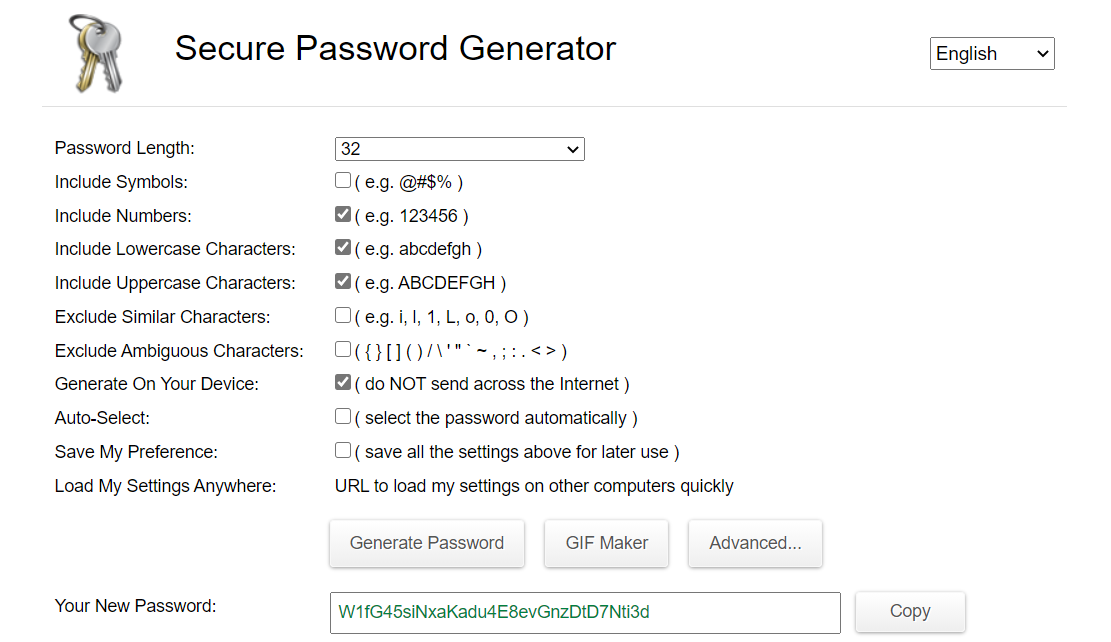
# הכנת אתגר 2 –

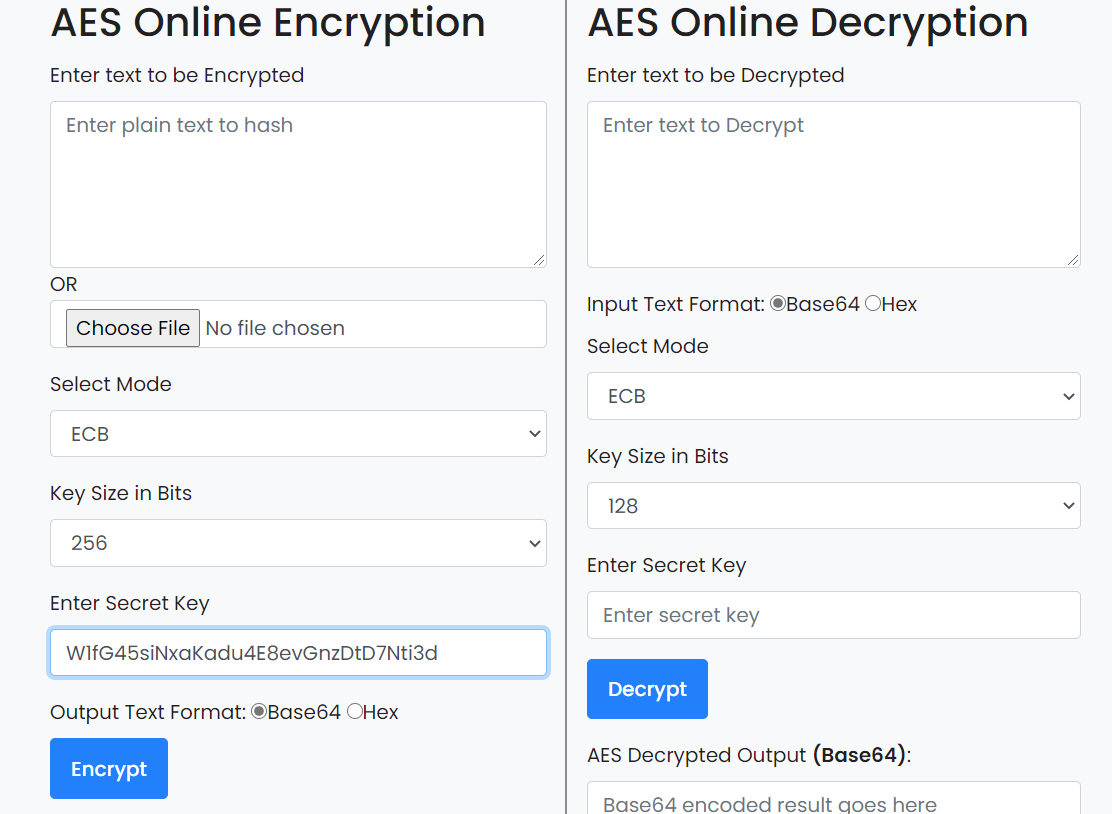
נייצר את סיפור הרקע בקובץ חדש –

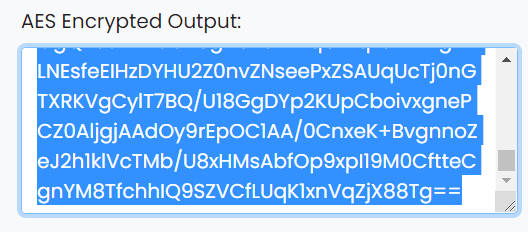
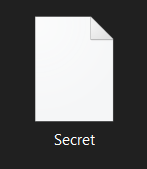
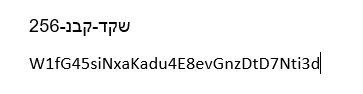
Bob has been acting strange lately. His neighbors say that he stays up all night, laughing out loud from his basement, and that weird lights are coming out of his house.  
This leads me to believe that he is planning something evil. I could not find any more information about his doings since he will not talk to anyone, so I asked Eve to help me.  
Eve was able to infiltrate his network and to extract some files that may help us solve this mystery, and maybe to prevent a mess from happening, but those files seem unusual in their nature and we were not able to find out what they contain.  
Maybe you could help us.

* תחילה נייצר קובץ וורד חדש ובו יהיה שמור הדגל שלנו - Afikoman{PotatoesGun}
* נרצה להצפין את הקובץ ולכן תחילה נייצר סיסמא חזקה באמצעות האתר הבא - [Strong Random Password Generator (passwordsgenerator.net)](https://passwordsgenerator.net/)
* נבחר אותיות גדולות, אותיות קטנות וספרות ונבטל את שאר האופציות.
* נלחץ Generate Password ונעתיק את הפלט שקיבלנו.



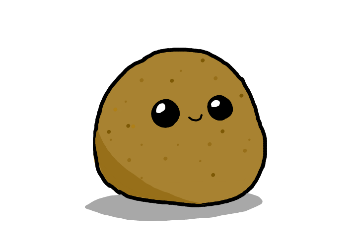
* את הקובץ נצפין באמצעות האתר הבא - [Online Tool for AES Encryption and Decryption (devglan.com)](https://www.devglan.com/online-tools/aes-encryption-decryption)
* נבחר במצב ECB 256 ביט ונדביק את המפתח ממקודם.
* כמו כן נבחר את הקובץ שאותו נצפין ונלחץ ENCRYPT.

