

Завдання:

This is normal text ciphered with a strong algorithm (Salsa20), but every line is ciphered with the same key and no nonce is being used.

Вирішення:

Так як всі рядки були зашифровані без солі і з одним і тим же ключем то ми маємо

$$\text{CipheredLine1} = \text{ClearLine1} \wedge \text{Key}$$

$$\text{CipheredLine2} = \text{ClearLine2} \wedge \text{Key}$$

...

$$\text{CipheredLineN} = \text{ClearLineN} \wedge \text{Key}$$

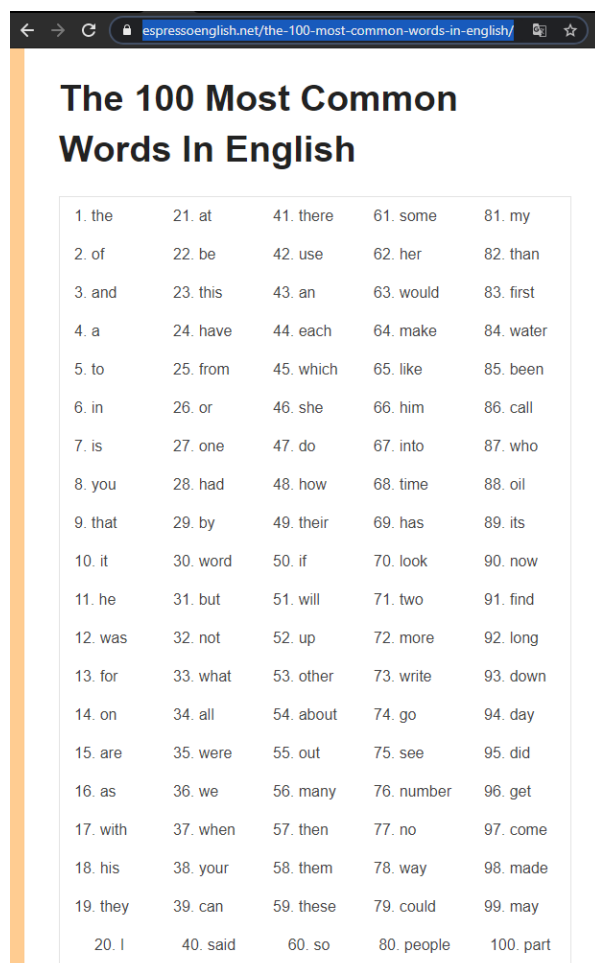
Тому ми можемо знехтувати ключем якщо заікорим між собою зашифровані рядки.

$$\text{CipheredLineI} \wedge \text{CipheredLineJ} = (\text{ClearLineI} \wedge \text{Key}) \wedge (\text{ClearLineJ} \wedge \text{Key}) = (\text{ClearLineI} \wedge \text{ClearLineJ}) \wedge (\text{Key} \wedge \text{Key}) = (\text{ClearLineI} \wedge \text{ClearLineJ})$$

Щоб розшифрувати, ми можемо підбирати найпопулярніші англійські слова та ікорити з $(\text{ClearLineI} \wedge \text{ClearLineJ})$. Якщо слово і справді зустрічається в якомусь із рядків то ми отримаємо частину іншого рядка.

Повторяючи ці дії можна знайти увесь текст в звичайному вигляді.

Почнемо з перебору найпопулярніших слів



1. the	21. at	41. there	61. some	81. my
2. of	22. be	42. use	62. her	82. than
3. and	23. this	43. an	63. would	83. first
4. a	24. have	44. each	64. make	84. water
5. to	25. from	45. which	65. like	85. been
6. in	26. or	46. she	66. him	86. call
7. is	27. one	47. do	67. into	87. who
8. you	28. had	48. how	68. time	88. oil
9. that	29. by	49. their	69. has	89. its
10. it	30. word	50. if	70. look	90. now
11. he	31. but	51. will	71. two	91. find
12. was	32. not	52. up	72. more	92. long
13. for	33. what	53. other	73. write	93. down
14. on	34. all	54. about	74. go	94. day
15. are	35. were	55. out	75. see	95. did
16. as	36. we	56. many	76. number	96. get
17. with	37. when	57. then	77. no	97. come
18. his	38. your	58. them	78. way	98. made
19. they	39. can	59. these	79. could	99. may
20. I	40. said	60. so	80. people	100. part

Перевіримо чи зустрічаються ці слова на початку рядків. Після слів одразу ж можна ставити символ “ ”.

