Institut National Supérieur des Sciences et Techniques d'Abéché

Département d'informatique

Niveau 2

Cours sur la cryptographie

Dispensé par :

M. Ahamat Mahamat Hassane

Préambule

- Ce cours est dispensé aux **étudiants** de la deuxième année de Licence en **Informatique** de l'Institut National Supérieur des Sciences et Techniques d'Abéché (INSTA).

- **Durée :** 30 H (10H de CM , 10H de TD et 10H de TP)
- **Evaluation :** DS (30%), EE (40%) et Projet (30%)

- **Manuel Pédagogique :**

-Support de cours ;

-Logiciel Anaconda (spyder) ;

Prérequis du cours :

- Mathématiques
- Algorithmique

Objectif du cours

- Comprendre les problématiques de cryptographie liées aux systèmes d'informations.
- Comprendre les principaux systèmes cryptographiques modernes utilisés pour la transmission et le stockage sécurisé de données.
- Comment analyser la sécurité des systèmes cryptographiques.
- Introduction aux infrastructures pour les systèmes à clé publique et clé secrète

Historique

- Vers 600 ans avant. J.-C, le roi de **Babylone Nabuchodonosor** écrivait le message qu'il souhaitait transmettre à ses généraux, sur le crâne préalablement rasé de ses esclaves
- Dans la Xème et VIIème siècle avant J.-C les Grecs ont utilisé le chiffrement de la **scytale spartiate**.

- Dans 200 avant J.-C apparait les premiers systèmes de cryptographie, ce sont les chiffrements par substitution ; il existe 4 types de substitutions :

- **Mono-alphabétique** : Remplace chaque lettre du message par une autre lettre de l'alphabet.
- **Poly-alphabétique** : Utilise une suite de chiffres mono- alphabétiques "la clé" réutilisée périodiquement.
- **Homophonique** : Fait correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.
- **Polygrammes** : Substitue un groupe de caractères dans le message par un autre groupe de caractères.

❖ Dans le 1er siècle avant J.-C lorsque **Jules César** envoyait des messages à ses généraux

❖ En 1586, le français **Blaise de Vigenère** élabore un système de substitution poly-alphabétique, connue sous le nom "chiffre de Vigenère

- En 1918, l'allemand **Arthur Scherbius** fit breveter sa machine à crypter, appelée **Enigma**
- RSA (Rivest, Shamir et Adleman en 1977). Il permet le chiffrement et la signature
- La cryptographie sur les courbes elliptiques (Koblitz et Miller en 1985) : ECC (**Elliptic Curve Cryptography**).
- L'algorithme de signature numérique **DSA** (Digital Signature Algorithm) proposé par le NIST (National Institute of Standards and Technology) en 1991.
- Et bien d'autres encore...

❖ Concepts de base

A) Définition

- ❖ Le mot cryptographie vient des deux mots grecs kryptons "secret" et graphie "écrire", c'est-à- dire écrire secrètement.
- ❖ La cryptographie est l'art de cacher une information pour la rendre inintelligible à toute personne ne connaissant pas un certain secret.
- ❖ La *cryptographie* est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données.

« « (cryptographie = "écriture cachée")» »

Objectifs:

Confidentialité,
Intégrité des données,
Authentification,
Non-répudiation.

- **Confidentialité** : garantir le secret de l'information transmise ou archivée.
- **Domaine militaire** : transmission de documents "secret défense", stratégies, plans
- **Domaine médical** : confidentialité des dossiers de patients
- **Domaine commercial** : pour les achats sur Internet, transmission sécurisée du numéro de carte bancaire
- **Domaine industriel** : transmission d'informations internes à l'entreprise à l'abris du regard des concurrents !

- **Les applications réelles de la cryptologie**
- Communications sécurisées :
  - Web : SSL/TLS, ssh, gpg
  - Sans fil : GSM, Wifi, Bluetooth
- Chiffrement des fichiers : EFS, TrueCrypt
- Protection de données personnelles : cartes de crédit, passeports électroniques et bien plus encore !

❖ Objectifs de la sécurité

La sécurité d'un système informatique a pour mission la protection des informations contre toutes divulgation, altération ou destruction.

•**Intimité et Confidentialité** : empêcher la divulgation d'informations à des entités(sites, organisations, personnes, etc.) non habilitées à les connaître.

•**Authentification :**
D'une information : prouver qu'une information provient de la source annoncée (auteur, émetteur).

