

Projet final : Cryptanalyse



Introduction

Hill-Climbing

Substitution

Transposition

Interface
Graphique

- UE LU2IN013
- YAZID Samy (Adem)
- KAOUCH Abdelssamad
- SENIHJI Wassim
- Double-majeure intensive
maths-info (PIMA)
- Juillet 2021

Introduction

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes
Un cryptosystème est composé

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Un cryptosystème est composé
- d'algorithmes de chiffrement

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Un cryptosystème est composé

- d'algorithmes de chiffrement
- de textes clairs

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Un cryptosystème est composé

- d'algorithmes de chiffrement
- de textes clairs
- de textes chiffrés

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Un cryptosystème est composé

- d'algorithmes de chiffrement
- de textes clairs
- de textes chiffrés
- de clés de chiffrement

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Un cryptosystème est composé

- d'algorithmes de chiffrement
- de textes clairs
- de textes chiffrés
- de clés de chiffrement

C'est ainsi que l'on aborde une
notion clé de ce projet :
le concept de cryptanalyse

Introduction

Introduction

Notre projet porte sur
l'automatisation de cryptosystèmes

Un cryptosystème est composé

- d'algorithmes de chiffrement
- de textes clairs
- de textes chiffrés
- de clés de chiffrement

C'est ainsi que l'on aborde une
notion clé de ce projet :
le concept de cryptanalyse

Mais qu'est-ce donc ?



Introduction



La cryptanalyse est la technique visant à déduire un texte clair à partir d'un texte chiffré sans être en possession de la clé de chiffrement

La cryptanalyse est la technique visant à déduire un texte clair à partir d'un texte chiffré sans être en possession de la clé de chiffrement

En pratique, on cherche la clé de chiffrement puis on applique la fonction réciproque de la fonction de chiffrement

CETTEFOISILNAMENAITQUETROISBERLINES

CETTEFOISILNAMENAITQUETROISBERLINES



CETTEFOISILNAMENAITQUETROISBERLINES



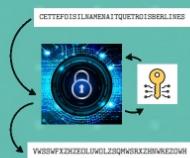
CETTEFOISILNAMENAITQUETROISBERLINES



VWSSWFXZHZEOLUWOLZSQMWSRXZHNWREZOWH

La cryptanalyse est la technique visant à déduire un texte clair à partir d'un texte chiffré sans être en possession de la clé de chiffrement

En pratique, on cherche la clé de chiffrement puis on applique la fonction réciproque de la fonction de chiffrement



Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Vive les bébé-licornes !

Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Vive les bébé-licornes !



VIVELESBEBELICORNES

Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Vive les bébé-licornes !



VIVELESBEBELICORNES

Pour palier cette perte d'information, nous avons étudié la liste des tétragrammes composant le message.

Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Vive les bébé-licornes !



VIVELESBEBELICORNES

Pour palier cette perte d'information, nous avons étudié la liste des tétragrammes composant le message.

Un mot de n caractères ($n \geq 4$) est composé de $n-3$ tétragrammes que l'on décompose de cette façon :

Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Vive les bébé-licornes !



VIVELESBEBELICORNES

Pour palier cette perte d'information, nous avons étudié la liste des tétragrammes composant le message.

Un mot de n caractères ($n \geq 4$) est composé de $n-3$ tétragrammes que l'on décompose de cette façon :

LICORNE

Lorsque l'on veut chiffrer un message, on essaye de le rendre le moins vulnérable à de potentielles attaques. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés sans espaces, ponctuation, caractères spéciaux et lettres minuscules :

Vive les bébé-licornes !



VIVELESBEBELICORNES

Pour palier cette perte d'information, nous avons étudié la liste des tétragrammes composant le message.

Un mot de n caractères ($n \geq 4$) est composé de $n-3$ tétragrammes que l'on décompose de cette façon :

LICORNE =LICO +ICOR +CORN +ORNE

La cryptanalyse est la technique visant à déduire un texte clair à partir d'un texte chiffré sans être en possession de la clé de chiffrement

En pratique, on cherche la clé de chiffrement puis on applique la fonction réciproque de la fonction de chiffrement



CETTEFOUSILSAMENAITQUETROISERLINES
VIVESBEBELICORNES

Lorsque l'on veut chiffrer un message, on essaie de le rendre le moins compréhensible possible. C'est pour cette raison que tout au long du projet, nous avons analysé des messages chiffrés, leurs espaces, ponctuation, caractères spéciaux et lettres immuables.

Vive les bébélicornes !

VIVELESBEBELICORNES

Pour déchiffrer cette partie d'information, nous avons utilisé la liste des tétragrammes composant le message.

