Parte 1: Aleatoriedad

Comando ENT

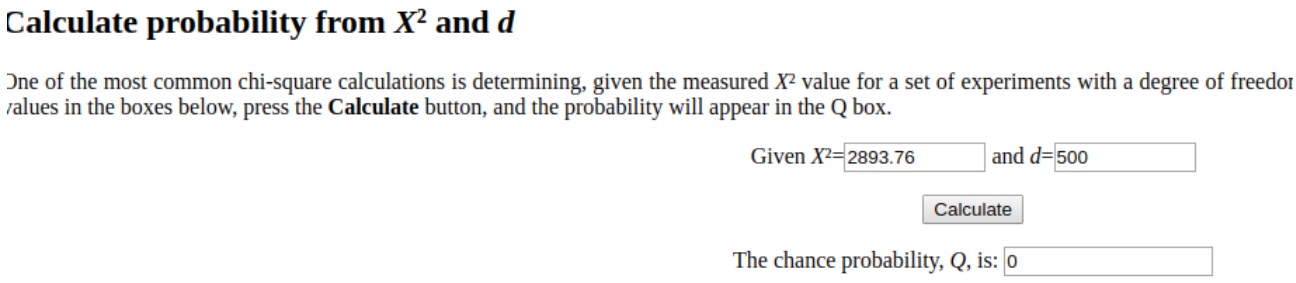
./ent -t /home/axxa/Documents/DEV/git/uc3m-Blockchain/bulk_direcciones_bitcoin.xlsx

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

- entropía de 7.9 que según la documentación indica que el fichero cuenta con 7.9 bits por carácter por lo cual tiene una alta densidad en información y se podría clasificar como una generación de dirección-llave con una aleatoriedad 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 podría demostrar su capacidad de generar valores aleatorios.



- La media aritmética resulta de sumar todos los bytes y dividirlos por el tamaño 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 correlación serial obtenemos 0.02 el cual es un valor cercano a 0 y con el cual podríamos concluir que la generación aleatoria de tuplas dirección-llave cuenta con una aleatoriedad notable dentro de todas las medidas acá tomadas.

Ejecutando ent con una billetera generada con encriptación 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 el serial correlation podemos decir que la aleatoriedad de estas tuplas se comporta mejor que generar la billetera sin encriptación BIP38 debido a que la entropía es ligeramente mayor,

chi-cuadrado se mantiene en 0%, la media aritmetica tiene menor distancia respecto a 127.5, y monte carlo pi esta más cercano al valor de PI.

Parte 2: Aleatoriedad con números pseudo aleatorios

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 entropía nos indica una densidad mayor al anterior ejemplo. El chi-cuadrado señala una probabilidad del 0.99% de generar una discrepancia, pero en caso contrario la media aritmética 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 correlación serial que dio mejores resultados.

Por tanto y si dejamos de lado la métrica 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 números

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 entropía de los demás, lo que señala una menor aleatoriedad, pero le fue mejor con chi-cuadrado con una probabilidad del 0% de generar discrepancia. Para la media aritmética aunque mejor que los casos 1, esta por debajo del caso 2 y cuenta con la métrica de monte Carlo más 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

fuente	File-bytes	Entropy	Chi-square	Mean	Monte-Carlo-Pi	Serial-Correlation
bitcoin	47542	7.960456	2893.769299	130.024126	3.066515	0.023483
bitcoin bip38	49046	7.964125	2705.199119	129.998369	3.077563	0.027915
openssl	5000000	7.999966	236.943462	127.461057	3.141452	0.000248
hotbits	2048	7.930864	200.5	129.452637	3.026393	-0.001077
hotbits apikey	2048	7.901284	271.25	126.242676	3.214076	-0.007434

Considerando que todas las métricas tienen el mismo peso de importancia para evaluar la aleatoriedad de un algoritmo, podemos concluir que la solución que más representa aleatoriedad dentro de las demás es la de openssl debido a que establece el mayor número de métricas con mayor valor. Por otro lado, el algoritmo de generación de billeteras bitcoin (Caso 1) representa el mas deficiente dentro de los 5 casos.

Parte 3: Ataques a hash

Se ejecutan ataques de tipo diccionario y fuerza bruta para los algoritmos sha1 y md5 y como resultado se puede concluir que para el caso del diccionario si el archivo que utilizamos como diccionario es lo suficientemente completo se puede llegar a crackear el hash sin importar el tipo de algoritmo utilizado ya que hashcat se encargara de aplicar el hash correspondiente a cada palabra del diccionario y la comparara con el hash objetivo. En el caso de ataques de tipo fuerza bruta podemos señalar que su apalancamiento radica en la potencia de la GPU ya que efectúa un hash por cada combinación alfanumérica hasta que el hash generado coincida con el hash objetivo. Adicional a esto también se puede concluir el por que es de vital importancia que las credenciales no deben contener palabras sino un código alfanumérico.

hashcat --force -m 100 -a 0 sha1hash_in_dict.txt rockyou.txt

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 5 secs

89677615c2ec030bc5542abbacb5c286b12096fe:Spring

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: SHA1
Hash.Target.....: 89677615c2ec030bc5542abbacb5c286b12096fe
Time.Started.....: Thu Apr 9 07:35:46 2020 (2 secs)
Time.Estimated...: Thu Apr 9 07:35:48 2020 (0 secs)
Guess.Base.....: File (rockyou.txt)

Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....:   107.8 kH/s (2.33ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 189440/14344385 (1.32%)
Rejected.....: 0/189440 (0.00%)
Restore.Point....: 188416/14344385 (1.31%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: becky21 -> Santana1

Started: Thu Apr 9 07:35:36 2020
Stopped: Thu Apr 9 07:35:50 2020

---

hashcat --force -m 100 -a 0 sha1hash_not_in_dict.txt rockyou.txt

Session.....: hashcat
Status.....: Running
Hash.Type.....: SHA1
Hash.Target.....: 20a1ad8d21dcddc5e25cec62f8ec9012155b847b
Time.Started.....: Thu Apr 9 07:43:56 2020 (14 secs)
Time.Estimated...: Thu Apr 9 07:44:45 2020 (35 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....:   292.1 kH/s (2.19ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 4046848/14344385 (28.21%)
Rejected.....: 0/4046848 (0.00%)
Restore.Point....: 4046848/14344385 (28.21%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: sakinah3sa -> sajuti

Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: SHA1
Hash.Target.....: 20a1ad8d21dcddc5e25cec62f8ec9012155b847b
Time.Started.....: Thu Apr 9 07:43:56 2020 (49 secs)
Time.Estimated...: Thu Apr 9 07:44:45 2020 (0 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....:   248.2 kH/s (2.24ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]

Started: Thu Apr 9 07:43:50 2020
Stopped: Thu Apr 9 07:44:47 2020

hashcat --force -m 0 -a 0 md5hash_in_dict.txt rockyou.txt

axxa@axxa:~/Documents/DEV/git/uc3m-Blockchain/practica1/parte3$ hashcat --force -m 0 -a 0 md5hash_in_dict.txt rockyou.txt
hashcat (v4.0.1) starting...

OpenCL Platform #1: The pocl project
==========
* Device #1: pthread-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 4096/13847 MB allocatable, 8MCU

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

En este caso de fuerza bruta, se efectúan cientos de búsquedas combinando caracteres como se puede ver en lo resaltado en amarillo

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_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