D'une personne (ou groupe ou organisation) : prouver que l'identité est bien celle annoncée.

•**Intégrité des informations :** Assurer que les informations n'ont pas été altérées par des personnes non autorisées ou inconnues.

- **Signature** : Le moyen de lier l'information à une entité.

- **Validation** : Les moyens de fournir l'autorisation d'utiliser ou de manipuler des informations.

- **Contrôle d'accès** : Limiter l'accès des ressources aux personnes privilégiées.

- **Certification** : L'approbations de l'information par une entité de confiance.

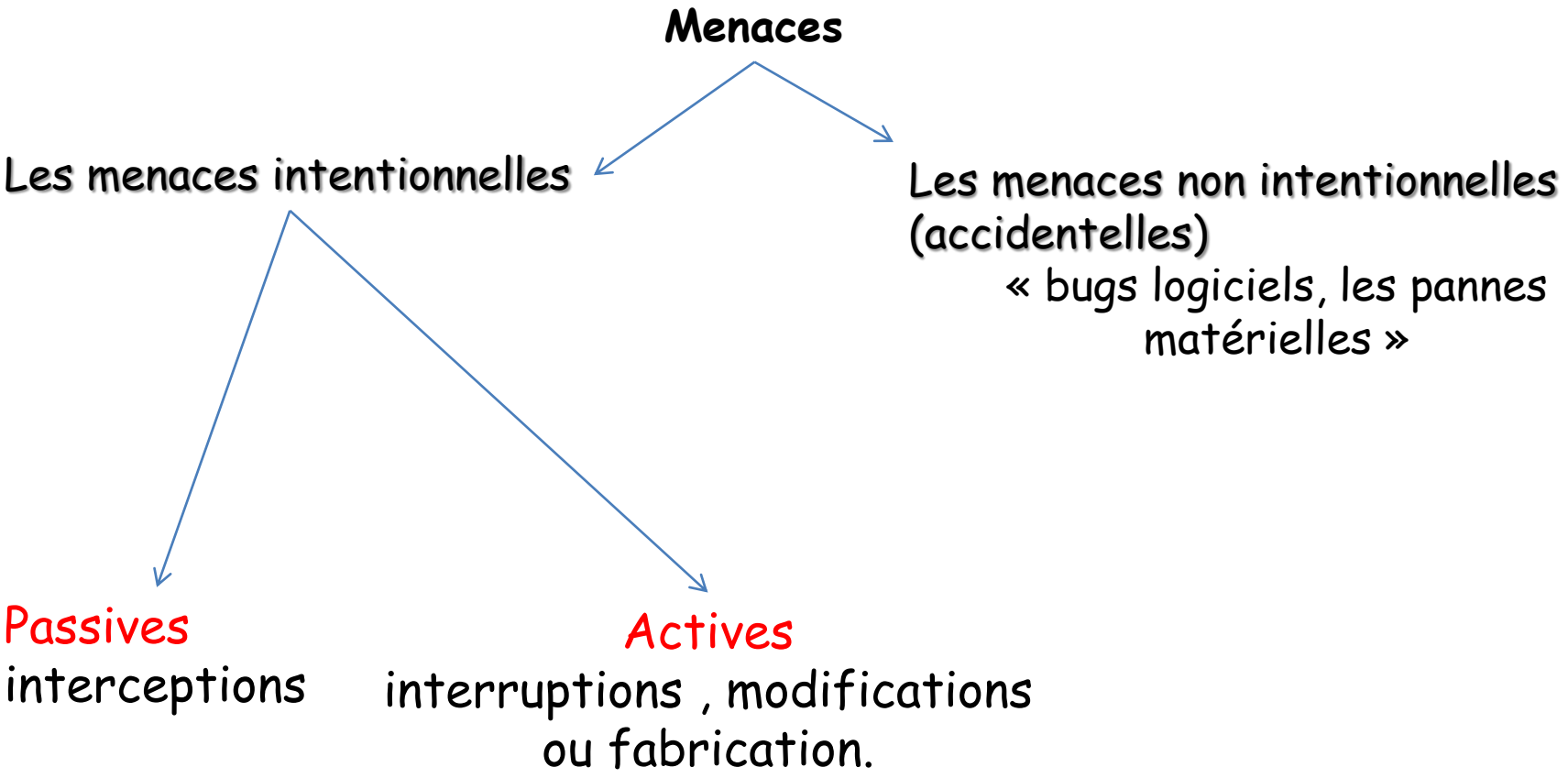
- **Réception** : Approuver la réception de l'information.

