The NSA DIANA Cipher

```
TTRFZ  PDMGA  FANIR  UZCQA  NVOBL

XZNWA  ZVYAS  KKIFE  EFULW  FJJHR

PUANQ  NENDY  GTMGS  ENIKM  HFXQH

QXDMZ  KLVJV  PBTUS  OXEVN  DZQJR

NFBUJ  BFFUT  XLNXS  DYOEV  FDPVY

QPFVN  WNJWD  SNHQR  EAKWK  QDKQH

KAQVS  WVWJU  OXDXK  YFJYY  QFWFY

NDUWS  CENLS  ZHZXI  NMJOR  QRMTK

PAVYR  UPXFV  CKRWG  LIRHF  BKOVJ

TJOBR  FCEEU  FKVZA  KRAYE  XVFCR

CDYVO  UTLTE  SCGJT  VWTDL  YUNXY

IVCKD  HTZMT  HNIAS  FTEVM  BUCDW

JCUQB  GQIIV  VQMKM  BFWIV  ZYQKW

DKXAJ  SBQZQ  FHYYI  OMSDN  CCRPQ

BVPOU  HRRFK  JLTSM  VECZV  MVSIG

XRMXY  POGWK  IIIHP  WVEUN  ZWPJO

YKVUR  JBQJJ  BEPKT  ZWCPL  JZTGM

ZESKM  VBQQL  BYDVQ  DMIJP  BDJPB

DAROU  NNVUK  OKWPH  ITDUF  PLKXG
```

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

This is reproduced from Hoofnagle & Garfinkel, Law and Policy for the Quantum Age (Cambridge University Press 2022) and converted to LaTeXby Khalil Mokhtari.

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).

In this version, the key auto-generates random characters with each build. But suppose that the key starts with the letter "L." 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 select the next letter from the key, and so on. Alice and Bob must have identical cards and must destroy them after the process.

Khalil Mokhtari serves as a research member and associate professor at the University of Khenchela, Algeria. He obtained his Ph.D. through the PROFAS B+ program, conducting research at the Laboratory of Systems Engineering of Versailles (LISV), University of Versailles UVSQ, France. His expertise lies in Applied Mathematics and Control Systems Engineering, with a focus on adaptive control, passivity, and positivity characterizations of control systems.