Coding Vigenère's Cipher Using Python (Based off of *Invent With Python* Chapter 19)

Lecture notes of Alexander Wood
CSCI 360 Cryptography and Cryptanalysis
awood@jjay.cuny.edu

John Jay College of Criminal Justice

These slides are based off of Chapter 19 of *Invent With Python*, available at the link below:

`https://inventwithpython.com/hacking/chapter19.html`

All images and information are taken from this page unless otherwise noted.

Vigenère's Cipher

Today we will write code for Vigenère's Cipher, described in the previous lecture.

History: Discovery

Vigenere (1523 - 1596)

The first record of this cipher is from 1553, penned by Italian cryptographer Giovan Battista Bellaso. It was later reinvented and popularised by Blaise de Vigenère.

History: Breaking Vigenere

Babbage (1791-1871)

This cipher remained unbroken until the 19th century! For a long time it was known as “le chiffre indéchiffrable” (“the indecipherable cipher”).

Charles Babbage (the “father of computers”) was the first person known to break this cipher.

Vigenère's Cipher

First, Alice (A) and Bob (B) decide upon a keyword. This is done offline, privately. Encryption follows the following steps:

1) Write out the plaintext message
2) Below it, write out the keyword, aligning each letter of the keyword below each letter of the plaintext. Repeat the keyword over and over until you reach the end of the plaintext.
3) "Add" these letters together using their values modulo 26, as computed in the coding exercises in the previous slides. (*Note that this corresponds to a different Caeser shift for each letter in the keyword!*)

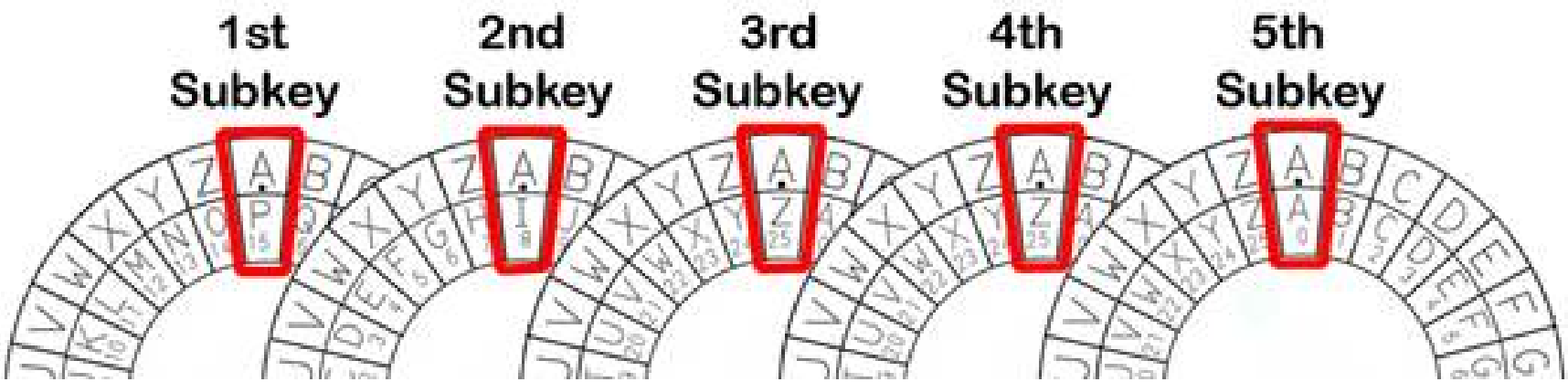
A Helpful Chart

For hand computations we can use the chart provided at `http://www.counton.org/explorer/codebreaking/vigenere-cipher.php`.

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	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

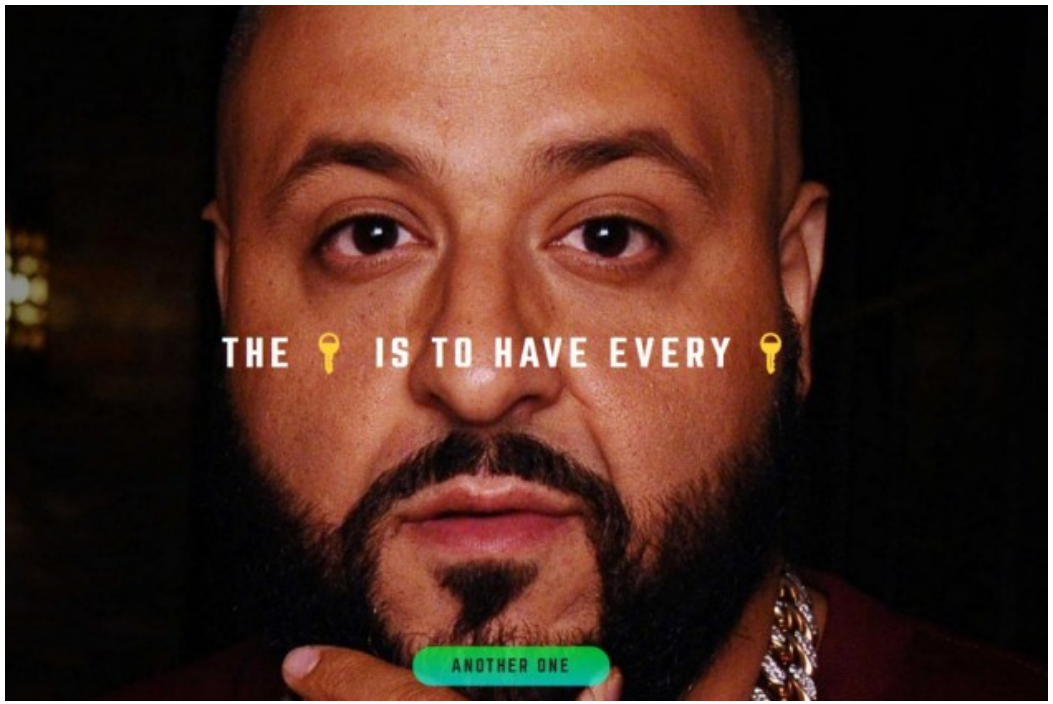
Vigenère's Cipher: Multiple Caesar Shifts

The key in Vigenère is a sequence of letters. Each letter can be considered a subkey. For instance, below the keyword is `PIZZA`. This image illustrates the use of the Caeser shift wheel for each letter in the key.



I got the keys

Last class we discussed how there are too many keys in the Vigenère's Cipher's keyspace for a brute force attack to be successful.



How can we determine the keyspace of Vigenère?

Keyspace

The size of the keyspace is determined by the length of the keyword!

Key Length	Equation	Possible Keys
1	26	= 26
2	26 × 26	= 676
3	676 × 26	= 17,576
4	17,576 × 26	= 456,976
5	456,976 × 26	= 11,881,376
6	11,881,376 × 26	= 308,915,776
7	308,915,776 × 26	= 8,031,810,176
8	8,031,810,176 × 26	= 208,827,064,576
9	208,827,064,576 × 26	= 5,429,503,678,976
10	5,429,503,678,976 × 26	= 141,167,095,653,376
11	141,167,095,653,376 × 26	= 3,670,344,486,987,776
12	3,670,344,486,987,776 × 26	= 95,428,956,661,682,176
13	95,428,956,661,682,176 × 26	= 2,481,152,873,203,736,576
14	2,481,152,873,203,736,576 × 26	= 64,509,974,703,297,150,976

Coding Vigenère

Now let's code Vigenère's cipher. The code will consist of three functions:

- `keygen`, which generates the key;
- `encrypt`, and
- `decrypt`

Coding: Keygen

The `keygen` function is somewhat trivial in this case; simply ask the user what key they would like to use and return this value.

What sort of error-checking can we include to make sure that the key is correctly constructed? (No lower-case letters, no spaces, no punctuation, etc)?

Coding: Encrypt

Make sure that you strip all spaces out of the plaintext message and make sure the plaintext is capitalized.

Coding: Decrypt

Now let's write the decryption function. If get the ciphertext by adding the plaintext to the keyword, how do we get the plaintext from the ciphertext?

Answer: We get the plaintext by subtracting the keyword from the ciphertext.

References

These slides are based off of Chapter 19 of *Invent With Python*, available at the link below:

`https://inventwithpython.com/hacking/chapter19.html`