

Comenzado el	domingo, 5 de diciembre de 2021, 11:38
Estado	Finalizado
Finalizado en	domingo, 5 de diciembre de 2021, 12:35
Tiempo empleado	57 minutos 33 segundos
Calificación	5,70 de 10,00 (57%)

1

Puntúa -0,20 sobre 0,50

Incorrecta

Els algorismes simètrics són:

Seleccione una:

- ☒ a. Permet xifrar grans quantitats de dades ✖
- ☐ b. A igual mida de les claus, són menys segurs que els asimètrics
- ☐ c. Son més ràpids
- ☐ d. Totes són correctes

La teva resposta és incorrecta.

La respuesta correcta es: Totes són correctes

2

Puntúa 0,50 sobre 0,50

Correcta

Quin és l'estàndard de xifrat per a claus simètriques?

Seleccione una:

- ☐ a. TWOFISH
- ☐ b. SHA-3
- ☒ c. AES ✔
- ☐ d. Triple-DES
- ☐ e. DES

La resposta és correcta.

La respuesta correcta es: AES

3

Puntúa 1,00 sobre 1,00

Correcta

Escriviu el codi que manca per completar la funció següent, de forma que la resposta sigui el byte[] data encriptat usant l'algorisme AES, en mode ECB i amb padding PKCS5P:

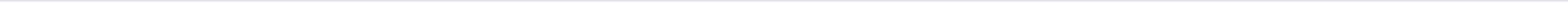
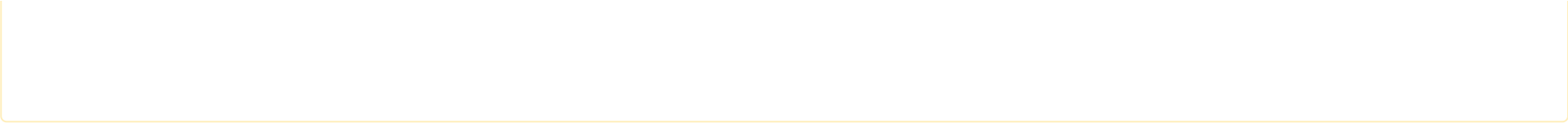
```
public byte[] encryptData(SecretKey sKey, byte[] data) {  
    byte[] encryptedData = null;  
    try {  
  
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");  
        cipher.init(Cipher.ENCRYPT_MODE, sKey);  
        encryptedData = cipher.doFinal(data);  
  
    } catch (Exception ex) {  
  
        System.err.println("Error xifrant les dades: " + ex);  
        return null;  
    }  
  
    return encryptedData;  
}
```

La resposta és correcta.

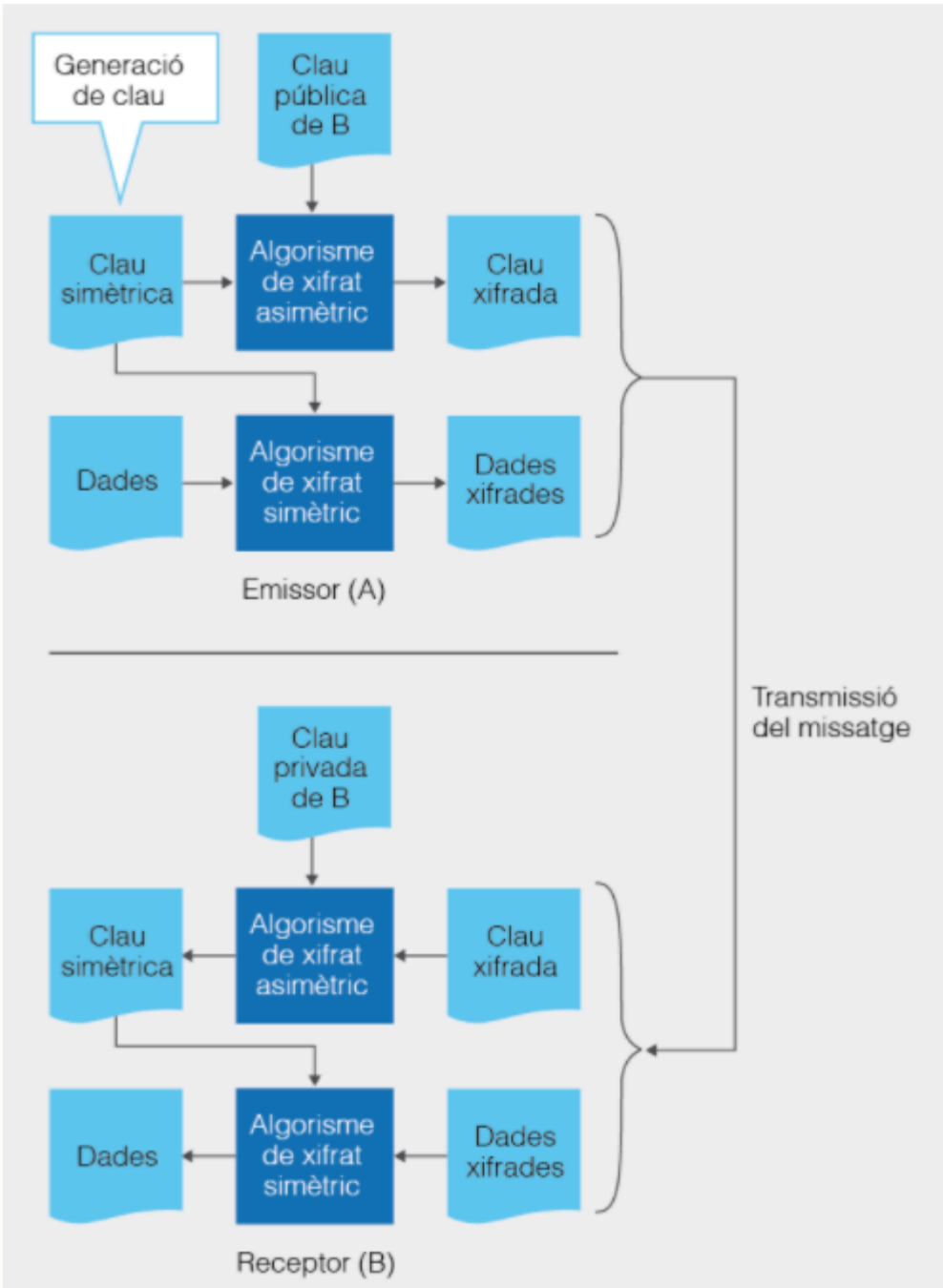
La respuesta correcta es:

