# 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

***CipheredLine1 = ClearLine1 ^ Key***

***CipheredLine2 = ClearLine2 ^ Key***

***…***

***CipheredLineN = ClearLineN ^ Key***

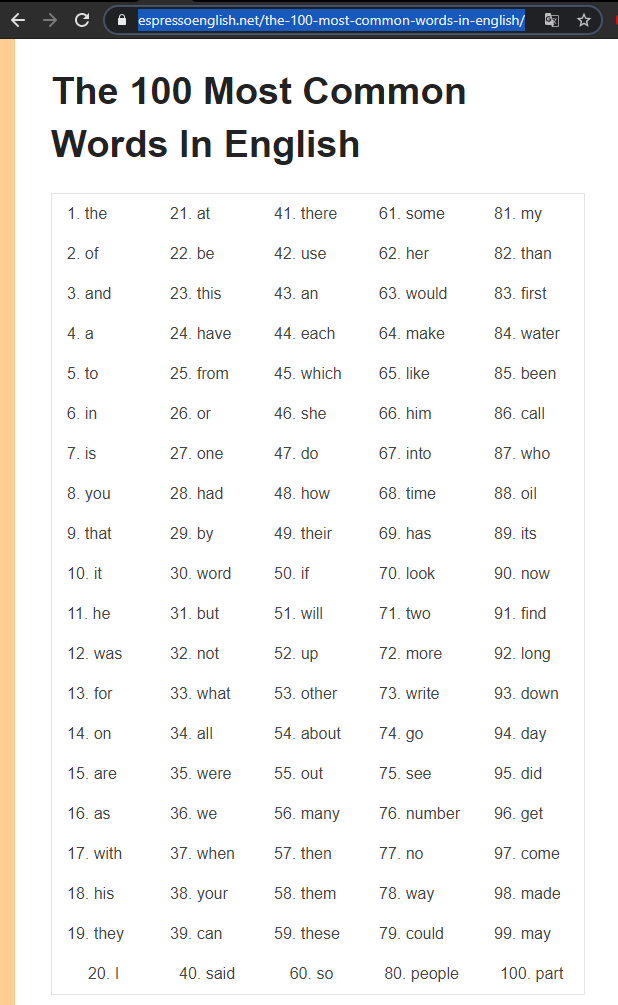
Тому ми можемо знехтувати ключем якщо заіксорим між собою зашифровані рядки.

***CipheredLineI ^ CipheredLineJ= (ClearLineI ^ Key) ^ (ClearLineJ ^ Key) = (ClearLineI ^ ClearLineJ) ^ ~~(Key ^ Key)~~ = (ClearLineI ^ ClearLineJ)***

Щоб розшифрувати, ми можемо підбирати найпопулярніші англійські слова та іксорити з ***(ClearLineI ^ ClearLineJ).*** Якщо слово і справді зустрічається в якомусь із рядків то ми отримаємо частину іншого рядка.

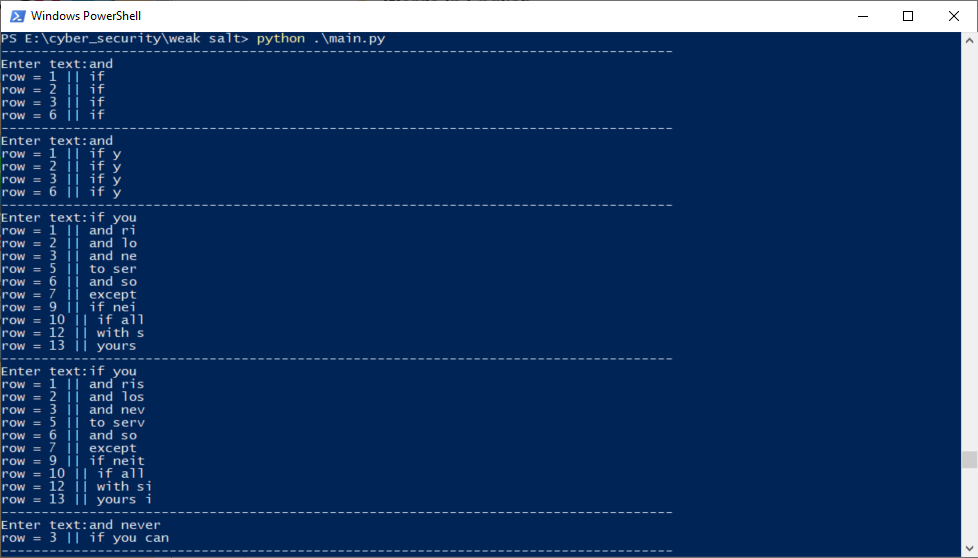
Повторяючи ці дії можна знайти увесь текс в звичайному вигляді.

