Introduction à la sécurité et à la cryptographie TP1 – Cryptanalyse historique

abdel-malik fofana

December 2023

1 Exercice 1

On va proceder par ordre croissant En francais la plus grande occurence est E donc u est surement E car u plus grand pourcentage

La 2eme plus grand occurence est A qui correspond ici potentiellement a E (second plus grand occurence dans le chiffrement)

Dans les bi occurence on A un E_ , en francais la bi occurence la plus courante est ES donc UJ = ES donc J = S

CJU -> ESE

EVU -> qui peut correspondre soit a ELA

VU -> DE (on vera que je m'etais trompé cést LE)

w est la moins occurent en francais donc w peut correspondre a une des lettres avec 0 occurence (y ou z)

Es est la plus grande bioccurence dans la langue francaise avec e a la fin est DE, ici DE pourait correspondre a

A est la 2eme lettre la plus presente en francais donc:

F-> N car la lettre suivant la plus represante

B -> T Car lettre suivante la plus represante

on remarque que l'on a S_ND_ESTINE , j'ai deviné son destin , j'ai recuprere les lettres

donc A ->0

D->R une fois ce mot trouver de fils en aiguille j'ai trouver tout les autres mots par exemple "histoire"

rhin etc ...

Le resultat est:

SON DESTIN EXCEPTIONNEL MARQUA LE MONDE ROMAIN ET L'HISTOIRE UNIVERSELLE AMBITIEUX ET BRILLANT IL S'APPUYA SUR LE COURANT REFORMATEUR ET DEMAGOGUE POUR SON ASCENSION POLITIQUE STRATEGE ET TACTICIEN HABILE IL REPOUSSA LES FRONTIERES ROMAINES JUSQU'AU RHIN ET A L'OCEAN ATLANTIQUE EN CONQUERANT LA GAULE PUIS UTILISA SES LEGIONS POUR S'EMPARER DU POUVOIR

2 Exercice 2

qeustion 1: KNFLGJIHMVCBNL = INDECHIFFRABLE

question 2 Voici la distance entre les repetitions qui nous permettent de trouver le pgcd qui est 6:

Distances	24	168	174	48	24	72									
PCGD des distances	6														

Lorsque l'on met l'indice 1: on remarque que q est le plus present donc que q est proche de e on en conclu que M est le premier indice en regardant sur la table

on fait cela avec les autres indices et les autres lettres en regardant sur la table (E , W , X , E et V qui correspond respectivement à A , S , T, E , R)

Bigramme chiffré	FE	DW	EE	EF	EJ	ET	KQ	QD	SK	TW
Nb. d'occurrences	9	7	6	6	6	6	6	6	6	6

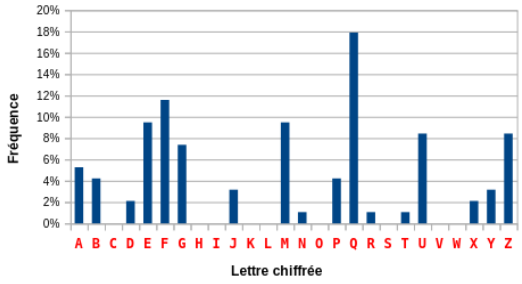
Trigramme chiffré	QDW	CQD	GEZ	JFE	XGF	YIP	ZFE	AFH	BAF	BBR
Nb. d'occurrences	4	3	3	3	3	3	3	2	2	2

Distances	24	168	174	48	24	72									
PCGD des distances	6														

Longueur de la clé	6
Sélectionner lettres d'indice	1

Mot clé :

1	2	3	4	5	6
M	A	S	T	E	R



Et on tombe sur la clé : MASTER

Le resultat est déchiffré est :