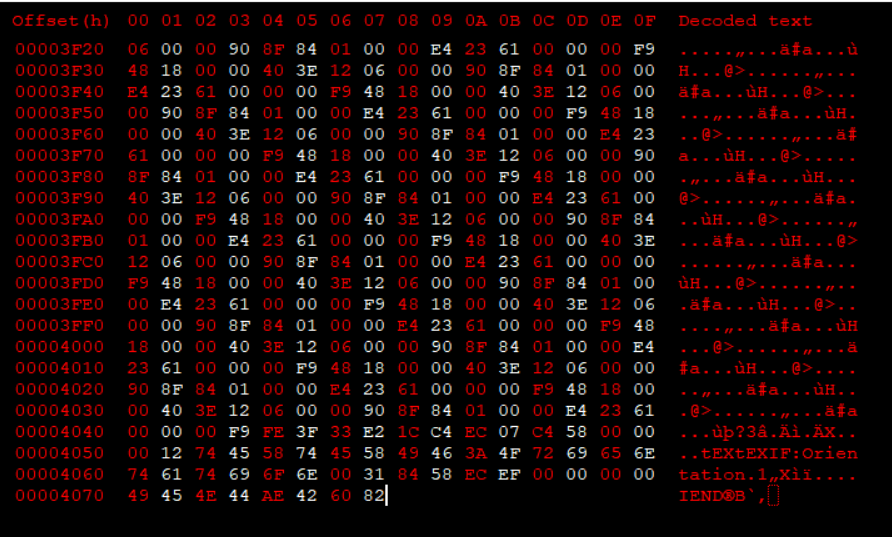


* קיבלנו את הפלט המוצפן הבא.
* נעתיק אותו לקובץ טקסט ונשמור בשם Secret.
* כעת נרצה לייצר קובץ המכיל את המידע על ההצפנה שלנו ואת המפתח.
* נפתח קובץ וורד חדש, נכניס בתוכו את המידע הבא ונשמור בשם Nothing.

שיטת ההצפנה כתובה בתוים בעברית ואם נקליד בשפה האנגלית נקבל בדיוק AES-ECB 256. קטע הסטרינג הינו המפתח שיצרנו. אלו ישמשו לפענוח.

* כעת נרצה להחביא את הקובץ החדש. נעשה זאת באמצעות תמונה של תפוח אדמה אותה ניקח מגוגל תמונות ובאמצעות Hex-editor.

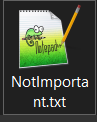




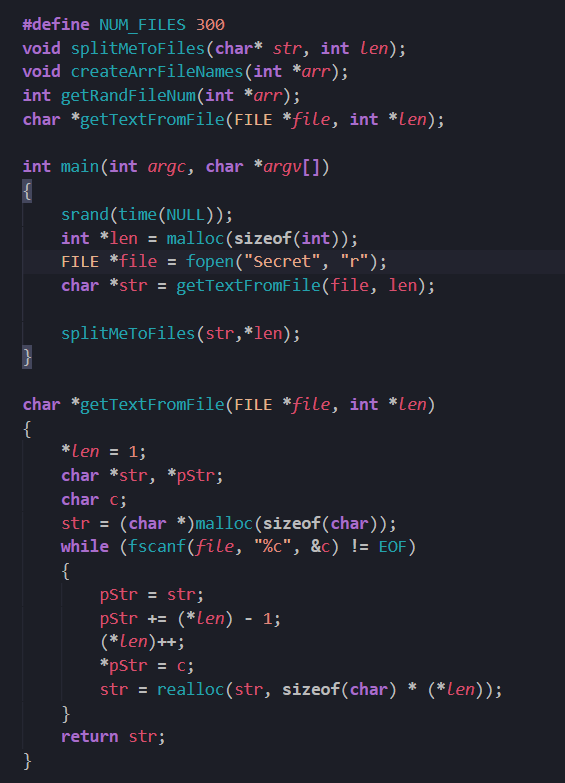
* נפתח את התמונה באמצעות HxD (התוכנה שאני השתמשתי), ונגיע לסוף הקובץ.
* ניתן לראות כי סוף הקובץ נמצא בהיסט 4078 שם נרצה להכניס את המידע של קובץ הוורד שלנו.
* נפתח את קובץ הוורד nothing באמצעות התוכנה הנ"ל ונעתיק את תוכנו אל סוף הקובץ של תפוח האדמה.
* נקבל קובץ חדש הנגמר בהיסט 6F3D.



* נשמור את פרטי ההיסט בקובץ חדש בשם NotImportant.



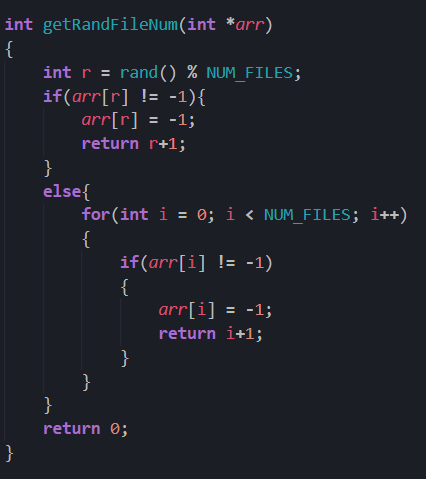
* הקובץ החדש אינו נחוץ למציאת הקובץ הטמון בתמונה אך נועד לרמוז על מיקום של משהו חבוי.
* נשמור את התמונה החדשה שלנו שמכילה את פרטי ההצפנה בשם חדש – Cute.png
* כעת – ניקח את הקובץ המוצפן שבנינו קודם לכן ומכיל את הדגל – Secret, ונרצה לפצל אותו למספר רב של קבצים!
* נבנה תוכנית C פשוטה באופן הבא –



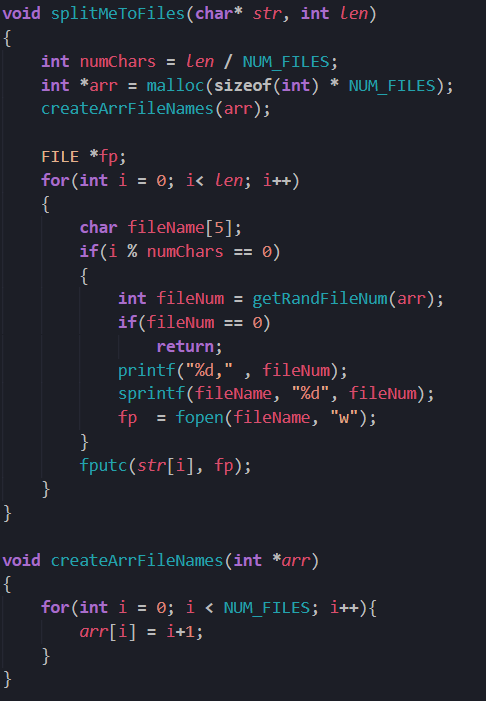
תחילה התוכנית מבצעת קריאה של קובץ אל מערך כפי שניתן לראות בgettextfromfile.

מספר הקבצים שנפצל את הקובץ שלנו

שם הקובץ עליו נעבוד



פונקציה המספקת שם קובץ רנדומלי מתוך מערך של שמות..



התוכנית מעבירה אל Splitmetofiles מערך תוים (של הקובץ אותו קראנו מקודם) והפונקציה מחלקת את אורך הקובץ למספר הקבצים אותם נרצה ליצר.