Un mot de n caractères (n>4) est composé de n-3 tétragrammes que l'on décompose de cette façon :

LICORNE = LICO + ICOR + CORN + ORNE

Projet final : Cryptanalyse



Introduction

Hill-Climbing

Substitution

Transposition

Interface
Graphique

Projet final : Cryptanalyse



Introduction



Hill-Climbing

Substitution

Transposition

Interface
Graphique

Projet final : Cryptanalyse



Introduction



Hill-Climbing

Substitution

Transposition

Interface
Graphique

Hill-Climbing

Exemple



Hill-Climbing

Au cours de ce projet,
l'algorithme employé pour
retrouver la clé de chiffrement
était celui du Hill-Climbing

Exemple

Hill-Climbing

Au cours de ce projet,
l'algorithme employé pour
retrouver la clé de chiffrement
était celui du Hill-Climbing

Il faut évaluer la clé actuelle à
l'aide de la "fitness function", et
tenter des modifications par
palier sur la clé (échange de
deux caractères de la clé)
jusqu'à obtenir une meilleure
version ou que le "freeze" soit
maximal

Exemple

Exemple

Exemple

Clé : (e_1, e_2, \dots, e_n)

Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f:n_uplet -> float

Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f : n_uplet -> float

float Val_Clé

Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f : n_uplet -> float

float Val_Cle

int Freeze

Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f : n_uplet -> float

float Val_Clé

int Freeze

(e1, e2, e3 , e4, e5)

Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f : n_uplet -> float

float Val_Clé

int Freeze

(e1, e2, e3 , e4, e5)

Val_Clé = f ((e1, e2, e3 , e4, e5))

Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f : n_uplet -> float

float Val_Clé

int Freeze

(e1, e2, e3 , e4, e5)

Val_Clé = f ((e1, e2, e3 , e4, e5))

(e1, e4, e3 , e2, e5)



Exemple

Clé : (e1, e2, ... , en)

Fonction de fitness : f : n_uplet -> float

float Val_Clé

int Freeze

(e1, e2, e3 , e4, e5)

Val_Clé = f ((e1, e2, e3 , e4, e5))

f((e1, e4, e3 , e2, e5))



Projet final : Cryptanalyse



Introduction



Hill-Climbing

Substitution

Transposition

Interface
Graphique

Projet final : Cryptanalyse



Introduction



Hill-Climbing



Substitution

Transposition

Interface
Graphique

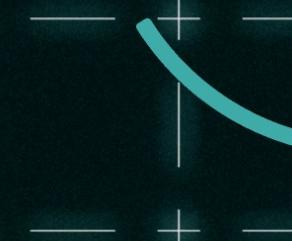
Projet final : Cryptanalyse



Introduction



Hill-Climbing



Substitution

Transposition

Interface
Graphique

Substitution

Chiffrement

Déchiffrement

fitness func

Substitution

La méthode de chiffrement par substitution consiste à changer dans le message chaque lettre de l'alphabet par une autre.

Chiffrement

Déchiffrement

Fitness func

Substitution

La méthode de chiffrement par substitution consiste à changer dans le message chaque lettre de l'alphabet par une autre.

On peut donc construire une clé à partir des correspondances entre l'alphabet du clair et du chiffré :

Chiffrement

Déchiffrement

Fitness func

Substitution

La méthode de chiffrement par substitution consiste à changer dans le message chaque lettre de l'alphabet par une autre.

On peut donc construire une clé à partir des correspondances entre l'alphabet du clair et du chiffré :

Alphabet clair :

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

Chiffrement

Déchiffrement

Fitness func

Substitution

La méthode de chiffrement par substitution consiste à changer dans le message chaque lettre de l'alphabet par une autre.

On peut donc construire une clé à partir des correspondances entre l'alphabet du clair et du chiffré :

Alphabet clair :

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

Exemple d'alphabet chiffré
(clé de chiffrement) :

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

Chiffrement

Déchiffrement

Fitness func

Chiffrement

Chiffrement

Pour le chiffrement, on prend le str msg_clair et pour chaque caractère le composant, on le remplace par le caractère à la même position dans la clé de chiffrement

Chiffrement

Pour le chiffrement, on prend le str msg_clair et pour chaque caractère le composant, on le remplace par le caractère à la même position dans la clé de chiffrement

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

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

BBLICORNE

Chiffrement

Pour le chiffrement, on prend le str msg_clair et pour chaque caractère le composant, on le remplace par le caractère à la même position dans la clé de chiffrement

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

Chiffrement

Pour le chiffrement, on prend le str msg_clair et pour chaque caractère le composant, on le remplace par le caractère à la même position dans la clé de chiffrement



Déchiffrement

Déchiffrement

Pour le déchiffrement, on prend le str msg_chiffre et pour chaque caractère le composant, on le remplace par le caractère à la même position dans l'alphabet clair

