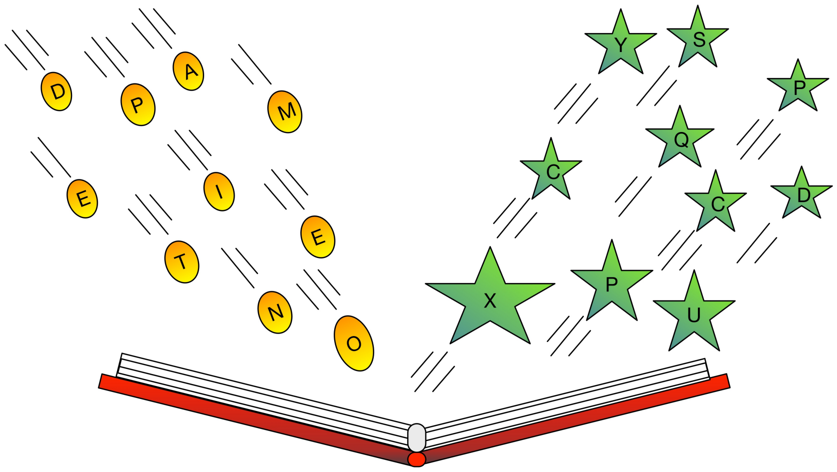
abitofcs4fn.org

One-time Pads

A **cipher** is a way to make a secret message.

Battles have been lost because ciphers were cracked and the messages read. A **one-time pad** is a kind of cipher that can't be cracked.

You make two copies of a book of random numbers. The book is the one-time pad. Each number is used to encrypt *one* letter.



British spies used one-time pads in World War II. So did those fighting racism in South Africa in the 1980s.

Computer Science activities with a sense of fun:
One-time pad: V1(16 June 2018)
Created by Paul Curzon
for Teaching London Computing: http://teachinglondoncomputing.org

How to make a One-time Pad

You will need

A Pack of cards

Two empty notebooks

Instructions

1. Shuffle the pack of cards.
2. Turn over the top card.
3. Look up the number for the card in the table and write it in the next space in the notebook.
4. Put the card back in the pack and shuffle.
5. Repeat from step 3 until you have enough numbers for your message.
6. Copy the numbers in to the second notebook.

Red Ace	1
Red Two	2
Red Three	3
Red Four	4
Red Five	5
Red Six	6
Red Seven	7
Red Eight	8
Red Nine	9
Red Ten	10
Red Jack	11
Red Queen	12
Red King	13
Black Ace	14
Black Two	15
Black Three	16
Black Four	17
Black Five	18
Black Six	19
Black Seven	20
Black Eight	21
Black Nine	22
Black Ten	23
Black Jack	24
Black Queen	25
Black King	26

Computer Science activities with a sense of fun:
One-time pad: V1(16 June 2018)
Created by Paul Curzon
for Teaching London Computing: http://teachinglondoncomputing.org

How to encrypt with a One-time Pad

To share secrets, Alice and Bob each take a copy of the one-time pad.

Alice crosses off the next unused number from the one-time pad. She counts forward that many letters in the alphabet from the next letter in her message (jumping back to A from Z). She writes down the letter she ends on.

For example, suppose the next seven numbers in the one-time pad are:

5 2 6 10 2 20 13.

To encrypt “LOVE YOU” Alice moves 5 letters on from L to get Q, 2 letters on from O to get Q (again), 6 letters on from V to get B (wrapping round from Z to A) and so on.

She sends QQBOAIH to Bob.

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

Computer Science activities with a sense of fun:
One-time pad: V1(16 June 2018)
Created by Paul Curzon
for Teaching London Computing: http://teachinglondoncomputing.org

How to decrypt with a One-time Pad

To decrypt the message, Bob starts at the same place in the one-time pad. Unlike Alice, he counts *back* through the alphabet from the letter in her message instead of forwards. The letter he ends on is the next letter of the original message.

Bob gets the message “QQBOAIH”. The next numbers in his one-time pad are also 5 2 6 10 2 20 13. He moves 5 letters *back* from Q to get L, 2 back from Q to get O, 6 back from B to get V (wrapping round from A back to Z), and so on. He writes LOVEYOU.

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

For you to do

1. Create your own one-time pad. Write a secret message to a friend.
2. Why do you think one-time pads aren’t used more often?

Computer Science activities with a sense of fun:
One-time pad: V1(16 June 2018)
Created by Paul Curzon
for Teaching London Computing: http://teachinglondoncomputing.org