# Laboratorio 1
# Criptografía y Seguridad Informática

Jorge Rodríguez Fraile, 100405951

# CrypTool

## Ejercicio 1

a) **Clave a:**
eL ALUMNO: apellido1 apellido2, nombre HA OBTENIDO LA CALIFICACIóN DE sobresaliente EN LA ASIGNATURA sti/csi.

Como empieza por la a minúscula, cambia las letras mayúsculas por las minúsculas, ya que las mayúsculas son las primeras a dar la vuelta a las minúsculas.
**Clave A:**
El alumno: APELLIDO1 APELLIDO2, NOMBRE ha obtenido la calificación de SOBRESALIENTE en la asignatura STI/CSI.

Como solo cambia las letras mayúsculas por mayúsculas y sustituye la letra por sí misma, el resultado es el mismo texto de entrada.
**Clave Z:**
dK zKTLMN: Zodkkhcn1 Zodkkhcn2, mnlaqd Gz NASDMHCN Kz BzKHEHBzBHóM CD
rnaqdrZkhdmsd DM Kz zRHFMzSTQz rsh/brh.

Están todas las letras desplazadas 1.

b) Todos los símbolos no contemplados en ajuste de Texto se suprimen.

## Ejercicio 2

a) **5x5:**
QT DT QT PS AD OR GU SH ON UL EG TK MK US AL AQ DE DK NS HG SI UT DK TQ ON AL AQ BL SB BL AU QU AO BG TM BP AL IK SM KT XA IR TO PL QA AF OT SI PH SB RY BQ TU OE KA HF HP LK NP HW TQ CH FT TG OT SI UA MT FZ CK CM OB HF VF OT HG HT EA NT OA YT AD UB TG HP HT QS DA RB OK ET NL EY BR XY XY YB DC MN FL PW PO QT UB YF CA NC OU OP QY UT VC HO EB CK SV FQ QA DK NS HO MT CM GB ST RO KA RA PI BO MB PH PQ UT DB DK HP SC TG AL TQ TZ TH GA IP TO VF TQ KB HS MB NV BS HT QL SV CK TQ OK WL BS AE SH NU XA ZT ST RO KA RA PI BO MB PQ UT OA GB KY MK OT NT OR QT HO PN CD PL RB ON MZ FA PL SI TN KQ OK KO QT PF BO KA PL QA KO ES BZ HS QS MB VS AL SV HK KY KT RA LN DE AD VF OT HG GT PF YT RB GM NT NI PI QU AO BG TM SV TH VF HC MB NU VS MT GD YT RB TM GM ZY

RE FE RE NC ES TU OM AS AU RM OD EL LI NG TH EN EX ED HA MS CH RO ED ER AU TH EN TI CA TI ON PR OT OC OL WI TH HI GH LE VE LP ET RI NE TS TE CH NI CA LR EP OR TB HE LS IN KI UN IV ER SI TY OF TE CH NO LO GY DI GI TA LS YS TE MS LA BO RA TO RY ES PO OF IN LA ND SE PT EM BE RH TX TP WX WX WT CS HU TF IP UB RE PO RT SB PS ZM BU RX RO WS MA BA DI AN DR NE ED HA MA LO GI CO FA UT HE NT IC AT IO NI NP RO CE ED IN GS OF TH ER OY AL SO CI ET YS ER IE SA IO HN AC LA RK AN DI ER EM YI AC OB AS UR VE YO FA UT HE NT IC AT IO NP RO TO CO LX LI TE RA TU RE MA NU SC RI PT AU GU ST RI CH AR DK EM ME RE RC AT HE RI NE ME AD OW SA ND IO NA TH AN MI LX LE NT HR EX ES YS

TE MS FO RC RY PT OG RA PH IC PR OT OC OL AN AL YS IS IO UR NA LO FC RY PT OL OG YX

No se recupera por completo en la matriz de 5x5 no están los números, ni símbolos especiales no los cifra y por tanto no los recuperamos.

