PRINCIPE ET ALGORITHME DU CRYPTAGE
utilisé dans Crypt.exe et Crypt Message.exe

Le principe du cryptage est simple : Il utilise la combinaison d'un mot de passe et du texte à coder par une fonction de ou exclusif :

Exemple :
mot de passe : 123456 (x31, x32, x33, x34, x35, x36)
message : Bonjour (x42, x6F, x6E, x6A, x6F, x75, x72)

Le codage de ce message serait :

Message	42	6F	6E	6A	6F	75	72
Mot de passe	31	32	33	34	35	36	31
Codé Message ou exclusif Mot de passe	73	5D	5D	5E	5A	43	43

Or, avec ce principe, le mot de passe serait relativement facile à trouver.

On utilise en plus une propagation de Checksum de type CRC8.
On appellera par la suite ce tableau CRC :

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0_	00	07	0E	09	1C	1B	12	15	38	3F	36	31	24	23	2A	2D
1_	70	77	7E	79	6C	6B	62	65	48	4F	46	41	54	53	5A	5D
2_	E0	E7	EE	E9	FC	FB	F2	F5	D8	DF	D6	D1	C4	C3	CA	CB
3_	90	97	9E	99	8C	8B	82	85	A8	AF	A6	A1	B4	B3	BA	BD
4_	C7	C0	C9	CE	DB	DC	D5	D2	FF	F8	F1	F6	E3	E4	ED	EA
5_	B7	B0	B9	BE	AB	AC	A5	A2	8F	88	81	86	93	94	9D	9A
6_	27	20	29	2E	3B	3C	35	32	1F	18	11	16	03	04	0D	0A
7_	57	50	59	5E	4B	4C	45	42	6F	68	61	66	73	74	7D	7A
8_	89	8E	87	80	95	92	9B	9C	B1	B6	BF	B8	AD	AA	A3	A4
9_	F9	FE	F7	F0	E5	E2	EB	EC	C1	C6	CF	C8	DD	DA	D3	D4
A_	69	6E	67	60	75	72	7B	7C	51	56	5F	58	4D	4A	43	44
B_	19	1E	17	10	05	02	0B	0C	21	26	2F	28	3D	3A	33	34
C_	4E	49	40	47	52	55	5C	5B	76	71	78	7F	6A	6D	64	63
D_	3E	39	30	37	22	25	2C	2B	06	01	08	0F	1A	1D	14	13
E_	AE	A9	A0	A7	B2	B5	BC	BB	96	91	98	9F	8A	8D	84	83
F_	DE	D9	D0	D7	C2	C5	CC	CB	E6	E1	E8	EF	FA	FD	F4	F3

Masque = CRC[Masque précédent] ou Exclusif Mot de passe
Au démarrage du programme le masque vaut Zéro

Exemple :
mot de passe : 123456 (x31, x32, x33, x34, x35, x36)
message : Bonjour (x42, x6F, x6E, x6A, x6F, x75, x72)

Le codage de ce message serait :

Masque précédent	00	31	A5	41	F4	F7	FD
CRC CRC[masque précédent]	00	97	72	C0	C2	CB	FD
Mot de passe	31	32	33	34	35	36	31
Nouveau masque Mot de passe ou exclusif CRC	31	A5	41	F4	F7	FD	CC
Message	42	6F	6E	6A	6F	75	72
Codé Message ou exclusif Nouveau masque	73	CA	2F	9E	98	88	BE

Avec ce principe, le cryptage et le décryptage sont fait de façon identique.

L'algorithme ci dessous montre comment fonctionne le cryptage et le décryptage. Il utilise le tableau CRC défini page précédente :