

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

NAVEGACIÓ PEL QÜESTIONARI

1 2 3 4 5

6 7

Acaba la revisió

Començat el Monday, 13 April 2015, 06:51

Estat Acabat

Completat el Monday, 13 April 2015, 07:57

Temps emprat 1 hora 5 minuts

Qualificació 10,00 sobre 10,00 (100%)

Pregunta 1

Correcte

Puntuació 1,00
sobre 1,00

Marca la
pregunta

El DES fa servir una permutació inicial i una permutació de sortida. Quines afirmacions són certes sobre aquestes permutacions?

Trieu-ne una o més:

- ☒ a. La mida de l'entrada és igual a la mida de sortida (64 bits). ✓ Totes dues permutacions prenen com a entrada 64 bits i en retornen també 64.
- ☐ b. Fan reducció de l'entrada (reben 64 bits i en retornen 56).
- ☐ c. Fan expansió de l'entrada (reben 56 bits i en retornen 64).
- ☒ d. $\sigma^{-1}(\sigma(M))=M$ ✓ La permutació inicial és la permutació inversa a la de sortida. Per tant, aplicar la permutació de sortida al resultat d'aplicar la permutació inicial sobre M ens dona el mateix M.
- ☒ e. $\sigma(\sigma^{-1}(M))=M$ ✓ La permutació inicial és la permutació inversa a la de sortida. Per tant, aplicar la permutació inicial al resultat d'aplicar la permutació de sortida sobre M ens dona el mateix M.

La resposta correcta és: $\sigma(\sigma^{-1}(M))=M$, $\sigma^{-1}(\sigma(M))=M$, La mida de l'entrada és igual a la mida de sortida (64 bits)..

Pregunta 2

Correcte

Puntuació 2,00
sobre 2,00

Marca la
pregunta

Suposem que tenim un criptosistema DES amb una clau $K = 385F5F4259544553$ (expressada en hexadecimal). Indiqueu quina serà la primera subclau, és a dir, el valor K_1 . Doneu el resultat amb els valors en hexadecimal en majúscules separats per un espai (p.e. C8 4D 56 E3).


Resposta:

B0 1A CA 9C A5 D9



Pregunta 3

Correcte

Puntuació 1,00
sobre 1,00 Marca la pregunta

Triple DES és una variant del DES que intenta augmentar la mida de la clau utilitzada pel DES bàsic. Tot i així, les implementacions de Triple DES es poden fer servir per xifrar i desxifrar en DES bàsic. Quina configuració d'una implementació de Triple DES és equivalent a xifrar amb DES bàsic?

Trieu-ne una:


- ☒ a. Fixar $k_1 = k_2$. ✓
- ☐ b. Encadenar dos xifradors Triple DES, de manera que la sortida del primer sigui l'entrada del segon.
- ☐ c. Encadenar tres xifradors Triple DES, de manera que la sortida d'un sigui l'entrada del següent.
- ☐ d. Fixar $k_1 = k_2^{-1}$.

Fixant $K_1=k_2$ estem xifrant, desxifrant i tornant a xifrar amb una mateixa clau. El resultat de xifrar i desxifrar amb una mateixa clau és el mateix valor d'entrada i, per tant, el resultat final consta només d'una etapa de xifratge. Per tant, fer servir 3DES amb $k_1=k_2$ és el mateix que fer servir DES.

La resposta correcta és: Fixar $k_1 = k_2$.

Pregunta 4

Correcte

Puntuació 1,00
sobre 1,00 Marca la pregunta

Donat un xifrador Rijndael amb clau de xifratge
A2F54240100D130CA9156CD4D85FB848B78B43AC6DDC6A86
i un bloc de text per xifrar
7AAA0D0C238124C71E275512FDB0042E38B949DD7A805E19

Quantes iteracions cal fer per xifrar aquest bloc de text en clar amb aquesta clau?


Resposta:



La resposta correcta és: 12

Pregunta 5

Correcte

Puntuació 2,00
sobre 2,00 Marca la pregunta

Suposem que tenim un criptosistema AES amb una clau de 128 bits definida pel valor B4B5C5542EE51F99D641778F7203015F i el text en clar de 128 bits que volem xifrar és C8F614742B2430EAC6547F2F0FBBFF09 .

Indiqueu quina serà la primera fila de la matriu d'estat després d'aplicar la transformació inicial, és a dir després d'aplicar la funció AddRoundKey. Indiqueu el resultat amb els valors en hexadecimal en majúscules separats per un espai (p.e. C8 4D 56 E3).

Resposta:

<http://cv.uoc.edu/moodos/mod/quiz/review.ph...>

La resposta correcta és: 7C 05 10 7D

Pregunta 6

Correcte

Puntuació 2,00
sobre 2,00

Marca la pregunta

Suposem que tenim la següent matriu d'estat

$$\begin{pmatrix} \text{fd} & 90 & 95 & 5a \\ 80 & \text{ce} & 66 & \text{e2} \\ 9f & 40 & 6e & 17 \\ 6d & 5c & \text{e6} & \text{ed} \end{pmatrix}$$

Trobeu quina serà la **primera fila** de la matriu de sortida per a la funció ByteSub. Doneu el resultat amb els valors en **hexadecimal en minúscules** separats per un espai (p.e. c8 4d 56 e3). Per a realitzar els càlculs, podeu utilitzar les caixes S de l'AES (http://en.wikipedia.org/wiki/Rijndael_S-box).

Resposta:



La resposta correcta és: 54 60 2a be

Pregunta 7

Correcte

Puntuació 1,00
sobre 1,00

Marca la pregunta

Suposem que la clau de xifratge d'un xifrador Rijndael expressada en hexadecimal és la següent:

97695B4E13A27750BABD12AA05DB6AA3 . Doneu-ne la primera subclau, és a dir, K(0). Doneu el resultat en hexadecimal en majúscules i sense espais.

Resposta:

La resposta correcta és:
97695B4E13A27750BABD12AA05DB6AA3

Acaba la revisió

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