Licence ISIL - 2020/2021

TD1

Exercice 1: CESAR

Le système le plus ancien est attribué à Jules César. Il consiste à un décalage de l'alphabet (dans le système original A étais remplacé par C, B par D, C par E, ...)

1. voici un texte chiffré obtenu avec la clé H:

SLUUL TPLZA ZBWWV ZLHCV PYAVB ALXBP WLTLU AZWLJ PHSUL JLZZH PYLWV BYPUA LYJLW ALYSL ZZPNU HBEAY HUZTP Z

Retrouver le texte clair.

2. voici un autre texte chiffré ; on ne connaît pas ici la clé utilisée.

FYPYQ LYELO TEUPD LTDOP DAZPX PDFYP YQLYE LOTEY ZYDLT DOPDA ZPDTP D

Retrouver le texte clair.

Exercice 2 : Chiffrement de Vigenère

- 1. Chiffrer le texte clair "thissystemisnotsecure", on donne m= 6 avec le mot-clé, CIPHER.
- 2. Ce cryptogramme a été obtenu par chiffrement de vigenère avec la clé « COPIE».

TWTVR GGTZX FSRWY TWGQP HOJBT CFIQV CZWMY TS Retrouver le texte clair.

		Lettre en clair																										
		A	В	C	D	Ε	F	G	Η	Ι	J	K	L	М	Ν	0	P	Q	R	S	T	U	V	W	Х	Y	Z	
	A	Α	В	С	D	Ε	F	G	Η	I	J	K	L	М	Ν	0	P	Q	R	S	T	U	V	W	Х	Y	Z	П
	В	В	С	D	E	F	G	Н	Ι	J	K	L	Μ	Ν	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	
	C	С	D	Ε	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	P	Q	R.	S	Т	U	V	W	Х	Y	Z	Α	В	
C l é U t i l l	D	D	Ε	F	G	Η	I	J	Κ	L	Μ	Ν	0	P	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	
	Ε	Ε	F	G	Н	Ι	J	Κ	L	М	Ν	0	P	Q	R	S	Τ	U	V	W	Х	Υ	Z	Α	В	С	D	
	F	F	G	Н	Ι	J	K	L	М	Ν	0	P	Q	R	S	T	U	V	W	Х	Y	Z	Α	В	С	D	Ε	
	G	G	Н	Ι	1	K	L	Μ	Ν	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	
	Η	Η	Ι	J	K.	L	Μ	Ν	0	P	Q	R	S	T	U	V	W	Х	Y	Z	А	В	С	D	Е	F	G	t t r e
	I	I	J	K	L	М	Ν	0	P	Q	R	S	T	U	V	W	Х	Y	Z	Α	В	C	D	Ε	F	G	Н	
	J	J	K	L	М	Ν	0	P	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	
	K	K	L	М	Ν	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	C	D	Ε	F	G	Η	Ι	J	
	L	L	М	Ν	0	Р	Q	R	5	T	U	V	W	Х	Y	Z	Α	В	С	D	E	F	G	Н	Ι	J	K	
	М	М	Ν	0	P	Q	R	S	Т	U	V	W	Х	Υ	Z	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	
	Ν	Ν	0	P	Q	R	S	T	U	V	W	Х	Y	Z	Α	В	С	D	E	F	G	Η	I	J	Κ	L	М	
	0	0	P	Q	R	S	T	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	Μ	Ν	
i	P	P	Q	R	S	Τ	U	V	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	I	J	Κ	L	М	Ν	0	f
é	Q	Q	R	S	T	U	V	W	Х	Υ	Z	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	М	Ν	0	P	f
e	R	R	S	Τ	U	V	W	Х	Υ	Z	Α	В	C	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	P	Q	ŕ
	S	S	Τ	U	V	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L	М	Ν	0	P	Q	R	e
	T	T	U	V	W	Х	Υ	Z	Α	В	C	D	E	F	G	Η	Ī	J	K	L	M	Ν	0	P	Q	R	S	
	U	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	М	N	O	P	Q	R	S	T	
	V	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Η	I	J	K	L	М	Ν	0	P	Q	R	S	Т	U	
	W	W	Х	Y	Z	Α	В	C	D	Е	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	P	Q	R	S	Т	U	V	
	Х	Х	Y	Z	A	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	Ν	0	P	Q	R	5	T	U	V	W	
	Y	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	l	K	L	М	Ν	0	P	Q	R	S	Т	U	V	W	Х	
	Z	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	Ν	0	P	Q	R	S	Т	U	V	W	Х	Y	