Escriviu el codi que manca per completar la funció següent, de forma que la resposta sigui el byte[] data encriptat usant l'algorisme AES, en mode ECB i amb padding PKCS5P:

```
public byte[] encryptData(SecretKey sKey, byte[] data) {  
    byte[] encryptedData = null;  
    try {  
  
        [Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");]  
        [cipher.init(Cipher.ENCRYPT_MODE, sKey);]  
        [encryptedData = cipher.doFinal(data);]  
  
    } catch (Exception ex) {  
  
        System.err.println("Error xifrant les dades: " + ex);  
        return null;  
    }  
  
    return encryptedData;  
}
```



La següent imatge pertany a



Selecione una:

- ☐ a. Signatura digital
- ☒ b. Sistema de clau embolcallada
Firma digital ✓
- ☐ c. Sistema de clau asimètrica
- ☐ d. Sistema de clau simètrica

La resposta és correcta.




La respuesta correcta es:
Sistema de clau embolcallada
Firma digital

5

Puntúa 0,50 sobre 0,50

Correcta

Inicialment, l'ús dels termes *criptografia* i *xifrat* eren pràcticament intercanviables. L'aplicació d'aquesta disciplina tradicionalment ha estat per assolir la privadesa en l'intercanvi de missatges. Però amb la popularitat d'Internet i la proliferació en l'intercanvi telemàtic de missatges o documents, es fa patent la necessitat de disposar d'altres serveis de seguretat més enllà del de la privadesa. Principalment, els següents (**heu d'omplir els buits amb les opcions que teniu possibles**)

-  : poder identificar si un document ha estat manipulats. Cal fer palès que aquest servei no evita la manipulació, només fa possible que sempre pugui ser detectada pel receptor.
-  : poder garantir quina és la identitat de l'autor del document, evitant que sigui suplantat.
-  : evitar que l'autor pugui negar que ell ha generat el document. El receptor pot demostrar a un tercer la identitat de qui ha emès realment el missatge.

La resposta és correcta.

La respuesta correcta es:

Inicialment, l'ús dels termes *criptografia* i *xifrat* eren pràcticament intercanviables. L'aplicació d'aquesta disciplina tradicionalment ha estat per assolir la privadesa en l'intercanvi de missatges. Però amb la popularitat d'Internet i la proliferació en l'intercanvi telemàtic de missatges o documents, es fa patent la necessitat de disposar d'altres serveis de seguretat més enllà del de la privadesa. Principalment, els següents (**heu d'omplir els buits amb les opcions que teniu possibles**)

- **[Integritat]**: poder identificar si un document ha estat manipulats. Cal fer palès que aquest servei no evita la manipulació, només fa possible que sempre pugui ser detectada pel receptor.
- **[Autenticació]**: poder garantir quina és la identitat de l'autor del document, evitant que sigui suplantat.
- **[No-repudi]**: evitar que l'autor pugui negar que ell ha generat el document. El receptor pot demostrar a un tercer la identitat de qui ha emès realment el missatge.