**6x6:**

UB LF UB JH TA 7G WE JT AB VU NT FB PU PF MH OG OL SU BF CO PT DI WB BF BU EQ OG OL SG JC SG HW KX SO AH EN XH OG IC HI UF UT MJ TO XD LO OA OT DI PH JC KU SL BW OE Y7 FO PE HP PD WL GX BU IP A1 EH OT DI WH NE C1 FC HC OB PE 3A OT PT JE ES QB OS QZ TA NS EH HP JE KH AT MS TL ET VZ S3 46 GO SM XQ XQ VO IA FW EG PX RE UB NS VB AE Y7 XI 03 KT VU WB XO JT EB FC OJ KZ LO BF CO JT NE HC HA CE VE FO MO CD BO HS PH PJ WB FA BF HP IT EH OG BU A2 EJ AS DC TO 3A BU FS AB 8Y 70 98 23 93 Y3 T7 37 94 YP HN JO FJ BQ JB KH LA UB J1 QC HA EB EX UW A0 EH EQ OG OL SG JC SG HW KX SO AH EN PF OT QB EV UB JT LW AI XD MS EQ FV AO 37 47 5Q CD CO ZK LB PV LT UB QD BO FO XD LO LT BC H2 AB KH NA JO OG OJ PG PU UF MO DW SU TA 3A OT PT HE QD QZ MS TH QB NI CD KX SO AH EN OJ EJ 3A PI NA VU JO NE GD QZ MS EN TH 14 18 73 Y1 37 45

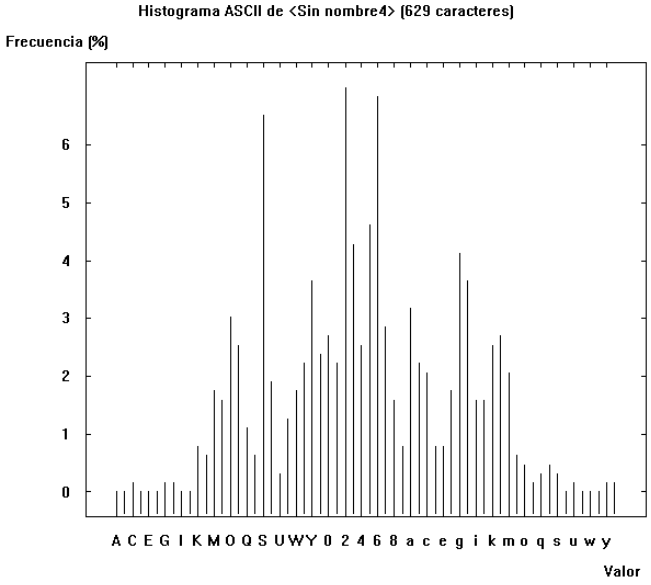
RE FE RE NC ES 1T UO MA SA UR MO DE LX LI NG TH EN EX ED HA MS CH RO ED ER AU TH EN TI CA TI ON PR OT OC OL WI TH HI GH LE VE LP ET RI NE TS TE CH NI CA LR EP OR TB 14 HE LS IN KI UN IV ER SI TY OF TE CH NO LO GY DI GI TA LS YS TE MS LA BO RA TO RY ES PO OF IN LA ND SE PT EM BE R1 9X 95 HT TP WX WX WT CS HU TF IP UB RE PO RT SB 14 PS Z2 MB UR RO WS MA BA DI AN DR NE ED HA MA LO GI CO FA UT HE NT IC AT IO NI NP RO CE ED IN GS OF TH ER OY AL SO CI ET YS ER IE SA 42 61 87 12 3X 32 71 19 89 3J OH NA CL AR KA ND JE RE MY JA CO BA SU RV EY OF AU TH EN TI CA TI ON PR OT OC OL LI TE RA TU RE MA NU SC RI PT AU GU ST 19 96 4R IC HA RD KE MX ME RE RC AT HE RI NE ME AD OW SA ND JO NA TH AN MI LX LE NT HR EX ES YS TE MS FO RC RY PT OG RA PH IC PR OT OC OL AN AL YS IS JO UR NA LO FC RY PT OL OG Y7 27 91 30 19 94

En este caso es posible recuperar los números, pero no los caracteres especiales como el punto, paréntesis, comillas <>, etc.

