

MESSAGGI

Se abbiamo di fronte un messaggio alfanumerico (numeri e lettere, ma anche simboli) o ad esempio una parola come CIAO, bisogna convertire le singole lettere in Codice Ascii ogni carattere (C, I, A, O) nel suo codice ASCII. (Una operazione diffusissima quanto necessaria e imprescindibile nell'utilizzo degli elaboratori). Uno per ogni carattere, in seguito vengono salvati in memoria, poi secondo RSA vengono cifrati in gruppi con le chiavi dell'RSA

0		32		64	@	96	`	128	Ç	160	á	192	L	224	Ó
1	☉	33	!	65	A	97	a	129	ü	161	í	193	⌂	225	Ô
2	☼	34	"	66	B	98	b	130	é	162	ó	194	⌂	226	Õ
3	♥	35	#	67	C	99	c	131	â	163	ú	195	⌂	227	Ö
4	♦	36	\$	68	D	100	d	132	ä	164	ñ	196	—	228	ó
5	♣	37	%	69	E	101	e	133	à	165	Ñ	197	+	229	Ô
6	♠	38	&	70	F	102	f	134	á	166	ª	198	â	230	µ
7	•	39	'	71	G	103	g	135	ç	167	º	199	Ã	231	þ
8	▣	40	(72	H	104	h	136	ê	168	¿	200	⌂	232	Þ
9	○	41)	73	I	105	i	137	ë	169	®	201	⌂	233	Ú
10	☒	42	*	74	J	106	j	138	è	170	¬	202	⌂	234	Û
11	♂	43	+	75	K	107	k	139	ï	171	½	203	⌂	235	Ü
12	♀	44	,	76	L	108	l	140	î	172	¼	204	⌂	236	Ý
13	🎵	45	-	77	M	109	m	141	ì	173	í	205	=	237	Ÿ
14	🎵	46	.	78	N	110	n	142	Ä	174	«	206	⌂	238	—
15	☼	47	/	79	O	111	o	143	Å	175	»	207	▣	239	˘
16	▶	48	0	80	P	112	p	144	É	176	⌂	208	ð	240	-
17	◀	49	1	81	Q	113	q	145	æ	177	⌂	209	Ð	241	±
18	↑	50	2	82	R	114	r	146	Æ	178	⌂	210	Ê	242	—
19	!!	51	3	83	S	115	s	147	ø	179	⌂	211	Ë	243	¾
20	¶	52	4	84	T	116	t	148	ö	180	⌂	212	Ë	244	¶
21	§	53	5	85	U	117	u	149	ò	181	Á	213	Ì	245	§
22	—	54	6	86	V	118	v	150	û	182	Â	214	Í	246	÷
23	↑	55	7	87	W	119	w	151	ù	183	Ã	215	Î	247	,
24	↑	56	8	88	X	120	x	152	ÿ	184	⌂	216	Ï	248	°
25	↓	57	9	89	Y	121	y	153	Ö	185	⌂	217	⌂	249	ˆ
26	→	58	:	90	Z	122	z	154	Ü	186	⌂	218	⌂	250	˙
27	←	59	;	91	[123	{	155	ø	187	⌂	219	⌂	251	¹
28	⌂	60	<	92	\	124		156	£	188	⌂	220	⌂	252	²
29	↔	61	=	93]	125	}	157	Ø	189	¢	221	⌂	253	³
30	▲	62	>	94	^	126	~	158	×	190	¥	222	⌂	254	■
31	▼	63	?	95	_	127	△	159	f	191	⌂	223	⌂	255	

ESEMPIO SEMPLIFICATO PER LA PAROLA CIAO IN ASCII = 67,73,66,79

p = 61, q = 53 // Scegliere due numeri primi
n = p * q = 61 * 53 = 3233 // Calcolo del Modulo n
phi = (p-1) * (q-1) = (61-1) * (53-1) = 3120 // Calcolo i coprimi (Eulero)

e = 17 // Chiave Pubblica
d = ModInverse(e, phi) = ModInverse(17, 3120) = 2753 // Chiave Privata

Messaggio in chiaro: CIAO (in ASCII = 67,73,66,79)

Messaggio cifrato: 641 1486 2790 1307

Messaggio decifrato: CIAO