Comenzado el	jueves, 24 de octubre de 2019, 21:28
Estado	Finalizado
Finalizado en	jueves, 24 de octubre de 2019, 22:57
Tiempo empleado	1 hora 28 minutos
Puntos	15,00/15,00
Calificación	**10,00** de 10,00 (**100**%)

Pregunta 1

Correcta

Puntúa 3,00 sobre 3,00

Sea $x^5 + x^3 + 1$ el polinomio de conexiones de un LFSR. Sabiendo que el estado inicial es 00011 , calculad los primeros 12 digitos de la secuencia de salida.

Considerad que el orden de bits en que se indica el estado inicial i el orden de bits en que se espera que indiqueis la salida es el mismo que se utiliza en el ejemplo de funcionamiento de un LFSR del apartado 2.3 del Módulo 3. En dicho ejemplo, la salida del LFSR se indicaria como 01010001

Respuesta:

110001101110

La respuesta correcta es: 110001101110

Pregunta 2

Correcta

Puntúa 1,00 sobre 1,00

Dado un LFSR de 5 celdas con un polinomio de conexiones primitivo, indicad cuanto vale el periodo y la complejidad lineal de la secuencia resultante.

Seleccione una:

- a. La complejidad lineal es 5 y el periodo 32
- b. La complejidad lineal es 10 y el periodo 16
- c. La complejidad lineal es 10 y el periodo 32
- d. La complejidad lineal es 5 y el periodo 31 ✓

La respuesta correcta es: La complejidad lineal es 5 y el periodo 31

Pregunta 3

Correcta

Puntúa 4,00 sobre 4,00

Calculad el polinomio de conexiones de un LFSR de 4 celdas sabiendo que los primeros 8 digitos de la secuencia de salida son 10101111 .

Considerad que el orden de bits en que se indica la salida es el mismo que se utiliza en el ejemplo de funcionamiento de un LFSR del apartado 2.3 del Módulo 3. En dicho ejemplo, la salida del LFSR se indicaria como 01010001

Seleccione una:

- a. $x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$
- b. $x^4 + x^2 + 1$
- c. $x^4 + x^3 + 1$ ✓
- d. $x^4 + x + 1$
- e. 1

La respuesta correcta es: $x^4 + x^3 + 1$

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

Aplica el test de frecuencia de bits individuales del NIST a la siguiente secuencia:

[0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0]

¿Cuál es el valor sobs que se obtiene?

Respuesta: 0,25819888974 ✓

La respuesta correcta es: 0,258198889747

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

Aplica el test de ráfagas del NIST a la siguiente secuencia:

[0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0]

¿Cuál es el valor Vn que se obtiene?

Respuesta: 7 ✓

La respuesta correcta es: 7

Pregunta 6

Correcta

Puntúa 1,00 sobre 1,00

Calculad la salida (el valor z) de un generador pseudoaleatorio Trivium en un instante dado t, teniendo en cuenta que los estados de los registros de desplazamiento en este instante son:

Estado del registro A: [0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0]

Estado del registro B: [0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0]

Estado del registro C: [0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0]

Respuesta: 0

La respuesta correcta es: 0

Pregunta 7

Correcta

Puntúa 1,00 sobre 1,00

Dado un cifrador Rijndael con clave de cifrado 8BCA77E6F2A5028DAFC82118C33C7EB2286D72EA394E348A y un bloque de texto para cifrar 559434503D47429C80EE0BB7AD8D0D61 .
¿Cuantas iteraciones requiere el Rijndael para cifrar este bloque de texto con esta clave?

Respuesta:

12

La respuesta correcta es: 12

Pregunta 8

Correcta

Puntúa 1,00 sobre 1,00

Supongamos que tenemos un criptosistema AES con una clave de 128 bits definida por el valor 38E15CF46D72BBA053861CFEAFDE8E83 y el texto en claro de 128 bits que queremos cifrar es 98C93D69AD90F93D0B7A6452F000288E .

Indicad el valor de la **primera fila** de la matriz de estado después de aplicar la transformación inicial, es decir después de aplicar la función AddRoundKey. Indicad el resultado con los **valores en hexadecimal en mayúsculas** separados por un espacio (p.e. C8 4D 56 E3).

Respuesta:

A0 C0 58 5F

La respuesta correcta es: A0 C0 58 5F

Pregunta 9

Correcta

Puntúa 1,00 sobre 1,00

Supongamos que tenemos la siguiente matriz de estado

$$\begin{pmatrix} d0 & c2 & 73 & 28 \\ 7b & cd & 6a & 21 \\ ab & c3 & 7f & 61 \\ 72 & 23 & fe & c1 \end{pmatrix}$$

Encontrad la **primera fila** de la matriz de salida de la función ByteSub. Indicar el resultado con los valores en **hexadecimal en minúsculas** separados por un espacio (p.e. c8 4d 56 e3). Para realizar los cálculos, podéis utilizar las cajas S del AES.

Respuesta:

70 25 8f 34

La respuesta correcta es: 70 25 8f 34

Pregunta 10

Correcta

Puntúa 1,00 sobre 1,00

Supongamos que la calve de cifrado de un cifrador Rijndael expresada en hexadecimal es la siguiente: 26556BE4A3F6EEDE504CB6F4977E943C . Indicad el valor de la primera subclave, es decir, K(0).

Respuesta:

26556BE4 A3F6EEDE 504C

La respuesta correcta es: 26556BE4A3F6EEDE504CB6F4977E943C

Comentario:

◄ PEC1

Ir a...

PEC3 ►