- **Anonymat** : Cacher l'identité d'une entité impliquée dans un processus.

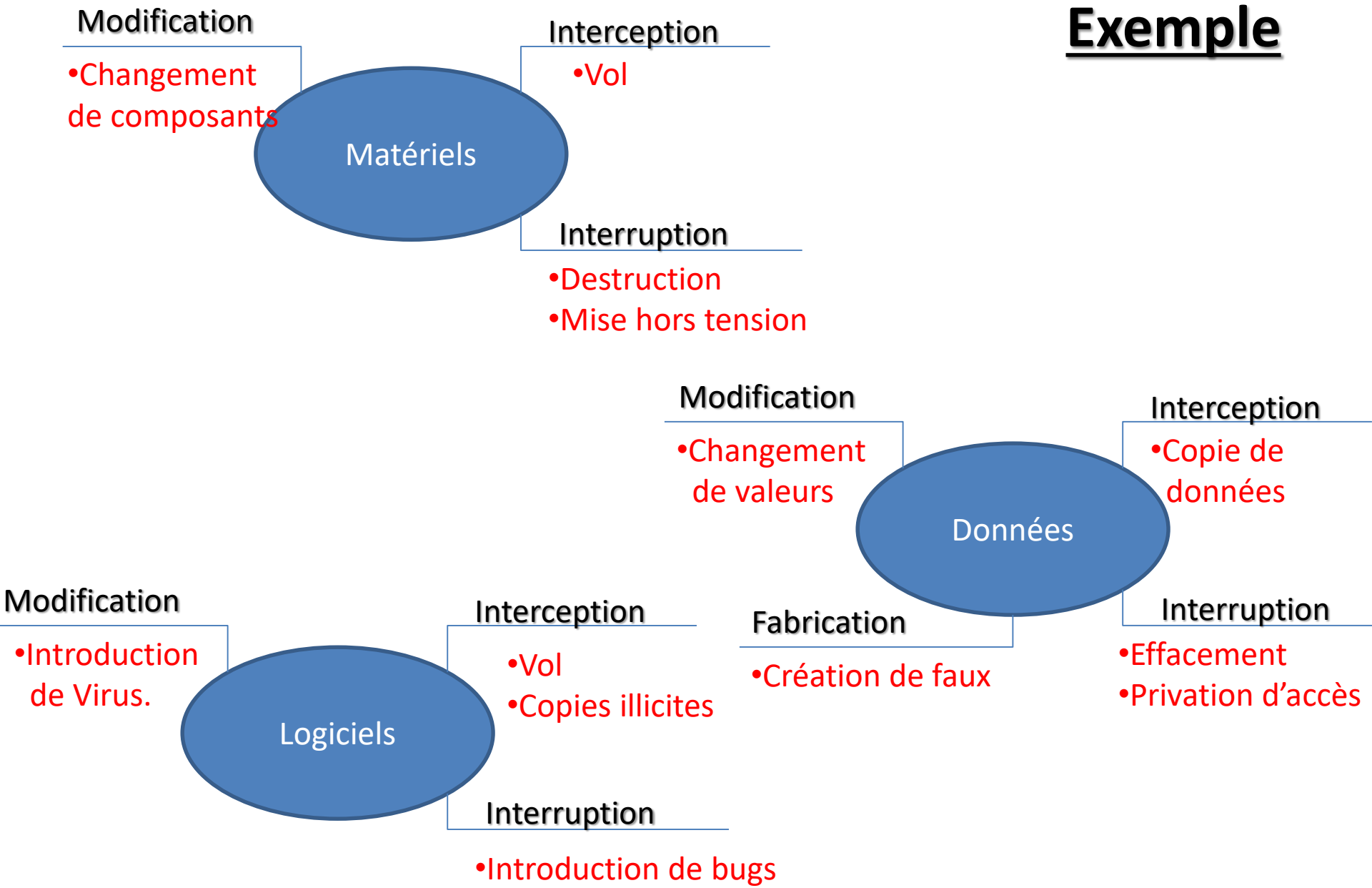
- **Non-répudiation** : Empêcher le démenti(nier) d'engagements ou d'actions précédentes.

❖ Menaces sur les systèmes informatiques

Dans un système informatique les menaces peuvent toucher les composants matériels, logiciels ou informationnels.



Exemple


Modification
•Changement de composants
Interception
•Vol
Matériels
Interruption
•Destruction
•Mise hors tension
Modification
•Changement de valeurs
Interception
•Copie de données
Données
Fabrication
•Création de faux
Interruption
•Effacement
•Privation d'accès
Modification
•Introduction de Virus.
Interception
•Vol
•Copies illicites
Logiciels
Interruption
•Introduction de bugs

❖ Terminologie

·**Communication** : la communication est l'action d'échanger quelque chose entre deux ou plusieurs personnes.

·**Message** : texte en claire compréhensible par l'expéditeur et le destinataire.

·**Chiffrement** :(encryption) : le processus de transformation d'un message de telle manière à le rendre incompréhensible.

·**Texte chiffré** : (cryptogramme) : résultat de l'opération de chiffrement.

·**Déchiffrement** :(décryptage) : processus de reconstruction du texte en clair à partir du texte chiffré.

·**Cryptographie** : L'art et la science de garder le secret des messages, pratiquée par des Cryptographes.

·**Cryptanalyse** : L'art de décrypter des messages chiffrés, pratiquée par des Cryptanalystes.

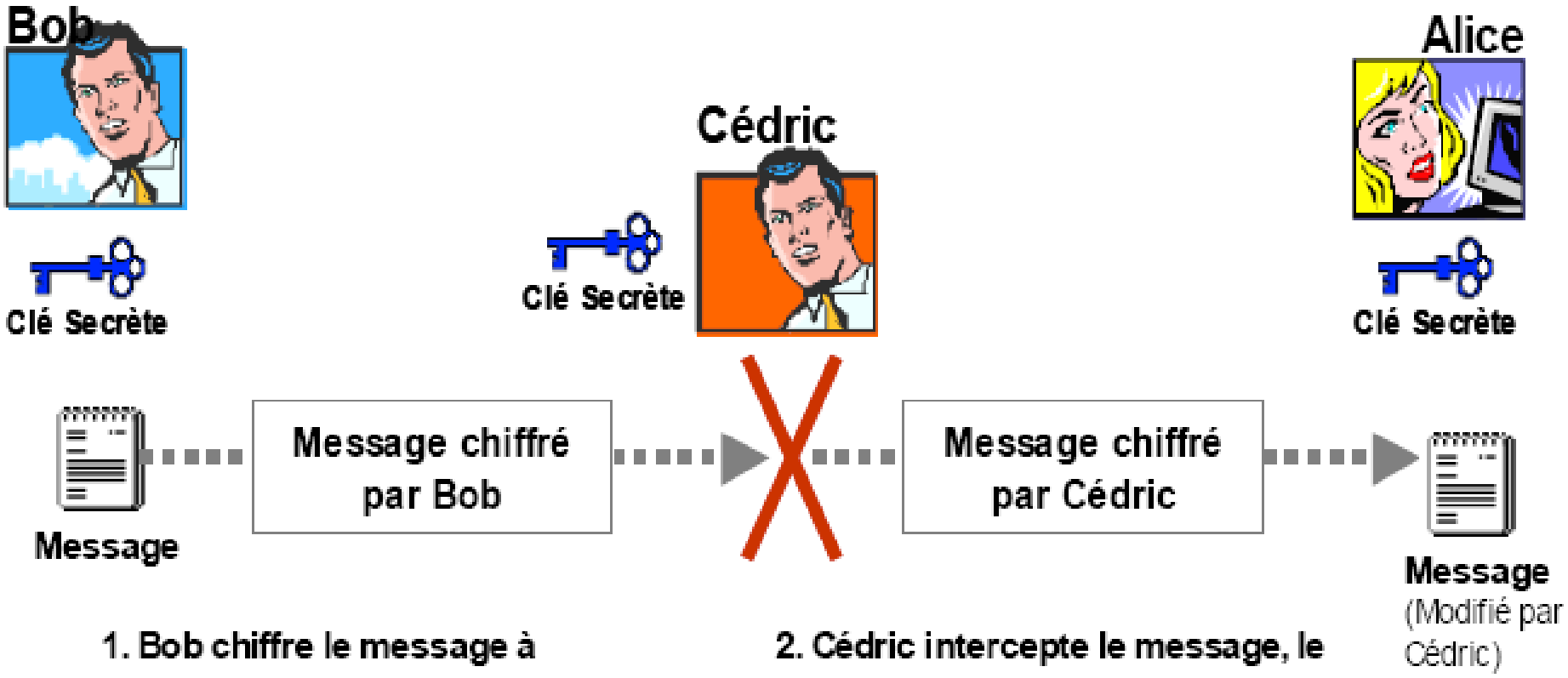
·**Cryptologie** : La branche des mathématiques qui traite de la Cryptographie et de la cryptanalyse, ses pratiquants sont appelés **cryptologues**.