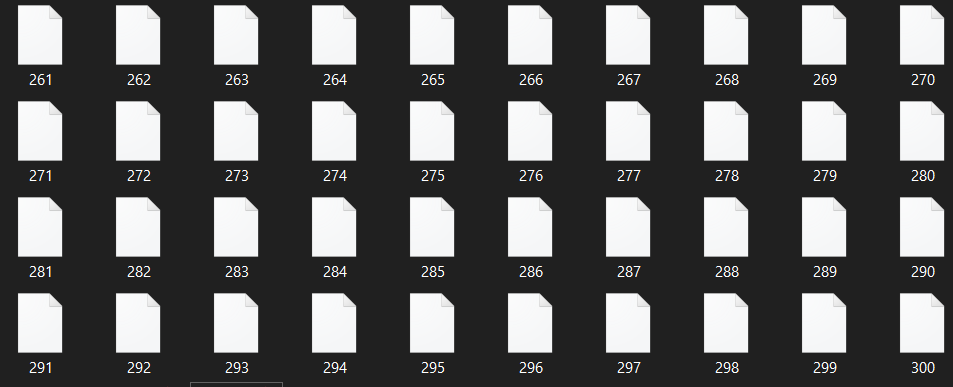
הפונקציה קוראת לפונקציה פשוטה נוספת שמייצרת מערך של מספרים מ1 ועד למספר הקבצים שלנו (הפונקציה התחתונה).

כעת עוברים בלולאה על אורך הקובץ, מבקשים שם קובץ מהפונקציה getrandfilenum (מספר בין 1 ל300)  
ומייצרים קובץ עבור מספר תווים שנקבע קודם לכן במשתנה numchars, כל זאת עד לקריאת כל הקובץ ועד ליצירת 300 קבצים שונים.

כמו כן מתבצעת הדפסה של שמות הקבצים לפי הסדר של ההרכבה! את הפלט הזה נרצה לשמור על מנת לשחזר את הקובץ מאוחר יותר.

* נשמור את הקובץ בשם splitter.c
* את הקובץ החדש שיצרנו נקמפל באמצעות הטרמינל –
* כעת נריץ באותה התיקיה בה נמצא הקובץ שלנו secret.



* לאחר ההרצה אנו מקבלים 300 קבצים שמכילים את הקובץ שלנו בחלקים. כמו כן נקבל את הפלט לשחזור – הסדר שלפיו פורק הקובץ ולפיו נרכיב אותו –

69,287,55,248,235,43,184,2,283,134,216,15,294,52,53,83,186,272,128,39,1,28,296,135,136,3,4,220,131,170,172,251,209,226,250,143,268,5,196,6,19,111,17,13,214,7,147,99,41,274,190,275,8,237,161,189,72,212,108,254,133,31,257,9,256,206,10,276,91,11,278,162,293,12,174,259,114,20,57,14,46,298,232,16,234,92,18,21,22,93,23,24,123,25,228,26,27,163,106,119,45,29,280,37,30,205,47,241,224,104,199,269,153,130,67,87,222,32,195,33,197,34,35,71,36,38,201,40,253,58,121,49,192,100,137,42,44,48,50,279,51,262,300,191,54,118,56,59,169,60,288,117,180,150,188,207,240,140,61,244,198,62,63,141,64,181,65,66,68,70,213,154,236,264,73,74,81,125,90,75,76,129,77,78,79,80,185,270,145,82,265,94,173,84,286,85,86,88,89,95,223,96,97,158,98,101,102,295,103,105,107,227,109,113,110,182,112,142,203,115,116,120,159,122,124,144,211,126,127,132,138,139,146,148,225,164,238,160,210,149,151,152,292,155,156,249,157,165,166,167,168,171,247,175,176,177,178,179,183,187,193,194,200,202,204,208,215,217,218,219,221,285,229,230,231,243,233,239,242,245,246,252,255,258,291,260,261,263,266,267,271,273,277,281,282,284,289,290,297,299

* נמיר את רצף התוים לbase64 באתר [Convert ASCII to Base64 - Online ASCII Tools](https://onlineasciitools.com/convert-ascii-to-base64) ונקבל –