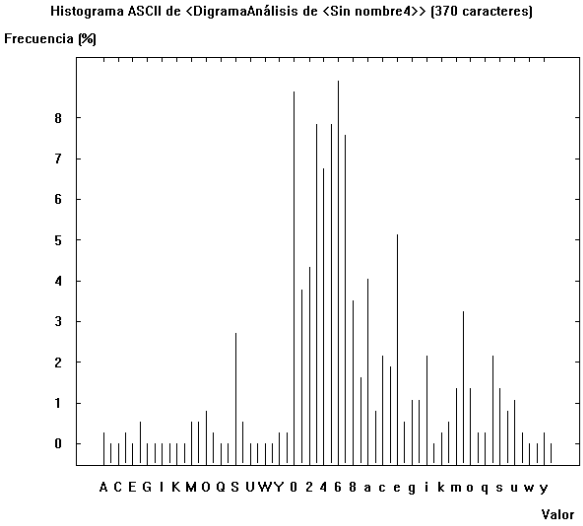
b) Se pone una X cuando en uno de los grupos aparecen dos letras iguales, pasa por ejemplo en la ll de Millen.

# Ejercicio 3

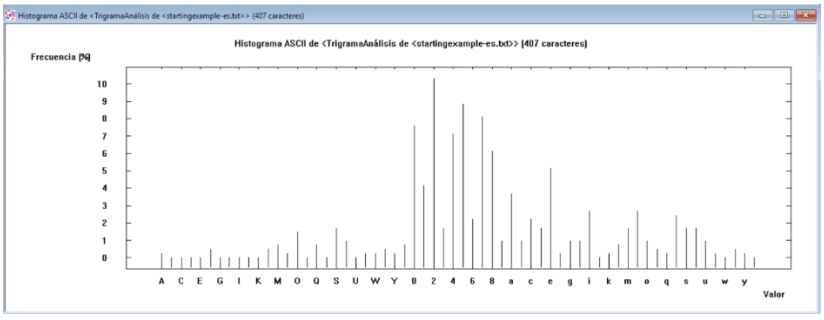
a) Instrucciones seguidas.
**b) Histograma:**




## Diagrama:




## Trigrama:



c) Nos permite saber las letras más frecuentes, de esta manera podemos saber analizando las letras más frecuentes en ingles cual corresponde con cada una de las del histograma. De esta manera podemos calcular la correspondencia.

d)

Cryptographic protocols are very difficult to design and implement correctly. Their correctness is crucial for the systems using their services, and therefore quite a lot of effort should be used to analyze their correctness. Finite-state analysis methods have been successfully used to verify hardware designs and communication protocols. However cryptographic protocols have some unique characteristics which make their analysis more difficult than that of normal protocols. The work done on applying finite-state analysis methods to cryptographic protocol verification is discussed. Special emphasis is put on the assumptions needed to enable finite-state analysis, and the limitations they introduce for the verification. November 27, 1998

e) Entropía del texto en claro, 4.25, y del texto cifrado, 5.16. Lo normal serie que la del texto cifrado fuese mayor, ya que desaparecerían las estructuras tan repetitivas del lenguaje, que hacen que sea menor la entropía.

## Ejercicio 4

Texto en castellano cifrado con sustitución monoalfabética:

03VTV UUV5B 4Q9BU B8V4Y BJ3VB VUUVE BOVLF BLBTY FUU9N BE9L9 YOVLA 9QVUU BQVY3 89UBT OFV4Q BTBO9 LF4B4 YVVTE VOB4Q 9J3VB U534V 4B49T VE3TF VTVV4 YOVUB TBUZV 4BTBQ BOTVB UL94B U534B YO9ZE VYBQV J3VUU V5BGB LBGBU UVO9B ULBTY FUU9E VO9L9 Z98F9 J3VTV YBOQB GB4NJ 3VO9L F4B4Y VTVQB GBEOF VTBE9 OUUV5 BOBUB LBGBU UVOFS BTVUU V59BU BE3VO YBQVU B8V4Y BN8F9 BUBTQ 9TQVT YOBFQ BTZ9S BTJ3V BUUFV TYBGB 4J3VB VUUVE BOVLF VO94Q 9TAVO Z9TBT Q94LV UUBT9 Q9T5O BLF9T BTQBZ BTJ3V QVUB4 YVQVU BE3VO YBQVU LBTYF UU9TV VTYBG B4T9U BSB4Q 9V4VT Y9T3L VQF9B LBT9J 3V34E 9OJ3V O9J3V B4QBG BOVL9 5FV4Q 9QV34 9TOBT YO9K9 T34B4 9ZGOV QVUEU B4VYB 3BZFU U94VT QVPFU 9ZVYO 9TBUT 9UZVO L3OF9 XC1WM WZFUU 94VTQ VPFU8 V43TX W7C2X WK3EF YVOM7 XCWWX 4VEY3 49CXX CMHH7 1ZB4B QBQVE 3VOL9 TJ3VT F4EVO Q94BT FTVUU BZB4Y 9L934 L3VO4 9BL3N BTVBU VUU9T TVOVL 95V4N BUF4T YB4YV TVUVO VEOVT V4Y9B Q94J3 FK9YV U9J3V QVTVB GBJ3V VOBJ3 VBU53 4V4B4 9ABLF BTVBU QVT38 V4FQB NBTFL 94VTY OB9L9 4YV4Y 9UUV5 9BUB8 V4YBN BUBTQ BZBTU BTL3B UVTL9 Z98FV O948V 4FO34 A9ZGO VQVBJ 3VUUB T3VOY VBOZB Q9NL9 4UB4S BNBQB O5BUU V4BTQ VZFVQ 9TVFG B4BV4 YOBOV 4UB8V 4YBEV O9Q94 J3FK9 YVL9U F5FV4 Q9E9O T3A3F QBT3Z FVQ9B USB4Q 9TVUB 8FTVO BQVEB EVU94 NQVTL 3GOFV 4Q9T3 TVL9N E9U89 O9T9O 9TYO9 L945V 4YFUY BUB4Y VN89S OVE9T BQBUV TQFK9

Proceso de descifrado:

Lo primero sabemos que es sustitución monoalfabética, por lo que se habrá usado Sustitución Monoalfabética Monográfica, Playfair y Hill. Como es el alfabeto completo, sin ñ, y con todos los números, son en total 36 posibles valores. El primer carácter será la A que valdrá 0.

Comenzamos por el primer método, probaremos los distintos valores de la constante de desplazamiento.

Desplazamiento puro: Probamos con los 36 (0-35) posibles desplazamientos, pero no nos arroja un texto que tenga sentido.

Decimación pura: Tampoco da resultados válidos.

Sustitución afín: Primero hallamos cuales son las letras que aparecen con más frecuencia en el texto cifrado, que son B, V y 9, para poderlas relacionar con las letras más frecuentes del castellano, que son A, E y O, y de esta manera averiguar aproximaciones al texto en claro. Habrá que hacer parejas de las letras frecuentes del cifrado y en claro, para poder hacer la prueba de correspondencia resolviendo una ecuación (C=a*M+b mod 36)

Primero probamos B-A y V-E:

1 = a*0+b mod 36 = b mod 36; b = 1.

21 = a*4+b mod 36 = 4a+1 mod 36;

4a= (21-1) mod 36 = 20 mod 36

Hallar a: 36= 4*9+0; mcd (4, 36) = 4 Habrá 4 soluciones.

Simplificamos 4|20: a= 5 mod 9

Las soluciones son: 5, 14, 23 y 32.

Las a y la b son coprimos. También debe ser invertible a para que pueda descifrarse, por lo que descartamos 14 y 32. No queda entonces: a= 5 o 23 y b= 1

Primer intento: a=5, b=1

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

0 1 2 3 4 5 6 7 8 9

26 27 28 29 30 31 32 33 34 35

Las letras se sustituyen: Se ha hecho manualmente el cálculo, se mete el correspondiente como clave en Cifrar/Descifrar/Simétrico/Sustitución…

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

BGLQV05AFKPUZ49EJOTY38DINSX27CHMRW16

Texto en claro:

FUESE LLEGA NDOAL AVENT AQUEA ELLEP ARECI ACAST ILLOY APOCO TRECH ODELL ADETU VOLAS RIEND ASARO CINAN TEESP ERAND OQUEA LGUNE NANOS EPUSI ESEEN TRELA SALME NASAD ARSEA LCONA LGUNA TROMP ETADE QUELL EGABA CABAL LEROA LCAST ILLOP EROCO MOVIO QUESE TARDA BANYQ UEROC INANT ESEDA BAPRI ESAPO RLLEG ARALA CABAL LERIZ ASELL EGOAL APUER TADEL AVENT AYVIO ALASD OSDES TRAID ASMOZ ASQUE ALLIE STABA NQUEA ELLEP ARECI EROND OSHER MOSAS DONCE LLASO

DOSGR ACIOS ASDAM ASQUE DELAN TEDEL APUER TADEL CASTI LLOSE ESTAB ANSOL AZAND OENES TOSUC EDIOA CASOQ UEUNP ORQUE ROQUE ANDAB ARECO GIEND ODEUN OSRAS TROJO SUNAN OMBRE DELPL ANETA UAMIL LONES DEKIL OMETR OSALS OLMER CURIO 03875 7MILL ONESD EKILV ENUS0 72310 7JUPI TER52 03770 NEPTU NO300 35442 8MANA DADEP UERCO SQUES INPER DONAS ISELL AMANT OCOUN CUERN OACUY ASEAL ELLOS SEREC OGENY ALINS TANTE SELER EPRES ENTOA DONQU IJOTE LOQUE DESEA BAQUE ERAQU EALGU NENAN OHACI ASEAL DESUV ENIDA YASIC ONEST RAOCO NTENT OLLEG OALAV ENTAY ALASD AMASL ASCUA LESCO MOVIE RONVE NIRUN HOMBR EDEAQ UELLA SUERT EARMA DOYCO NLANZ AYADA RGALL ENASD EMIED OSEIB ANAEN TRARE NLAVE NTAPE RODON QUIJO TECOL IGIEN DOPOR SUHUI DASUM IEDOA LZAND OSELA VISER ADEPA PELON YDESC UBRIE NDOSU SECOY POLVO ROSOR OSTRO CONGE NTILT ALANT EYVOZ REPOS ADALE SDIJO

# ENT

## Ejercicio 1

a) **doc**:
Entropy = 4.206582 bits per byte.

Optimum compression would reduce the size
of this 71680-byte file by 47 percent.

Chi square distribution for 71680 samples is 5041318.18, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 45.4639 (127.5 = random).
Monte Carlo value for Pi is 3.816842458 (error 21.49 percent).
Serial correlation coefficient is 0.540488 (totally uncorrelated = 0.0).

La entropía está lejos de ser la ideal, hay que observar el resto de pruebas, pero no parece aleatorio.
El índice aleatorio es malo, mucha información esta repetida por lo que la podría eliminar y no se notaría.
La chi-cuadrado es muy baja no es válida.
La media está lejos de ser 127.5.
Monte Carlo, los puntos no estarán distribuidos uniformemente, indica que no es aleatorio.
La correlación es alta, está demasiado ceca del 1, definitivamente no es aleatorio.

**c:**
Entropy = 4.846849 bits per byte.

Optimum compression would reduce the size
of this 7989-byte file by 39 percent.

Chi square distribution for 7989 samples is 158914.00, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 73.3497 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is 0.471176 (totally uncorrelated = 0.0).

NO es aleatorio
**jpeg:**
Entropy = 7.976906 bits per byte.

Optimum compression would reduce the size
of this 1344317-byte file by 0 percent.

Chi square distribution for 1344317 samples is 43454.94, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 129.2505 (127.5 = random).
Monte Carlo value for Pi is 3.115455341 (error 0.83 percent).
Serial correlation coefficient is 0.003607 (totally uncorrelated = 0.0).

Le entropía es bastante buena.
Este formato es bastante bueno, es aleatorio.

**gif:**
Entropy = 7.985225 bits per byte.

Optimum compression would reduce the size
of this 21602-byte file by 0 percent.

Chi square distribution for 21602 samples is 431.11, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 128.9456 (127.5 = random).
Monte Carlo value for Pi is 3.102222222 (error 1.25 percent).
Serial correlation coefficient is 0.013769 (totally uncorrelated = 0.0).

La entropía está muy cercana a la ideal, que es 8, no se pude reducir mas, la media falla un poco, Monte Carlo es aceptable y la correclacion cercana a 0.
Los resultados son bastante buenos, para casi todas las pruebas, pero además de la Media y Monte Carlo, la Chi cuadrado es muy mala. Por lo que no es aleatorio.