·**Cryptosystème** : Un algorithme cryptographique, plus toutes les clés possibles et tous les protocoles qui le font fonctionner.

Il existe deux grandes familles de chiffrement à base de clés : le chiffrement symétrique "à clé secrète", et le chiffrement asymétrique "à clé publique".

❖ Chiffrement symétrique

Si Alice, Bob et Cédric partage le même lien de communication alors ils partagent la même clé de chiffrement symétrique



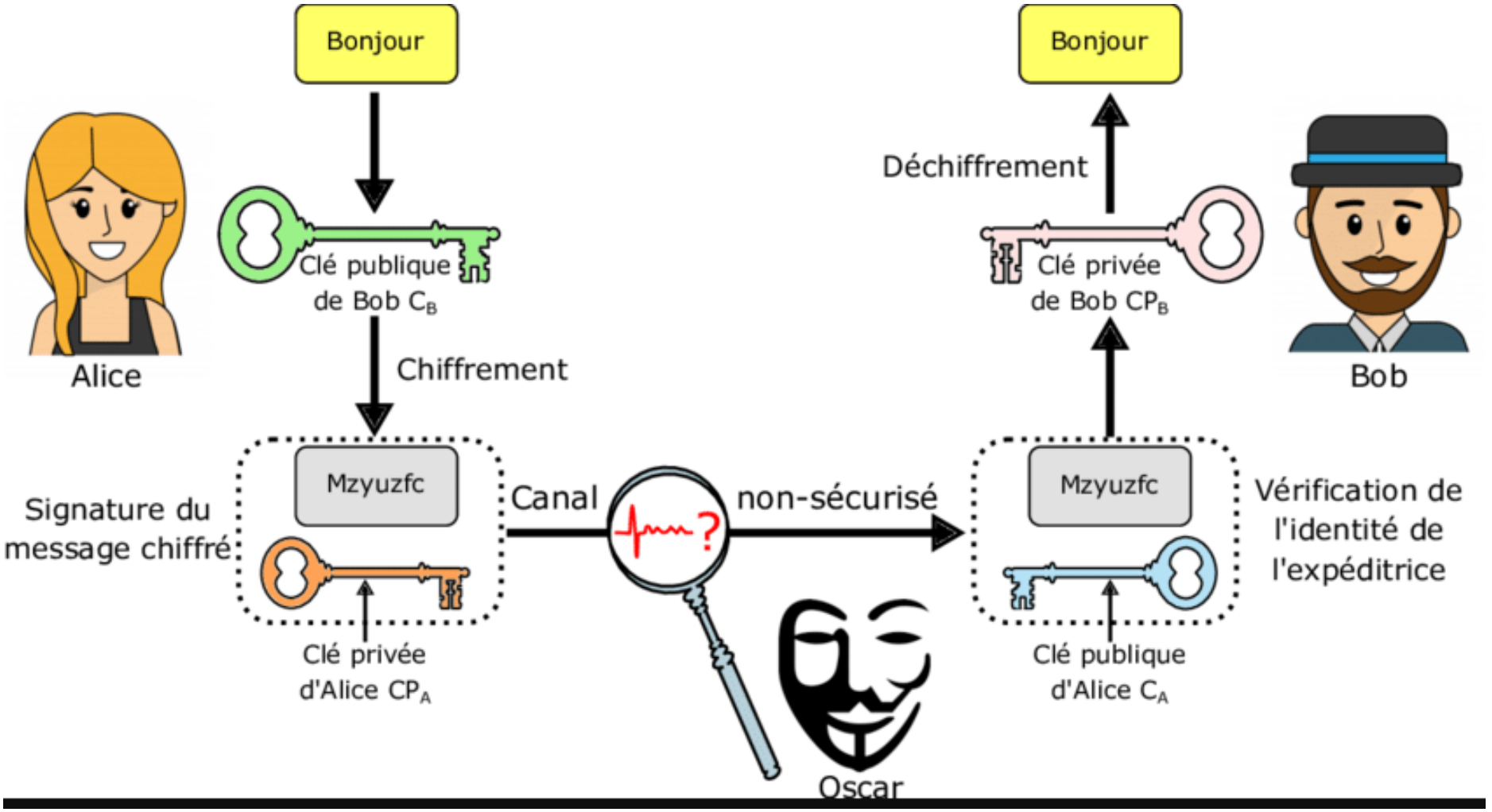
On distingue deux types de chiffrement dans cette famille : le chiffrement par blocs et le chiffrement par flot.