“the ” та “of ” не дали зрозумілого результату. А от “and ” показав цікавіший результат:

```
Windows PowerShell
PS E:\cyber_security\weak salt> python .\main.py

Enter text:and
row = 1 || if
row = 2 || if
row = 3 || if
row = 6 || if

Enter text:and
row = 1 || if y
row = 2 || if y
row = 3 || if y
row = 6 || if y

Enter text:if you
row = 1 || and ri
row = 2 || and lo
row = 3 || and ne
row = 5 || to ser
row = 6 || and so
row = 7 || except
row = 9 || if nei
row = 10 || if all
row = 12 || with s
row = 13 || yours

Enter text:if you
row = 1 || and ris
row = 2 || and los
row = 3 || and nev
row = 5 || to serv
row = 6 || and so
row = 7 || except
row = 9 || if neit
row = 10 || if all
row = 12 || with si
row = 13 || yours i

Enter text:and never
row = 3 || if you can
```

Тепер ми бачимо що в інших рядках зустрічається “if y”.

Спробуємо “if you ”

Знову отримуємо позитивний результат.

Так продовжуємо підбирати найочевидніші варіанти

```
Windows PowerShell

Enter text:if you can
row = 1 || and risk it
row = 2 || and lose, a
row = 3 || and never b
row = 5 || to serve yo
row = 6 || and so hold
row = 7 || except the
row = 9 || if neither
row = 10 || if all men
row = 12 || with sixty
row = 13 || yours is th

Enter text:and risk if

Enter text:and risk it
row = 1 || if you can

Enter text:and risk it
row = 1 || if you can m

Enter text:to serve your
row = 5 || if you can mak

Enter text:if you can make
row = 1 || and risk it on o
row = 2 || and lose, and st
row = 3 || and never breath
row = 4 || if you can force
row = 5 || to serve your tu
row = 6 || and so hold on w
row = 7 || except the will
row = 8 || if you can talk
row = 9 || if neither foes
row = 10 || if all men count
row = 11 || if you can fill
row = 12 || with sixty secon
row = 13 || yours is the Ear

Enter text:with sixty second
```

```
Windows PowerShell
Enter text:with sixty second
row = 12 || if you can make o
-----
Enter text:if you can make one
row = 1 || and risk it on one t
row = 2 || and lose, and start
row = 3 || and never breathe a
row = 4 || if you can force you
row = 5 || to serve your turn l
row = 6 || and so hold on when
row = 7 || except the Will whic
row = 8 || if you can talk with
row = 9 || if neither foes nor
row = 10 || if all men count wit
row = 11 || if you can fill the
row = 13 || yours is the Earth a
-----
Enter text:and lose, and start again
row = 2 || if you can make one heap
-----
Enter text:if you can make one heap
row = 1 || and risk it on one turn o
row = 2 || and lose, and start again
row = 3 || and never breathe a word
row = 4 || if you can force your hea
row = 5 || to serve your turn long a
row = 6 || and so hold on when there
row = 7 || except the Will which say
row = 8 || if you can talk with crow
row = 9 || if neither foes nor lovin
row = 10 || if all men count with you
row = 11 || if you can fill the unifor
row = 13 || yours is the Earth and ev
-----
Enter text:yours is the Earth and ever
row = 13 || if you can make one heap of
-----
Enter text:if you can make one heap of
row = 1 || and risk it on one turn of p
row = 2 || and lose, and start again at
row = 3 || and never breathe a word abo
```

```
Windows PowerShell
Enter text:if you can make one heap of
row = 1 || and risk it on one turn of p
row = 2 || and lose, and start again at
row = 3 || and never breathe a word abo
row = 4 || if you can force your heart
row = 5 || to serve your turn long afte
row = 6 || and so hold on when there is
row = 7 || except the Will which says t
row = 8 || if you can talk with crowds
row = 9 || if neither foes nor loving f
row = 10 || if all men count with you, b
row = 11 || if you can fill the unforgiv
row = 13 || yours is the Earth and every
-----
Enter text:to serve your turn long after
row = 5 || if you can make one heap of al
-----
Enter text:if you can make one heap of all
row = 1 || and risk it on one turn of pitch
row = 2 || and lose, and start again at you
row = 3 || and never breathe a word about y
row = 4 || if you can force your heart and
row = 5 || to serve your turn long after th
row = 6 || and so hold on when there is not
row = 7 || except the Will which says to th
row = 8 || if you can talk with crowds and
row = 9 || if neither foes nor loving frien
row = 10 || if all men count with you, but n
row = 11 || if you can fill the unforgiving
row = 13 || yours is the Earth and everything
-----
Enter text:yours is the Earth and everything
row = 13 || if you can make one heap of all yo
-----
Enter text:if you can make one heap of all you
row = 2 || and lose, and start again at your b
row = 3 || and never breathe a word about your
row = 4 || if you can force your heart and ner
row = 5 || to serve your turn long after they
row = 6 || and so hold on when there is nothin
row = 8 || if you can talk with crowds and kee
```

```
Windows PowerShell

Enter text:if you can make one heap of all
row = 1 | and risk it on one turn of pitch
row = 2 | and lose, and start again at you
row = 3 | and never breathe a word about y
row = 4 | if you can force your heart and
row = 5 | to serve your turn long after th
row = 6 | and so hold on when there is not
row = 7 | except the will which says to th
row = 8 | if you can talk with crowds and
row = 9 | if neither foes nor loving frien
row = 10 | if all men count with you, but n
row = 11 | if you can fill the unforgiving
row = 13 | yours is the Earth and everythin

Enter text:yours is the Earth and everything
row = 13 | if you can make one heap of all yo

Enter text:if you can make one heap of all you
row = 2 | and lose, and start again at your b
row = 3 | and never breathe a word about your
row = 4 | if you can force your heart and ner
row = 5 | to serve your turn long after they
row = 6 | and so hold on when there is nothin
row = 8 | if you can talk with crowds and kee
row = 9 | if neither foes nor loving friends
row = 10 | if all men count with you, but none
row = 11 | if you can fill the unforgiving min
row = 13 | yours is the Earth and everything t

Enter text:and so hold on when there is nothing
row = 6 | if you can make one heap of all your

Enter text:if you can make one heap of all your
row = 2 | and lose, and start again at your beg
row = 3 | and never breathe a word about your l
row = 4 | if you can force your heart and nerve
row = 5 | to serve your turn long after they ar
row = 6 | and so hold on when there is nothing
row = 8 | if you can talk with crowds and keep
row = 9 | if neither foes nor loving friends ca
row = 10 | if all men count with you, but none t
row = 11 | if you can fill the unforgiving minut
row = 13 | yours is the Earth and everything tha

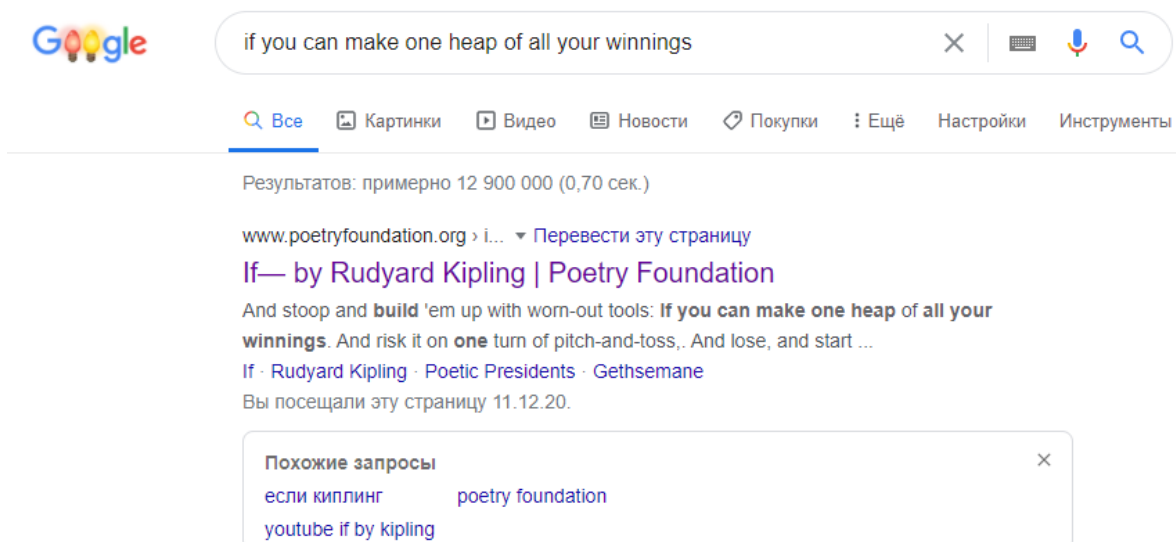
Enter text:and lose, and start again at your beg
row = 2 | if you can make one heap of all your

Enter text:And lose, and start again at your beginnings
row = 2 | If you can make one heap of all your winning

Enter text:and lose, and start again at your beginnings
row = 2 | if you can make one heap of all your winning

Enter text:if you can make one heap of all your winning
row = 2 | and lose, and start again at your beginnings
row = 4 | if you can force your heart and nerve and si
row = 5 | to serve your turn long after they are gone,
row = 6 | and so hold on when there is nothing in you
row = 8 | if you can talk with crowds and keep your vi
row = 9 | if neither foes nor loving friends can hurt
row = 10 | if all men count with you, but none too much
row = 11 | if you can fill the unforgiving minute
```

Ми маємо достатньо тексту, тому можемо просто скористатися допомогою сервісу Google, щоб визначити автора тексту



Автор тексту RUDYARD KIPLING

I сам текст:

If you can keep your head when all about you
Are losing theirs and blaming it on you,
If you can trust yourself when all men doubt you,
But make allowance for their doubting too;
If you can wait and not be tired by waiting,
Or being lied about, don't deal in lies,
Or being hated, don't give way to hating,
And yet don't look too good, nor talk too wise:

If you can dream—and not make dreams your master;
If you can think—and not make thoughts your aim;
If you can meet with Triumph and Disaster
And treat those two impostors just the same;
If you can bear to hear the truth you've spoken
Twisted by knaves to make a trap for fools,
Or watch the things you gave your life to, broken,
And stoop and build 'em up with worn-out tools: