

Example of One-time Pad Encryption

WORD	CODE
a	1
after	2
am	3
an	4
and	5
are	6
be	7
before	8
do	9
eat	10
for	11
go	12
good	13
have	14
he	15
her	16
here	17
him	18
I	19
in	20
is	21
it	22
lunch	23
me	24
not	25
on	26
out	27
room	28
see	29
she	30
that	31
the	32
this	33
to	34
want	35
was	36
we	37
were	38
what	39
when	40
will	41
with	42
work	43
you	44

RANDOM NUMBERS

	0	1	2	3	4	5	6	7	8	9
0	62	38	75	47	60	33	69	45	60	54
1	85	59	35	32	8	82	61	64	56	37
2	17	99	59	9	6	26	21	15	37	16
3	95	10	21	70	53	94	80	79	36	11
4	6	79	50	89	34	52	32	40	99	67
5	41	85	79	95	56	41	36	88	51	8
6	13	95	24	57	51	1	75	55	39	24
7	54	14	78	6	89	80	6	50	59	32
8	75	33	41	48	20	36	50	27	29	49
9	33	2	20	24	27	8	47	31	61	51

Every word is represented by a 2-digit number.

To encode a message:

1. Pick a column and row number to begin selecting random numbers from.
2. For each word in your message, add the corresponding 2-digit number to the next random number down. If any sum is over 99, ignore the hundreds' digit.

For example, suppose we want to encode the message, "I want to eat lunch with you". We can begin anywhere in the random number table, so let's pick column 7 and row 0. To each word number in our message, we need to add a number down from the list of random numbers. Note that the message must begin with "70", so the recipient knows where we started in random number table.

original:	19	35	34	10	23	42	44	
random:	45	64	15	79	40	88	55	
sum:	70	64	99	49	89	63	30	99 <---- We send this.

It's interesting to note that the number 99 appears twice in the ciphertext, but it's just a coincidence. In other words, it's not the same word being used twice.