Cryptographie pour la robotique

Comment protéger les messages dans le cas de la robotique?

Sommaire

Formule de cryptage:

x : Lettre à coder
e : Encodage de x
n : Clef de l'algorithme

$$E \equiv x+n \ [26]$$

Texte 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
Texte chiffré	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

Table de chiffrement pour n=3

Texte clair	A	U	C	U	N		D	A	N	G	E	R		N		A		E	T	E		D	E	T	E	C	T	E	E
Texte chiffré	D	X	F	X	Q		G	D	Q	J	H	U		Q		D		H	W	H		G	H	W	H	F	W	H	H

Exemple d'encodage pour n=3

Formule de décryptage:

x : Lettre à coder
e : Encodage de x
n : Clef de l'algorithme

$$e \equiv x+n \ [26]$$

e : Lettre à décoder
D : Décodage de x
n : Clef de l'algorithme

$$D \equiv e-n \ [26]$$

Texte chiffré	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
Texte clair	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

Table de déchiffrement pour n=3

Augmentation de la robustesse par composition des chiffrements?

Etape 1 : Premier chiffrement

$E1 \equiv x1+n1 \ [26]$

Etape 2 : Deuxième chiffrement

$E2 \equiv x2+n2 \ [26]$

Etape 3 : Composition

$E \equiv (x+n1)+n2 \ [26]$ → $E \equiv x + (n1+n2) \ [26]$

1^{er} chiffrement

→ La complexité reste inchangée.

Chiffrement affine

Cryptage :

x : Lettre à coder

e : Encodage de x

(a,b) : Clef de l'algorithme

$E \equiv ax+b\ [26]$

Un exemple: $E \equiv 3x + 7\ [26]$

$ROBOT_{non\_crypté} \equiv$ 17 14 1 14 20

$ROBOT_{crypté} \equiv (3*17+7)\ (3*14+7)\ (3*1+7)\ (3*14+7)\ (3*20+7)\ [26] \equiv 58\ 49\ 10\ 49\ 67\ [26] \equiv 6\ 23\ 10\ 23\ 15\ [26] \equiv$ GXKXP

Chiffrement affine

Cryptage :

x : Lettre à coder
e : Encodage de x
(a,b) : Clef de l'algorithme

$E \equiv ax+b\ [26]$

Décryptage : $ax+b \equiv e\ [26] \rightarrow ax \equiv e-b\ [26] \rightarrow (a^{-1}a) \equiv a^{-1}(e-b) \equiv 1$

On peut trouver a^{-1} à la condition que pgcd(a,26)=1 (cf Bachet-Bézout)
→ Seulement 12 valeurs de a possibles.

Cryptage :

x : Lettre à coder
e : Encodage de x
(a,b) : Clef de l'algorithme

$E \equiv ax+b \ [26]$

Composition de clef :

Soit une clef (a1,b1) et une clef (a2,b2)
La composition devient : $a2(a1\ x + b1) + b2 = a1a2x + a2b1 + b2$

→ Même complexité avec $a = a1a2$ et $b = a2b1 + b2$

Chiffrement de Vigenère

Concept : La clef n'est plus la même pour chaque lettre

Etape 1 : Transformer les lettres du message et de la clef en nombre ∈ [0,25]

Etape 2 : Dupliquer la clef autant de fois que nécessaire sous le message

Etape 3 : Réaliser un chiffrement de César lettre par lettre

A	U	C	U	N		D	A	N	G	E	R		N		A		E	T	E		D	E	T	E	C	T	E	E
0	**20**	**2**	**20**	**13**		**3**	**0**	**13**	**6**	**4**	**17**		**13**		**0**		**4**	**19**	**4**		**3**	**4**	**19**	**4**	**2**	**19**	**4**	**4**
S	A	F	E	S		A	F	E	S	A	F		E		S		A	F	E		S	A	F	E	S	A	F	E
18	0	5	4	18		0	5	4	18	0	5		4		18		0	5	4		18	0	5	4	18	0	5	4
18	20	7	24	31		3	5	17	24	4	22		17		18		4	24	8		21	4	24	8	20	19	9	8
S	U	H	Y	F		D	F	R	Y	E	W		R		S		E	Y	I		V	E	Y	I	U	T	J	i

