

Las cajas de sustitución (cajas S) constituyen la piedra angular en criptografía para lograr que los cifradores por bloque exhiban la ineludible propiedad de no linealidad. En efecto, si la o las cajas S de un determinado cifrador por bloque no alcanzan una alta no linealidad, entonces se considera que tal algoritmo no podrá ofrecer una seguridad adecuada para impedir que información confidencial pueda ser develada por entidades no autorizadas.

Dada su definición, es claro que el número de funciones booleanas elegibles para diseñar una caja S de n bits de entrada y m bits de salida está dado por 2^{m2^n} , de tal manera que aun para valores moderados de n y m el tamaño del espacio de búsqueda de este problema tiene un tamaño desmesurado.

Sin embargo, no todas las funciones booleanas son apropiadas para construir buenas cajas S . Además de la ya mencionada propiedad de no linealidad, algunas de las principales propiedades criptográficas requeridas para dichas funciones booleanas incluyen: balance, alto grado algebraico, criterio de avalancha estricto, orden de inmunidad, etcétera.

Durante el desarrollo de esta práctica hemos aprovechado las cajas S de los algoritmos DES y AES para crear dos rutinas en C que demuestran la no linealidad de estas funciones booleanas. Estas dos rutinas han sido llamadas **linealidadSBoxesDES** y **linealidadSBoxesAES**. Ambas rutinas reciben como argumento de ejecución “-n N”, donde N es un número natural que indica el número de veces que se quiere probar la no linealidad. La salida de estos dos programas se incluye a continuación para $N=10$:

```
iMac-de-Jose:P2 Jose$ ./linealidadSBoxesAES -n 10
ITERACION 1:
a=c9
b=80
f(a)=dd
f(b)=cd
f(a+b)=3b
f(a)+f(b)=aa
ITERACION 2:
a=2f
b=5e
f(a)=15
f(b)=58
f(a+b)=5d
f(a)+f(b)=6d
ITERACION 3:
a=df
b=94
f(a)=9e
f(b)=22
f(a+b)=8f
f(a)+f(b)=c0
ITERACION 4:
a=d5
b=42
f(a)=3
f(b)=2c
f(a+b)=f0
f(a)+f(b)=2f
ITERACION 5:
a=85
b=b5
f(a)=97
f(b)=d5
f(a+b)=80
f(a)+f(b)=6c
ITERACION 6:
a=65
b=26
f(a)=4d
f(b)=f7
f(a+b)=3d
f(a)+f(b)=44
ITERACION 7:
a=fa
b=71
f(a)=2d
f(b)=a3
f(a+b)=7f
f(a)+f(b)=d0
ITERACION 8:
a=74
b=47
f(a)=92
f(b)=a0
f(a+b)=ea
f(a)+f(b)=32
ITERACION 9:
a=81
b=82
f(a)=c
f(b)=13
f(a+b)=7b
f(a)+f(b)=1f
ITERACION 10:
a=61
b=db
f(a)=ef
f(b)=b9
f(a+b)=eb
f(a)+f(b)=a8
iMac-de-Jose:P2 Jose$
```

```
iMac-de-Jose:P2 Jose$ ./linealidadSBoxesDES -n 10
ITERACION 1:
f(a):00110000 01011111 01100010 10111101
f(b):01100001 10001010 10011000 00010100
f(a+b):10001100 00100001 10100101 00010100
f(a)+f(b):01010001 11010101 11111010 10101001
ITERACION 2:
f(a):11101101 00001001 11111000 11000011
f(b):10101010 00011000 01100011 11011110
f(a+b):11111000 00111111 00011010 00101111
f(a)+f(b):01000111 00010001 10011011 00011101
ITERACION 3:
f(a):11011100 01000110 00111101 00000000
f(b):00110011 11101111 01010111 10010001
f(a+b):01001010 10011110 00101001 00010011
f(a)+f(b):11101111 10101001 01101010 10010001
ITERACION 4:
f(a):11111010 11010111 11000101 11011110
f(b):11100111 10000100 10001001 01111110
f(a+b):01000011 01010100 10100010 01011101
f(a)+f(b):00011101 01010011 01001100 10100000
ITERACION 5:
f(a):10000110 11011110 11001001 10000111
f(b):01101010 11010000 10111000 11101001
f(a+b):10111011 00110001 11100011 11111001
f(a)+f(b):11101100 00001110 01110001 01101110
ITERACION 6:
f(a):00110010 11010110 11000100 10100111
f(b):10100011 01010111 01111000 01011101
f(a+b):10110001 10110110 10000101 00011001
f(a)+f(b):10010001 10000001 10111100 11111010
ITERACION 7:
f(a):10100001 10110000 11011110 01110011
f(b):00101110 11001011 10011010 01111111
f(a+b):01101101 11010010 00010000 11101100
f(a)+f(b):10001111 01111011 01000100 00001100
ITERACION 8:
f(a):11110010 01111011 01000000 11111111
f(b):10111011 11011110 10100100 00001100
f(a+b):01011111 10101101 10011101 01101110
f(a)+f(b):01001001 10100101 11100100 11110011
ITERACION 9:
f(a):11100101 10010110 10110111 10101100
f(b):11000110 00011001 10101011 11001000
f(a+b):00010010 10110101 01100110 10110101
f(a)+f(b):00100011 10001111 00011100 01100100
ITERACION 10:
f(a):10111100 11001001 10001100 11011111
f(b):10011101 11000011 01000101 10110000
f(a+b):00111001 10010110 10110000 10110010
f(a)+f(b):00100001 00001010 11001001 01101111
iMac-de-Jose:P2 Jose$
```

Para comprobar la no linealidad de las SBOXES en ambos casos, basta con fijarse en que se cumple la siguiente igualdad:

$$f(a)+f(b)=f(a+b)+K;$$

Donde K sería lo que llamaríamos constante de no linealidad (si fuese 0 la función sería lineal).

En resumen, los principales criterios para construir unas buenas S-Boxes son los siguientes:

- **Balance:** Esta propiedad es muy deseable para evitar ataques cripto-diferenciales tales como los introducidos por A. Shamir contra el algoritmo DES
- **Alta no linealidad:** Esta propiedad reduce el efecto de los ataques por criptoanálisis lineal. Como se discutió antes, la no linealidad de una función booleana puede ser calculada directamente de la transformada de Walsh-Hadamard
- **Autocorrelación:** Este valor es proporcional al desbalance de todas las derivadas de primer orden de la función booleana. Valores pequeños son considerados como buenos mientras que un valor grande es considerado un símbolo de debilidad. Las funciones curvas gozan de una autocorrelación mínima, por lo que optimizan esta propiedad.

- **Indicador absoluto:** Indicador absoluto de una función booleana denotado por $M(f)$ está dado por $|r_{\max}|$ el máximo valor absoluto en $r_{\hat{f}}(s)$. Se considera que una función booleana con un $M(f)$ pequeño es criptográficamente deseable. Nuevamente las funciones curvas son las mejores, ya que su indicador absoluto es 0.
- **Efecto avalancha:** Está relacionado con la autocorrelación y se define con respecto a un bit específico de entrada tal que al complementarlo resulta en un cambio en el bit de salida con una probabilidad de 1/2. El criterio de avalancha estricto (SAC por sus siglas en inglés), requiere los efectos avalancha de todos los bits de entrada. Se dice que una función booleana satisface el criterio de avalancha estricto si al complementar un solo bit de entrada resulta en un cambio en un bit de salida con una probabilidad de 1/2. Puede demostrarse fácilmente que una función booleana f con función de autocorrelación $r_{\hat{f}}(s)$, satisface el criterio de avalancha estricto si y sólo si $r_{\hat{f}}(s) = 0$ para toda s con peso de Hamming $H(s)=1$