

Inici ► Cursos ► Semestre 20142 ► 142_05_601_01 : Criptografia aula 1 ► Proves d'Avaluació Continuada (PACs) ► PAC-2-Flux

NAVEGACIÓ PEL QÜESTIONARI

1 2 3 4

Acaba la revisió

Començat el Tuesday, 7 April 2015, 10:30

Estat Acabat

Completat el Tuesday, 7 April 2015, 11:12

Temps emprat 42 minuts 28 segons

Qualificació 10,00 sobre 10,00 (100%)

Pregunta 1

Correcte

Puntuació 3,00
sobre 3,00

Marca la pregunta

Sigui $x^5 + x^4 + x^3 + x^2 + 1$ el polinomi de connexions d'un LFSR. Sabent que l'estat inicial és 10101, calculeu-ne els primers 10 dígets de la seqüència de sortida.

Considereu que l'ordre dels bits en que s'indica l'estat inicial i l'ordre dels bits en que s'espera que indiqueu la sortida és el mateix que s'utilitza en l'exemple de funcionament d'un LFSR de l'apartat 2.2 del Mòdul 3. En aquell exemple, la sortida de l'LFSR s'indicaria com 01010001

Resposta:

1010100011



La resposta correcta és: 1010100011

Pregunta 2

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

Donat un LFSR de 12 cel·les amb un polinomi de connexions primitiu, indiqueu quan val el període i la complexitat lineal de la seqüència resultant.

Trieu-ne una:



- a. La complexitat lineal es 12 i el període 4095 ✓
- b. La complexitat lineal es 24 i el període 2048
- c. La complexitat lineal es 24 i el període 4096
- d. La complexitat lineal es 12 i el període 4096

La resposta correcta és: La complexitat lineal es 12 i el període 4095.

Pregunta 3

Correcte

Puntuació 4,00
sobre 4,00

Marca la pregunta

Trobeu el polinomi de connexions d'un LFSR de 4 cel·les sabent que els primers 8 dígets de la seqüència de sortida són 10111100

Considereu que l'ordre dels bits en que s'indica la sortida és el mateix que s'utilitza en l'exemple de funcionament d'un LFSR de

l'apartat 2.2 del Mòdul 3. En aquell exemple, la sortida de l'LFSR
<http://cv.uoc.edu/moodos/mod/quiz/review.ph...>
s'indicaria com 01010001

Trieu-ne una:

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

La resposta correcta és: $x^4 + x^3 + 1$.

Pregunta 4

Correcte

Puntuació 2,00
sobre 2,00

🚩 Marca la
pregunta

Indiqueu els graus dels polinomis que ha de tenir un generador de Massey-Rueppel per a generar una seqüència de període 253921 donat el factor de velocitat 28. Doneu la resposta usant el format [n,l] sense que importi l'ordre (per exemple: [13,7] o bé [7,13])

Resposta:

[5,13]



La resposta correcta és: [5,13]

Acaba la revisió

Heu entrat com Jose Vicente Gómez Jiménez (Sortida)
142_05_601_01 : Criptografia aula 1