**bmp:**
Entropy = 6.898953 bits per byte.

Optimum compression would reduce the size
of this 75088-byte file by 13 percent.

Chi square distribution for 75088 samples is 763343.67, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 82.0634 (127.5 = random).

Monte Carlo value for Pi is 3.384689148 (error 7.74 percent).
Serial correlation coefficient is 0.026482 (totally uncorrelated = 0.0).

No aleatorio, la chi cuadrado da resultados muy malos.

b) Las imágenes han dado bastantes mejores resultados en lo referido a aleatoriedad, son archivos que tienen mucha menos información y más comprimibles. Sin embargo, las imágenes tienen mucha más información y dan mejores resultados aquellos formatos que no son comprimidos.

Doc. y c son poco aleatorios, dado que los archivos de texto contienen lenguaje que no es para nada aleatorio.

Jpeg, gif son bastante mas aleatorios, al tratarse de imágenes y no haber tanta redundancia, pero no podemos descartar que sean verdaderamente aleatorios.

Bmp da resultados que descartan por completo que sea aleatorio.

## Ejercicio 2

a) openssl rand [options] num: Genera un fichero aleatorio de núm. bits.

Options: [-out r1000 -rand FILE] El fichero de salida es r1000 y la semilla para el generador de números pseudoaleatorios se coge del fichero FILE (o de cualquier otro fichero). Con la misma semilla se generan resultados distintos.

R1000:
Entropy = 6.022706 bits per byte.

Optimum compression would reduce the size of this 1378-byte file by 24 percent.

Chi square distribution for 1378 samples is 4180.06, and randomly would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 83.2054 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is 0.161037 (totally uncorrelated = 0.0).

R1000000:
Entropy = 6.044381 bits per byte.

Optimum compression would reduce the size
of this 1375004-byte file by 24 percent.

Chi square distribution for 1375004 samples is 3958583.15, and randomly would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 83.3311 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is 0.114682 (totally uncorrelated = 0.0).

La diferencia entre ambos documentos es muy pequeña, lo importante es que la semilla original sea buena, no la cantidad de valores que extraigamos. Por muchos valores que generemos no mejorara, si no da lugar a buenas series de números.

## Ejercicio 3

a) Doc. comprimido .zip:
Entropy = 7.981167 bits per byte.

Optimum compression would reduce the size
of this 16898-byte file by 0 percent.

Chi square distribution for 16898 samples is 453.31, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 126.5527 (127.5 = random).
Monte Carlo value for Pi is 3.160511364 (error 0.60 percent).
Serial correlation coefficient is 0.018805 (totally uncorrelated = 0.0).

La entropía del comprimido es mucho más alta pasa de 4 a prácticamente perfecta, esto se debe a que cuando comprime elimina lo repetido y que es prescindible. Tras comprimir está limpio.

b) Doc. cifrado aes256:
Entropy = 7.997527 bits per byte.

Optimum compression would reduce the size
of this 71712-byte file by 0 percent.

Chi square distribution for 71712 samples is 245.85, and randomly
would exceed this value 64.81 percent of the times.

Arithmetic mean value of data bytes is 127.2822 (127.5 = random).
Monte Carlo value for Pi is 3.149933066 (error 0.27 percent).
Serial correlation coefficient is 0.004273 (totally uncorrelated = 0.0).

La entropía del original era pésima, pero tras cifrarlo es casi perfecta. Tanto que el original es muy probable que sea aleatorio y el original es casi seguro que no sea aleatorio. Mejora mucho al cifrar.

c) Ambos pesan 10 KB, esto se debe a como se puede ver en el apartado b el grado de compresión optimo es 0. Por lo que el tamaño se ha podido reducir un 0%.
La entropía cuando está cifrado y cuando es comprimido son muy buenas ya que ambos tienen un proceso que elimina las redundancias que haya, por ello ambos mejoran tanto del original. La original tenía entropía bastante mala y esto hacía que determináramos que no era aleatorio, sin embargo, cuando ciframos o comprimimos elimina todas las repeticiones, dando un resultado casi perfecto.