

Introduction

- La Stéganographie,

Introduction

- La Stéganographie,
- Origine de la cryptographie,

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Les 3 critères

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Les 3 critères

- Confidentialité,

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Les 3 critères

- Confidentialité,
- Authenticité,

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Les 3 critères

- Confidentialité,
- Authenticité,
- intégrité

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Les 3 critères

- Confidentialité,
- Authenticité,
- intégrité

Introduction

- La Stéganographie,
- Origine de la cryptographie,
- Ronald Rivest et le cryptage RSA

Les 3 critères

- Confidentialité,
- Authenticité,
- intégrité

Symétrique		Asymétrique
Mono	Poly	l'ère informatique
Decalage	Hill	SSL
Affine	Enigma	DES
Chaine	Porta	RSA
Permutation	ADFGVX	Fn de hachage
Substitution	Vigenere	

Développement

Produit sur le marché

Développement

Produit sur le marché

1 www.decode.fr,

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),
- 3 Axcypite

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),
- 3 Axcyppte

Phase de développement

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),
- 3 Axcypite

Phase de développement

- 1 Identification,

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),
- 3 Axcypite

Phase de développement

- 1 Identification,
- 2 Définition,

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),
- 3 Axcrypte

Phase de développement

- 1 Identification,
- 2 Définition,
- 3 Réalisation,

Développement

Produit sur le marché

- 1 www.decode.fr,
- 2 Decrypto (Google Play Store),
- 3 Axcrypte

Phase de développement

- 1 Identification,
- 2 Définition,
- 3 Réalisation,
- 4 Finalisation

Substitution

Exemple de chiffrement :

alphabet 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

Substitution

Exemple de chiffrement :

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

Substitution

Exemple de chiffrement :

alphabet 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

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

texte en clair : "PRESENTATION DU PROJET"

Substitution

Exemple de chiffrement :

alphabet 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

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

texte en clair : "PRESENTATION DU PROJET"

message chiffré => KAJBJEYRYTIEMPKAIOJY

Substitution

Elements :

alphabet 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

liste fréquence des lettres dans langue française : e,s,a,n,t,i,r,u,l,o,d...

liste fréquence lettres dans le texte : h,m,v,z,c,u,x,b,s,f,l,y,p,r,t,n,g,a...

texte

BXSXBDVHAHVPCHRUHSYHVHVMUMZBZVHLFUCAHYCZLMHCBH
YGZPPCHTHSMLXCVUNVMZMUMZFSTFSFXBLGXNHMZRUH

Substitution

Elements :

alphabet 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

liste fréquence des lettres dans langue française : e,s,a,n,t,i,r,u,l,o,d...

liste fréquence lettres dans le texte : h,m,v,z,c,u,x,b,s,f,l,y,p,r,t,n,g,a...

texte

BXSXBDV^eA^eVPC^eRU^eSY^eV^eVMUMZBZV^eLFUCA^eYCZLM^eCB^eYGZ
PPC^eT^eSMLXCVUNVMZMUMZFSTFSFXBLGXN^eMZRUE

-(es/se), (el/le), (er/re), (et/te), (em/me)

Substitution

Elements :

alphabet 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

liste fréquence des lettres dans langue française : e,s,a,n,t,i,r,u,l,o,d...

liste fréquence lettres dans le texte : h,m,v,z,c,u,x,b,s,f,l,y,p,r,t,n,g,a...

texte

BXSXBDseAesPCeRUeSYesesMUMZBZseLFUCAeYC
ZLMeCBeyGZPPCeTeSMLXCsunsmZMUMZFSTFSFXBLGXNeMZRUe

-(eM/Me), esM

Substitution

Elements :

alphabet 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

liste fréquence des lettres dans langue française : e,s,a,n,t,i,r,u,l,o,d...

liste fréquence lettres dans le texte : h,m,v,z,c,u,x,b,s,f,l,y,p,r,t,n,g,a...

texte

BXSXBDseAesPCeRUeSYesestUtZBZseLFUCAeYC
ZLteCBeyGZPPCeTeStLXCsUNstZtUtZFSTFSFXBLGXNetZRUE

-tz

Substitution

Elements :

alphabet 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

liste fréquence des lettres dans langue française : e,s,a,n,t,i,r,u,l,o,d...

liste fréquence lettres dans le texte : h,m,v,z,c,u,x,b,s,f,l,y,p,r,t,n,g,a...

texte

BXSXBDseAesPCeRUeSYesestUtiBiseLFUCAeYC
iLteCBeyGiPPCeTeStLXCsunstitUtifSTFSFXBLGXNetiRUe

-de,le,re,me

Substitution

Elements :

alphabet 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

liste fréquence des lettres dans langue française : e,s,a,n,t,i,r,u,l,o,d...

liste fréquence lettres dans le texte : h,m,v,z,c,u,x,b,s,f,l,y,p,r,t,n,g,a...

texte

BXSXBDseAesPrerUesyestUtibiSELFURaeyr

iLterBeYGiPPreTeStLXrsUNstitUtifSTFSFXBLGXNetiRUe

Substitution

resultat :

l'analyse des frequences est utilisé pour decr
ipter le chiffrement par substitution monoalphabetique

texte

texte dechiffré : "l'analyse des frequences est utilisé pour decripter le
chiffrement par substitution mono-alphabetique"

Un exemple de cryptage

texte clair

A T T A Q U E

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
clée	B	U	T	B	U	T	B

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
clée	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
clée	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
clée	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5
modulo 26	1	13	12	1	10	13	5

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
clée	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5
modulo 26	1	13	12	1	10	13	5
texte crypté	B	N	M	B	K	N	F

Un exemple de cryptage

texte clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
clée	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5
modulo 26	1	13	12	1	10	13	5
texte crypté	B	N	M	B	K	N	F

Un exemple de decryptage (partie 1)

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQUEQERBWRVX
 UOAKXAOSXXWEAHBWEJMNQMNKERFVEXWTRZXWIAKLXFPSK
 AUTEMNDCMGTSXMXBTUIADNGMGPSRELXNIELXVRVPRTULH
 DNQWTWDTYGBPMXTFALJHASVBFXNGLLCHRZBWELEKMSSIK
 NBHWRIGNMGJSLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLX
 RRIMGNSNRVCHRQHAHEYVTAQEBBIPEEWEVKAKOEWADREMX
 MTBHHCHRTKDNVRZCHRCLQOHPWQAIWYNRMGVOIIFKEE

Un exemple de cryptage

text clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
cle	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5
modulo 26	1	13	12	1	10	13	5
text crypté	B	N	M	B	K	N	F

Un exemple de decryptage (partie 1)

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQUEQERBWVRVX
 UOAKXAOSXXWEAHBWEJMNQMNKERFVEXWTRZXWIAKLXFPSK
 AUTEMNDCMGTSXMXBTUIADNGMGPSRELXNIELXVRVPRTLH
 DNQWTWDTYGBPMXTFALJHASVBFXNGLL**CHR**ZBWELEKMSSIK
 NBHWIRIGNMGJSLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLX
 RRIMGNSNRV**CHR**QHAHEYVTAQEBBIPPEWEVKAKOEWADREMX
 MTBHHCHRTKDNVRZ**CHR**CLQOHPWQAIWXNRMGVOIIFKEE

Un exemple de cryptage

text clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
cle	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5
modulo 26	1	13	12	1	10	13	5
text crypté	B	N	M	B	K	N	F

Un exemple de decryptage (partie 1)