6

Puntúa 1,00 sobre 1,00

Correcta

Donat el codi següent:

```
private static byte[] hashSHA1(File file) throws Exception{
    final MessageDigest messageDigest = MessageDigest.getInstance("SHA2");
    try (InputStream is = new BufferedInputStream(new FileInputStream(file))) {
        final byte[] buffer = new byte[1024];
        for(int read = 0; (read = is.read(buffer)) != -1;) {
            messageDigest.update(buffer, 0, read);
        }
    }
    return messageDigest.digest();
}
```

Què és el que està retornant el mètode?

Seleccione una:

- ☒ a. El hash del fitxer ✓
- ☐ b. El hash del fitxer utilitzant una funció resum MD5
- ☐ c. Cap de les respostes és correcta
- ☐ d. La signatura digital del fitxer

La teva resposta és correcta.

La respuesta correcta es: El hash del fitxer

- Tenim un missatge a enviar: M
- Alice té una clau privada A_{Priv} , i una pública A_{Pub} ,
- Bob té una clau privada B_{Priv} , i una pública B_{Pub} ,

Recordeu, cada persona coneix les seves claus i les públiques dels altres. Per tant, en el nostre cas:

- Alice coneix les seves claus i B_{Pub}
- Bob coneix les seves claus i A_{Pub}

Es defineix la notació següent per a l'exercici:

- $E_{A_{Pub}}(M) \rightarrow$ indica que A encripta amb la seva clau pública el missatge M
- $D_{A_{Pub}}(M) \rightarrow$ indica que A descripta amb la seva clau pública el missatge M

Per exemple, si fem:

$D_{A_{Priv}}(E_{A_{Pub}}(M)) \rightarrow$ el resultat és M (si encriptem amb la pública i descriptem amb la privada, missatge descodificat !)

$D_{A_{Pub}}(E_{A_{Priv}}(M)) \rightarrow$ el resultat és M (si encriptem amb la privada i descriptem amb la pública, missatge descodificat !)

Operació per obtenir el missatge encriptat X	Qui pot fer l'operació?	Qui pot desfer l'operació?	Operació inversa	Quina funcionalitat aconseguim ?
	A / B / Tothom	Només A / Només B / A i B conjuntament / Tothom		
$X := E_{A_{Priv}}(M)$	A	Tothom	$M = D_{A_{Pub}}(X)$	Assegurem que el missatge és de A (no repudi)
$X := E_{B_{Priv}}(M)$				

Heu de triar la resposta correcta que fa referència a l'operació $X := E_{B_{Priv}}(M)$

Selecione una:

- ☒ a.
- | | | | | |
|--------------------------|---|--------|----------------------|---|
| $X := E_{B_{Priv}}(M)$ | B | Tothom | $M = D_{B_{Pub}}(X)$ | Assegurem que el missatge és de B (no repudi) |
|--------------------------|---|--------|----------------------|---|
- ✓
- ☐ b.
- | | | | | |
|--------------------------|---|--------|----------------------|---|
| $X := E_{B_{Priv}}(M)$ | B | Tothom | $M = D_{A_{Pub}}(X)$ | Assegurem que el missatge és de A (no repudi) |
|--------------------------|---|--------|----------------------|---|
- ☐ c.

$X := E_{B_{priv}}(M)$	Tothom	B	$M = D_{B_{pub}}(X)$	Assegurem que el missatge és de B (no repudi)
------------------------	--------	---	----------------------	---

☐ d.

$X := E_{B_{priv}}(M)$	Tothom	Tothom	$M = D_{B_{pub}}(X)$	Assegurem que el missatge és de B (no repudi)
------------------------	--------	--------	----------------------	---

La teva resposta és correcta.

La respuesta correcta es:

$X := E_{B_{priv}}(M)$	B	Tothom	$M = D_{B_{pub}}(X)$	Assegurem que el missatge és de B (no repudi)
------------------------	---	--------	----------------------	---

- Tenim un missatge a enviar: M
- Alice té una clau privada A_{Priv} , i una pública A_{Pub} ,
- Bob té una clau privada B_{Priv} , i una pública B_{Pub} ,

Recordeu, cada persona coneix les seves claus i les públiques dels altres. Per tant, en el nostre cas:

- Alice coneix les seves claus i B_{Pub}
- Bob coneix les seves claus i A_{Pub}

Es defineix la notació següent per a l'exercici:

- $E_{A_{Pub}}(M) \rightarrow$ indica que A encripta amb la seva clau pública el missatge M
- $D_{A_{Pub}}(M) \rightarrow$ indica que A descripta amb la seva clau pública el missatge M

Per exemple, si fem:

$D_{A_{Priv}}(E_{A_{Pub}}(M)) \rightarrow$ el resultat és M (si encriptem amb la pública i descriptem amb la privada, missatge descodificat!)

$D_{A_{Pub}}(E_{A_{Priv}}(M)) \rightarrow$ el resultat és M (si encriptem amb la privada i descriptem amb la pública, missatge descodificat!)

Operació per obtenir el missatge encriptat X	Qui pot fer l'operació?	Qui pot desfer l'operació?	Operació inversa	Quina funcionalitat aconseguim ?
	A / B / Tothom	Només A / Només B / A i B conjuntament / Tothom		
$X := E_{A_{Priv}}(M)$	A	Tothom	$M = D_{A_{Pub}}(X)$	Assegurem que el missatge és de A (no repudi)
$X := E_{A_{Pub}}(M)$				

Heu de triar la resposta correcta que fa referència a l'operació $X := E_{A_{Pub}}(M)$

Selecione una:

- ☒ a.
- | | | | | |
|-----------------------|---|--------|-----------------------|---|
| $X := E_{A_{Pub}}(M)$ | A | Tothom | $M = D_{A_{Priv}}(X)$ | Assegurem que només A pot llegir el missatge (privacitat) |
|-----------------------|---|--------|-----------------------|---|
- ✗
- ☐ b.
- | | | | | |
|-----------------------|--------|---------|----------------------|---|
| $X := E_{A_{Pub}}(M)$ | Tothom | Només A | $M = D_{A_{Pub}}(X)$ | Assegurem que només A pot llegir el missatge (privacitat) |
|-----------------------|--------|---------|----------------------|---|
- ☐ c.

$X := E_{A_{pub}}(M)$	Tothom	Només A	$M = D_{A_{priv}}(X)$	Assegurem que només A pot llegir el missatge (privacitat)
-----------------------	--------	---------	-----------------------	---

☐ d.

$X := E_{A_{pub}}(M)$	Tothom	Només A	$M = D_{A_{priv}}(X)$	Assegurem que el missatge és de A (no repudi)
-----------------------	--------	---------	-----------------------	---

La teva resposta és incorrecta.

La respuesta correcta es:

$X := E_{A_{pub}}(M)$	Tothom	Només A	$M = D_{A_{priv}}(X)$	Assegurem que només A pot llegir el missatge (privacitat)
-----------------------	--------	---------	-----------------------	---

- Tenim un missatge a enviar: M
- Alice té una clau privada A_{Priv} , i una pública A_{Pub} ,
- Bob té una clau privada B_{Priv} , i una pública B_{Pub} ,

Recordeu, cada persona coneix les seves claus i les públiques dels altres. Per tant, en el nostre cas:

- Alice coneix les seves claus i B_{Pub}
- Bob coneix les seves claus i A_{Pub}

Es defineix la notació següent per a l'exercici:

- $E_{A_{Pub}}(M) \rightarrow$ indica que A encripta amb la seva clau pública el missatge M
- $D_{A_{Pub}}(M) \rightarrow$ indica que A descripta amb la seva clau pública el missatge M

Per exemple, si fem:

$D_{A_{Priv}}(E_{A_{Pub}}(M)) \rightarrow$ el resultat és M (si encriptem amb la pública i descriptem amb la privada, missatge descodificat!)

$D_{A_{Pub}}(E_{A_{Priv}}(M)) \rightarrow$ el resultat és M (si encriptem amb la privada i descriptem amb la pública, missatge descodificat!)

Operació per obtenir el missatge encriptat X	Qui pot fer l'operació?	Qui pot desfer l'operació?	Operació inversa	Quina funcionalitat aconseguim ?
	A / B / Tothom	Només A / Només B / A i B conjuntament / Tothom		
$X := E_{A_{Priv}}(M)$	A	Tothom	$M = D_{A_{Pub}}(X)$	Assegurem que el missatge és de A (no repudi)
$X := E_{B_{Pub}}(M)$				

Heu de triar la resposta correcta que fa referència a l'operació $X := E_{B_{Pub}}(M)$

Selecione una:

- ☒ a.
- | | | | | |
|-------------------------|---|--------|-----------------------|---|
| $X := E_{B_{Pub}}(M)$ | B | Tothom | $M = D_{B_{Priv}}(X)$ | Assegurem que només B pot llegir el missatge (privacitat) |
|-------------------------|---|--------|-----------------------|---|
- ✗
- ☐ b.
- | | | | | |
|-------------------------|--------|---------|-----------------------|---|
| $X := E_{B_{Pub}}(M)$ | Tothom | Només B | $M = D_{A_{Priv}}(X)$ | Assegurem que només A pot llegir el missatge (privacitat) |
|-------------------------|--------|---------|-----------------------|---|
- ☐ c.

$X := E_{B_{pub}}(M)$	Tothom	Només B	$M = D_{B_{priv}}(X)$	Assegurem que el missatge és de B (no repudi)
-----------------------	--------	---------	-----------------------	--

☐ d.

$X := E_{B_{pub}}(M)$	Tothom	Només B	$M = D_{B_{priv}}(X)$	Assegurem que només B pot llegir el missatge (privacitat)
-----------------------	--------	---------	-----------------------	---

La teva resposta és incorrecta.

La respuesta correcta es:

$X := E_{B_{pub}}(M)$	Tothom	Només B	$M = D_{B_{priv}}(X)$	Assegurem que només B pot llegir el missatge (privacitat)
-----------------------	--------	---------	-----------------------	---

- Tenim un missatge a enviar: M
- Alice té una clau privada A_{priv} , i una pública A_{pub} ,
- Bob té una clau privada B_{priv} , i una pública B_{pub} ,

Recordeu, cada persona coneix les seves claus i les públiques dels altres. Per tant, en el nostre cas:

- Alice coneix les seves claus i B_{pub}
- Bob coneix les seves claus i A_{pub}

Es defineix la notació següent per a l'exercici:

- $E_{A_{pub}}(M) \rightarrow$ indica que A encripta amb la seva clau pública el missatge M
- $D_{A_{pub}}(M) \rightarrow$ indica que A descripta amb la seva clau pública el missatge M

Per exemple, si fem:

$D_{A_{priv}}(E_{A_{pub}}(M)) \rightarrow$ el resultat és M (si encriptem amb la pública i descriptem amb la privada, missatge descodificat !)

$D_{A_{pub}}(E_{A_{priv}}(M)) \rightarrow$ el resultat és M (si encriptem amb la privada i descriptem amb la pública, missatge descodificat !)

Operació per obtenir el missatge encriptat X	Qui pot fer l'operació?	Qui pot desfer l'operació?	Operació inversa	Quina funcionalitat aconseguim ?
	A / B / Tothom	Només A / Només B / A i B conjuntament / Tothom		
$X := E_{A_{priv}}(M)$	A	Tothom	$M = D_{A_{pub}}(X)$	Assegurem que el missatge és de A (no repudi)
$tmp := E_{A_{priv}}(M)$ $X := E_{B_{pub}}(tmp)$				

Heu de triar la resposta correcta que fa referència a l'operació

$tmp := E_{A_{priv}}(M)$
 $X := E_{B_{pub}}(tmp)$

Seleccione una:

- ☐ a.
- | | | | | |
|---|---|---------|---|---|
| $tmp := E_{A_{priv}}(M)$
$X := E_{B_{pub}}(tmp)$ | A | Només B | $tmp := D_{B_{pub}}(X)$
$M := D_{A_{priv}}(tmp)$ | Assegurem que només B pot llegir el missatge (privacitat), i garantim que A és l'autor (no repudi). |
|---|---|---------|---|---|
- ☐ b.

$tmp := E_{A_{priv}}(M)$ $X := E_{B_{pub}}(tmp)$	B	Només A	$tmp := D_{B_{priv}}(tmp)$ $M := D_{A_{pub}}(X)$	Assegurem que només B pot llegir el missatge (privacitat), i garantim que A és l'autor (no repudi).
---	---	---------	---	---

☐ c.

$tmp := E_{A_{priv}}(M)$ $X := E_{B_{pub}}(tmp)$	A	Només B	$tmp := D_{B_{priv}}(X)$ $M := D_{A_{pub}}(tmp)$	Assegurem que només B pot llegir el missatge (privacitat), i garantim que A és l'autor (no repudi).
---	---	---------	---	---

☒ d.

$tmp := E_{A_{priv}}(M)$ $X := E_{B_{pub}}(tmp)$	A	Només B	$tmp := D_{B_{priv}}(X)$ $M := D_{A_{pub}}(tmp)$	Assegurem que només A pot llegir el missatge (privacitat), i garantim que B és l'autor (no repudi).
---	---	---------	---	---

✖

La teva resposta és incorrecta.

La respuesta correcta es:

$tmp := E_{A_{priv}}(M)$ $X := E_{B_{pub}}(tmp)$	A	Només B	$tmp := D_{B_{priv}}(X)$ $M := D_{A_{pub}}(tmp)$	Assegurem que només B pot llegir el missatge (privacitat), i garantim que A és l'autor (no repudi).
---	---	---------	---	---

- Tenim un missatge a enviar: M
- Alice té una clau privada A_{Priv} , i una pública A_{Pub} ,
- Bob té una clau privada B_{Priv} , i una pública B_{Pub} ,

Recordeu, cada persona coneix les seves claus i les públiques dels altres. Per tant, en el nostre cas:

- Alice coneix les seves claus i B_{Pub}
- Bob coneix les seves claus i A_{Pub}

Es defineix la notació següent per a l'exercici:

- $E_{A_{Pub}}(M) \rightarrow$ indica que A encripta amb la seva clau pública el missatge M
- $D_{A_{Pub}}(M) \rightarrow$ indica que A descripta amb la seva clau pública el missatge M

Per exemple, si fem:

$D_{A_{Priv}}(E_{A_{Pub}}(M)) \rightarrow$ el resultat és M (si encriptem amb la pública i descriptem amb la privada, missatge descodificat !)

$D_{A_{Pub}}(E_{A_{Priv}}(M)) \rightarrow$ el resultat és M (si encriptem amb la privada i descriptem amb la pública, missatge descodificat !)

Operació per obtenir el missatge encriptat X	Qui pot fer l'operació?	Qui pot desfer l'operació?	Operació inversa	Quina funcionalitat aconseguim ?
	A / B / Tothom	Només A / Només B / A i B conjuntament / Tothom		
$X := E_{A_{Priv}}(M)$	A	Tothom	$M = D_{A_{Pub}}(X)$	Assegurem que el missatge és de A (no repudi)
$tmp := E_{A_{Pub}}(M)$ $X := E_{B_{Pub}}(tmp)$				

Heu de triar la resposta correcta que fa referència a l'operació

$tmp := E_{A_{Pub}}(M)$
 $X := E_{B_{Pub}}(tmp)$

Selecione una:

- ☒ a.
- | | | | | |
|--|--------|--------------------|--|---|
| $tmp := E_{A_{Pub}}(M)$
$X := E_{B_{Pub}}(tmp)$ | Tothom | A i B conjuntament | $tmp := D_{B_{Priv}}(X)$
$M := D_{A_{Priv}}(tmp)$ | Només podrem llegir el missatge si A i B el descripten en equip, primer un i després l'altre! |
|--|--------|--------------------|--|---|



- ☐ b.

tmp := E _{Apub} (M) X := E _{Bpub} (tmp)	Tothom	A i B conjuntament	tmp := D _{Bpriv} (X) M := D _{Apub} (tmp)	Només podrem llegir el missatge si A i B el descrypten en equip, primer un i després l'altre!
--	--------	--------------------	---	---

☐ c.

tmp := E _{Apub} (M) X := E _{Bpub} (tmp)	Tothom	A i B conjuntament	tmp := D _{Bpub} (X) M := D _{Apriv} (tmp)	Només podrem llegir el missatge si A i B el descrypten en equip, primer un i després l'altre!
--	--------	--------------------	---	---

☐ d.

tmp := E _{Apub} (M) X := E _{Bpub} (tmp)	A i B conjuntament	A i B conjuntament	tmp := D _{Bpriv} (X) M := D _{Apriv} (X)	Només podrem llegir el missatge si A i B el descrypten en equip, primer un i després l'altre!
--	--------------------	--------------------	--	---

La teva resposta és correcta.

La respuesta correcta es:

tmp := E _{Apub} (M) X := E _{Bpub} (tmp)	Tothom	A i B conjuntament	tmp := D _{Bpriv} (X) M := D _{Apriv} (tmp)	Només podrem llegir el missatge si A i B el descrypten en equip, primer un i després l'altre!
--	--------	--------------------	--	---

ROT13 (de l'anglès rotate by 13 places: «girar 13 posicions», de vegades escrit amb guió ROT-13) és un xifratge per substitució simple que substitueix cada lletra per la seva corresponent situada 13 posicions després en l'alfabet. ROT13 és un exemple del xifratge de Cèsar, desenvolupat a l'antiga Roma.

En l'alfabet llatí bàsic, de 26 caràcters, ROT13 és el seu propi invers; és a dir, per desfer ROT13, s'aplica el mateix algorisme, per tant, la mateixa acció es pot utilitzar per a la codificació i la decodificació. L'algorisme no proporciona pràcticament cap seguretat criptogràfica i se'l cita sovint com un exemple canònic de xifrat feble.

ROT13 s'usa en els fòrums d'Internet com a mitjà d'ocultació d'espòilers o filtracions, bromes, solucions de trencaclosques, i materials ofensius a la mirada fortuïta. Aquest criptosistema ha inspirat diversos jocs de lletres i paraules a Internet i s'esmenta sovint en converses de grups de discussió.

