**Laboratorio 1**

**Criptografía y**

**Seguridad Informática**

Jorge Rodríguez Fraile, 100405951

# CrypTool

## Ejercicio 1

1. **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 si 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.

1. .

## Ejercicio 2

1. **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

**6x6:**

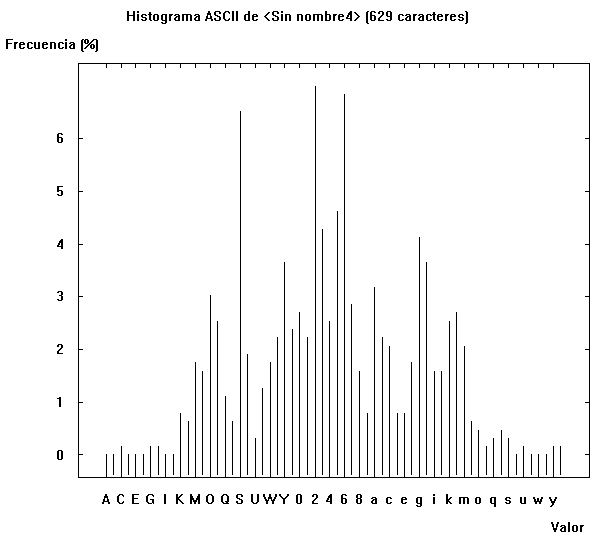
UB LF UB JH TA 7G WE JT AB VU NT FB PU PF MH OG OL SU BF CO PT DI WB BF BU EQ OG OL SG JC SG HW KX SO AH EN XH OG IC HI UF UT MJ TO XD LO OA OT DI PH JC KU SL BW OE Y7 FO PE HP PD WL GX BU IP A1 EH OT DI WH NE C1 FC HC OB PE 3A OT PT JE ES QB OS QZ TA NS EH HP JE KH AT MS TL ET VZ S3 46 GO SM XQ XQ VO 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

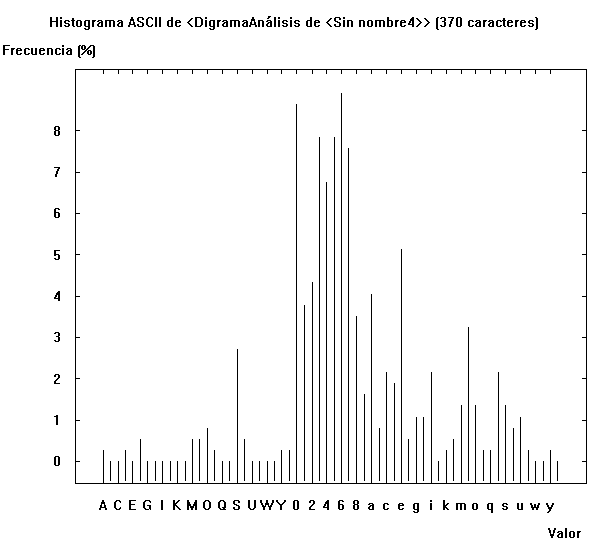
1. .

## Ejercicio 3

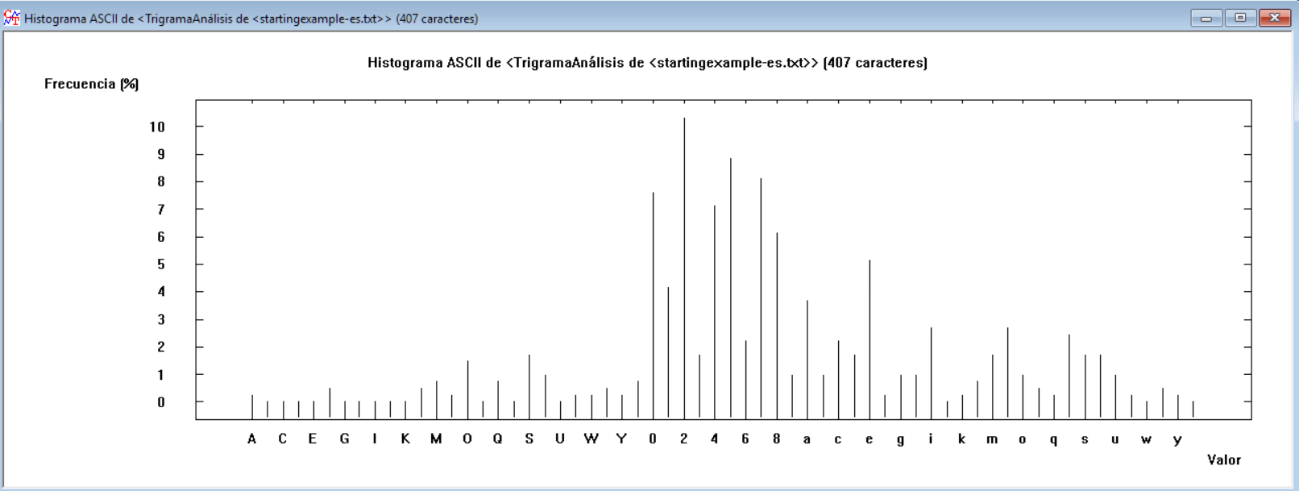
1. **Histograma:**



**Diagrama:**



**Trigrama:**



1. .
2. 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.

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

1. Entropía 4.25.

## Ejercicio 4

# ENT

## Ejercicio 1

1. **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 esta 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 esta 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 esta muy cercana a la ideal, que es 8.

Los resultados son bastante buenos, para todas las pruebas, por lo que 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).

XXXXXXXXXXXXXXX

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

Doc y c no son poco aleatorios.

Jpeg, gif son bastante aleatorios.

Bmp da resultados que aparentemente parece que es aleatorio.

## Ejercicio 2

1. 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

1. 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 mas 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.

1. 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.

1. 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 esta 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.