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQUEQERBWVRVX
 UOAKXAOSXXWEAHBWEJMNQMNKERFVEXWTRZXWIAKLXFPSK
 AUTEMNDCMGTSXMXBTUIADNGMGPSRELXNIELXVRVPRTULH
 DNQWTWDTYGBPMXTFALJHASVBFXNGLL**CHR**ZBWELEKMSSIK
 NBHWIRIGNMGJSLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLX
 RRIMGNSNRV**CHR**QHAIEYEVTAQEBBIPPEWEVKAKOEWADREMX
 MTBHHCHRTKDNVRZ**CHR**CLQOHPWQAIWXNRMGVOIIFKEE
 Distances : 165 ,235 et 285

Un exemple de cryptage

text clair	A	T	T	A	Q	U	E
equivalent entier	0	19	19	0	16	20	4
cle	B	U	T	B	U	T	B
equivalent entier	1	20	19	1	20	19	1
la somme	1	39	38	1	36	39	5
modulo 26	1	13	12	1	10	13	5
text crypté	B	N	M	B	K	N	F

Un exemple de decryptage (partie 1)

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQUEQERBWVRVX
 UOAKXAOSXXWEAHBWEJMNQMNKERFVEXWTRZXWIAKLXFPSK
 AUTEMNDCMGTSXMXBTUIADNGMGPSRELXNIELXVRVPRTULH
 DNQWTWDTYGBPMXTFALJHASVBFXNGLL**CHR**ZBWELEKMSSIK
 NBHWIRIGNMGJSLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLX
 RRIMGNSNRV**CHR**QHAIEYEVTAQEBBIPPEEWEVKAKOEWADREMX
 MTBHHCHRTKDNVRZ**CHR**CLQOHPWQAIWXNRMGVOIIFKEE

Distances : 165 ,235 et 285

PGCD (165,235,285) = 5

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté		C	H	R	E	E	V	O	A	H	M	A	E	R
-------------	--	---	---	---	---	---	---	---	---	---	---	---	---	---

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17
cle	J	A	N	E	T	J	A	N	E	T	J	A	N

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17
cle	J	A	N	E	T	J	A	N	E	T	J	A	N
equivalent entier	9	0	13	4	19	9	0	13	4	19	9	0	13

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17
cle	J	A	N	E	T	J	A	N	E	T	J	A	N
equivalent entier	9	0	13	4	19	9	0	13	4	19	9	0	13
la difference	-7	7	4	0	-15	12	14	-13	3	-7	-9	4	4

Un exemple de decryptage (partie 2)

$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17
cle	J	A	N	E	T	J	A	N	E	T	J	A	N
equivalent entier	9	0	13	4	19	9	0	13	4	19	9	0	13
la difference	-7	7	4	0	-15	12	14	-13	3	-7	-9	4	4
modulo 26	19	7	4	0	11	12	14	13	3	19	17	4	4

Un exemple de decryptage (partie 2)

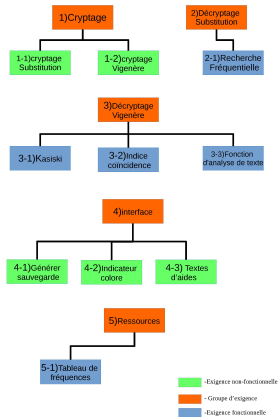
$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

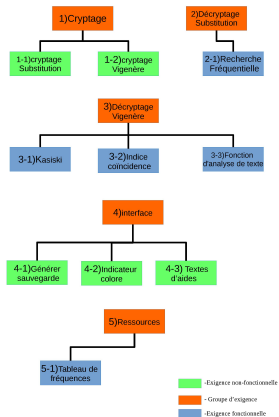
text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17
cle	J	A	N	E	T	J	A	N	E	T	J	A	N
equivalent entier	9	0	13	4	19	9	0	13	4	19	9	0	13
la difference	-7	7	4	0	-15	12	14	-13	3	-7	-9	4	4
modulo 26	19	7	4	0	11	12	14	13	3	19	17	4	4
text clair	T	H	E	A	L	M	O	N	D	T	R	E	E

Un exemple de decryptage (partie 2)