- **Chiffrement par blocs** : traite le message en clair par groupes de bits appelés bloc, chaque bloc est chiffré l'un après l'autre.

- **Chiffrement par flot** : appelé aussi chiffrement continu, traite l'information bit à bit.

Quelque exemple de systèmes cryptographiques qui utilise le chiffrement symétrique : DES (Data Encryptions Standard), AES (Advanced Encryptions Standard), chiffre césar.

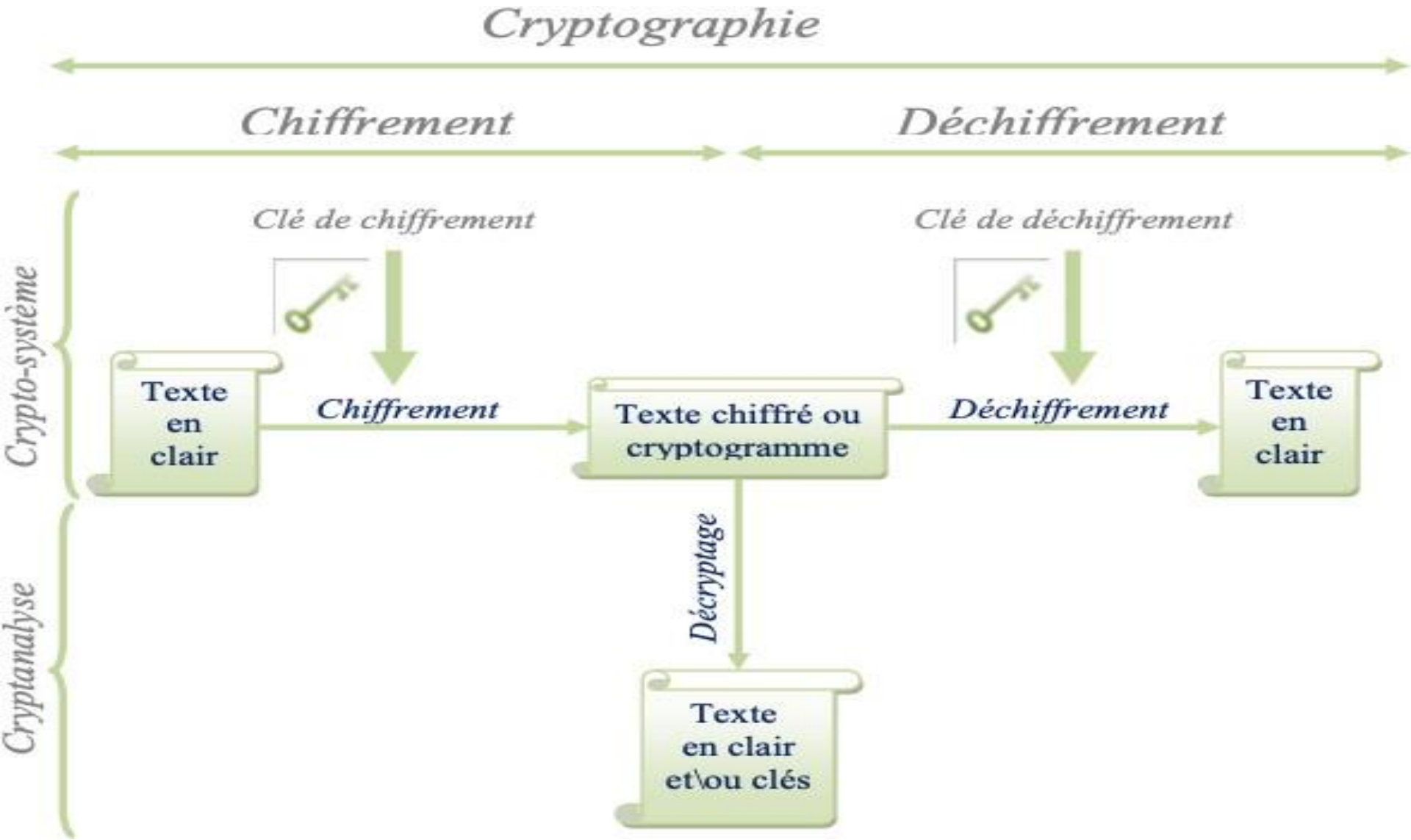
❖ Chiffrement asymétrique



Quelques exemples de systèmes cryptographiques qui utilise le chiffrement asymétrique :

- **RSA**: (Rives Shamir Adleman) c'est un algorithme utilisé pour chiffrer les données ou pour les signé,
- **Diffie-Hellman** : c'est un protocole d'échange des clés.
- **DSA** :(Digital Signature Algorithm) c'est un algorithme de signature.
- **ElGamal** : c'est un algorithme utilisé à la fois pour le chiffrement et pour la signature.

