1.5 Lesson 4 : Vigenere cipher

Vigenère Cipher (fixed key, or auto-key) is a type of polyalphabetic substitution cipher : the cipher alphabet is changed regularly during the encryption process.

Exercise 19

1. Watch “Encryption and Le chiffre indéchiffrable” by Simon Lehna Singh (till 2’30”)
2. What is the key word in the video? .....

   .....
3. What is the relation between Vigenère cipher and a Caesar’s shift? .....

   .....
4. What is the strength of the Vigenère cipher? .....

   .....

   .....
5. Encipher the plaintext “UMBRELLA” using the key “DOG”, and “PEANUT” using the key “CAT”

Plaintext	U	M	B	R	E	L	L	A	**Plaintext**	P	E	A	N	U	T
Key	D	O	G	D	O	G	D	O	**Key**						
Ciphertext	X								**Ciphertext**						

6. What do you notice ? .....

   .....

   .....
7. The ciphertext “BPFAGAMELXINIWJZMEURFVRDRXQJEXYFPV” was encrypted using the key “FIRST”. Decrypt it!

Plaintext																				
Key																				
Ciphertext	B	P	F	A	G	A	M	E	L	X	I	N	I	W	J	Z	M	E	U	R

Plaintext														
Key														
Ciphertext	F	V	R	D	R	X	Q	J	E	X	Y	P	F	V

Exercise 20 — Breaking the code ! (part 3).

1. Watch “Encryption and Le chiffre indéchiffrable” by Simon Lehna Singh (full excerpt)
2. Explain accurately the differrence between a mono-alphabetic cipher and a poly-alphabetic cipher. .....
   .....
   .....
3. With a Vigenère cipher , if your key is 4 letters long, in how many ways could each letter of the alphabet be encrypted? .....
   .....
4. According to Babbage, to decrypt a cipher text enciphered with the Vigenère encryption :
   a) What do you have to spot first in your ciphertext? .....
      .....
   b) What do you compute then? .....
      .....
   c) What piece of information does this gives you? .....
      .....
   d) What is the link between the Vigenère cipher and the Caesar cipher? .....
      .....
   e) What do you do next? .....
      .....
      .....

   (letter matching with the first letter of the key/frequency analysis/compute the shift)
5. Use this link Document1 to get the ciphertext obtained with a Vigenère cipher. Use online cracking tool at `https://simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html` to find out the key and break the cipher. Alternate ciphertext Document2
6. Research Charles Babbage and answer the following questions :
   a) Where and when did Babbage live? .....
   b) Why is he famous? .....

	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	V
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	W
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	X
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