NjksMjg3LDU1LDI0OCwyMzUsNDMsMTg0LDIsMjgzLDEzNCwyMTYsMTUsMjk0LDUyLDUzLDgzLDE4

NiwyNzIsMTI4LDM5LDEsMjgsMjk2LDEzNSwxMzYsMyw0LDIyMCwxMzEsMTcwLDE3MiwyNTEsMjA5

LDIyNiwyNTAsMTQzLDI2OCw1LDE5Niw2LDE5LDExMSwxNywxMywyMTQsNywxNDcsOTksNDEsMjc0

LDE5MCwyNzUsOCwyMzcsMTYxLDE4OSw3MiwyMTIsMTA4LDI1NCwxMzMsMzEsMjU3LDksMjU2LDIw

NiwxMCwyNzYsOTEsMTEsMjc4LDE2MiwyOTMsMTIsMTc0LDI1OSwxMTQsMjAsNTcsMTQsNDYsMjk4

LDIzMiwxNiwyMzQsOTIsMTgsMjEsMjIsOTMsMjMsMjQsMTIzLDI1LDIyOCwyNiwyNywxNjMsMTA2

LDExOSw0NSwyOSwyODAsMzcsMzAsMjA1LDQ3LDI0MSwyMjQsMTA0LDE5OSwyNjksMTUzLDEzMCw2

Nyw4NywyMjIsMzIsMTk1LDMzLDE5NywzNCwzNSw3MSwzNiwzOCwyMDEsNDAsMjUzLDU4LDEyMSw0

OSwxOTIsMTAwLDEzNyw0Miw0NCw0OCw1MCwyNzksNTEsMjYyLDMwMCwxOTEsNTQsMTE4LDU2LDU5

LDE2OSw2MCwyODgsMTE3LDE4MCwxNTAsMTg4LDIwNywyNDAsMTQwLDYxLDI0NCwxOTgsNjIsNjMs

MTQxLDY0LDE4MSw2NSw2Niw2OCw3MCwyMTMsMTU0LDIzNiwyNjQsNzMsNzQsODEsMTI1LDkwLDc1

LDc2LDEyOSw3Nyw3OCw3OSw4MCwxODUsMjcwLDE0NSw4MiwyNjUsOTQsMTczLDg0LDI4Niw4NSw4

Niw4OCw4OSw5NSwyMjMsOTYsOTcsMTU4LDk4LDEwMSwxMDIsMjk1LDEwMywxMDUsMTA3LDIyNywx

MDksMTEzLDExMCwxODIsMTEyLDE0MiwyMDMsMTE1LDExNiwxMjAsMTU5LDEyMiwxMjQsMTQ0LDIx

MSwxMjYsMTI3LDEzMiwxMzgsMTM5LDE0NiwxNDgsMjI1LDE2NCwyMzgsMTYwLDIxMCwxNDksMTUx

LDE1MiwyOTIsMTU1LDE1NiwyNDksMTU3LDE2NSwxNjYsMTY3LDE2OCwxNzEsMjQ3LDE3NSwxNzYs

MTc3LDE3OCwxNzksMTgzLDE4NywxOTMsMTk0LDIwMCwyMDIsMjA0LDIwOCwyMTUsMjE3LDIxOCwy

MTksMjIxLDI4NSwyMjksMjMwLDIzMSwyNDMsMjMzLDIzOSwyNDIsMjQ1LDI0NiwyNTIsMjU1LDI1

OCwyOTEsMjYwLDI2MSwyNjMsMjY2LDI2NywyNzEsMjczLDI3NywyODEsMjgyLDI4NCwyODksMjkw

LDI5NywyOTk=

* נשמור את הרצף הנ"ל בקובץ חדש ונקרא לו orderAndChaos.txt.
* את הקובץ החדש נשים בתיקית האתגר.
* האתגר שלנו מוכן ! בהצלחה !!