Déchiffrement

Pour le déchiffrement, on prend le str msg_chiffre et pour chaque caractère le composant, on le remplace par le caractère à la même position dans l'alphabet clair

ZGEBJDLIHWMNYFOPAXQRSTUCKV

ABCDEFGHIJKLMNOPQRSTUVWXYZ

GGNHEOXFJ

Déchiffrement

Pour le déchiffrement, on prend le str msg_chiffre et pour chaque caractère le composant, on le remplace par le caractère à la même position dans l'alphabet clair

ZGEBJDLIHWMNYFOPAXQRSTUCKV
↓ ↓ ↓ ↓ ↓ ↓ ↓
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

GGNHEOXFJ

Déchiffrement

Pour le déchiffrement, on prend le str msg_chiffre et pour chaque caractère le composant, on le remplace par le caractère à la même position dans l'alphabet clair

ZGEBJDLIHWMNYFOPAXQRSTUCKV
↓ ↓ ↓ ↓ ↓ ↓ ↓
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

GGNHEOXFJ
BBLICORNE



fitness func

fitness func

On prend chaque tétragramme de la chaîne de caractère et on somme les logarithmes en base 10 du nombre d'apparition du tétragramme choisi dans le dictionnaire théorique.

fitness func

On prend chaque tétragramme de la chaîne de caractère et on somme les logarithmes en base 10 du nombre d'apparition du tétragramme choisi dans le dictionnaire théorique.

Soient f la fitness function et g la fonction qui associe une clé du dictionnaire théorique à sa valeur, alors

fitness func

On prend chaque tétragramme de la chaîne de caractère et on somme les logarithmes en base 10 du nombre d'apparition du tétragramme choisi dans le dictionnaire théorique.

Soient f la fitness function et g la fonction qui associe une clé du dictionnaire théorique à sa valeur, alors

$$f(\text{PROJET}) = \log_{10}(g(\text{PROJ})) + \log_{10}(g(\text{ROJE})) + \log_{10}(g(\text{OJET}))$$

fitness func

On prend chaque tétragramme de la chaîne de caractère et on somme les logarithmes en base 10 du nombre d'apparition du tétragramme choisi dans le dictionnaire théorique.

Soient f la fitness function et g la fonction qui associe une clé du dictionnaire théorique à sa valeur, alors

$$f(\text{PROJET}) = \log_{10}(g(\text{PROJ})) + \log_{10}(g(\text{ROJE})) + \log_{10}(g(\text{OJET}))$$

Dans le Hill-Climbing, on cherche donc à maximiser la valeur de f

Projet final : Cryptanalyse



Introduction



Hill-Climbing



Substitution

Transposition

Interface
Graphique

Projet final : Cryptanalyse



Introduction



Substitution



Hill-Climbing



Transposition



Interface
Graphique



Projet final : Cryptanalyse



Introduction



Hill-Climbing



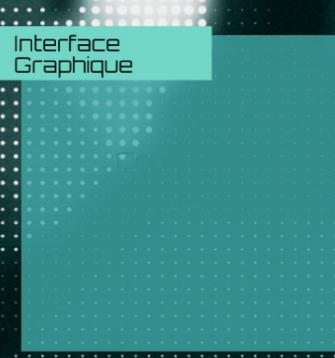
Substitution



Transposition



Interface
Graphique



Transposition

Déchiffrement

fitness func

Transposition

La méthode de chiffrement par transposition consiste à écrire le message sur des lignes de longueur fixe, puis permuter les colonnes obtenues et enfin, relire le texte colonne par colonne.

Déchiffrement

fitness func

Transposition

La méthode de chiffrement par transposition consiste à écrire le message sur des lignes de longueur fixe, puis permuter les colonnes obtenues et enfin, relire le texte colonne par colonne.

La clé sera l'ordre de lecture des colonnes

Déchiffrement

fitness func

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

On complétera, si nécessaire, la dernière ligne avec ce qu'on appelle un caractère de padding (ici X)

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

On complétera, si nécessaire, la dernière ligne avec ce qu'on appelle un caractère de padding (ici X)

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

Ici, la clé de chiffrement est 587139246

On complétera, si nécessaire, la dernière ligne avec ce qu'on appelle un caractère de padding (ici X)

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

Ici, la clé de chiffrement est 587139246

Et le message chiffré est DNMNUAXDTEPEWX...IEEURNX

Transposition

La méthode de chiffrement par transposition consiste à écrire le message sur des lignes de longueur fixe, puis permuter les colonnes obtenues et enfin, relire le texte colonne par colonne.

