THE UNBREAKABLE CIPHER – USE ONE-TIME PAD ONLY ONCE

	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	0	1	2	3	4	5	6	7	8	9
A	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
C	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
D	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
E	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
G	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
H	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
I	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
J	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
K	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
L	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
M	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O
O	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P
P	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q
Q	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R
R	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S
S	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T
T	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U
U	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V
V	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W
W	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y	X
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z	Y
Y	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	Z
Z	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
0	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1
1	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3	2
2	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4	3
3	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5	4
4	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6	5
5	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7	6
6	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8	7
7	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9	8
8	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	9
9	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	0	1	2	3
6	4	5	6	7	8	9

Theory	
Encryption	C[i] = K[i] – P[i] (mod 36)
Decryption	P[i] = K[i] – C[i] (mod 36)
Pseudo-key	PK[i] = C[i] + PM[i] (mod 36)

P	Plaintext	K	Encryption key
C	Ciphertext		
P M	Pseudomessage	P K	Pseudokey

Alt	
0	→ .
1	→ ,
2	→ ?
3	→ :

Numbers	
0 0	→ 0
0 1	→ 1
1 0	→ 1 0
2 3	→ 2 3
1 5 7	→ 1 5 7