

Algorithms and Data Structures for Data Science

lab_cipher

CS 277

Brad Solomon

February 10, 2023



UNIVERSITY OF
ILLINOIS
URBANA - CHAMPAIGN

Department of Computer Science

Learning Objectives

Practice manipulating items and list indices

Write open-ended code with multiple valid algorithmic approaches

Learn fun trivia about cryptography

Substitution Ciphers

Plaintext:

A	B	C	D	E	U
C	I	P	H	E	R

Ciphertext:

BAD DUDE

Caesar Cipher

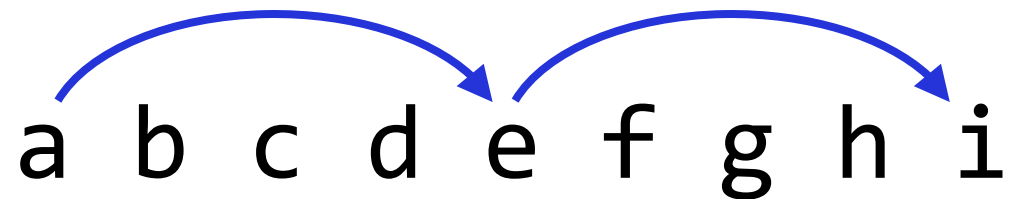
Plaintext:

A	B	C	D	E	U
---	---	---	---	---	---

Ciphertext:

E	F	G	H	I	Y
---	---	---	---	---	---

BAD DUDE



Vigenere Cipher

Plaintext:

D	D	D	B	B	D
E	R	E	C	P	E

Ciphertext:

Keyword:

B	O	B
---	---	---

Offset:

A	0
B	1
C	2
D	3
...	...

$c_i = i^{\text{th}}$ letter of the cipher $k_j = j^{\text{th}}$ letter of the key

$p_i = i^{\text{th}}$ letter of the text $\Sigma = \text{alphabet}$

$$c_i = \left(p_i + \text{offset}(k_j) \right) \% |\Sigma|$$

Vigenere Cipher

Plaintext:

D	D	D	B	B	D
---	---	---	---	---	---

Ciphertext:

A	D	E	D	B	E
---	---	---	---	---	---

Keyword:

C	A	B
---	---	---

Plain

	A	B	C	D	E
A	A	B	C	D	E
B	B	C	D	E	A
C	C	D	E	A	B
D	D	E	A	B	C
E	E	A	B	C	D

Key

Python Strings

Python strings have built-in lists for sets of characters

Well supported languages often can make your life easier!

```
1 alpha = list(string.ascii_lowercase)
2 print(alpha)
3 # ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i',
4  'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
5  't', 'u', 'v', 'w', 'x', 'y', 'z']
6
7 whitespace = ' \t\n\r\v\f'
8 ascii_lowercase = 'abcdefghijklmnopqrstuvwxyz'
9 ascii_uppercase = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
10 ascii_letters = ascii_lowercase + ascii_uppercase
11 digits = '0123456789'
12 hexdigits = digits + 'abcdef' + 'ABCDEF'
13 octdigits = '01234567'
14 punctuation = !"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~
15 printable = digits + ascii_letters + punctuation
16 + whitespace
17
18
```

Python 2D lists


```
1 outerList = []
2
3 for i in range(5):
4     innerList = []
5
6     for j in range(5):
7         innerList.append(i+j)
8
9     outerList.append(innerList)
10
11 print(outerList)
12
13 print(outerList[3][1])
14
15
16
17
18
```


Python 2D lists

0	1	2	3	4
1	2	3	4	5
2	3	4	5	6
3	4	5	6	7
4	5	6	7	8

```
1 outerList = []
2
3 for i in range(5):
4     innerList = []
5
6     for j in range(5):
7         innerList.append(i+j)
8
9     outerList.append(innerList)
10
11 print(outerList)
12
13 print(outerList[3][1])
14
15
16
17
18
```

Coding the lab

- 1) Create one or more lists of all allowed characters
- 2) Consider how you can swap all characters using a single integer
- 3) Consider how you can swap all characters using a single character
- 4) Extend single character solution to a full Vigenere encoding
- 5) Consider how to reverse both ciphers