La clé sera l'ordre de lecture des colonnes

On complétera, si nécessaire, la dernière ligne avec ce qu'on appelle un caractère de padding (ici X)

1	2	3	4	5	6	7	8	9
M	C	O	N	D	E	S	T	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	E	R	E	R
L	E	N	A	N	D	E	R	I
C	H	S	X	X	X	X	X	X

1	2	3	4	5	6	7	8	9
D	D	S	M	S	A	I	I	J
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	M	A	V	O	S	E	U
U	E	R	R	E	R	E	R	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

Ici, la clé de chiffrement est 587139246

Et le message chiffré est DNMMNUAXDTEPEWX...IEURNX

Déchiffrement

fitness func

Transposition

La méthode de chiffrement par transposition consiste à écrire le message sur des lignes de longueur fixe, puis permuter les colonnes obtenues et enfin, relire le texte colonne par colonne.

La clé sera l'ordre de lecture des colonnes

On complétera, si nécessaire, la dernière ligne avec ce qu'on appelle un caractère de padding (ici X)

1	2	3	4	5	6	7	8	9
M			D			O		
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	E	R	E	R
L			A	N	D	E	R	I
C	H	S	X	X	X	X	X	X

1	2	3	4	5	6	7	8	9
D	D	S	M	S	A	I		
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	M	A	V	O	S	E	U
E	F	R	E	R	E	R	R	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

Ici, la clé de chiffrement est 587139246

Et le message chiffré est DNMMNUAXDTEPEWX...IEEURNX

Exemple issu de "La sécurité des données" de Mme Valérie Ménissier-Morain.

Déchiffrement

fitness func

Déchiffrement

Déchiffrement

La méthode de déchiffrement par transposition consiste à écrire le message des colonnes de taille fixe (égale à `len(msg)/taille_cle`), puis à réinitialiser l'ordre des colonnes et enfin relire le texte ligne par ligne

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

La clé de chiffrement est 587139246

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

La clé de chiffrement est 587139246
 Et le message chiffré est DNMNUAXDTEPEWX...IEEURNX

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X

Déchiffrement

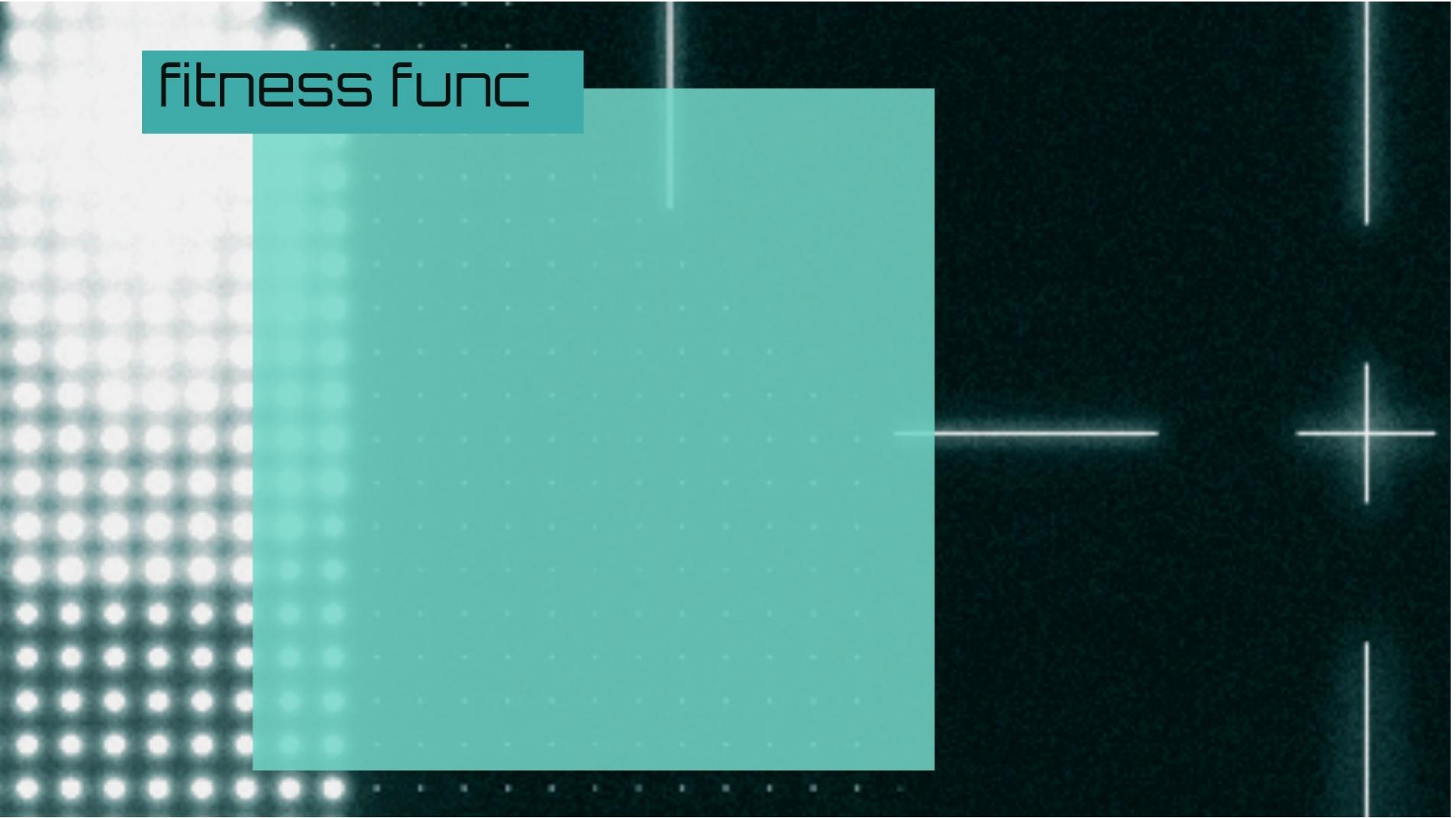
La méthode de déchiffrement par transposition consiste à écrire le message des colonnes de taille fixe (égale à $\text{len}(\text{msg})/\text{taille_cle}$), puis à réinitialiser l'ordre des colonnes et enfin relire le texte ligne par ligne

