Dice Encryption: One-Time Pad

By Lexzach

Edited by Sour Dani

Preparation:

Note: You and your recipient *must* have the same One-Time Pad and it is *very important* that your key must be at minimum the same length as the message you intend to encrypt.

Repeat these steps until you have a key that is *at least* the length of your intended encrypted message:

1. Roll both dice.

2. From your perspective figure out which dice is the leftmost and which is the rightmost.

3. Use the chart on page 5 to figure out what character corresponds with your dice roll. For example, if I rolled a 3 on the left dice, and a 5 on the right dice, the corresponding letter would be **Q**.

4. Add that character to a chunk, once that chunk reaches 5 characters, make a new chunk.

Note: Your chunks and pad may differ in length than the provided example.

Here is an example One-Time Pad (**NOT USED IN LATER EXAMPLES**):

5IQ88 1DLQ9 0ZSUW
1DBBZ Z7C6C ONH55
6HZRY LA55E 0DJ43

Encryption:

Example message	**ATTAC KATDA WN**
Example One-Time Pad	**VERYS ECRET KEY**

Note: This method does NOT allow for spaces, if your message needs spaces, consider using a `0` as a substitute for a space. Your key will contain random letters and numbers, but for this example, we're using a simplified key for demonstration purposes.

In this example we're going to pretend that the key we generated earlier resulted in:

VERYS ECRET KEY

1. Using the chart, convert each character of your message to its corresponding number. The encoded example message would be:
01 20 20 01 03 11 01 20 04 01 23 14

2. Using the chart, convert each character of your One-Time Pad to its corresponding number. The encoded example One-Time Pad would be:
22 05 18 25 19 05 03 18 05 20 11 05 25

3. Put the encoded message next to the encoded One-Time Pad like so:
01 20 20 01 03 11 01 20 04 01 23 14
22 05 18 25 19 05 03 18 05 20 11 05 25

4. Now *add* the columns, if you go over 35, loop back to zero. For example, look at column 3 with 20 and 18. Added together, they equal 38. Since 38 is over by three, we loop back around to zero and count up 3. Since 25 at the end is not used, we don't include it. The above message now equals this:
23 25 03 26 22 16 04 03 09 21 34 19

5. Convert the numbers back into characters using the chart. The above message is represented as:
WYCZV PDCIU 7S

Congratulations! You now have an encrypted message! Assuming you used the dice method to generate the key, this message should be *impossible* to decrypt without the One-Time Pad.

Decryption:

Example message	**WYCZV PDCIU 7S**
Example One-Time Pad	**VERYS ECRET KEY**

1. Using the chart, convert each character of the encrypted message to its corresponding number. The encoded example message would be:
23 25 03 26 22 16 04 03 09 21 34 19

2. Using the chart, convert each character of your One-Time Pad to its corresponding number. The encoded example One-Time Pad would be:
22 05 18 25 19 05 03 18 05 20 11 05 25

3. Put the encrypted message next to the encoded One-Time Pad like so:
23 25 03 26 22 16 04 03 09 21 34 19
22 05 18 25 19 05 03 18 05 20 11 05 25

4. Now *subtract* the columns, if you go under zero, loop back to 35. For example, look at column 3 with 03 and 18. Subtracted, they equal -15. Since -15 is under by 15, we loop back around to 35 and count down 15, which means the final number is 20. Since 25 at the end is not used, we don't use it. The above message now equals this:
01 20 20 01 03 11 01 20 04 01 23 14

5. Convert the numbers back into characters using the chart. The above message is represented as:
ATTAC KATDA WN

Congratulations! You have a decrypted message!

Left Dice	Right Dice	Character	Number
1	1	A	01
1	2	B	02
1	3	C	03
1	4	D	04
1	5	E	05
1	6	F	06
2	1	G	07
2	2	H	08
2	3	I	09
2	4	J	10
2	5	K	11
2	6	L	12
3	1	M	13
3	2	N	14
3	3	O	15
3	4	P	16
3	5	Q	17
3	6	R	18
4	1	S	19
4	2	T	20
4	3	U	21
4	4	V	22
4	5	W	23
4	6	X	24
5	1	Y	25
5	2	Z	26
5	3	1	27
5	4	2	28
5	5	3	29
5	6	4	30
6	1	5	31
6	2	6	32
6	3	7	33
6	4	8	34
6	5	9	35
6	6	0	00