Parte 1

Comando ENT

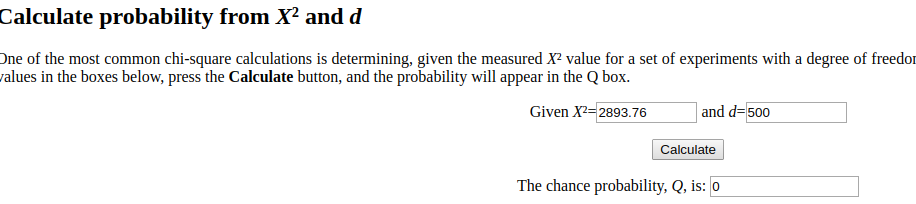
./ent -t /home/axxa/Documents/DEV/git/uc3m-Blockchain/bulk\_direcciones\_bitcoin.xlsx

Salida ENT

Caso 1:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File-bytes | Entropy | Chi-square | Mean | Monte-Carlo-Pi | Serial-Correlation |
| 47542 | 7.960456 | 2893.769299 | 130.024126 | 3.066515 | 0.023483 |

* Entropia de 7.9 que segun la documentacion indica que el fichero cuenta con 7.9 bits por caracter por lo cual tiene una alta densidad en informacion y se podria clasificar como una generacion de direccion-llave con una aletoriedad importante
* Chi-cuadrado de 2893.76 indicando que con una muestra de 500 hay una probabilidad de 0% de generar un valor igual, lo cual podria demostrar su capacidad de generar valores aleatorios.



* La media aritmetica resulta de sumar todos los bytes y dividirlos por el tamanio del fichero. Para este caso la media tiene un valor de 130 lo cual determina que la data esta cercana a ser aleatoria.
* 3.06 para la medida de monte carlo pi que se acerca a PI con una diferencia de 0.08 que establece una aleatoriedad suficiente.
* Para la correlacion serial obtenemos 0.02 el cual es un valor cercano a 0 y con el cual podriamos concluir que la generacion aleatoria de tuplas direccion-llave cuenta con una aletoriedad notable dentro de todas las medidas aca tomadas.

Ejecutando ent con una billetera generada con encriptacion tipo BIP38 tenemos los siguientes valores:

Caso 1.1:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File-bytes | Entropy | Chi-square | Mean | Monte-Carlo-Pi | Serial-Correlation |
| 49046 | 7.964125 | 2705.199119 | 129.998369 | 3.077563 | 0.027915 |

Exceptuando la serial correlation podemos decir que la aleatoriedad de estas tuplas se comporta mejor que generar la billetera sin encriptacion BIP38 debido a que la entropia es ligeramente mayor, chi-cuadrado se mantiene en 0%, la media aritmetica tiene menor distancia respecto a 127.5, y monte carlo pi esta mas cercano al valor de PI.

Parte 2

Se genera un fichero con una secuencia de numeros pseudo aleatoria con openssl

El fichero contiene una muestra con 312500 numeros

Caso 2:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File-bytes | Entropy | Chi-square | Mean | Monte-Carlo-Pi | Serial-Correlation |
| 5000000 | 7.999966 | 236.943462 | 127.461057 | 3.141452 | 0.000248 |

En este caso entropia nos indica una densidad mayor al anterior ejemplo. El chi-cuadrado seniala una probabilidad del 0.99% de generar una discrepancia, pero en caso contrario la media aritmetica tiene un valor muy cercano a 127,5 el cual considera una aleatoriedad mejor al caso 1 y junto con monte carlo pi y la correlacion serial que dio mejores resultados.

Por tanto y si dejaramos de lado la metrica de chi-square podriamos decir que el caso 2 da una mayor aleatoriedad que el caso 1

Utilizando el generador de hotbits:

El fichero contiene una muestra con 128 numeros

Caso 2.1:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File-bytes | Entropy | Chi-square | Mean | Monte-Carlo-Pi | Serial-Correlation |
| 2048 | 7.930864 | 200.5 | 129.452637 | 3.026393 | -0.001077 |

Este caso cuenta con la menor entropia de los demas, lo que seniala una menor aleatoriedad, pero le fue mejor con chi-cuadrado con una probabilidad del 0% de generar discrepancia. Para la media aritmetica aunque mejor que los casos 1, esta por debajo del caso 2 y cuenta con la metrica de monte carlo mas baja.

Caso 2.2:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File-bytes | Entropy | Chi-square | Mean | Monte-Carlo-Pi | Serial-Correlation |
| 2048 | 7.901284 | 271.25 | 126.242676 | 3.214076 | -0.007434 |

Conclusiones



Considerando que todas las metricas tienen el mismo peso de importancia para evaluar la aleatoriedad de un algoritmo, podriamos concluir que la solucion que mas representa aletoriedad dentro de las demas es la de openssl debido a que establece el mayor numero de metricas con mayor valor. Por otro lado el algoritmo de generacion de billeteras bitcoin (Caso 1) representa el mas deficiente dentro de los 5 casos.

Ataques a hash

INFO: All hashes found in potfile! Use --show to display them.