La clé de chiffrement est 587139246

Et le message chiffré est DNMNUAXDTEPEWX...IEEURNX

5	8	7	1	3	9	2	4	6
D	D	S	M	I	O	A	S	I
N	T	S	N	O	Q	C	N	E
M	E	M	U	N	P	A	D	E
N	P	S	A	V	O	S	E	U
U	E	R	U	B	R	R	E	R
A	W	D	L	S	I	E	S	N
X	X	X	C	S	X	H	X	X

1	2	3	4	5	6	7	8	9
M	A	I	S	D	I	S	D	O
N	C	O	N	N	E	S	T	Q
U	A	N	D	M	E	M	E	P
A	S	V	E	N	U	S	P	O
U	R	B	E	U	R	R	E	R
L	E	S	S	A	N	D	W	I
C	H	S	X	X	X	X	X	X



fitness func

fitness func

On utilise la même cœur de fonction que pour la substitution, à une différence près, on travaille avec une condition supplémentaire sur les caractères de padding.

fitness func

On utilise la même cœur de fonction que pour la substitution, à une différence près, on travaille avec une condition supplémentaire sur les caractères de padding.

La fitness function augmente très fortement pour chaque caractère de padding successif à la fin du message clair

fitness func

On utilise la même cœur de fonction que pour la substitution, à une différence près, on travaille avec une condition supplémentaire sur les caractères de padding.

La fitness function augmente très fortement pour chaque caractère de padding successif à la fin du message clair