UN JOUR DE BATAILLE CONTRE LES ROMAINS, PANORAMIX LE DRUIDE ASSISTE À LA BATAILLE, LAISSANT LA SURVEILLANCE DE SA HUTTE. ASTERIX A ALORS UNE IDÉE : FAIRE BOIRE UN PEU DE POTION MAGIQUE À OBÉLIX, DE FAÇON QU'IL PRENNE UN PEU DE FORCE ET DE CONFIANCE EN LUI. LES DEUX ENFANTS SE RENDENT ENSEMBLE, DISCRÈTEMENT, DANS LA HUTTE DU DRUIDE, ET ASTERIX INDIQUÉ À OBÉLIX DE S'HISSER SUR LE BORD DE LA MARMITE. C'EST À CE MOMENT QUE PANORAMIX REVIENT DANS SA HUTTE. ASTERIX FAIT TOMBER OBÉLIX DANS LA MARMITE ET RÉUSSIT À SORTIR DOUCEMENT DE LA HUTTE. PEU APRÈS, PANORAMIX RESSORT DE SA HUTTE, TENANT BOUT DE BRAS UN OBÉLIX QUI A BU L'INTÉGRALITÉ DE LA MARMITE DE POTION MAGIQUE. C'EST CE JOUR-LÀ LA SEULE BETISE CONNUE D'ASTERIX.

Texte en clair :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	U	N	J	O	U	R	D	E	B	A	T	A	I	L	L	E	C	O	N	T
2	R	E	L	E	S	R	O	M	A	I	N	S	P	A	N	O	R	A	M	I
3	X	L	E	D	R	U	I	D	E	A	S	S	I	S	T	E	A	L	A	B
4	A	T	A	I	L	L	E	D	E	L	A	I	S	S	A	N	T	L	A	S
5	U	R	V	E	I	L	L	A	N	C	E	D	E	S	A	H	U	T	T	E
6	A	S	T	E	R	I	X	A	A	L	O	R	S	U	N	E	I	D	E	E
7	F	A	I	R	E	B	O	I	R	E	U	N	P	E	U	D	E	P	O	T
8	I	O	N	M	A	G	I	Q	U	E	A	O	B	E	L	I	X	D	E	F
9	A	C	O	N	Q	U	I	L	P	R	E	N	N	E	U	N	P	E	U	D
10	E	F	O	R	C	E	E	T	D	E	C	O	N	F	I	A	N	C	E	E
11	N	L	U	I	L	E	S	D	E	U	X	E	N	F	A	N	T	S	S	E
12	R	E	N	D	E	N	T	E	N	S	E	M	B	L	E	D	I	S	C	R
13	E	T	E	M	E	N	T	D	A	N	S	L	A	H	U	T	T	E	D	U
14	D	R	U	I	D	E	E	T	A	S	T	E	R	I	X	A	I	D	E	O
15	B	E	L	I	X	A	S	E	H	I	S	S	E	R	S	U	R	L	E	B
16	O	R	D	D	E	L	A	M	A	R	M	I	T	E	C	E	S	T	A	C
17	E	M	O	M	E	N	T	Q	U	E	P	A	N	O	R	A	M	I	X	R
18	E	V	I	E	N	T	D	A	N	S	S	A	H	U	T	T	E	A	S	T
19	E	R	I	X	F	A	I	T	A	L	O	R	S	T	O	M	B	E	R	O
20	B	E	L	I	X	D	A	N	S	L	A	M	A	R	M	I	T	E	E	T
21	R	E	U	S	S	I	T	A	S	O	R	T	I	R	E	N	D	O	U	C
22	E	D	E	L	A	H	U	T	T	E	P	E	U	A	P	R	E	S	P	A
23	N	O	R	A	M	I	X	R	E	S	S	O	R	T	D	E	S	A	H	U
24	T	T	E	T	E	N	A	N	T	A	B	O	U	T	D	E	B	R	A	S
25	U	N	O	B	E	L	I	X	Q	U	I	A	B	U	L	I	N	T	E	G
26	R	A	L	I	T	E	D	E	L	A	M	A	R	M	I	T	E	D	E	P
27	O	T	I	O	N	M	A	G	I	Q	U	E	C	E	S	T	A	C	E	J
28	O	U	R	L	A	S	E	U	L	E	B	E	T	I	S	E	C	O	N	N
29	U	E	D	A	S	T	E	R	I	X										

Comme on devait le rendre rapidement veuillez excusez mes fautes d'orthographes