Chiffrement de Vigenère

Décryptage : On applique la transformé inverse

Formule générale :
Soit une clef d'encodage c1c2c3c4
La clef de décryptage est (-c1 [26])(-c2 [26])(-c3 [26])(-c4 [26])

Détermination de la clef inverse :
Ici la clef était : SAFE= 18 0 5 4
x1 x2 x3 x4 devient : (x1+18) (x2+0) (x3+5) (x4+4)

Pour revenir au texte de base on doit donc prendre la clef -18 0 -5 -4
Ce qui donne modulo 26 : 8 0 21 22
Ce qui fait le mot : I A V W

Chiffrement de Vigenère

Augmentation de la robustesse par composition des chiffrements?

Cas 1 : Clefs de même taille

Prendre une clef 1 : table et une clef 2 : robot

Revient à faire une clef globale (t+r) (a+o) (b+b) (l+o) (e+t) = (19+17) (0+14) (1+1) (11+14) (4+19) [26] = 10 14 2 25 23 = k o c z x

→ En fait on a juste changé de clef! Pas de meilleure robustesse

Cas 2 : Clefs de tailles différentes

Clef 1 : 1 12 22 5 7 17

Clef 2 : 7 21 9 18

Revient à faire la clef suivante (1+7) (12+21) (22+9) (5+18) (7+7) (17+21) (1+9) (12+18) (22+7) (5+21) (7+9) (17+18)
= 8 33 31 23 14 38 10 30 29 26 16 35

→ En fait on change la taille de la clef : taille = ppcm(taille(clef1),taille(clef2))

L'attaque « brute force »

Brute force : Tester une à une toutes les possibilités.

Pour un Chiffrement César : E = x + n : 26 possibilités pour n

Pour un Chiffrement Affine : E = ax + b : 12 * 26 = 312 possibilités

Pour un Chiffrement de Vigénère : c =c1c2c3…cn : 26^n possibilités
Pour n = 7 on obtient 8 milliards de clefs possibles…

Fréquence d'apparition des lettres en français

Méthode d'attaque de Vigenère

Première étape : Déterminer la longueur de la clef

• **Idée :** Regarder les distances entre 2 apparitions d'un même motif.
1er cas : La même suite de lettre a été codée par la même partie de la clef
2ème cas : Des lettres différentes codées avec des parties différentes de la clef ont donné la même suite de lettre. (1 chance sur 17 000)