Projet final : Cryptanalyse



Introduction



Hill-Climbing



Substitution



Transposition



Interface
Graphique



Projet final : Cryptanalyse



Introduction



Hill-Climbing



Substitution



Transposition



Interface
Graphique

Projet final : Cryptanalyse



Introduction



Hill-Climbing



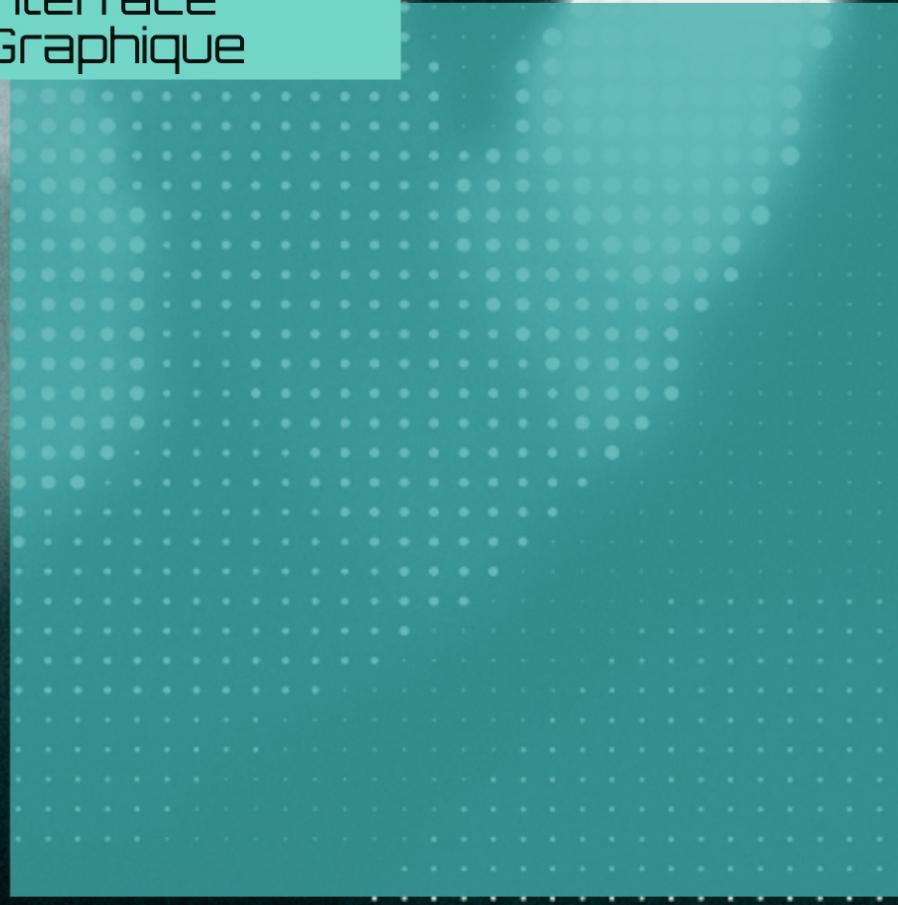
Substitution



Transposition



Interface
Graphique



Interface
Graphique



Menu



Substitution



Transposition

Interface Graphique

Afin d'améliorer les conditions d'utilisation des fonctions par l'utilisateur, nous avons décidé d'implémenter une interface graphique.

Menu

Substitution

Transposition

Interface Graphique

Afin d'améliorer les conditions d'utilisation des fonctions par l'utilisateur, nous avons décidé d'implémenter une interface graphique.

Elle est décomposée en 3 parties :

- Un menu principal
- La partie substitution
- La partie transposition (à taille de colonnes et caractère de padding fixés)