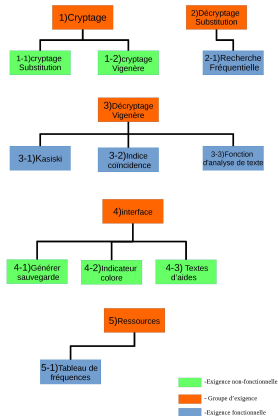
$$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$$

text crypté	C	H	R	E	E	V	O	A	H	M	A	E	R
equivalent entier	2	7	17	4	4	21	14	0	7	12	0	4	17
cle	J	A	N	E	T	J	A	N	E	T	J	A	N
equivalent entier	9	0	13	4	19	9	0	13	4	19	9	0	13
la difference	-7	7	4	0	-15	12	14	-13	3	-7	-9	4	4
modulo 26	19	7	4	0	11	12	14	13	3	19	17	4	4
text clair	T	H	E	A	L	M	O	N	D	T	R	E	E



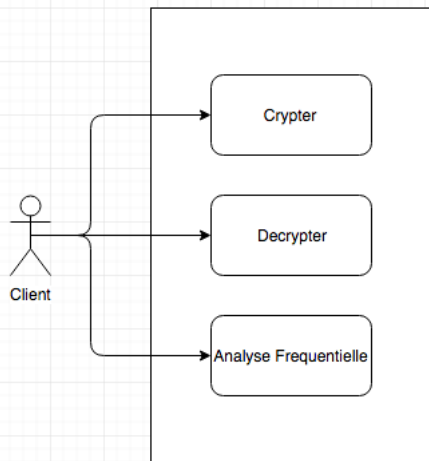


Número de l'exigence : 5.1	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation Tableaux des fréquences des lettres.	
Description : Utiliser un tableau des fréquences des lettres pour décrypter une chiffrement de Vigenère.	
Justification : Besoin d'un tableau contenant les fréquences d'apparition des lettres de l'alphabet dans une langue.	
Origine : Demande du développeur : L'utilisation de ce tableaux est essentielle au décryptage.	
Critères de satisfaction : Obtenir ce tableaux dans les différents langages(anglais, français).	
Contentement du maître d'ouvrage : 5	Mécontentement du maître d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Découverte après recherche	



Número de exigence : 5.1	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation: Tableaux des fréquences des lettres.	
Description : Utiliser un tableau des fréquences des lettres pour décrypter une chiffrement de Vigenère.	
Justification : Besoin d'un tableau contenant les fréquences d'apparition des lettres de l'alphabet dans une langue.	
Origine : Demande du développeur : L'utilisation de ce tableaux est essentielle au décryptage.	
Critères de satisfaction : Obtenir ce tableaux dans les différents langages(anglais, français)	
Contentement du maître d'ouvrage : 5	Mécontentement du maître d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Découverte après recherche	

Número de exigence : 4.2	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation: Indicateurs couleurs	
Description : Mettre en relief avec des couleurs les digrammes et trigrammes qui se répètent dans le texte et qui sont très peu fréquent dans la langue d'origine du texte attaquer.	
Justification : Permet d'obtenir une interface simple et efficace.	
Origine : Demande du développeur pour aider l'utilisateur.	
Critères de satisfaction : Attribuer une couleur spécifique à certains caractères. (digrammes, trigrammes)	
Contentement du maître d'ouvrage : 3	Mécontentement du maître d'ouvrage : 1
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Envisager après réflexion	