La vostra tasca

Heu d'omplir els buits del programa que simuli el xifrat de ROT13. Per tal de facilitar-ho, suposarem que el text sol té lletres (sense números i espais). Les lletres seran les corresponents a l'alfabet català (26 caràcters).

Aquest mètode substitueix cada lletra del text per una altra lletra que es troba 13 posicions endavant a l'alfabet. A més a més, es considera circular, el que vol dir que després de la “z” ve la “a”. Per exemple si la N és 4, la “a” serà la “d”, la “b” en la “i” i així successivament.

Per tal d'aplicar ROT13 a una part d'un text només cal examinar-ne els caràcters alfabètics i substituir-los cadascun per la lletra situada **13 posicions** més endavant en l'alfabet, seguint pel principi si cal. Així, en l'alfabet català de 26 caràcters, la **A es converteix en N**, la B esdevé O, i així successivament fins a la M, que es converteix en Z.

Llavors la seqüència continua pel principi de l'alfabet: la N es converteix en A, la O es converteix en B, i així successivament fins a la Z, que es converteix en M.

Els nombres, símbols, espais en blanc i tots els altres caràcters no es modifiquen. Com que hi ha 26 lletres en l'alfabet en català i $26 = 2 \times 13$, la funció ROT13 és la **seva pròpia funció inversa**. **Utilitzem la mateixa funció tant per xifrar com per desxifrar.**

En altres paraules, dues aplicacions successives de ROT13 restauren el text original (en [matemàtiques](#), això de vegades s'anomena una [involució](#); en [criptografia](#), un [xifrat recíproc](#)). La transformació es pot realitzar usant una [lookup table](#), com ara la següent:

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm

L'exercici ha d'encriptar el text “*Hola Mundo*” o qualsevol altre.

En el primer cas el resultat serà: Ubyn Zhaqb

Si torneu a emprar la funció ROT13 el resultat hauria de ser **Hola Mundo** un altre cop.

```

public class Rot13 {

    static String cadena = "Hola Mundo";    //cadena de caràcters

    public static void main(String[] args) {

        System.out.println("text a xifrar: "+cadena);    //imprimeix la cadena per pantalla.

        String str1 = rot13(cadena);    //xifra la cadena i la guarda a str1

        System.out.println("text xifrat: "+str1);    //imprimeix str1 per pantalla

        String str2 = rot13(str1);    //desxifra str1 i es guarda a str2

        System.out.println("text dexifrat:" +str2);    //imprimeix str2 per pantalla

        if(  ✖ )
            System.out.println("Després de xifrar i desxifrar el missatge hem obtingut el mateix text");
        else
            System.out.println("ERROR!");
    }

    /**
     * Xifra o Desxifra una cadena de caràcters amb ROT13.
     *
     *
     * @return una cadena de caràcters xifrada o desxifrada.
     */
    static String rot13(String cadena) {
        char c;

        StringBuilder temp = new StringBuilder();    //crea un StringBuilder per construir la cadena resultant en la variable
temp

        for (int i = 0 ; i < [1] ; i++) {    //comença el bucle per analitzar els caràcters de la cadena
            c =  ✔ ;    //obté el caràcter de la posició actual de la cadena i
es guarda en la variable c

            if (c >= 'A' && c < 'N') {    //compara c amb A i N
                 ✔    //si és igual o major que A i menor que N, es realitza
un desplaçament sumant-1'hi 13
            } else if (c >= 'N' && c <= 'Z') {    //compara c con N i Z
                c -= 13;    //si és igual o major que N i igual o menor que Z, es realitza un desplaçament
restant 13
            } else if (c >= 'a' && c < 'n') {    //compara c con a i n
                c += 13;    //si és igual o major que a i menor que n, es realitza un desplaçament sumant-
1'hi 13
            } else if (  ✖ {    //compara c con n i z
                 ✔    //si és igual o major que n i igual o menor que z, es
realitza un desplaçament restant 13
            }
        }
    }

```

```
temp.append(c);  
}  
  
return temp.toString();  
}  
}
```

La resposta és parcialment correcta.

Ha seleccionado correctamente 4.

La respuesta correcta es:

ROT13 (de l'anglès rotate by 13 places: «girar 13 posicions», de vegades escrit amb guió ROT-13) és un xifratge per substitució simple que substitueix cada lletra per la seva corresponent situada 13 posicions després en l'alfabet. ROT13 és un exemple del xifratge de Cèsar, desenvolupat a l'antiga Roma.

En l'alfabet llatí bàsic, de 26 caràcters, ROT13 és el seu propi invers; és a dir, per desfer ROT13, s'aplica el mateix algorisme, per tant, la mateixa acció es pot utilitzar per a la codificació i la decodificació. L'algorisme no proporciona pràcticament cap seguretat criptogràfica i se'l cita sovint com un exemple canònic de xifrat feble.

ROT13 s'usa en els fòrums d'Internet com a mitjà d'ocultació d'espòilers o filtracions, bromes, solucions de trencaclosques, i materials ofensius a la mirada fortuïta. Aquest criptosistema ha inspirat diversos jocs de lletres i paraules a Internet i s'esmenta sovint en converses de grups de discussió.

La vostra tasca

Heu d'omplir els buits del programa que simuli el xifrat de ROT13. Per tal de facilitar-ho, suposarem que el text sol té lletres (sense números i espais). Les lletres seran les corresponents a l'alfabet català (26 caràcters).

Aquest mètode substitueix cada lletra del text per una altra lletra que es troba 13 posicions endavant a l'alfabet. A més a més, es considera circular, el que vol dir que després de la “z” ve la “a”. Per exemple si la N és 4, la “a” serà la “d”, la “b” en la “i” i així successivament.

Per tal d'aplicar ROT13 a una part d'un text només cal examinar-ne els caràcters alfabètics i substituir-los cadascun per la lletra situada **13 posicions** més endavant en l'alfabet, seguint pel principi si cal. Així, en l'alfabet català de 26 caràcters, la **A es converteix en N**, la B esdevé O, i així successivament fins a la M, que es converteix en Z.

Llavors la seqüència continua pel principi de l'alfabet: la N es converteix en A, la O es converteix en B, i així successivament fins a la Z, que es converteix en M.

Els nombres, símbols, espais en blanc i tots els altres caràcters no es modifiquen. Com que hi ha 26 lletres en l'alfabet en català i $26 = 2 \times 13$, la funció ROT13 és la **seva pròpia funció inversa**. **Utilitzem la mateixa funció tant per xifrar com per desxifrar.**

En altres paraules, dues aplicacions successives de ROT13 restauren el text original (en [matemàtiques](#), això de vegades s'anomena una [involució](#); en [criptografia](#), un [xifrat recíproc](#)). La transformació es pot realitzar usant una [lookup table](#), com ara la següent:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz  
NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm
```

L'exercici ha d'encriptar el text “*Hola Mundo*” o qualsevol altre.

En el primer cas el resultat serà: Ubyn Zhaqb

Si torneu a emprar la funció ROT13 el resultat hauria de ser **Hola Mundo** un altre cop.

```

public class Rot13 {

    static String cadena = "Hola Mundo";    //cadena de caràcters

    public static void main(String[] args) {

        System.out.println("text a xifrar: "+cadena);    //imprimeix la cadena per pantalla.
        String str1 = rot13(cadena);    //xifra la cadena i la guarda a str1
        System.out.println("text xifrat: "+str1);    //imprimeix str1 per pantalla

        String str2 = rot13(str1);    //desxifra str1 i es guarda a str2
        System.out.println("text dexifrat:" +str2);    //imprimeix str2 per pantalla

        if([str2.equals(cadena)])
            System.out.println("Després de xifrar i desxifrar el missatge hem obtingut el mateix text");
        else
            System.out.println("ERROR!");
    }

    /**
     * Xifra o Desxifra una cadena de caràcters amb ROT13.
     *
     * @return una cadena de caràcters xifrada o desxifrada.
     */
    static String rot13(String cadena) {
        char c;
        StringBuilder temp = new StringBuilder();    //crea un StringBuilder per construir la cadena resultant en la
variable temp

        for (int i = 0 ; i < [1] ; i++) {    //comença el bucle per analitzar els caràcters de la cadena
            c = [cadena.charAt(i)];    //obté el caràcter de la posició actual de la cadena i es
guarda en la variable c

            if (c >= 'A' && c < 'N') {    //compara c amb A i N
                [c += 13];    //si és igual o major que A i menor que N, es realitza un desplaçament
sumant-1'hi 13
            } else if (c >= 'N' && c <= 'Z') {    //compara c con N i Z
                c -= 13;    //si és igual o major que N i igual o menor que Z, es realitza un
desplaçament restant 13
            } else if (c >= 'a' && c < 'n') {    //compara c con a i n
                c += 13;    //si és igual o major que a i menor que n, es realitza un desplaçament
sumant-1'hi 13
            } else if [(c>= 'n' && c <= 'z')] {    //compara c con n i z
                [c -= 13];    //si és igual o major que n i igual o menor que z, es realitza un
desplaçament restant 13
            }

            [temp.append(c); ]    //afegeix c en temp
        }

        return temp.toString();    //retornem la variable temp, que conté la cadena xifrada o desxifrada
    }
}

```