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG
```

Motifs se répétant dans un texte crypté

Méthode d'attaque de Vigenère

Analyse de l'espace de l'espace de répétition

• Hypothèse : Une répétition est causée par une même suite de lettre codée par une même partie de la clef.

→ La longueur de la clef est un diviseur de l'espace de répétition

		Longueurs de clef possibles			
Séquence répétée	Espace de répétition	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

Tableaux des diviseurs des espaces de répétition

Méthode d'attaque de Vigenère

Deuxième étape : Déterminer la clef par analyse fréquentielle

• **Méthode:** Si la clef est de taille 5 on coupe le texte en 5 « sous-textes »

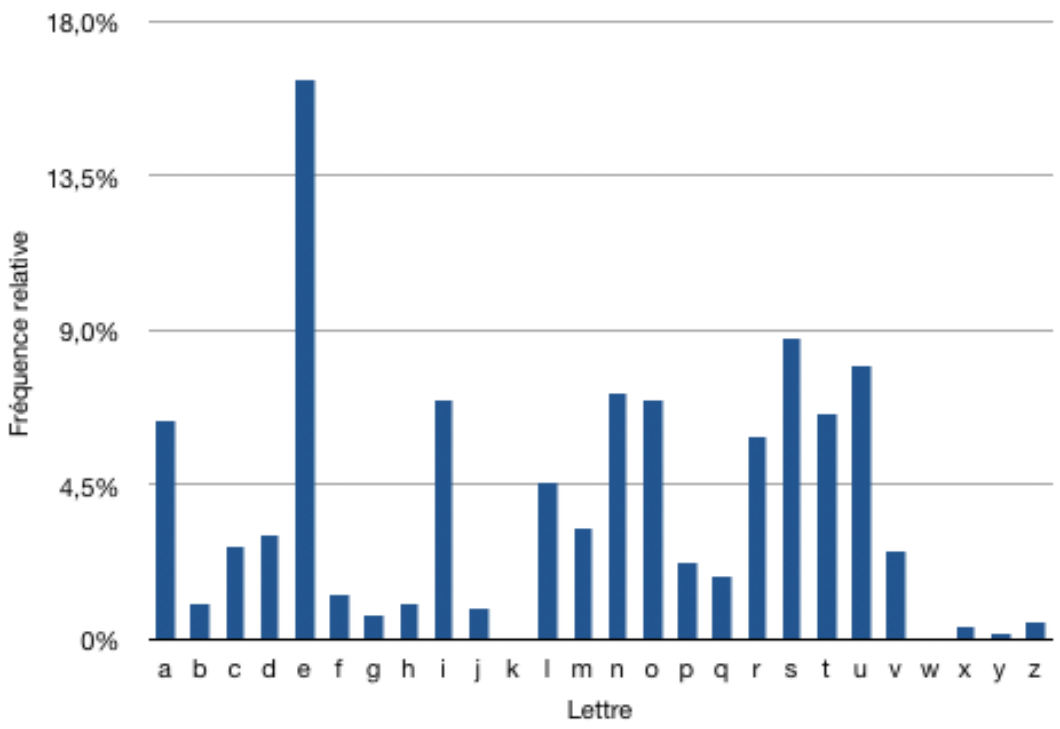
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG

Sous-texte 1 : KFJKKWM… DWVJ
Sous-texte 2 : QVUGJU … CTGG
…
Sous-texte 5: EUUEMQ … HUI

Méthode d'attaque de Vigenère

Deuxième étape : Déterminer la clef par analyse de la clef

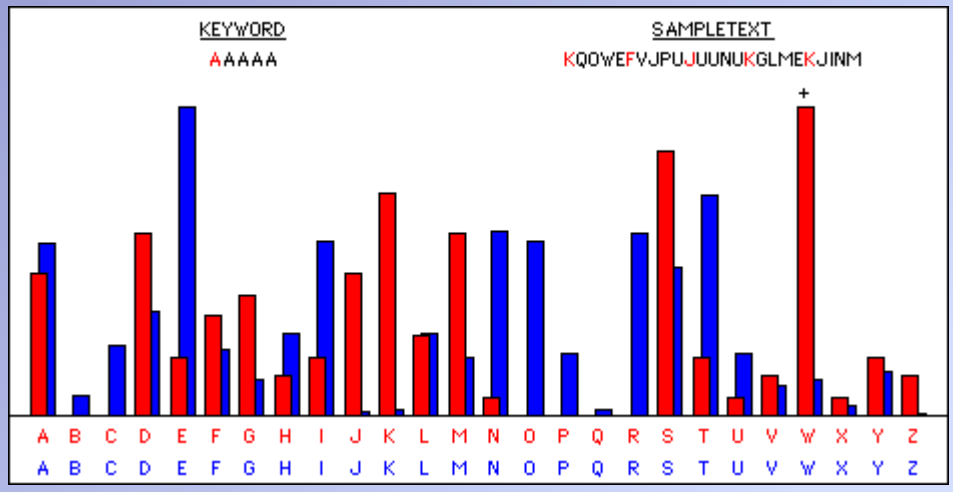
• **Idée :** Certaines lettres apparaissent plus que d'autres dans chaque langage.

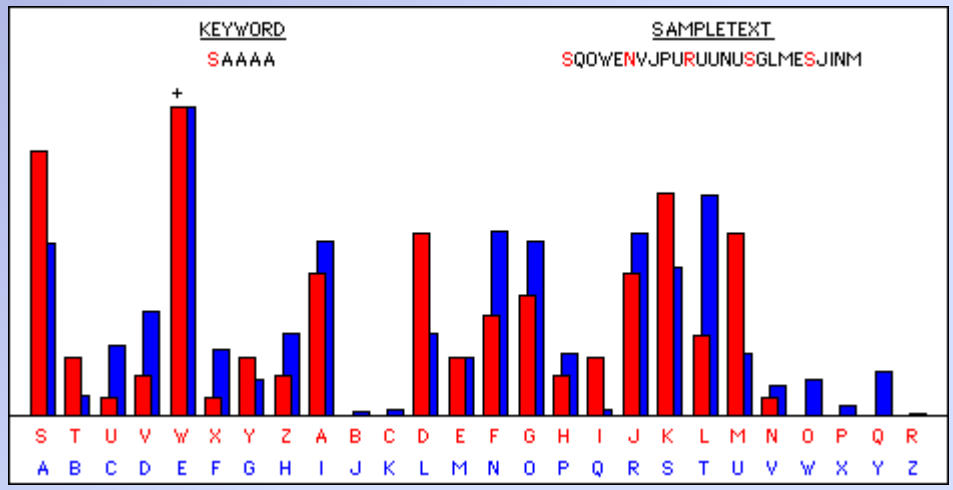


Fréquence d'apparition des lettres en français

Méthode d'attaque de Vigenère

Deuxième étape : Déterminer la clef par analyse fréquentielle



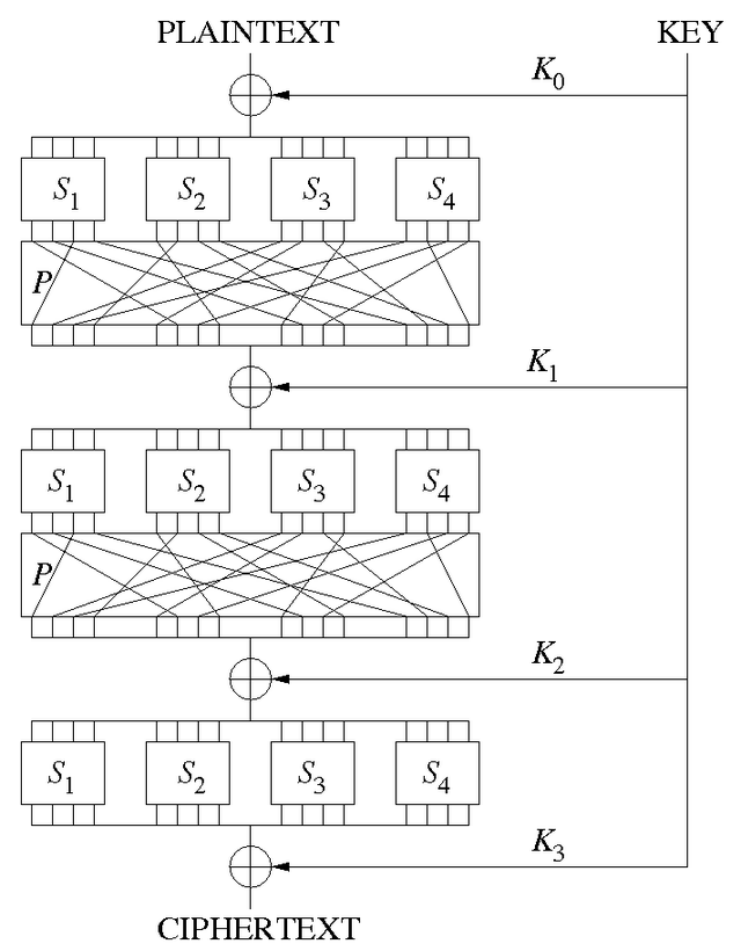