Interface graphique

Cryptage Vigenère

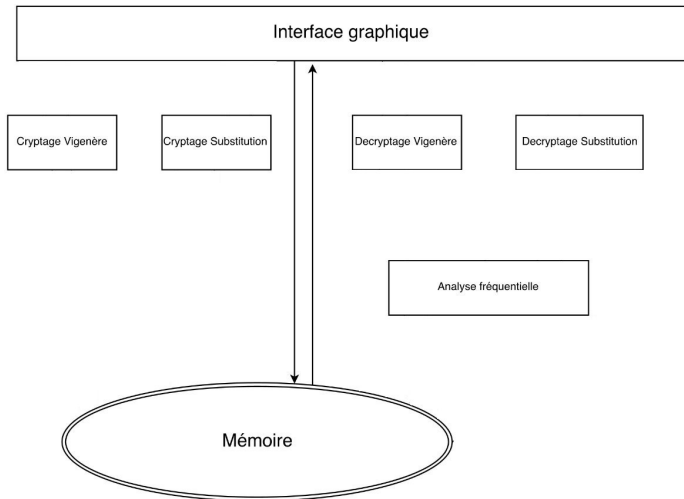
Cryptage Substitution

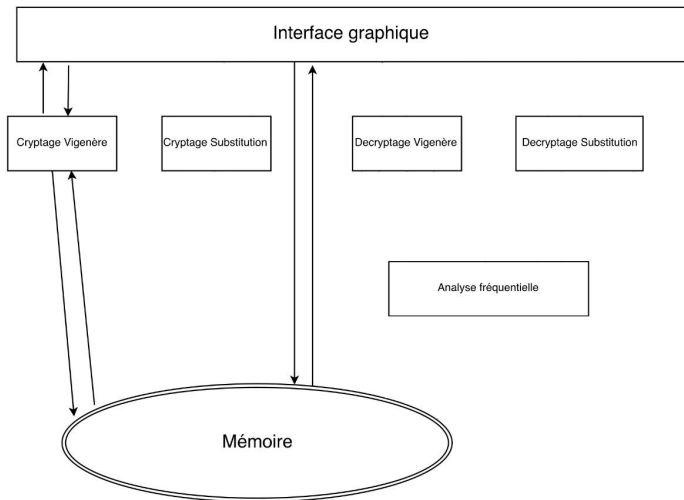
Decryptage Vigenère

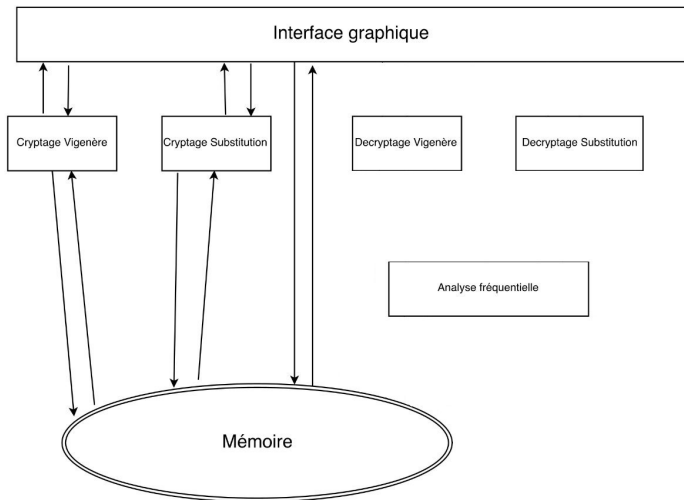
Decryptage Substitution

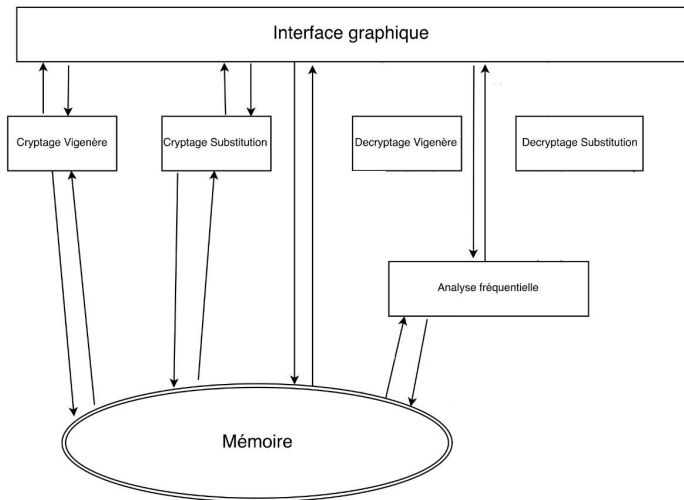
Analyse fréquentielle

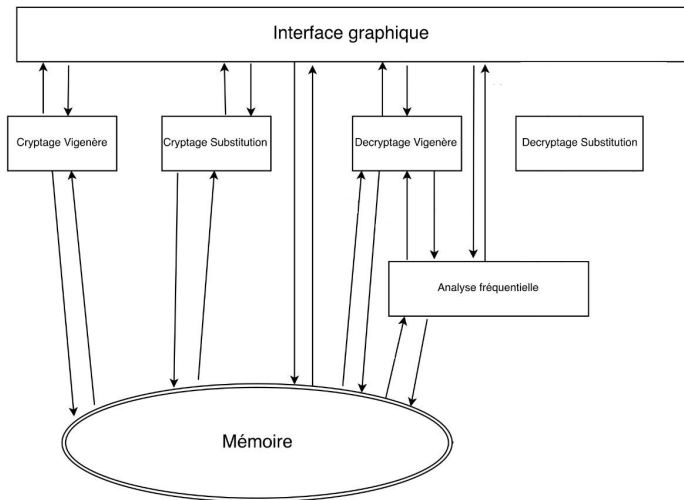
Mémoire

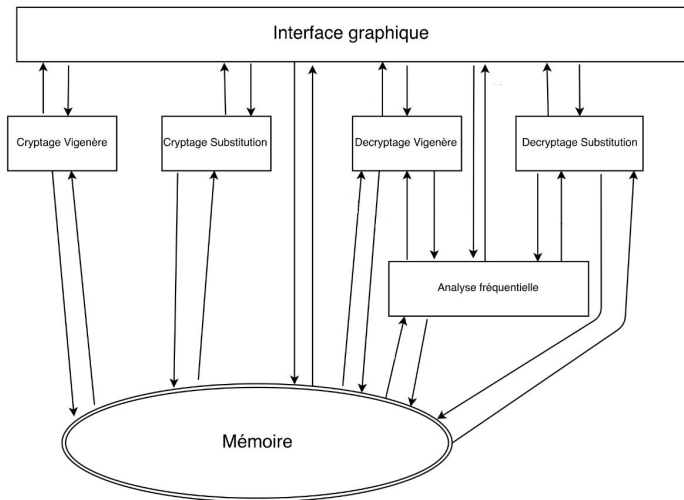












Hypothèse du coûts en nombre de ligne

Module	Cout (ligne)	Personne(s) en charge
Décryptage Vigenere	200	Chouipe & Alabi
Décryptage Substitution	150	Lienhardt & Alabi
Cryptage Vigenere	50	El Harti
Cryptage Substitution	50	El Harti
Analyse Fréquentiel	50	El Harti
Interface Graphique	1000	Benyamna & Capdenat
Total	1500	

Hypothèse du coûts en nombre de ligne

Module	Cout (ligne)	Personne(s) en charge
Décryptage Vigenere	200	Chouipe & Alabi
Décryptage Substitution	150	Lienhardt & Alabi
Cryptage Vigenere	50	El Harti
Cryptage Substitution	50	El Harti
Analyse Fréquentiel	50	El Harti
Interface Graphique	1000	Benyamna & Capdenat
Total	1500	

Choix du language

- Language C

Hypothèse du coûts en nombre de ligne

Module	Cout (ligne)	Personne(s) en charge
Décryptage Vigenere	200	Chouipe & Alabi
Décryptage Substitution	150	Lienhardt & Alabi
Cryptage Vigenere	50	El Harti
Cryptage Substitution	50	El Harti
Analyse Fréquentiel	50	El Harti
Interface Graphique	1000	Benyamna & Capdenat
Total	1500	

Choix du langage

- Language C
- Bibliothèque GTK

Conclusion

Conclusion

