Binary One-Time Pad Encryption Worksheet Instructions

by David Hartkop CC-BY 2019

About:

- >The One-Time Pad is a classic encryption technique, and is the only known form of encryption that is truly unbreakable. (If used properly)
- >Your message is scrambled with a random key that is the same length as the message.
- >You can only use the key once.
- >This workseet requires a non-biased key of 0's and 1's. These binary digits can be the results of *coin flips.
- *Coin Flip Technique: Hold coin edgewise. Drop coin onto flat clean cement floor from height higher than your knees. Allow coin to settle. Read coin.

Step 1: Prepare Two Worksheets

- 11>Print two duplicate copies of the Binary One-Time Pad Encryption Worksheet.
- 1.2> Place one sheet exactly over the other so that a pushpin can poke through both sheets in exactly the same locations. NOTE: This produces 2 and only 2 copies of the key.
- 1.3 > Flip a coin for each cell in the row named "Random Key." If it is HEADS, then punch a hole. If it is TAILS, then don't punch a hole. NOTE: You'll need 5 rolls per letter!
- 1.4 > Give one punched worksheet to a friend. Your sheet will encode a message, your friend's sheet will decode the message.

*These sheets must be kept secret. Don't transmit the sheet or the key over the internet. Deliver the paper in person, via trusted agent, or by drone.

Message ->

Message Bin ->

Random Key ->

Coded Msa ->

Coded Msa ->

EXAMPLE: Each 'x' was a HEADS roll, and would have a hole punched through it. -->

Step 2: Encode your message

- 2.1> Write your message one letter at a time in the big boxes in the row marked 'Message'. Example below is the super top secret message "CAT".
- 2.2 Use the provided 'Alphabet to 5-bit binary table' to convert each letter into a set of five 1's and 0's. Write them into the "Message Bin" row.
- 2.3 > Perform an *XOR operation, column by column to fill in the row marked 'Coded Msg'
 - *XOR means you just do this:
 - 23.1 If the Random Key IS punched, then the Coded Message cell equals the opposite of the Message Bin Cell. (1 and 0 are opposites)
 - 23.2 If the Random Key is NOT punched, then the Coded Message cell equals the Message Bin Cell.
- 24>Transmit the Coded Message to your friend. Do not ever re-use the random key that was generated. Ideally, the key will be burned after using.

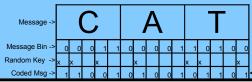
Alphabet to 5-bit binary table:

SPACE	Α	В	С	D	Е	F	G	Н	- 1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010

EXAMPLE: The secret message in this example is just the word "CAT" -->

The letters are translated into 5 bit binary using the table -->

This row has holes randomly punched. --> If the random key cell has a punch, reverse the bit, else copy it -->



1<-- This string of bits can be emailed.</p>

Step 3: Decode your message

- 3.1 > Your friend will decode this message with her identical worksheet by working through the encoding process in reverse.
 - 3.1.1 > First, she'll put the coded message in the bottom row. Then she'll use the Random Key row to XOR bits up into the Message Bin row. Finally, she'll convert 5 bit bin to letters.
 - 3.1.2 Be sure to never use bits over if you are going to encrypt a reply. Always destroy used tables so you don't accidently re-use.

Binary One-Time Pad Encryption Worksheet

Alphabet to 5-bit binary table:

SPACE	Α	В	C	D	Е	F	G	Н	_	J	K	L	M	N	0	Р	Q	R	S	Т	J	V	W	Х	Υ	Z
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010

Message -> Message Bin -> Random Key ->												H																			H			H	
Coded Msg ->								<u> </u>										<u> </u>			<u>ш</u> Т		<u> </u>												Щ
				Н		Н		Ε		_			<u>+</u>	Н		E				H		H		Н	_	H	\pm	Н			Н	\pm		\Box	
			+					+		+			+						+					H	+	H					H	+		H	$\frac{1}{1}$
																																			\equiv
										+	Ŧ		+	H		H	+	\exists	Ŧ		$\frac{1}{1}$		#		Ŧ	Ħ	Ŧ		Ŧ	ŧ	H	Ŧ			\mp