



Práctica 2: Seguridad Perfecta y Criptografía Simétrica

27 de octubre de 2016

Índice

| | | |
|----|---|---|
| 1. | Seguridad Perfecta | 1 |
| a. | Comprobación empírica de la Seguridad Perfecta del cifrado de desplazamiento: . . | 1 |
| 2. | Implementación del DES | 2 |
| a. | Programación del DES | 2 |
| b. | Programación del Triple DES (OPCIONAL) | 3 |
| 3. | Principios de diseño del DES | 3 |
| a. | Estudio de la no linealidad de las S-boxes del DES | 3 |
| b. | Estudio del Efecto de Avalancha | 3 |
| c. | Estudio de los criterios SAC y BIC (OPCIONAL) | 3 |
| d. | Construcción de <i>S-boxes</i> propias (OPCIONAL) | 3 |
| 4. | Principios de diseño del AES | 4 |
| a. | Estudio de la no linealidad de las S-boxes del AES | 4 |
| b. | Generación de las S-boxes AES (OPCIONAL) | 4 |
| c. | Programación del AES (OPCIONAL) | 4 |

Resumen

El objetivo de esta práctica es la familiarización con los conceptos de seguridad perfecta, entropía y con los métodos de cifrado simétrico tomando como referencia el *Data Encryption Standard (DES)* y el *Advanced Encryption Standard (AES)*. Para ello se procederá a su implementación y al estudio de diversos elementos básicos de su estructura.

Introducción

Se deberá elaborar una memoria sobre la práctica (en un fichero en formato pdf) que explique detalladamente la realización de todos los apartados con todos sus resultados correspondientes. En la memoria se podrá integrar el código necesario para entender la práctica correctamente. La elaboración de esta memoria es indispensable para la superación de la práctica.

Problemas

1. Seguridad Perfecta

a. Comprobación empírica de la Seguridad Perfecta del cifrado de desplazamiento:

Comprobar mediante un programa que el método de cifrado de desplazamiento:

1. Consigue Seguridad Perfecta si se eligen las claves con igual probabilidad.

*2. No consigue Seguridad Perfecta si las claves no son equiprobables.*

Recordar que la definición de Seguridad Perfecta asume que cada elemento de texto plano se cifra con una clave distinta. Por ello, se deberán utilizar dos métodos distintos de cambio de clave entre un elemento de texto plano y el siguiente: uno elegirá claves de manera equiprobable y el otro no.

El programa tendrá la siguiente interfaz:

```
seg-perf {-P | -I} [-i file_in] [-o file_out]
```

Explicación de los argumentos:

-P se utiliza el método equiprobable.

-I se utiliza el método no equiprobable.

En todo caso, la salida consistirá en las probabilidades $P_p(x)$ de los elementos de texto plano, y las probabilidades condicionadas $P_p(x|y)$ para cada elemento de texto plano y de texto cifrado, con el siguiente formato:

$P_p(A) = \%lf$

$P_p(B) = \%lf$

...

$P_p(Z) = \%lf$

$P_p(A|A) = \%lf$ $P_p(A|B) = \%lf$... $P_p(A|Z) = \%lf$

$P_p(B|A) = \%lf$ $P_p(B|B) = \%lf$... $P_p(B|Z) = \%lf$

...

$P_p(Z|A) = \%lf$ $P_p(Z|B) = \%lf$... $P_p(Z|Z) = \%lf$

Donde $\%lf$ representa un double de C impreso de la forma estándar, y las distintas probabilidades condicionadas van separadas por espacios.

En la memoria se comentarán entre otros los siguientes aspectos:

1. *Esquemas de cambio de clave implementados para los modos -P y -I.*
2. *Resultados obtenidos para los dos modos con distintos casos de prueba, en función del tamaño del mensaje cifrado.*

2. Implementación del DES

a. Programación del DES

Programa el método de DES de 16 rondas en el modo ECB [1, 2, 3, 4]. Se creará el programa llamado **desECB** que recibirá argumentos de acuerdo con el siguiente esquema:

```
desECB {-C | -D -k clave} [-i file_in] [-o file_out]
```

Explicación de los argumentos:

-C el programa cifra

-D el programa descifra



-k clave de 64 bits: 56 bits + 8 bits de paridad

-i fichero de entrada

-o fichero de salida

Si la longitud en bits del fichero de entrada no es múltiplo de 64, se añadirán los caracteres necesarios para que lo sea.

Cuando se cifre un texto, el programa generará automáticamente la clave de cifrado y la mostrará en la salida estándar para poder utilizarla en el modo de descifrado. La clave tendrá 56 bits de datos más 8 bits de paridad impar. Los bits de paridad ocuparán las posiciones 8, 16, 24, 32, 40, 48, 56 y 64.

Para facilitar la codificación de al algoritmo se proporciona el fichero [6]. Este fichero contiene los valores numéricos de las 8 *S-boxes* del algoritmo DES y diversas permutaciones que necesitas. Para depurar el DES te puede servir el apartado “Depurar el DES” en la pagina moodle de la asignatura. Comprueba que el modo ECB no es bueno para mensajes largos y estructurados, como por ejemplo imágenes:

http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation.

b. Programación del Triple DES (OPCIONAL)

Utilizando los programas implementados en los apartados anteriores, programar el Triple DES en el modo de operación CBC (consultar [2, 5] para los modos de operación en Triple DES). Para ello, se creará un programa con la siguiente interfaz:

```
tripleDES {-C | -D} {-k clave -v IV} [-i file_in] [-o file_out]
```

Se deberá tener en cuenta que la clave especificada se dividirá en las tres claves de cifrado de cada DES, por lo que será una clave de 168 bits con 24 bits de paridad. De nuevo, para los modos -C y -D deberá comprobarse el cumplimiento de dicha paridad cuando corresponda.

3. Principios de diseño del DES

a. Estudio de la no linealidad de las S-boxes del DES

Estudiar la no linealidad de las S-boxes del DES y para ello construir un programa que haga las medidas adecuadas para comprobar tal hecho.

b. Estudio del Efecto de Avalanche

Estudia experimentalmente el efecto avalanche del algoritmo DES en el bloque y la clave, para cada una de las rondas del algoritmo. Para ello diseña los programas que creas conveniente para probarlos con diferentes bloques y claves para el algoritmo.

c. El Criterio de Avalanche Estricto (SAC) y el Criterio de Independencia de Bits (BIC) (OPCIONAL)

Estudia los criterios *SAC* y *BIC* en función del número de iteraciones para las cajas *S* del DES. Explica en qué consiste cada una de estas características del DES y analiza, utilizando la implementación realizada para el apartado anterior, cómo se manifiestan a través del proceso de cifrado DES.

d. Construcción de S-boxes propias (OPCIONAL)

Describe los criterios de diseño seguidos para el diseño de las *S-boxes* del algoritmo DES [?]. Basándote en ellos, construye nuevas *S-boxes* con 6 bits de entrada y 4 bits de salida. Explica los criterios de diseño seguidos en la construcción de estas *S-boxes* y el método seguido para su aplicación.



4. Principios de diseño del AES

a. Estudio de la no linealidad de las S-boxes del AES

Estudiar la no linealidad de las S-boxes del AES y para ello construir un programa que haga las medidas adecuadas para comprobar tal hecho (mirar la documentación adicional en la página de moodle de la asignatura [7]).

b. Generación de las S-boxes AES (OPCIONAL)

Implementar los algoritmos de Euclides y de Euclides extendido para $GF(2^8)$ con $m(x) = x^8 + x^4 + x^3 + x + 1$ (polinomio irreducible del AES). Utilizando dichos algoritmos, codificar un programa que calcule las S-boxes para el AES, tanto la directa como la inversa. La interfaz será:

`SBOX_AES {-C | -D} [-o file_out]`

Donde:

-C calcular la S-box directa.

-D calcular la S-box inversa.

Comprobar la corrección de la implementación comparando las S-boxes obtenidas con las reales del AES, que pueden consultarse en las páginas 16 y 22 de [8] y de [9].

c. Programación del AES (OPCIONAL)

Programar el método de AES de 16 rondas en el modo CBC [9, 3, 4]. Se creará el programa llamado `desCBC` que recibirá argumentos de acuerdo con el siguiente esquema:

`AesCBC {-C | -D -k clave} [-i file_in] [-o file_out]`

Información complementaria

Plazo de realización y entrega: La realización será los días 27/10/2016, 03/11/2016, 10/11/2016, 17/11/2016 y la entrega el día 23/11/2016 (23:55 horas).

Bibliografía de referencia

- [1] FIPS 46-3 (<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>).
- [2] NIST 800-67 (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf>).
- [3] FIPS 81 (<http://csrc.nist.gov/publications/fips/fips81/fips81.htm>).
- [4] NIST Special Publication 800-38A (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38A.pdf>).
- [5] NIST 800-20 (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-20.pdf>).
- [6] DES_tables.c (ver moodle)
- [7] AES_tables.c (ver moodle)
- [8] FIPS 197: Advanced Encryption Standard (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>).
- [9] AES según los autores (<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.36.640>).