❖ Principe de la cryptographie



❖ ***Modèle mathématique :***

5-Uple **{*P,C,K,E,D*}** :

•***P*** : espace des messages en clair.

•***C*** : est un ensemble appelé espace des messages chiffrés (cryptogrammes).

•***K*** : espace des clés ; ses éléments sont les clés de chiffrement.

•***E*** ={ E_K :kϵ ***K*** } est une famille de fonctions E_K : ***P→C*** .

•***D*** ={ D_K :kϵ ***K*** } est une famille de fonctions D_K : ***C → P*** .

•*A chaque clé* ***k1*** ϵ ***K*** est associé une clé ***k2*** ϵ ***K*** tel que

$D_{K2}(E_{K1}(M))=M$ *pour tout message* ***M*** ϵ ***P***.

Exemple

Déchiffer le message suivant :
« CPOKPVS MF NPOEF »

Indice n°1 : les espaces restent des espaces
Indice n°2 : l'alphabet a été décalé

Clé : chaque lettre a été décalée d'un rang

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

Décalage =1 position à droite

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	A

« CPOKPVS MF NPOEF »

« BONJOUR LE MONDE »

Exemple (suite)

Modèle mathématique

1) Nous identifions les lettres par des chiffres pour permettre le calcul.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2) $\{P,C,K,E,D\}$

$P=C=K=\{0,1,..25\}$

3) **Chiffrement**

$E = \{ E_k : k \in K \}$; $E_k : P \rightarrow C$

tel que:

Pour un $x \in P$: $x \longmapsto x+k$

$E_k(x)=(x+k) \bmod 26$

4) **Déchiffrement**

$D = \{ D_k : k \in K \}$; $D_k : C \rightarrow P$

tel que:

Pour un $x \in C$: $x \longmapsto X-k$

$D_k(x)=(x-k) \bmod 26$

❖ La cryptographie classique

A) Chiffrement par transposition

- Transposition par blocs
- Transposition avec clé simple

B) Chiffrement par substitution

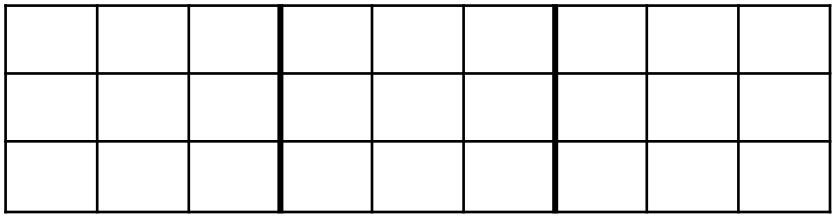
- chiffrement de César
- Masque Jetable
- Le chiffre de Hill

a) Transposition par blocs

On écrit le message en clair dans un tableau de dimension prédéfinie, avant de relever le texte chiffré en le lisant selon un procédé convenu.

Exemple: écriture dans des blocs de 3*3 en ligne.

JE SUIS INFORMATICIEN



Chiffrement: Lecture par colonne

Déchiffrement

Cheminement inverse.

b) Transposition avec clé simple

Un mot clé est utilisé pour définir une clé numérique.

Cette clé est obtenue en numérotant les lettres du mot clé selon l'ordre de leur apparition dans l'alphabet.

Le message est alors chiffré en l'écrivant dans un tableau dont le nombre de colonnes coïncide avec le nombre de lettres du mot clé et en recopiant ses colonnes dans l'ordre de la clé numérique.