Fréquence max en W au lieu de E.

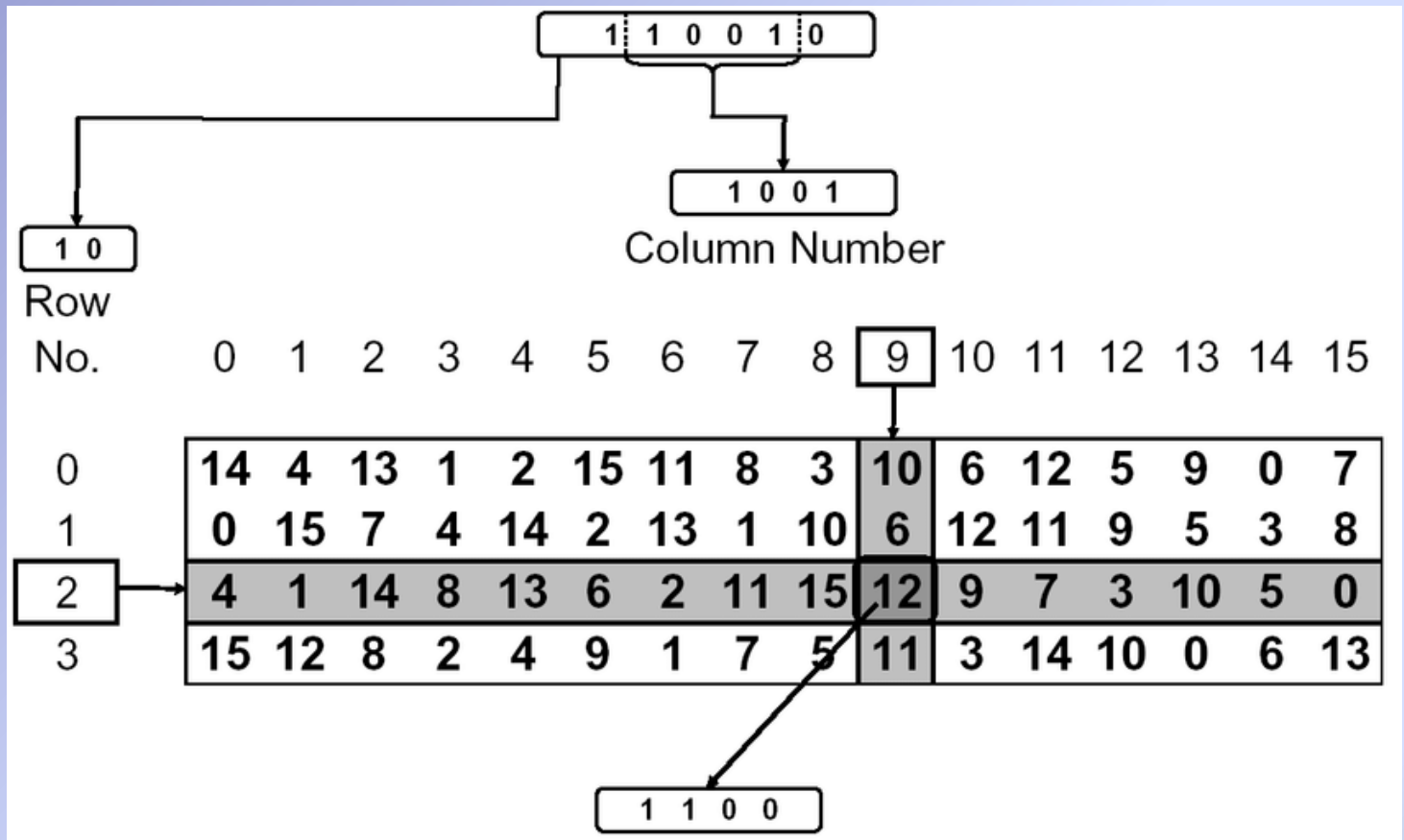
Défaut des méthodes précédente : Les cryptages conservent l'ordre des lettres.

Réponse envisagée :

Utilisation de blocs de permutation



Zoom sur la S-box :



DES (Data Encryption System) : 1977 – 1999
- Trop lent à l'exécution
- Espace de clef trop petit

AES (Advanced Encryption Standard) : 2000 – Aujourd'hui
- Seul algorithme de chiffrement approuvé par la NSA pour les informations top secrètes
- Algorithme le plus utilisé et le plus fiable

AES en chiffre : 3 tailles de clef possibles : 128, 192 ou 256 bits

$2^{256} = 10^{77}$ clefs possibles

Comparaison : 10^{78} atomes dans l'univers…