Fais un One-Time-Pad

Par Daniel TANT

Voici un procédé de chiffrement particulièrement efficace, inventé en 1882 et utilisé pendant la Seconde guerre mondiale.

Son principe est de n'utiliser chaque clé qu'une fois, car elle doit être détruite après l'envoi du message. Le carnet de clés peut être un tableau de statistiques, une liste obtenue par un logiciel générateur de clés, ou un petit carnet pour une durée déterminée.

Prenons par exemple le message : « *inutile de venir, je pars* ». et la clé : 52194637830842579183 qui est la clé de départ du 3ème jour du premier mois, date à laquelle le message a été rédigé.

Superposons sur la feuille de message, le clair et en dessous la clé. Pour chaque lettre, la clé donne le décalage dans l'alphabet, entre le clair et le chiffré. Exemple pour le I, 5 lettres plus loin dans l'alphabet donne un N (JKLMN), puis le N donne deux lettres plus loin dans l'alphabet le P, le V vient une lettre après le U, Dans le cas du T après être arrivé à Z il convient de reprendre l'alphabet à la lettre A donc T +9 (UVWXYZABC) = C. et ainsi de suite.

Clair	**I**	**N**	**U**	**T**	**I**	**L**	**E**	**D**	**E**	**V**	**E**	**N**	**I**	**R**	**J**	**E**	**P**	**A**	**R**	**S**
Clé	**5**	**2**	**1**	**9**	**4**	**6**	**3**	**7**	**8**	**3**	**0**	**8**	**4**	**2**	**5**	**7**	**9**	**1**	**8**	**3**
Chiffre	N	P	V	C	M	R	H	K	M	Y	E	V	M	T	O	L	Y	B	Z	V

Le message, découpé en groupes de 5 lettres, est donc : NPVCM RHKMY EVMTO LYBZV.
Si le message compte un nombre de lettres non divisible par 5, compléter avec des lettres nulles, c'est à dire sans signification.

En page suivante, voici un modèle de clés sur deux mois pour l'One-Time-Pad.

Et sur la troisième page, fais ton code One-Time-Pad pour deux mois également

Association des Réservistes du Chiffre et de la Sécurité de l'Information

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	26
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

Association des Réservistes du Chiffre et de la Sécurité de l'Information

Codes One-Time-Pad

Jour du mois	codes					jour du mois	codes				
1	3	0	1	5	9	1	2	7	1	4	8
2	9	4	3	8	9	2	6	0	2	5	1
3	5	2	1	9	4	3	9	4	8	0	2
4	6	3	7	8	3	4	1	7	2	5	4
5	0	8	4	2	5	5	9	1	3	2	5
6	7	9	1	8	3	6	7	0	4	1	3
7	9	2	8	5	9	7	9	0	1	5	6
7	1	4	0	6	2	7	2	8	4	2	7
8	7	9	7	5	1	8	1	3	5	0	6
9	4	2	6	8	9	9	4	6	1	5	4
10	7	0	5	4	9	10	0	8	3	1	5
11	6	9	5	9	7	11	2	6	1	4	7
12	0	1	2	2	8	12	5	9	0	1	3
13	4	9	2	6	9	13	4	5	6	4	1
14	7	0	1	8	5	14	0	2	7	3	5
15	1	7	6	0	4	15	1	6	2	5	4
16	2	9	7	5	9	16	3	1	9	0	8
17	6	4	7	0	1	17	4	5	3	1	2
18	9	5	2	6	8	18	3	6	2	4	0
19	1	5	7	8	5	19	6	1	3	0	2
20	0	4	6	2	7	20	7	3	2	5	3
21	5	6	1	9	3	21	1	2	9	3	0
22	0	2	4	7	9	22	5	4	2	1	6
23	7	6	1	5	2	23	4	3	0	1	5
24	6	7	8	6	0	24	3	8	7	3	4
25	2	8	5	4	1	25	2	0	9	5	1
26	6	2	0	7	6	26	8	1	3	0	6
27	4	5	8	0	9	27	4	9	2	5	3
28	1	2	6	4	7	28	2	1	7	9	4
29	8	0	4	1	8	29	0	4	1	5	6
30	5	6	7	4	9	30	7	3	2	0	1
31	0	1	8	2	0	31	2	5	3	4	8

Association des Réservistes du Chiffre et de la Sécurité de l'Information

Codes One-Time-Pad

Jour du mois	codes	jour du mois	codes
1	. . . . .	1	. . . . .
2	. . . . .	2	. . . . .
3	. . . . .	3	. . . . .
4	. . . . .	4	. . . . .
5	. . . . .	5	. . . . .
6	. . . . .	6	. . . . .
7	. . . . .	7	. . . . .
7	. . . . .	7	. . . . .
8	. . . . .	8	. . . . .
9	. . . . .	9	. . . . .
10	. . . . .	10	. . . . .
11	. . . . .	11	. . . . .
12	. . . . .	12	. . . . .
13	. . . . .	13	. . . . .
14	. . . . .	14	. . . . .
15	. . . . .	15	. . . . .
16	. . . . .	16	. . . . .
17	. . . . .	17	. . . . .
18	. . . . .	18	. . . . .
19	. . . . .	19	. . . . .
20	. . . . .	20	. . . . .
21	. . . . .	21	. . . . .
22	. . . . .	22	. . . . .
23	. . . . .	23	. . . . .
24	. . . . .	24	. . . . .
25	. . . . .	25	. . . . .
26	. . . . .	26	. . . . .
27	. . . . .	27	. . . . .
28	. . . . .	28	. . . . .
29	. . . . .	29	. . . . .
30	. . . . .	30	. . . . .
31	. . . . .	31	. . . . .