Started: Thu Apr 9 15:15:11 2020

Stopped: Thu Apr 9 15:15:11 2020

axxa@axxa:~/Documents/DEV/git/uc3m-Blockchain/practica1/parte3$ hashcat --force -m 0 -a 0 md5hash\_in\_dict.txt rockyou.txt --show

38008dd81c2f4d7985ecf6e0ce8af1d1:Spring

hashcat --force -m 0 -a 0 md5hash\_not\_in\_dict.txt rockyou.txt

Session..........: hashcat

Status...........: Exhausted

Hash.Type........: MD5

Hash.Target......: 02edbe757416310369078cf7e9aac4a5

Time.Started.....: Thu Apr 9 15:17:21 2020 (2 secs)

Time.Estimated...: Thu Apr 9 15:17:23 2020 (0 secs)

Guess.Base.......: File (rockyou.txt)

Guess.Queue......: 1/1 (100.00%)

Speed.Dev.#1.....: 7474.6 kH/s (0.52ms)

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 14344387/14344387 (100.00%)

Rejected.........: 0/14344387 (0.00%)

Restore.Point....: 14344387/14344387 (100.00%)

Candidates.#1....: km81088 -> clarus

HWMon.Dev.#1.....: N/A

Started: Thu Apr 9 15:17:20 2020

Stopped: Thu Apr 9 15:17:23 2020

------------------------------------------------------------BRUTE FORCE

hashcat --force -m 100 -a 3 sha1hash\_not\_in\_dict.txt

Session..........: hashcat

Status...........: Exhausted

Hash.Type........: SHA1

Hash.Target......: 20a1ad8d21dcddc5e25cec62f8ec9012155b847b

Time.Started.....: Thu Apr 9 18:13:26 2020 (3 secs)

Time.Estimated...: Thu Apr 9 18:13:29 2020 (0 secs)

Guess.Mask.......: ?1?2?2?2?2 [5]

Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d\*!$@\_, -4 Undefined

Guess.Queue......: 5/15 (33.33%)

Speed.Dev.#1.....: 45477.6 kH/s (5.30ms)

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 104136192/104136192 (100.00%)

Rejected.........: 0/104136192 (0.00%)

Restore.Point....: 1679616/1679616 (100.00%)

Candidates.#1....: 6f7qx -> Xqxvq

HWMon.Dev.#1.....: N/A

Session..........: hashcat

Status...........: Quit

Hash.Type........: SHA1

Hash.Target......: 20a1ad8d21dcddc5e25cec62f8ec9012155b847b

Time.Started.....: Thu Apr 9 18:13:29 2020 (37 secs)

Time.Estimated...: Thu Apr 9 18:14:45 2020 (39 secs)

Guess.Mask.......: ?1?2?2?2?2?2 [6]

Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d\*!$@\_, -4 Undefined

Guess.Queue......: 6/15 (40.00%)

Speed.Dev.#1.....: 48986.6 kH/s (10.54ms)

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 1796079616/3748902912 (47.91%)

Rejected.........: 0/1796079616 (0.00%)

Restore.Point....: 802816/1679616 (47.80%)

Candidates.#1....: 28dhy7 -> hsq0b3

HWMon.Dev.#1.....: N/A

hashcat --force -m 100 -a 3 sha1hash\_in\_dict.txt

axxa@axxa:~/Documents/DEV/git/uc3m-Blockchain/practica1/parte3$ hashcat --force -m 100 -a 3 sha1hash\_in\_dict.txt --show

89677615c2ec030bc5542abbacb5c286b12096fe:Spring

hashcat --force -m 0 -a 3 md5hash\_in\_dict.txt

hashcat --force -m 0 -a 3 md5hash\_not\_in\_dict.txt

Session..........: hashcat

Status...........: Running

Hash.Type........: MD5

Hash.Target......: 02edbe757416310369078cf7e9aac4a5

Time.Started.....: Thu Apr 9 18:08:27 2020 (2 mins, 14 secs)

Time.Estimated...: Thu Apr 9 18:30:24 2020 (19 mins, 43 secs)

Guess.Mask.......: ?1?2?2?2?2?2?2 [7]

Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d\*!$@\_, -4 Undefined

Guess.Queue......: 7/15 (46.67%)

Speed.Dev.#1.....: 102.6 MH/s (10.09ms)

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 13531742208/134960504832 (10.03%)

Rejected.........: 0/13531742208 (0.00%)

Restore.Point....: 167936/1679616 (10.00%)

Candidates.#1....: nclwrke -> zcl65ho

HWMon.Dev.#1.....: N/A

Session..........: hashcat

Status...........: Running

Hash.Type........: MD5

Hash.Target......: 02edbe757416310369078cf7e9aac4a5

Time.Started.....: Thu Apr 9 18:08:27 2020 (2 mins, 43 secs)

Time.Estimated...: Thu Apr 9 18:30:34 2020 (19 mins, 24 secs)

Guess.Mask.......: ?1?2?2?2?2?2?2 [7]

Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d\*!$@\_, -4 Undefined

Guess.Queue......: 7/15 (46.67%)

Speed.Dev.#1.....: 101.8 MH/s (10.17ms)

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 16469721088/134960504832 (12.20%)

Rejected.........: 0/16469721088 (0.00%)

Restore.Point....: 204800/1679616 (12.19%)

Candidates.#1....: 3qawebr -> Cis6evy

HWMon.Dev.#1.....: N/A

Session..........: hashcat

Status...........: Quit

Hash.Type........: MD5

Hash.Target......: 02edbe757416310369078cf7e9aac4a5

Time.Started.....: Thu Apr 9 18:08:27 2020 (2 mins, 57 secs)

Time.Estimated...: Thu Apr 9 18:30:36 2020 (19 mins, 12 secs)

Guess.Mask.......: ?1?2?2?2?2?2?2 [7]

Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d\*!$@\_, -4 Undefined

Guess.Queue......: 7/15 (46.67%)

Speed.Dev.#1.....: 101.6 MH/s (10.19ms)

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 17898405888/134960504832 (13.26%)

Rejected.........: 0/17898405888 (0.00%)

Restore.Point....: 221184/1679616 (13.17%)

Candidates.#1....: T0geh72 -> Q0gz2en

HWMon.Dev.#1.....: N/A

Started: Thu Apr 9 18:07:43 2020

Stopped: Thu Apr 9 18:11:25 2020