One-Time Pad simple, unbreakable encryption

The other side of this sheet is a one-time pad. Each pad is part of a pair of one sending and one receiving pad which share One-Time Pad values. The sending pad can be used to encrypt a short message, and the receiving pad can decrypt it.

The process of encryption/decryption is easy to perform and provides unbreakable message secrecy assuming some restrictions are followed:

- **NEVER** take a picture of the one-time pad, photocopy it, or enter the contents into a computer of any kind.
- **NEVER** allow anyone access to (or even a glance of) the one-time pad who you wouldn't want to know the contents of a message that will be sent/received with it.
- **NEVER** use a single pad for two different messages. And **NEVER** use a receiving pad for sending since your partner could encrypt a message with the sending pad as well. The result is two messages using the same pad.
- **ALWAYS** send the entirety of the pad's encrypted message, even unused portions (which will just be the one-time pad values). The length of a message can reveal much about its contents.
- **ALWAYS** carefully follow the instructions in this sheet. There are many ways that secrets can be leaked.

Encrypting a Message to Send

You will write your message on one of the 'One-Time Pad for Sending' sheets. Each pad has a number of rows each with four lines which are described in the top-left box. Write your message using only the characters from the Character Conversion Table below and place the characters in the boxes on the first line (using as many rows as necessary). If the message is short, it is worth repeating it to help if the message is corrupted during communication. In the next line write the two digits (one box each) associated with each character using the Character Conversion Table. For each digit, subtract the One-Time Pad value below (which will already be filled in) from it. If the value of the subtraction is less than 0, then add 10 to get the result. So for example: 5 - 7 = -2 → -2 + 10 = 8. Place the result in the last line of the row.

Copy the encrypted message down on a separate piece of paper being careful to double-check for any errors. You can now send the message to the owner of the pair's receiving pad using whatever method is appropriate.

Decrypting a Message you Received

Use the first eight digits of the message to identify which 'One-Time Pad for Receiving' to use, then write the encrypted message in the first line, one digit per box. For each digit, add the corresponding One-Time Pad value. If the sum is greater than or equal to 10, subtract 10 from it. For example: 4 + 8 = 12 → 12 - 10 = 2. Put the result in the character codes line. For each pair of digits in the character codes line, find the corresponding character in the Character Conversion Table and write it in the last line. That last line should be the decrypted message.

Character Conversion Table

_	00	'0'	10	J	20	T	30	+	40
'1'	01	A	11	K	21	U	31	-	41
'2'	02	B	12	L	22	V	32	=	42
'3'	03	C	13	M	23	W	33	?	43
'4'	04	D	14	N	24	X	34	(	44
'5'	05	E	15	O	25	Y	35	)	45
'6'	06	F	16	P	26	Z	36	&	46
'7'	07	G	17	Q	27	.	37	#	47
'8'	08	H	18	R	28	:	38	@	48
'9'	09	I	19	S	29	,	39	!	49

Example

Message to Encrypt	H		E		Y	
Character Codes	1	8	1	5	3	5
One-Time Pad Values	8	0	6	5	5	3
Encrypted Message	3	8	5	0	8	2

⬇

Encrypted Message	3	8	5	0	8	2
One-Time Pad Value	8	0	6	5	5	3
Character Codes	1	8	1	5	3	5
Decrypted Message	H		E		Y	

2023-03-31 NathanMcRae.name

One-Time Pad for Sending

Message

Character Codes

One-Time Pad

Encrypted Msg.

First eight digits of encrypted message are to identify which pad was used

_	00	'0'	10	J	20	T	30	+	40
'1'	01	A	11	K	21	U	31	-	41
'2'	02	B	12	L	22	V	32	=	42
'3'	03	C	13	M	23	W	33	?	43
'4'	04	D	14	N	24	X	34	(	44
'5'	05	E	15	O	25	Y	35	)	45
'6'	06	F	16	P	26	Z	36	&	46
'7'	07	G	17	Q	27	.	37	#	47
'8'	08	H	18	R	28	:	38	@	48
'9'	09	I	19	S	29	,	39	!	49

Encrypted message = (Converted character - One-time Pad) % 10