**Question 1**

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

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. σ(σ^(-1)(M))=M Correcta | 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 dóna el mateix M. |
|  | b. La mida de l'entrada és igual a la mida de sortida (64 bits). Correcta | Totes dues permutacions prenen com a entrada 64 bits i en retornen també 64. |
|  | c. σ^(-1)(σ(M))=M Correcta | 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 dóna el mateix M. |
|  | d. Fan expansió de l'entrada (reben 56 bits i en retornen 64). Incorrecta |  |
|  | e. Fan reducció de l'entrada (reben 64 bits i en retornen 56). Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

Question 2

Suposem que tenim un criptosistema DES amb una clau K = 5F4341455341525F (expressada en hexadecimal). Indiqueu quina serà la primera subclau, és a dir, el valor K1. Doneu el resultat amb els valors en hexadecimal en majúscules separats per un espai (p.e. C8 4D 56 E3).

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 3**

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 una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. Fixar k1 = k2. Correcta |  |
|  | b. Encadenar dos xifradors Triple DES, de manera que la sortida del primer sigui l'entrada del segon. Incorrecta |  |
|  | c. Encadenar tres xifradors Triple DES, de manera que la sortida d'un sigui l'entrada del següent. Incorrecta |  |
|  | d. Fixar k1 = k2^(-1). Incorrecta |  |

Fixant K1=k2 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 k1=k2 és el mateix que fer servir DES.

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 4**

Donat un xifrador Rijndael amb clau de xifratge 742167C42CB88AD1AD2CB6349D517F8601292AD48FD0913B i un bloc de text per xifrar F1BA021A9D587AE672ACA970975E0FEEF756EE4BD47C5F00

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

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 5**

Suposem que tenim un criptosistema AES amb una clau de 128 bits definida pel valor 68CFF378D1243D74DC13B18994B996D4 i el text en clar de 128 bits que volem xifrar és 5641F35EFE0502A2FD3258C83792ED6A .

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

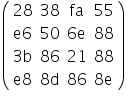
Correcta

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 6**

Suposem que tenim la següent matriu d'estat



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

Correcta

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 7**

Suposem que la clau de xifratge d’un xifrador Rijndael expressada en hexadecimal és la següent: 9D78DFBA8E2AAD2B3FD98A5914FD64E3 . Doneu-ne la primera subclau, és a dir, K(0).Doneu el resultat en hexadecimal en majúscules i sense espais.

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.