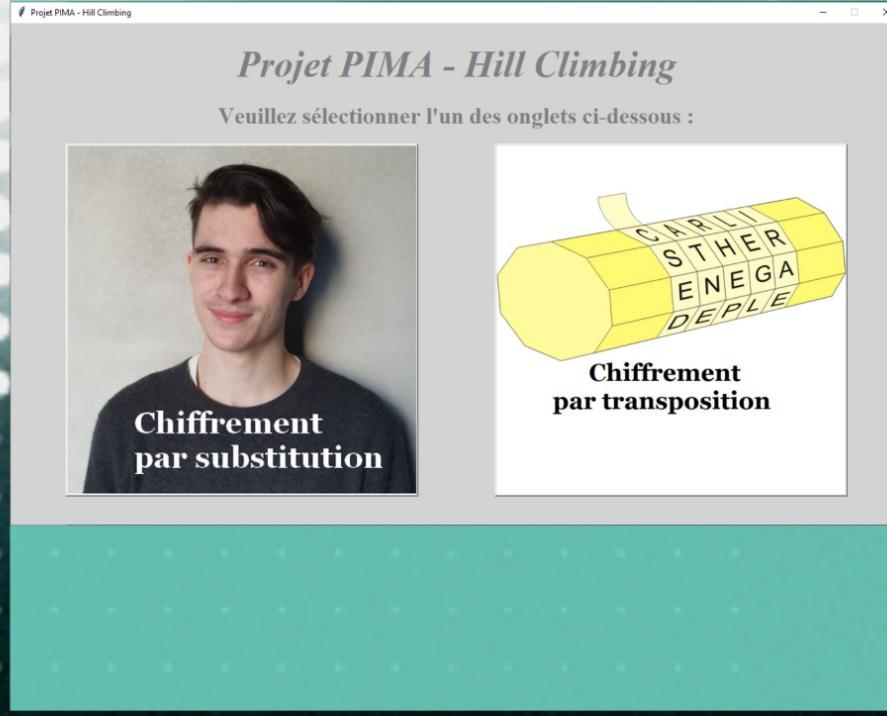
Menu

Substitution

Transposition

Menu

Menu

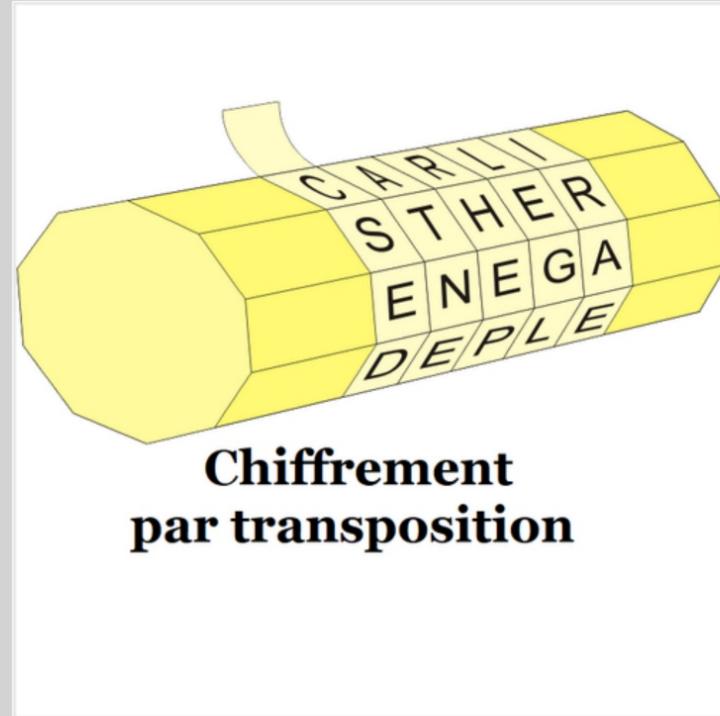


Projet PIMA - Hill Climbing

Veuillez sélectionner l'un des onglets ci-dessous :

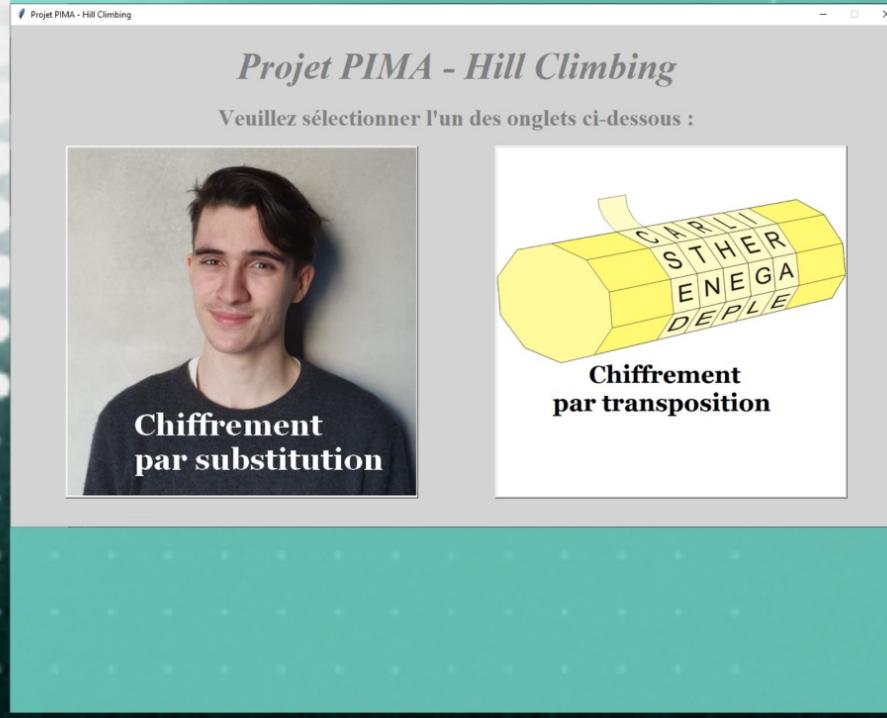


**Chiffrement
par substitution**



**Chiffrement
par transposition**

Menu



Substitution

Substitution



Décryptage de chiffrement par substitution

Le message déchiffré s'affichera ici-même

L'alphabet/clé de chiffrement est : ABCDEFGHIJKLMNOPQRSTUVWXYZ

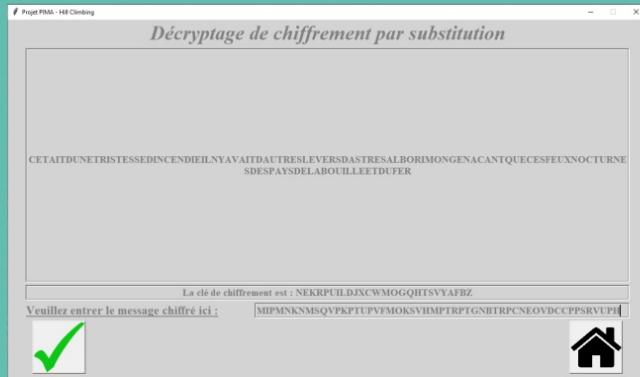
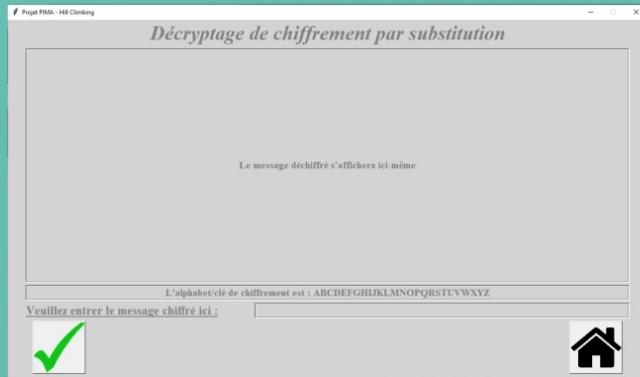
Veuillez entrer le message chiffré ici :



