



# Note technique

## Codage ASCII

ASCII (Americian Standard Code for Information Interchange) est une norme de codage des caractères informatiques apparue au début des années 60. Le codage ASCII est conçu pour pouvoir encoder les caractères latins non accentués et les principaux caractères spéciaux afin de pouvoir écrire des textes en anglais. Bien que limité (impossible d'écrire un texte en français par exemple), le codage ASCII est encore activement utilisé car compatible avec la quasi-totalité des appareils en circulation. Pour les systèmes plus modernes, d'autres codages plus complets (unicode ...) sont à privilégier.

La table ASCII définit 128 caractères. A chaque caractère est associée une valeur sur 8 bits (bien que 7 bits soient suffisants, il est plus commode se représenter un caractère sur un octet avec le bit de poids fort à 0 car les systèmes informatiques raisonnent sur des octets). Cette valeur peut être représentée sous forme octale, décimale ou hexadécimale (le plus souvent). Les caractères 0 à 31 et 127 ne sont pas affichables sur un écran ; ils correspondent en réalité à des commandes ou à des instructions (retour à la ligne, tabulation ...).

## ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	\$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	}
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Table ASCII : <https://commons.wikimedia.org/wiki/File:ASCII-Table-wide.svg>

## Chiffre de César

Le chiffrement de César (ou code César) est une méthode de chiffrement simple utilisée jadis par Jules César dans ses correspondances secrètes.

La méthode repose sur la permutation circulaire des lettres de l'alphabet. Ainsi un message en clair est chiffré en décalant chaque lettre du message de  $K$  rangs vers la droite. Si le décalage provoque un dépassement, on reboucle au début. Par exemple si  $K = 3$ , la lettre « A » est remplacée par D, « g » remplacé par « j » et « Y » par « B » ... Le déchiffrement s'effectue de la même manière en décalant les lettres du chiffré de  $K$  rangs vers la gauche, en rebouclant en cas de dépassement. La sécurité du chiffre de César repose sur la connaissance de  $K$  (la clef du chiffrement). Elle doit être connue pour pouvoir déchiffrer le message.

### Exemple de code chiffré avec $K = 7$

*Message clair* : Gloire à César !

*Message chiffré* : Nsvpyl h Jlzhy !

Dans l'alphabet latin, seules les lettres sont modifiées (les caractères spéciaux restent inchangés). Ainsi il n'y a que 26 clefs possibles pour chiffrer/déchiffrer un message ( $K = 0$  à  $K = 25$ ). Le chiffrement par code César n'est donc pas du tout sûr car il peut être cassé avec une attaque par force brute (26 tentatives à effectuer dans le pire des cas).