Clé= MASTER
Texte : JE SUIS INFORMATICIEN

b) Transposition avec clé simple (suite)

M	A	S	T	E	R
3	1	5	6	2	4
J	E		S	U	I
S		I	N	F	O
R	M	A	T	I	C
I	E	N			

Résultat : E_MEUFI_JSRIIOC__IANSNT

Déchiffrement:

Cheminement inverse

❖ Chiffrement par substitution

a) Chiffrement de César

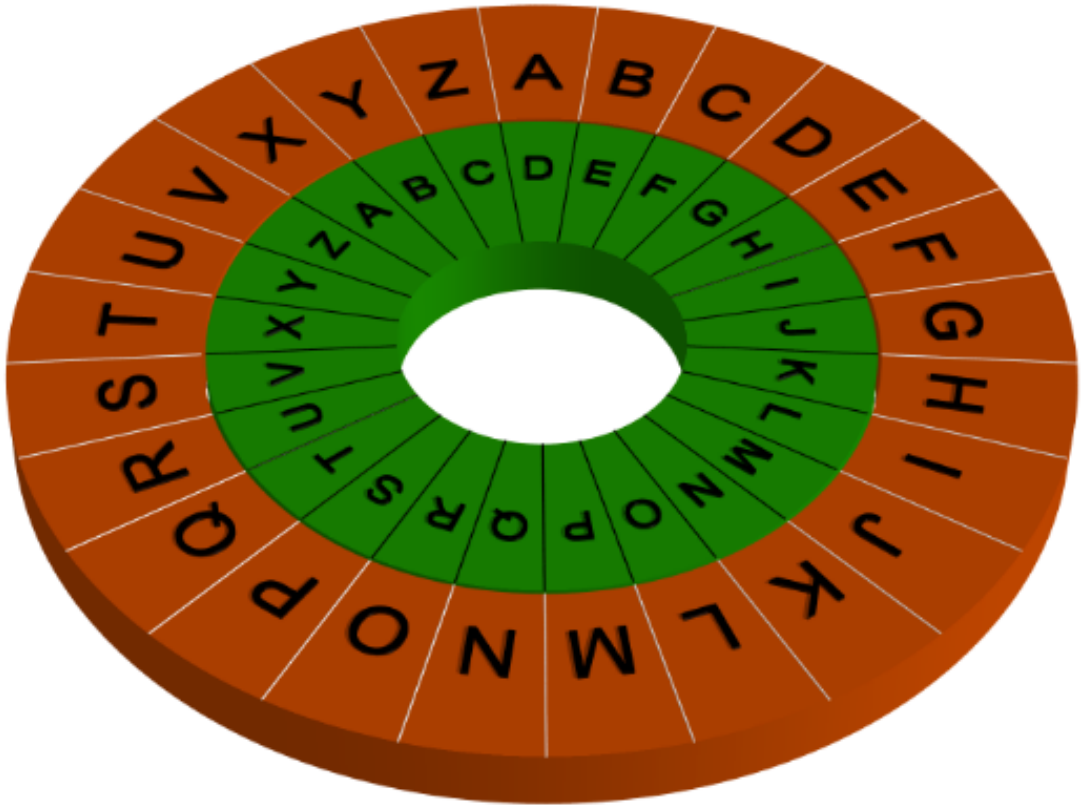
Chiffrement : chaque lettre du texte en clair est remplacée par la lettre située **n** rangs plus loin dans l'alphabet.

Déchiffrement : s'effectue en remplaçant les lettres du texte crypté par celles situées **n** rangs avant dans l'alphabet.

Pour ses communications importantes à son armée, César cryptait ses messages. Ce que l'on appelle le chiffrement de César est un décalage des lettres : pour crypter un message, A devient D,B devient E,C devient F,...

$A \longmapsto D \quad B \longmapsto E \quad C \longmapsto F \quad \ldots \quad W \longmapsto Z \quad X \longmapsto A \quad Y \longmapsto B \quad Z \longmapsto C$

Pour prendre en compte aussi les dernières lettres de l'alphabet, il est plus judicieux de représenter l'alphabet sur un anneau. Ce décalage est un **décalage circulaire** sur les lettres de l'alphabet.



Pour déchiffrer le message de César, il suffit de décaler les lettres dans l'autre sens, **D** se déchiffre en **A**,**E** en **B**,...

Exemple

Pour un code décalé de **onze** positions, le chiffrement est donc le suivant :

Le même tableau sert au chiffrement et au déchiffrement.

Algorithme Cesar;

Chiffrement

Entrées : Un message clair M et un décalage d

$y := (x + d) \bmod 26$

Sortie : Un message chiffré C

Déchiffrement

Entrées : Un message chiffré C et le décalage d

$x := (y - d) \bmod 26$

Sortie : Le message clair M

ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp