- -

L F H N Y Z A H S B J R N X K B Y N F V K O Z A T

V R Z T H J P C S U R U S Y Q J V X M N V L O E L

P O D Y V J J L V J X F S M L H P L G A Z X V Z Y

T S U I O X B M K J M D S H D N P M P I O Z V O Z

E Y J V F O B X K R P M T X Y Y T K G K A T O P E

N M C J K F P N S V S M Z Z N Q Q Z Y N C Y S D E

Y I I U J T U R R Z Q M R D E Y O V R J M O C G Y

H A L O K N M I I N C A I D Y R D T K H Z D Z M P

O I N D S C M O F E X G B V J C A Y S O I S B M U

K I S Z X O Z J I M D B R C Y B N B V Z L F B X T

R J C T I N W I F H I M N S F R U V V C U I T R N

N Q Q N Q Z U B Z B E P V J X N C Z X Y F B T E X

V E I O E M D V T N G S S N G L R Z V G U K U Q X

P Q F R I Q C F A A N L T K E D X M D A Q A I M U

M E I M Q L Q T W P M V B N X M N U U K A C P X A

A Y G F S Z N F D U S Y M V X I Y I P O R J C E K

P E D P Q J F V I O M Y L I X G V T N C Q Q X X H

F S G N A U D T L B U N K A H H A R M G T Z Y X H

U G B O A J X M F Y H T U N M W C T X M Q F L S Y

A	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 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
B	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 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 Z
C	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 X W V U T S R Q P O N M L K J I H G F E D C B A Z Y
D	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 W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
E	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 V U T S R Q P O N M L K J I H G F E D C B A Z Y X W
F	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 U T S R Q P O N M L K J I H G F E D C B A Z Y X W V
G	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 T S R Q P O N M L K J I H G F E D C B A Z Y X W V U
H	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 S R Q P O N M L K J I H G F E D C B A Z Y X W V U T
I	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 R Q P O N M L K J I H G F E D C B A Z Y X W V U T S
J	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 Q P O N M L K J I H G F E D C B A Z Y X W V U T S R
K	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 P O N M L K J I H G F E D C B A Z Y X W V U T S R Q
L	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 O N M L K J I H G F E D C B A Z Y X W V U T S R Q P
M	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 N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
N	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 M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
O	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 L K J I H G F E D C B A Z Y X W V U T S R Q P O N M
P	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 K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
Q	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 J I H G F E D C B A Z Y X W V U T S R Q P O N M L K
R	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 I H G F E D C B A Z Y X W V U T S R Q P O N M L K J
S	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 H G F E D C B A Z Y X W V U T S R Q P O N M L K J I
T	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 G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
U	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 F E D C B A Z Y X W V U T S R Q P O N M L K J I H G
V	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 E D C B A Z Y X W V U T S R Q P O N M L K J I H G F
W	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 D C B A Z Y X W V U T S R Q P O N M L K J I H G F E
X	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 C B A Z Y X W V U T S R Q P O N M L K J I H G F E D
Y	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 B A Z Y X W V U T S R Q P O N M L K J I H G F E D C
Z	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 A 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

Figure 1: This table from the NSA's DIANA program illustrates how one-time pads produce messages with keys the same length of ciphertext. The key is on the left- hand side. The right-hand side is the table used to convert plain text to ciphertext (and vice versa). This key starts with the letter "L," so the user encrypting a message would use the L row on the table to choose the first letter of ciphertext. Assume that Alice wants to say "The Magic Words Are Squeamish Ossifrage" to Bob. To encrypt, Alice notes the first letter from the key, left-hand pane, which is L. Turning to the table, row L, and then to the letter T, the corresponding ciphertext underneath the T is a V. To encrypt the next letter, Alice would then use F from the key to locate the letter H and choose the ciphertext N, and so on. Alice and Bob must have identical cards and must destroy them after the process. This version of the DIANA cipher appeared in Hoofnagle & Garfinkel, The Quantum Age, Cambridge University Press 2022, and was adapted to Latex by Malik @hadimalik1 on Fiverr