SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

AES-128

47283630T

Carlos Navas López

090169

Nº de trabajo: 1

INTRODUCCIÓN

AES (Advanced Encryption Standard), también conocido como Rijndael, es un cifrado por bloques desarrollado por dos criptólogos belgas: Joan Daemen y Vincent Rijmen. En el año 2000, Rijndael ganó el concurso del NIST para convertirse en el algoritmo estándar de cifrado (AES). En noviembre de 2001 se publicó en el FIPS (Estándar Federal de Procesamiento de la Información) 197 donde se asumía oficialmente.

DESARROLLO

Durante la realización de la práctica se va a utilizar el siguiente cifrador de aes128[1] (en el modo CBC) que obtiene resultados satisfactorios con los vectores de prueba de su especificación[2].

He realizado una implementación en Javascript del grueso de la práctica (con la que se van a realizar los siguientes pasos), que puede ser descargada y probada en la siguiente url[3].

El programa está documentado, pero como resumen su funcionamiento es el siguiente:

1- Recibe una o más strings generadas de manera aleatoria (en mi caso generadas aquí) [4]
2- Partimos la string de 63 caracteres en 3 partes de 16 caracteres. Los primeros 16 para el texto a cifrar, los siguientes 16 para el vector de inicialización IV, los siguientes 16 para la clave y el resto se deshecha.
3- Se realiza la conversión a bytes para el cifrador y a bits para las modificaciones que serán necesarias en el paso 4.
4- Se generan n * 3 números aleatorios entre 0 y 127 (a elección del usuario, en mi caso de prueba 100). Los n primeros los usaremos para determinar el bit a modificar del texto. Los n siguientes para modificar el IV y los n últimos para la clave. Para generarlos utilizaremos la siguiente función[5]
5- Se realizan todas las operaciones de cifrado correspondientes y se calculan los datos necesarios.
6- Se imprimen los datos por pantalla y se genera un histograma.

Las siguientes cadenas (de 63 caracteres, usadas como se explica en el punto 3) han sido elegidas como base para realizar a partir de cada una de ellas las modificaciones. A partir de estos datos, podemos empezar a realizar los cálculos.

bmaQtwo6uf0hWVVHsJnZOdi90U8EZZtgkCSMPD20oDfrjnqtRmKi3yHiw46YuFW

dufWrSjAkgaVPXsAM0YfrcWRqTfbi332pqrDmRyvDpxomLZzJTIcepZOtAYe9Rt

TGgeW7f0v0ebbknQ9TbMtqeFpNqfBzIli7Pvxv4kmzzapiNNjMuV4glySz4S75X

ISeeuFBcnKagX9MJIwQGyK5ZLhw5ydnhxYdZ5gJFHAk5AEdDMtf1CZnZQV5Qju6

1FGIHbhBtwocZYZrzs4UQ6cQJHlDSRnoJw03QI6MJiZijyvczzqRKoL9YTTtmv8

ntVPv6PtdVKGUBWWluSfEyBo44SlmF75PQx8vru0Xw5zoWREpgchWlAYy5xrWJy

FierLyVMZfkLjVV6RmpZuZMUSUouqaWw0w6RexwkbxAVOwougnnhjddUjk6AlON

glssiwUQlXoaWvq2inTkyCMIa4aTi5OBpGTmHGMOEImH2zhmD1SitkV6ssLcYOT

A0W766lVILz9L2TzRiYnpc8qoG4oZcW4g79DqxZAQqxH27YEpiztorJIcp1tFXr

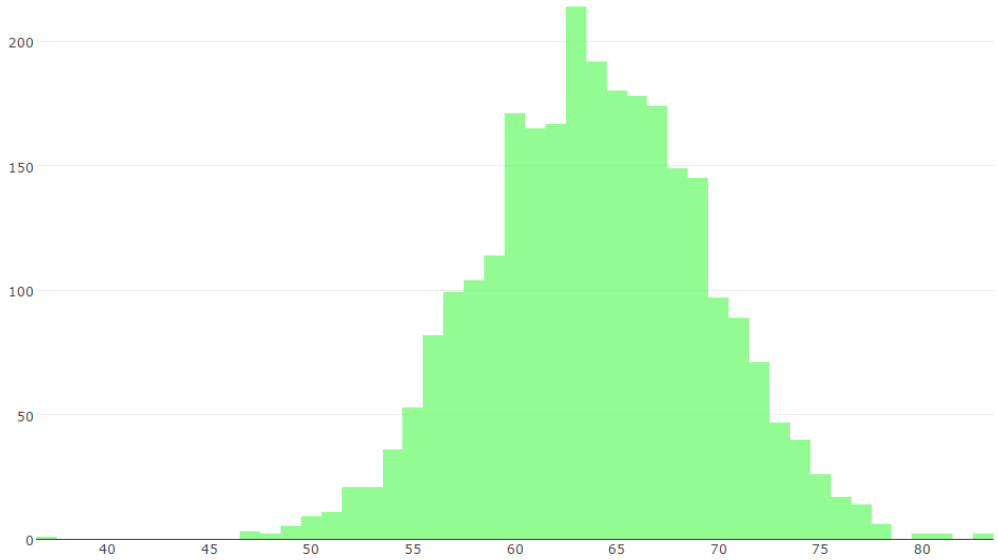
sx787frDXNusxJXa9J2f8GPNpaQjgsNTBsGgtkyGhg7ztN4iXVnK3vY9sUoZbzM

xsk8ICQK7MScUZovRKtRzaEw2wbnk1HVC35srTZMQCxgu7uixcoGvax1FNGwx6N

TIko4CNmEFydq1ZZcS0INUfXfGiQrPWtWXJI6IDa1cvVHD2MwRIfkOwVPx9GQo3

Q57wkPhW4BcXVlGQVf1X8yMoCSHjDYq3MyPSO81byBCn5o2pj04jmSFoLMZftij

Aquí tenemos el histograma:



Cálculo de valores estadísticos:

Los valores calculados han sido los siguientes:

- Moda: 63 (valor más repetido de las muestras)
- Media: 64.06 (Suma de todos los valores dividido entre el número de muestras)
- Desviación estándar: 5.50 (Raíz cuadrada del sumatorio del resultado de restar cada uno de los valores de la muestra con la media y elevarlos al cuadrado dividido entre el número de elementos menos uno)
- Incertidumbre: 0.10 (Dividir la desviación estándar o típica entre la raíz cuadrada del número de elementos de la muestra)

Con las muestras que he empleado, obtengo que la incertidumbre es de un 10%. Por ello podemos decir que el número de pruebas realizado es suficiente, pero si utilizáramos más cadenas obtendríamos un resultado mas preciso.

Los valores anteriores, en caso de un Oráculo Aleatorio perfecto serían los siguientes:

- Moda: 64 (Ya que todos los valores serían 64 debido a que ningún carácter se repetiría)
- Media: 64
- Desviación estándar: 0 (Debido a que todos los valores son iguales)
- Incertidumbre: 0 (Depende directamente de la desviación estándar)

Con estos datos, puedo decir que el cifrado AES-128 en su variante CBC puede equipararse con un oráculo aleatorio, pero no con un oráculo aleatorio perfecto.

BIBLIOGRAFÍA

1. https://github.com/ricmoo/aes-js
2. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf
3. https://github.com/Navas23/PracticaSTI
4. https://www.grc.com/passwords.htm
5. https://developer.mozilla.org/en-US/docs/Web/API/RandomSource/getRandomValues
6. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard