Comenzado el	sábado, 14 de marzo de 2020, 15:11
Estado	Finalizado
Finalizado en	sábado, 14 de marzo de 2020, 15:56
Tiempo empleado	45 minutos 30 segundos
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 11001 , calculad los primeros 11 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:

10011111000

La respuesta correcta es: 10011111000

Pregunta 2

Correcta

Puntúa 1,00 sobre 1,00

Dado un LFSR de 9 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 9 y el periodo 512
- b. La complejidad lineal es 9 y el periodo 511 ✓
- c. La complejidad lineal es 18 y el periodo 256
- d. La complejidad lineal es 18 y el periodo 512

La respuesta correcta es: La complejidad lineal es 9 y el periodo 511

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. $x^4 + x + 1$
- b. $x^8 + x^7 + x^6 + x^5 + x^2 + 1$
- c. $x^4 + x^3 + 1$ ✓
- d. $x^3 + x + 1$
- e. $x^4 + x^2 + x + 1$

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

¿Cuál es el valor sobs que se obtiene?

Respuesta: 0,2294157339 ✓

La respuesta correcta es: 0,229415733871

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

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

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

¿Cuál es el valor Vn que se obtiene?

Respuesta: 11 ✓

La respuesta correcta es: 11

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

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

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

Respuesta: 1

La respuesta correcta es: 1

Pregunta 7

Correcta

Puntúa 1,00 sobre 1,00

Dado un cifrador Rijndael con clave de cifrado 395579209C052993B2063B7741ECB2EC339BEFC9120A729D y un bloque de texto para cifrar 2016350BDC9B9CFE618D38E59112D967C3E15AD3FEA60404 .
¿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 D05B926E83BE982F8642D8494E04EB9B y el texto en claro de 128 bits que queremos cifrar es 197F93FF1235FE1FAC7FA6C92970904F .

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:

C9 91 2A 67

La respuesta correcta es: C9 91 2A 67

Pregunta 9

Correcta

Puntúa 1,00 sobre 1,00

Supongamos que tenemos la siguiente matriz de estado

$$\begin{pmatrix} e8 & 8a & 69 & fc \\ f3 & 56 & 8a & e7 \\ 43 & 13 & ca & 1d \\ 88 & 91 & df & 07 \end{pmatrix}$$

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:

9b 7e f9 b0

La respuesta correcta es: 9b 7e f9 b0

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: C93682AC8FB0A34F14CCE93602978956 . Indicad el valor de la primera subclave, es decir, K(0).

Respuesta:

C93682AC8FB0A34F14

La respuesta correcta es: C93682AC8FB0A34F14CCE93602978956

◄ PEC1 Ir a... PEC3 ►