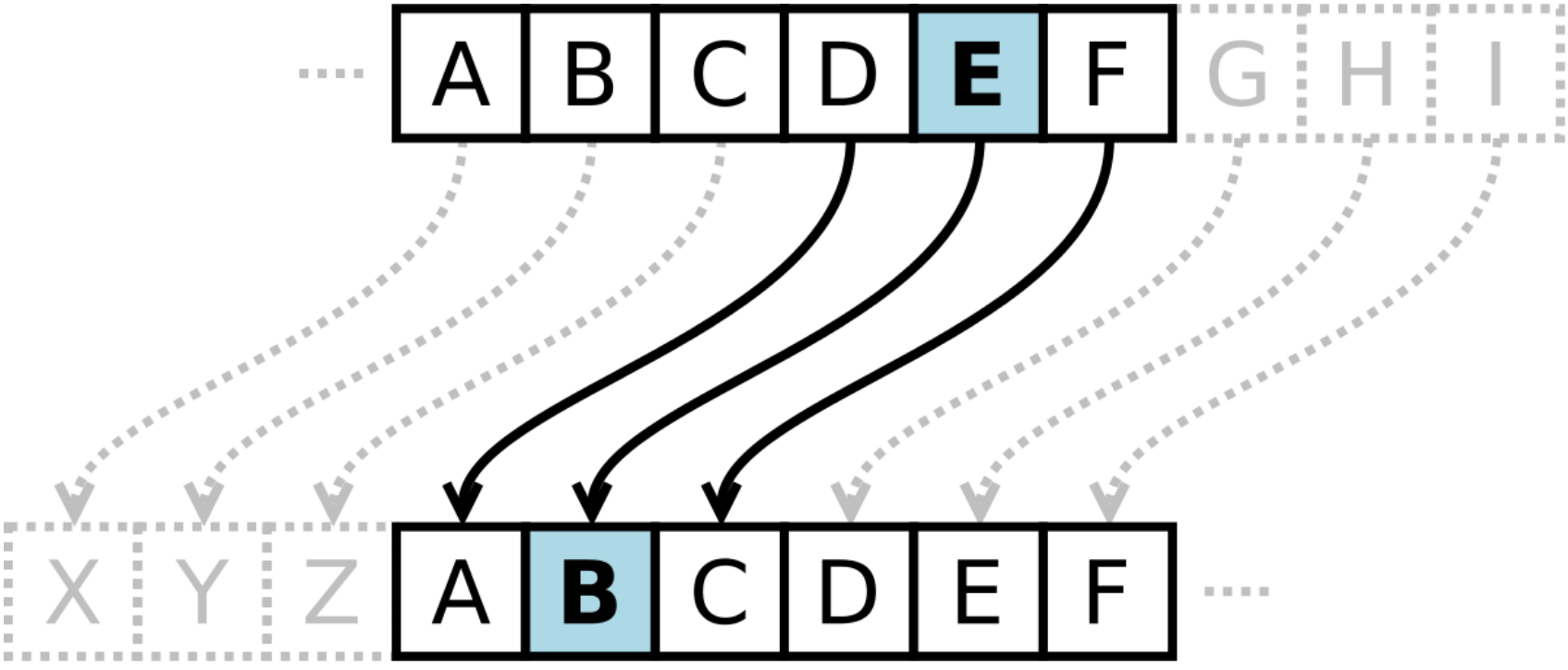

Figure 1: An illustration of the Caesar cipher

Attack

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%

Caesar Cipher Decoder

Given some text encrypted with the Caesar cipher, can we decode it?

```
cipher_text = """
L pxvw qrw ihdu.
Ihdu lv wkh plqg-nloohu.
Ihdu lv wkh olwwoh-ghdwk wkdw eulqjv wrwdo
  reolwhudwlrq.
L zloo idfh pb ihdu.
L zloo shuplw lw wr sdvv ryhu ph dqg wkurxjk ph.
Dqg zkhq lw kdv jrqh sdvw, L zloo wxuq wkh lqqhu
  hbh wr vhh lwv sdwk.
Zkhuh wkh ihdu kdv jrqh wkhuh zloo eh qrwklqj.
  Rqob L zloo uhpdlq.
"""
```

Outline

1. Count the frequency of each letter

1. Count the frequency of each letter
2. Find the most frequent letter

1. Count the frequency of each letter
2. Find the most frequent letter
3. Calculate a shift with the assumption that ‘e’ is the most common letter

1. Count the frequency of each letter
2. Find the most frequent letter
3. Calculate a shift with the assumption that ‘e’ is the most common letter
4. Shift the cipher text letters back

1. Count the frequency of each letter
2. Find the most frequent letter
3. Calculate a shift with the assumption that ‘e’ is the most common letter
4. Shift the cipher text letters back
5. Output the decrypted message.

Frequency Count

```
letter_freq = {}
for letter in cipher_text:
  if letter in letter_freq:
    letter_freq[letter] += 1
  else:
    letter_freq[letter] = 1
```

```
letter_freq = {}
for letter in cipher_text:
  if letter.isalpha():      # addition
    if letter in letter_freq:
      letter_freq[letter] += 1
    else:
      letter_freq[letter] = 1
```

Find the Most Frequent

```
most_letter = ""
most_letter_count = 0
for letter, count in letter_freq.items():
  if count > most_letter_count:
    most_letter = letter
    most_letter_count = count
```

Calculate Shift

Difference between the highest letter and the letter 'e'. `ord()` is the function to do this.

```
shift = ord(highest_letter) - ord('e')
```

Shift Message Back

```
plain_text = ""
for letter in cipher_text:
    plain_letter_ord = ord(letter) - shift
    plain_text += chr(plain_letter_ord)
```

```
plain_text = ""
for letter in cipher_text:
  if letter.isalpha():
    plain_letter_ord = ord(letter) - shift
    plain_text += chr(plain_letter_ord)
  else:
    plain_text += letter
```

Decryption Complete

See the code in Codio for this code in action.

Caesar Cipher Counterexample

What is the following word?

“Mdcc”

Jazz - 3

Limits

What are the limits of the Caesar cipher?

1. Short cipher text
2. Non-letter characters
3. Frequency analysis
4. Languages

The Caesar Cipher Continued

Left Off

```
plain_text = ""
for letter in cipher_text:
  if letter.isalpha():
    plain_letter_ord = ord(letter) - shift
    plain_text += chr(plain_letter_ord)
  else:
    plain_text += letter
```

```
plain_text = ""
for letter in cipher_text:
  if letter.isalpha():
    plain_text += wrap_around_shift(letter, shift) # desir
  else:
    plain_text += letter
```

Wrap around shifting

1. Convert a letter to a number in the alphabet
2. Shift that number by the shift value
3. Ensure that is a valid number in the alphabet (i.e 0 <= n <= 25)
4. Convert the shifted value back to a letter in ASCII

Brief Aside: How do computers store letters?

Binary

Everything in a computer is just a 1 or a 0. We often combine these into sets of 1s and 0s called *bytes*. A byte has 8 *bits*. By assigning different meanings to the numbers between 0 and 255 (

$$2^8 - 1$$

), we can associate different *semantic* values with those numbers.

ASCII

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Figure 3: The Ascii table

```
>>> ord('a')
97

>>> ord('b')
98

>>> ord('!')
33
```

```
>>> # The shift between e and h
>>> ord('h') - ord('e')
3
```

```
shift = ord(highest_letter) - ord('e')
...
plain_letter_ord = ord(letter) - shift
plain_text += chr(plain_letter_ord)
```

Handling Edge Cases

```
shift = ord('I') - ord('e')
shift == -28
```

- This number is negative
- This number is greater than 26 (the letters in the alphabet)
- Capitals and lower case aren't next to each other
- We would get random characters if we try to shift outside the alphabet

Handle Negative

How could we handle this negative number?

What way should we make it positive?

```
shift = -28
while shift < 0:
  shift += 26
```

Modular Arithmetic

How many integers are there?

How many numbers are there?

Are there more numbers than integers?

What would it mean to do math if there weren't infinite integers?

(Addition? Multiplication? Number bases?)

Enter Modular Arithmetic

Modular Arithmetic is a form of mathematics that works with a finite number set.

What is 11:00 am plus 50 minutes?


REPAIRS & RESTORATIONS
EST 1894
BLOOMSBURY
CLOCKS
LONDON
STANDARD TIME
12
1
2
3
4
5
6
7
8
9
10
11

43 minutes plus 1 hour 17 minutes is 2 hours.

or

$43 + 117 = 200$ *(with some modular magic)*

What does this have to do with the alphabet?

What is $s + x$?

p

```
>>> (ord('s') - 97) + (ord('x') - 97)
41
>>> chr((41 % 26) + 97)
'p'
```

Using the modulus operator (remember **%**), we can calculate what the remainder of adding numbers is!

Wrap around shifting

1. Convert a letter to a number in the alphabet
2. Shift that number by the shift value
3. Ensure that is a valid number in the alphabet (i.e 0 <= n <= 25)
4. Convert the shifted value back to a letter in ASCII

Letter to Alpha Number

```
def ord_to_letter_num(letter):

  return letter_num
```

```
def ord_to_letter_num(letter):
  letter_ord = ord(letter)

  return letter_num
```

```
def ord_to_letter_num(letter):
  letter_ord = ord(letter)
  letter_num = letter_ord - 97
  return letter_num
```

Wrap Around Shift

```
def round_shift(letter, shift):

  return chr(plain_num + 97)
```

```
def round_shift(letter, shift):
  cipher_num = ord_to_letter_num(letter)

  return chr(plain_num + 97)
```

```
def round_shift(letter, shift):
  cipher_num = ord_to_letter_num(letter)
  plain_num = (cipher_num - shift) % 26
  return chr(plain_num + 97)
```

Call this function

```
plain_text = ""
for letter in cipher_text:
  if letter.isalpha():
    plain_text += wrap_around_shift(letter, shift) # desir
  else:
    plain_text += letter
```

Result

```
c must not fear.
zear is the mind-killer.
zear is the little-death that brings total obliteration.
c will face my fear.
c will permit it to pass over me and through me.
und when it has gone past, c will turn the inner eye to see
qhere the fear has gone there will be nothing. inly c will
```

Handling Capital letters

Live code demo

A Brief Aside: Unicode

Figure 5: *An-nyeong* an informal Korean greeting