CAST-256

EL EFECTO AVALANCHA

Melero Chaves, Daniel v130229

SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN | 02/11/2015

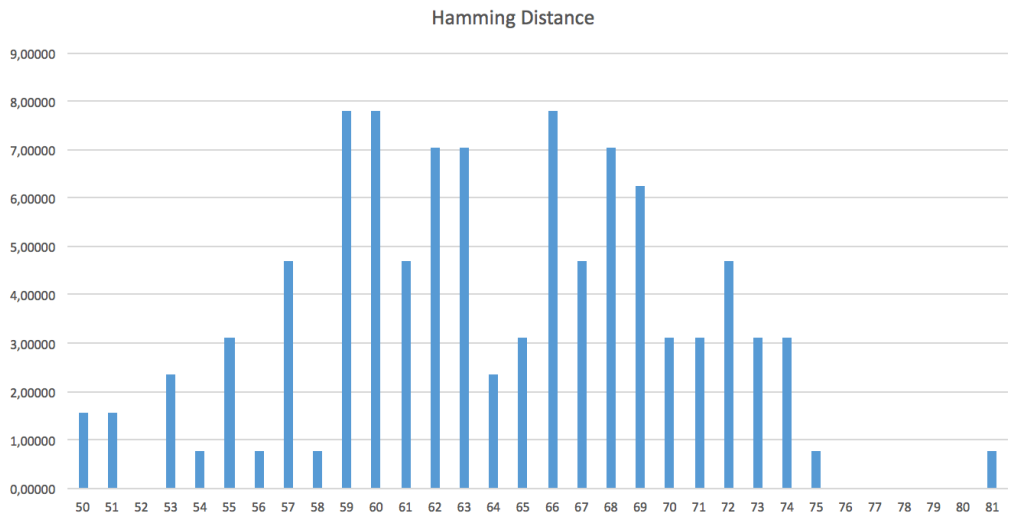
Estudio del efecto avalancha en el método de cifrado CAST-256

Para poder realizar el estudio del efecto avalancha sobre el CAST-256 lo primero que he realizado ha sido informarme y comprender el modo de funcionamiento que lleva a cabo dicho método de cifrado, para posteriormente realizar dicho estudio. Para calcular el efecto avalancha, que consisten en medir como se propaga el cambio de un simple bit de la entrada sobre los resultados que se obtienen a la salida del método de cifrado, adjunto un código que he creado a partir de otros códigos encontrados por internet.

Para comprobar que el código era funcional, encontré varios vectores de prueba para el método de cifrado y de esta manera afirmar el correcto funcionamiento del código. En el código adjunto se encuentra escrito uno de dichos vectores.

Los argumentos que necesita el CAST-256 son bloques de texto en claro de 128 bits y claves de 128, 160, 192, 224 o 256 bits. Dado que los vectores de prueba son de 128 bits de texto y 128 bits de clave, he optado por realizar el estudio con estos tamaños. El tamaño de muestras que he empleado es todo el rango del método, es decir, he usado 128 vectores de 128 bits cada uno modificando solo un bit para que el estudió fuera lo más completo y exacto posible. La ventaja es que al tener un código para realizar el estudio puedes automatizar el proceso para cualquier número de vectores a usar.

En la siguiente imagen adjuntada se puede apreciar el calculo de las distancias de Hamming para las salidas del cifrador. En el eje de abscisas se encuentran las distancias de Hamming, en las que solo se ven reflejado los datos del intervalo 50 a 81 ya que es en este intervalo donde se encuentran todas las distancias de Hamming distintas de cero y en el eje de ordenadas el porcentaje de aparición de dichas distancias Hamming en relación a los 128 vectores usados.



A partir del histograma obtenido, pasamos al calculo de los siguientes valores estadísticos (media, moda, varianza y desviación). Dichos cálculos se han realizado en el código adjunto menos la moda.

La media se calcula realizando el sumatorio de todas las distancias de Hamming y dicho sumatorio se divide por el número de pruebas realizadas.
La moda es la distancia de Hamming con mayor porcentaje de aparición.
La varianza se calcula realizando el sumario de la distancia de Hamming menos la media y todo ello elevado al cuadrado y posteriormente se divide por el número de pruebas realizadas.
La desviación se calcula realizando la raíz cuadrada de la varianza.

- Media: 63.984375
- Moda: 59, 60 y 66
- Varianza: 68.85913276672363
- Desviación: 8.298140319777898

Tanto los resultados de las distancias de Hamming como los cálculos de los valores estadístico se encuentran plasmados en el fichero "resultados.txt" que a su vez también muestra la salida por pantalla que realiza el programa con el que he llevado a cabo la realización de este estudio.

Sabiendo que un oráculo aleatorio es un heurística que genera secuencias aleatorias y uniformemente distribuidas, si nuestro método de cifrado se comportase como un oráculo aleatorio la distancia media de Hamming se consideraría la mitad de los bits de entrada que usa dicho método, en este caso, como en el CAST-256 se usan 128 bits de entrada la distancia de Hamming que se obtendría si este método funcionara como un oráculo aleatorio sería de 64, es decir, de 64 bits diferentes de la entrada.

Se puede ver por los resultado reflejados en el histograma que el CAST-256 las distancias medias de Hamming se encuentran englobadas, con mayor porcentaje de aparición, en el intervalo 59 a 69 bits diferentes, como el valor 64 se encuentra centro de este intervalo se puede asumir que el CAST-256 se asemeja al funcionamiento de un oráculo aleatorio.

La conclusiones de haber realizado dicho estudio son las siguientes:

- Se puede considerar la posibilidad de que el CAST-256 sea un buen método de cifrado ya que se asemeja bastante al funcionamiento de un oráculo aleatorio cuando se modifica un único bit del mensaje en claro.
- Viendo las distancias de Hamming que se generan con el espacio de muestra que he elegido, que supongo significativo, podemos ver que se trata de un cifrador que va a cifrar mostrando muy poca correlación entre la entrada y la salida, y por lo tanto es muy recomendable desde el punto de vista estadístico.

Referencias

1. https://es.wikipedia.org/wiki/Modelo_de_oráculo_aleatorio
2. http://stackoverflow.com/questions/16260752/using-for-loop-to-get-the-hamming-distance-between-2-strings
3. http://tools.ietf.org/html/rfc2612#page-10
4. http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html
5. http://stackoverflow.com/questions/17972024/java-bouncycastle-cast6engine-cast-256-encrypting
6. http://stackoverflow.com/questions/17943277/java-encryption-cast-256
7. http://stackoverflow.com/questions/9246326/convert-hexadecimal-string-hex-to-a-binary-string
8. https://es.wikipedia.org/wiki/Varianza
9. https://es.wikipedia.org/wiki/Desviación_t%C3%ADpica