

Protecció i Seguretat

- 1- Què s'entén per Privacitat, Autenticitat, Integritat i No Repudiació
- 2- Quina diferència hi ha entre Protecció i Seguretat
- 3- Per què cal fer control d'accés un cop ja s'ha fet l'autenticació
- 4- Quins mètodes d'autenticació hi han
- 5- Quin problema té l'ús de matrius d'accés
- 6- Quines diferències hi han entre les Capabilities i les ACLs
- 7- Quina és una bona combinació d'ACLs i Capabilities
- 8- Quan es poden tenir problemes de seguretat en les comunicacions i com ajuda l'ús de criptografia
- 9- Quines són les dues grans classes d'algorismes d'encryptació
- 10- Què és una clau i per què és important el seu tamany
- 11- Quins avantatges té la criptografia simètrica sobre l'asimètrica i viceversa
- 12- Com es pot combinar l'ús de la criptografia simètrica i l'asimètrica per solventar els problemes
- 13- Com s'han de fer servir les claus quan s'usa criptografia asimètrica per aconseguir:
 - 13.a- privacitat
 - 13.b- autenticitat
- 14- Per a què serveix una signatura digital
- 15- Com es fa una signatura digital
- 16- Què fan les autoritats de certificació
- 17- Què és i com es fa un certificat digital
- 18- Com es pot comprovar l'autenticitat d'un certificat digital
- 19- Explicar alguns exemples d'ús de la criptografia en l'àmbit de la informàtica
- 20- Com afecta l'aspecte legal a l'utilització de la criptografia en l'àmbit civil
- 21- Per a què ens pot servir un CERT
- 22- Com afecta la potència de càlcul dels ordenadors al fet que un algorisme criptogràfic es consideri segur o no
- 23- Per què una aplicació pot requerir l'utilització d'un algorisme d'encryptació simètric, un d'assimètric i un de creació de resum (anomenat digest o MAC)

Sincronització

- 1- Per què és necessari tenir mecanismes de sincronització
- 2- Quins problemes hi han de cara a la sincronització quan es treballa amb un SOD
- 3- Per què cal sincronitzar els rellotges periòdicament
- 4- Què cal tenir en compte de cara a sincronitzar els rellotges
- 5- Quins tipus de sincronització de rellotges hi han i per a què és útil cada una d'elles
- 6- Quines són les implicacions de l'existència d'un temps de propagació dels missatges (TPM) pel que fa a la sincronització dels rellotges
- 7- Avaluar cada un dels algorismes de sincronització: utilitat, avantatges, inconvenients, ...
- 8- Quins són alguns dels serveis de sincronització i informació de temps existents i en que es basen
- 9- Ens quins casos és suficient una ordenació d'events
- 10- En referència a la relació ocorregut-abans:
 - 10.a- explicar les característiques fonamentals
 - 10.b- per què ens dona només una ordenació parcial dels events
- 11- En referència als rellotges lògics:
 - 11.a- Quin és el seu funcionament
 - 11.b- Quin paper juga l'enviament de missatges entre nodes del sistema en la seva sincronització
- 12- Com es pot aconseguir una ordenació total dels events

- 13- Per què no es pot usar un semàfor per a tractar una exclusió mútua en un SOD
- 14- Avaluar cada un dels algorismes d'exclusió mútua: utilitat, avantatges, inconvenients, ...
- 15- Definir una transacció atòmica i explicar les seves característiques i utilitats
- 16- Què s'entén per commit i per rollback
- 17- En què es basa l'evitació d'abraçades mortals i quins són els seus inconvenients
- 18- Quines són les 4 condicions necessàries per a que es doni una abraçada mortal
- 19- En què es basa la prevenció d'abraçades mortals
- 20- Avaluar el mecanisme de prevenció d'abraçades mortals amb:
 - 20.a- peticions col·lectives
 - 20.b- peticions ordenades
 - 20.c- apropiació de recursos
- 21- Avaluar els algorismes d'apropriació de recursos: Wait-Die i Wait-Wound
- 22- Quins són els aspectes importants de la detecció i recuperació d'abraçades mortals
- 23- Per a què serveix un algorisme d'elecció

Fiabilitat

- 1- Què s'entén per una fallada i quins tipus hi han
- 2- En què consisteix l'evitació de fallades
- 3- Què s'entén per tolerància a fallades
- 4- Quantes rèpliques són necessàries per a ser tolerant a fallades de tipus:
 - 4.a- fallar-parar
 - 4.b- bizantí
- 5- Quines tècniques vistes al curs de CASO són útils per a la detecció i recuperació de fallades
- 6- Per què es diu que cal replicar, però que cal fer-ho amb seny