利用 JSON 的格式加密

{"app":[{"d":"d001","k":"2A01127314150617181906","m":"7301"}]}

第一欄位 d 為裝置 ID,例如裝置: d001

第二欄位 k 為金鑰,必須通過金鑰認證,程式才會執行

利用身分證加上時間的混淆,讓接收端任證金鑰格式無誤後就會開始執行程式

身分證:

2-1:身分證一共有 10 碼,假設身分證為 A123456789

縣市代碼跟代表數字:

台北市開頭是 A,數字為 10	宜蘭縣開頭是 G,數字為 16	南投縣開頭是 M,數字為 21
高雄縣開頭是 S,數字為 26	陽明山開頭是 Y,數字為 31	台中市開頭是 B,數字為 11
桃園縣開頭是 H,數字為 17	彰化縣開頭是 N,數字為 22	屏東縣開頭是 T,數字為 27
連江縣開頭是 Z,數字為 33	基隆市開頭是 C,數字為 12	嘉義市開頭是 I,數字為 34
新竹市開頭是 O,數字為 35	花蓮縣開頭是 U,數字為 28	台南市開頭是 D,數字為 13
新竹縣開頭是 J,數字為 18	雲林縣開頭是 P,數字為 23	台東縣開頭是 V,數字為 29
高雄市開頭是 E,數字為 14	苗栗縣開頭是 K,數字為 19	嘉義縣開頭是 Q,數字為 24
金門縣開頭是 W,數字為 32	台北縣開頭是 F,數字為 15	台中縣開頭是 L,數字為 20
台南縣開頭是 R,數字為 25	澎湖縣開頭是 X,數字為 30	

性別數字代表

性別	男生	女生
數字	1	2

以身分證字號整體規劃如下：

Y	x8	x7	x6	x5	x4	x3	x2	x1	Z
A	1	2	3	4	5	6	7	8	9
英文	性別	編號 1	編號 2	編號 3	編號 4	編號 5	編號 6	編號 7	檢查碼

Z 為檢查碼,來驗證身分證到底正不正確

檢驗碼公式:

Z =

10-(Y + x8 * 8 + x7 * 7 + x6 * 6 + x5 * 5 + x4 * 4 + x3 * 3 + x2 * 2 + x1 * 1)%10

Y = 個位數字 * 9 + 十位數字/10

先求 Y ,A 為台北市等於 10 為十位數字,不是個位數
所以
Y = 0 * 9 + 10/10

Y=1

開始帶入 Z 檢查碼公式
10-(1 + 1 * 8 + 2 * 7 + 3 * 6 + 4 * 5 + 5 * 4 + 6 * 3 + 7 * 2 + 8 * 1)%10

簡化(1):
10 - (1 + 8 + 14 + 18 +20 + 20 + 18 + 14 + 8) % 10

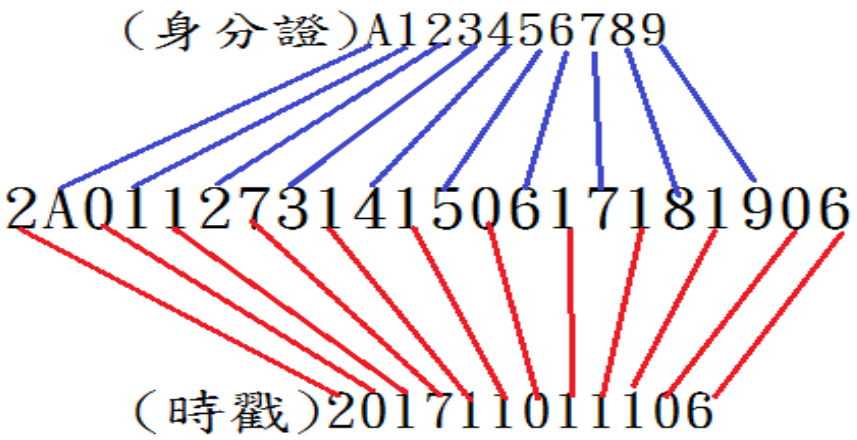
簡化(2)
10-(121)%10
說明:
121%10　是取餘數 , 121/10=12,餘 1

10-1=9　最後檢查碼為 9

2-2:時間格式 2017 年 11 月 01 日 11 點 06 分
簡化為:
201711011106

主要時戳驗證,產生即時的時間,接收端會有 5 分鐘內的容許性
但是過了時間過了 5 分鐘,此訊息就不能在用了

2-3:訊息混淆,利用身分證加上時戳
(身分證)A123456789 加上(時戳)201711011106
混淆的方式如下圖:



第三欄位 m 為指令訊息,1 左翻 ,2 右翻

最後利用 rot47 加密
ROT47 使用範圍較廣的 ASCII 字符集

ASCII 字符集圖表如下(10 進制):

	A	B	C	D	E	F	G	H	I	J	K	L
1	10進制	16進制	字元	10進制	16進制	字元	10進制	16進制	字元	10進制	16進制	字元
2	33	21	!	57	39	9	81	51	Q	105	69	i
3	34	22	"	58	3A	:	82	52	R	106	6A	j
4	35	23	#	59	3B	;	83	53	S	107	6B	k
5	36	24	$	60	3C	<	84	54	T	108	6C	l
6	37	25	%	61	3D	=	85	55	U	109	6D	m
7	38	26	&	62	3E	>	86	56	V	110	6E	n
8	39	27	'	63	3F	?	87	57	W	111	6F	o
9	40	28	(	64	40	@	88	58	X	112	70	p
10	41	29	)	65	41	A	89	59	Y	113	71	q
11	42	2A	*	66	42	B	90	5A	Z	114	72	r
12	43	2B	+	67	43	C	91	5B	[	115	73	s
13	44	2C	,	68	44	D	92	5C	\	116	74	t
14	45	2D	-	69	45	E	93	5D	]	117	75	u
15	46	2E	.	70	46	F	94	5E	^	118	76	v
16	47	2F	/	71	47	G	95	5F	_	119	77	w
17	48	30	0	72	48	H	96	60	`	120	78	x
18	49	31	1	73	49	I	97	61	a	121	79	y
19	50	32	2	74	4A	J	98	62	b	122	7A	z
20	51	33	3	75	4B	K	99	63	c	123	7B	{
21	52	34	4	76	4C	L	100	64	d	124	7C	|
22	53	35	5	77	4D	M	101	65	e	125	7D	}
23	54	36	6	78	4E	N	102	66	f	126	7E	~
24	55	37	7	79	4F	O	103	67	g	127	7F	
25	56	38	8	80	50	P	104	68	h	128	80	

假設字元{, 10 進制為 123
123+46=76, 超過 126 則循環從 33 開始
123+46=169-126=43+33=76
10 進制 76 的字元為 L
所以 L 取代了{,以此類推

{"app":[{"d":"d001","k":"2A011273141506171819O6","m":"7301"}]}
編碼:
LQ2AAQi,LQ5QiQ‘Q[Q<QiQap_‘‘afb‘c‘d_e‘f‘g‘h_eQ[Q>QiQ‘‘__QN.N