Substitution



Substitution



Décryptage de chiffrement par substitution

CETAITDUNETRISTESSEDINCENDIEILNYAVAITDAUTRESLEVERSASTRESALBORIMONGENACANTQUECESFEUXNOCTURNE
SDESPAYSDELA BOUILLEETDUER

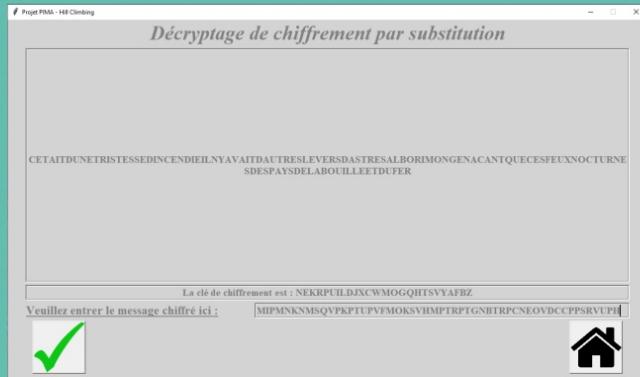
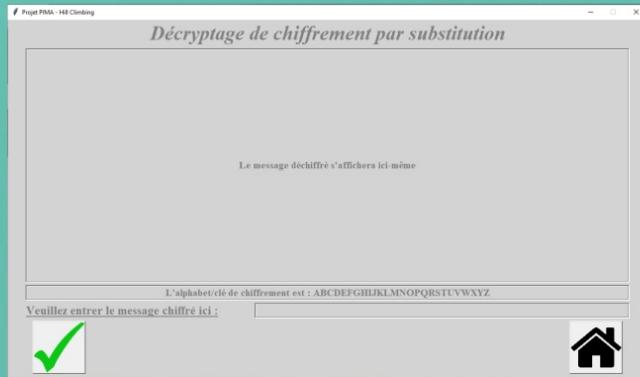
La clé de chiffrement est : NEKRPUILDJXCWMQHHTSVYAFBZ

Veuillez entrer le message chiffré ici :

MIPMNKNMSQVPKPTUPVFMOKSVHMPTRPTGNBTRPCNEOVDCCPPSRVUPH



Substitution



Transposition

Transposition



Décryptage de chiffrement par transposition

Le message déchiffré s'affichera ici-même

La clé de chiffrement est : 123456789

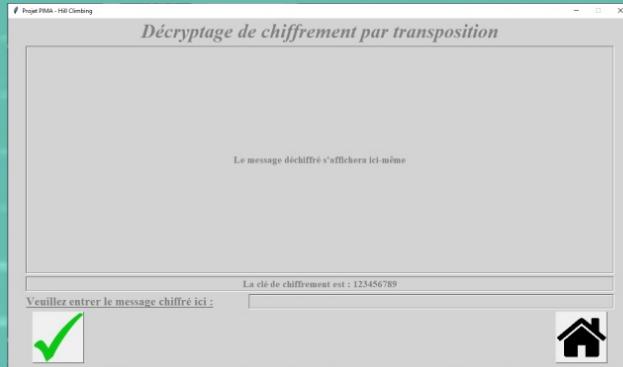
Veuillez entrer le message chiffré ici :



Transposition



Transposition



Décryptage de chiffrement par transposition

MAISDISDONCONNESTQUANDMEMEPASVENUSPOURBEURRELESSANDWICHES

La clé de chiffrement est : 587139246

Veuillez entrer le message chiffré ici :

DNMMNUA&DTEPEW&SSMSRD&MNUAULCIONVBSSOQPORI&ACASREHSNDEE



Transposition



Projet final : Cryptanalyse



Introduction



Hill-Climbing



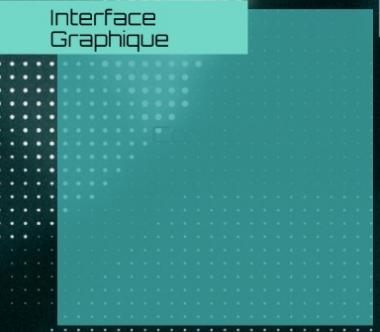
Substitution



Transposition



Interface
Graphique



Projet final : Cryptanalyse



Introduction



Hill-Climbing



Substitution



Transposition



Interface
Graphique











FIN