Instrucciones para la realización del Ejercicio Práctico

El objetivo de este ejercicio práctico es que el alumno sea capaz de implementar una primitiva criptográfica, asignada por sorteo, y estudiar en ella lo que se conoce como el Efecto Avalancha.

Se conoce como Efecto Avalancha[1], aquel efecto (diferencia) que se observa a la salida de una función criptográfica al complementar un bit (efecto de primer orden) de los argumentos de la entrada de esa función.

El Efecto Avalancha pone de manifiesto el grado de correlación[2] que hay entre la entrada y la salida de la función estudiada. Se caracteriza por ser una propiedad de toda la función por lo que, en principio, debería estudiarse para todo el espacio de entrada de la función.

Dado que los espacios de entrada de las funciones criptográficas es inmenso, la caracterización del Efecto Avalancha sólo puede ser de naturaleza estadística. Al no poder probar todos los elementos del espacio de entrada, se debe elegir (al azar, homogéneamente y de forma uniforme) un subconjunto de ellos y ver cuál ese efecto en cada caso particular.

Para medir el efecto que tiene el cambio en la entrada, se calculara la Distancia de Hamming[3] de las dos salidas, y se acumulará en un histograma[4] que, al terminar el experimento (una vez procesadas todas las muestras), mostrará la distribución de probabilidad[5] del número de cambios.

Habrá que determinar cuál debe ser el tamaño de la muestra[6] (número de pruebas) para conseguir una calidad suficiente (p. ej. Significación del 90-95% o incertidumbres del 10-5%) en la forma de esa distribución y en los parámetros estadísticos[7] que la describan (moda, media, desviación, asimetría, curtosis, etc.)

Habrá que establecer cuáles son los resultados esperados para este experimento en el caso en el que la función criptográfica estudiada se comportase como una función aleatoria perfecta, sin correlación alguna, como un Oráculo Aleatorio[8].

Habrá que comparar los resultados experimentales obtenidos con los esperados y concluir el grado de similitud[9], o distinguibilidad, que puede tener la función criptográfica estudiada respecto al resultado ideal para esa distancia utilizada (la distancia de Hamming).

---

[1] Ver https://en.wikipedia.org/wiki/Avalanche_effect
[2] Ver https://en.wikipedia.org/wiki/Correlation_and_dependence
[3] Ver https://en.wikipedia.org/wiki/Hamming_distance
[4] Ver https://en.wikipedia.org/wiki/Histogram
[5] Ver https://en.wikipedia.org/wiki/Probability_distribution
[6] Ver https://en.wikipedia.org/wiki/Sample_(statistics)
[7] Ver https://en.wikipedia.org/wiki/Statistic
[8] Ver https://en.wikipedia.org/wiki/Random_oracle
[9] Ver https://en.wikipedia.org/wiki/Likelihood_function

Normas

Los resultados se plasmarán en una **memoria en PDF** de no más de **DOS PÁGINAS A4** (caratula, indica y referencias no incluidas en ese límite).

La redacción debe ser clara, precisa y debe incluir todos los elementos esenciales para la correcta comprensión de lo que se ha hecho y de los resultados que se han obtenido.

Sólo a título informativo, decir que existen numerosas librerías criptográficas que se pueden utilizar para la realización de esta práctica[10], sin embargo, hay que estar completamente seguros de que las funciones que se están utilizando implementan correctamente el algoritmo. Para ello hay que encontrar en la literatura Vectores de Prueba[11] y probarlos en el código empleado antes de seguir adelante.

En la memoria se indicará claramente:

- Cómo, concretamente, se ha realizado el experimento y en qué ha consistido (aportar como Adjunto el material necesario para poder repetirlo en el futuro).
- Los vectores de prueba o validación que se han empleado para estar seguros de que la función de código utilizada es realmente la que se pretende.
- Cuántos y cuáles argumentos distintos se han considerado dentro de la función criptográfica estudiada.
- Cuáles han sido los tamaños de las muestras empleadas y por qué se han elegido esos tamaños (justificar la respuesta).
- Histograma, con calidad, en el que se muestre la distribución obtenida.
- Cómo se calculan concretamente los valores de los estadísticos calculados (media, moda, desviación, etc.)
- Cuáles son los valores obtenidos de los estadísticos calculados (media, moda, desviación, etc.) y cómo deben interpretarse.
- Describir justificadamente cuáles son los valores esperados para todo lo anterior si la función se comportase como un Oráculo Aleatorio perfecto.
- Comparar cuantitativamente los resultados esperados y los resultados obtenidos.
- Determinar la similitud de la función criptográfica estudiada con un Oráculo Aleatorio. Indicar el grado de significación de estas conclusiones.

Asignación

La asignación se hace, como en otros años, utilizando la componente numérica del **DNI**, **NIE** o **Pasaporte** (por este orden) y una constante aleatoria que se determinará el día que se realice el sorteo de estos ejercicios. La aritmética a utilizar es la aritmética[12] **módulo 59**.

A título de ejemplo, supongamos que el DNI es el 123456789-Z y que la constante sorteada es 569.874, en ese caso, la práctica que le correspondería a ese alumno sería:

$$(123.456.789 * 569.874) \bmod 59 = \mathbf{21}$$

Que debe calcularse del siguiente modo

$$((123.456.789 \bmod 59) * (569.874 \bmod 59)) \bmod 59 = (56 * 52) \bmod 59 = 21$$

[10] Algunos ejemplos son OpenSSL, Bouncy Castle, Cryptlib, Crypto++, NaCl y PyCrypto
[11] Ver https://en.wikipedia.org/wiki/Test_vector
[12] Ver https://en.wikipedia.org/wiki/Modular_arithmetic

La lista de algoritmos a estudiar es la siguiente:

0. AES-128
1. AES-192
2. AES-256,
3. BLOWFISH
4. CAMELLIA,
5. CAST-128,
6. CAST-256
7. DES CBC-MAC,
8. DES,
9. GOST 28147-89
10. GOST R 34.11-94
11. HMAC-MD5,
12. HMAC-RIPEMD-160,
13. HMAC-SHA-1,
14. HMAC-SHA-224
15. HMAC-SHA-256
16. HMAC-SHA-384
17. HMAC-SHA-512
18. IDEA,
19. MARS,
20. MD2,
21. MD4,
22. MD5,
23. MDC-2,
24. PANAMA,
25. PBKDF1
26. PBKDF2
27. POLY1305-AES
28. RC2,
29. RC4,
30. RC5,
31. RC6,
32. RIPEMD-128,
33. RIPEMD-160,
34. RIPEMD-256,
35. RIPEMD-320,
36. SALSA20,
37. SEED,
38. SERPENT,
39. SHA-1,
40. SHA-224,
41. SHA-256,
42. SHA-384
43. SHA-512,
44. SHACAL-2
45. SHA-3 (256)
46. SHA-3 (512)
47. SKIJACK,
48. SOSEMANUK,
49. TEA,
50. TIGER,
51. Triple DES 112,
52. Triple DES 168,
53. TWOFISH,
54. XTEA
55. VMAC,
56. WHIRLPOOL,
57. XSALSA20
58. XTEA,