Почнемо з перебору найпопулярніших слів



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

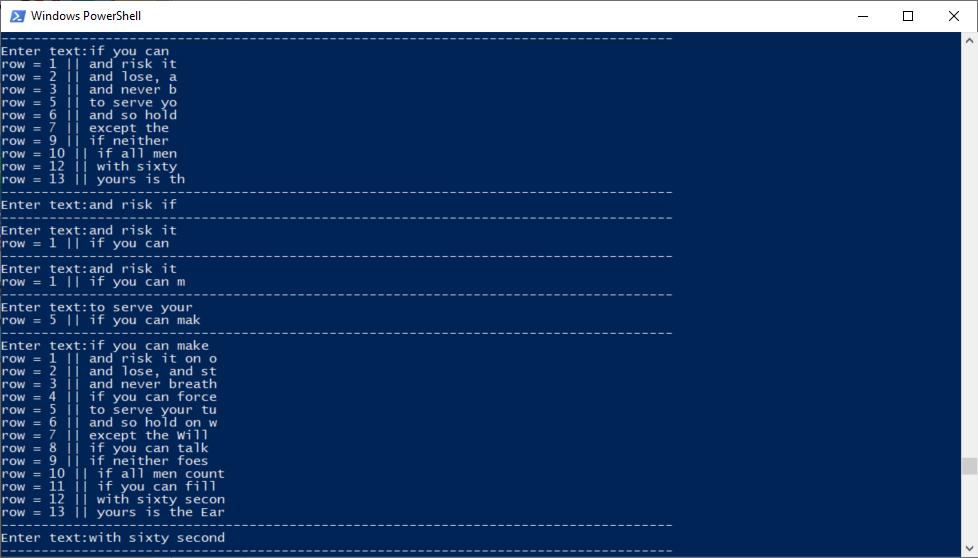
“the ” та “of ” не дали зрозумілого результату. А от “and ” показав цікавіший результат:

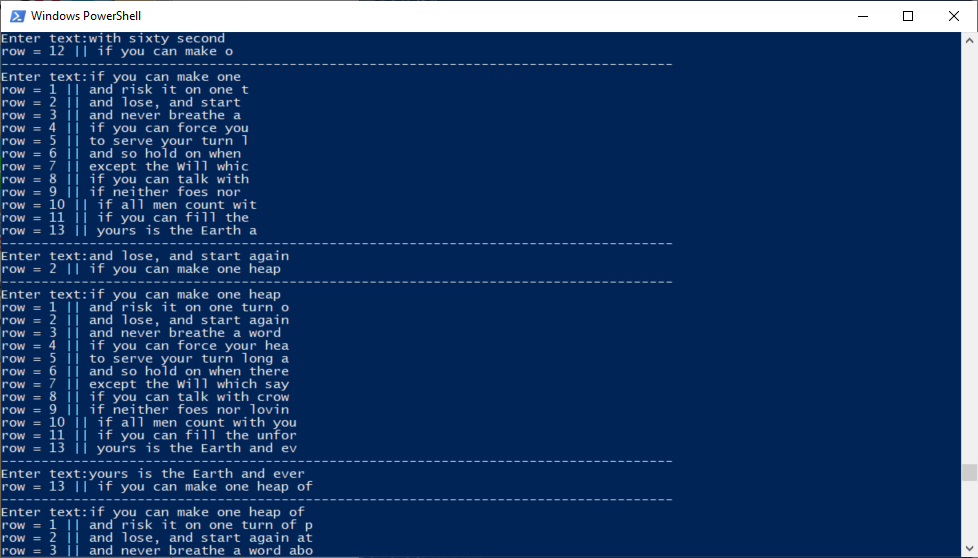


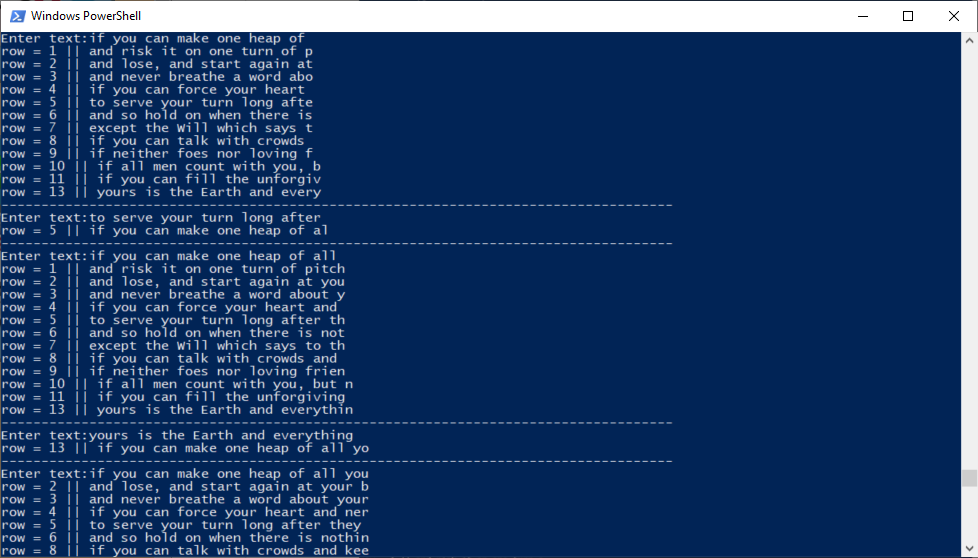
Тепер ми бачимо шо в інших рядках зустрічається “if y”.

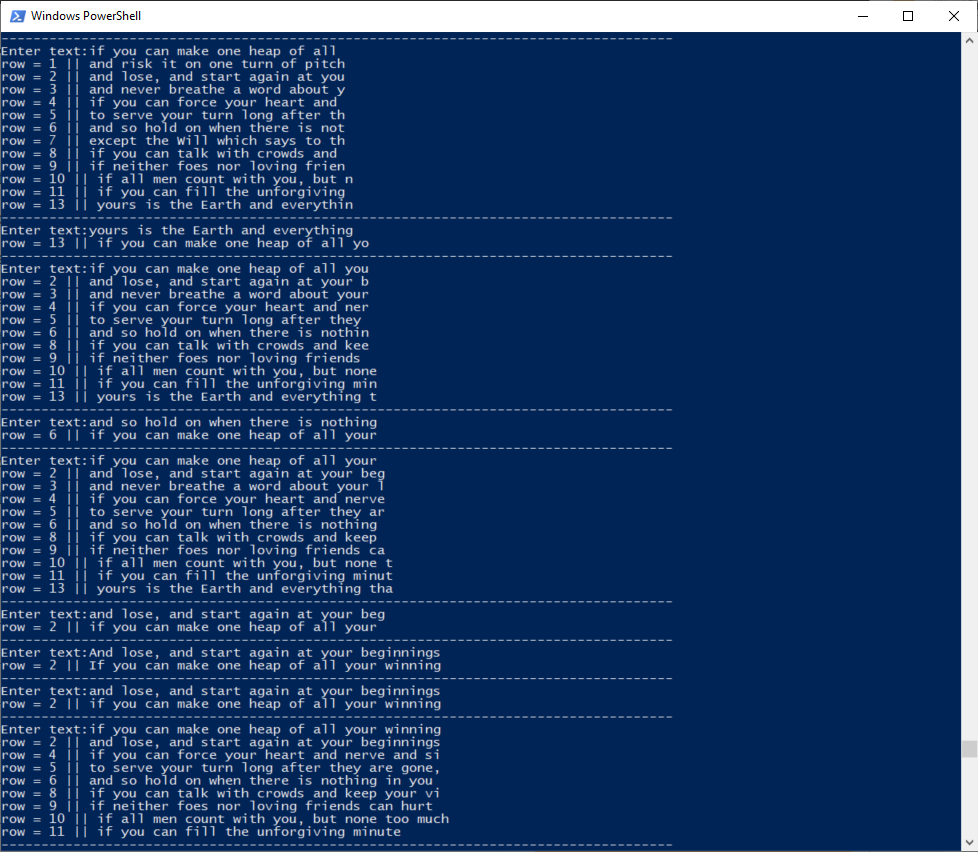
Спробуємо “if you “

Знову отримуєио позитивний результат.  
Так продовжуємо підбирати найочевидніші варіанти

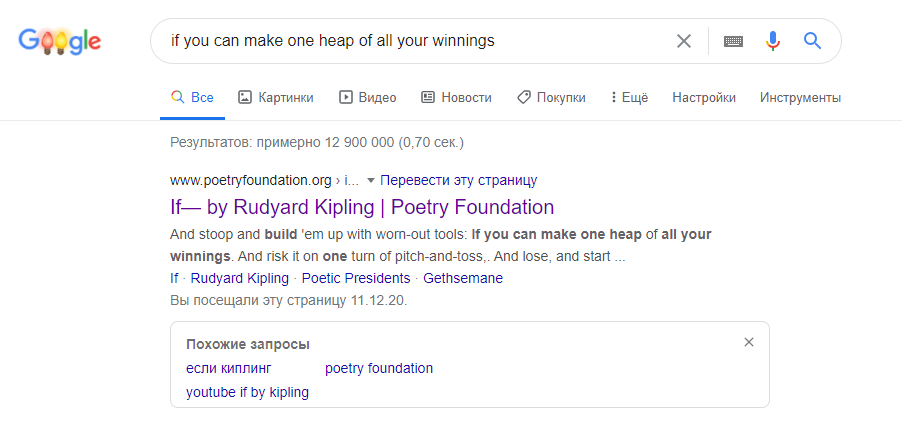








Ми маємо достатньо тексту, тому можемо просто скористатися допомогою сервісу Google, щоб визначити автора тексту



Автор тексту [RUDYARD KIPLING](https://www.poetryfoundation.org/poets/rudyard-kipling)

І 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: