UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria de Manresa

Final d'Aplicacions i Serveis

19 de juny de 2025 | Enginyeria de Sistemes TIC | 120 MINUTS

COGNOMS:

NOM: SUBGRUP:

Exercici 1 [14 punts]. Responeu cert (C) o fals (F) a les següents frases. Justifiqueu la resposta. Respostes i justificacions contradictòries no compten. Resposta o justificació incorrectes resten 1/2 punt. Les respostes sense justificació sumen o resten la meitat. Si no hi ha resposta (C) o (F) no compten.

a) No és possible tenir integritat de les comunicacions sense tenir confidencialitat.

b) No és possible tenir confidencialitat sense tenir integritat.

c) Si tenim confidencialitat a la capa d'aplicació no cal tenir confidencialitat a les capes inferiors.

d) Per a que dos interlocutors pactin una clau de sessió cal fer servir sempre xifrat asimètric per l'intercanvi de la clau de sessió.

e) Els registres TXT del DNS estan definits per permetre augmentar la fiabilitat del servei de correu.

f) Els servidors DNS Autoritat accepten normalment consultes recursives.

g) Els servidors DNS locals accepten normalment consultes recursives i realitzen consultes iteratives.

h) Si una persona genera el parell de claus públic i privat, pot signar missatges per a ella mateixa i xifrar missatges per a tothom.

i) Un certificat digital és el resultat de xifrar el valor de la clau privada d'una identitat, fent servir la clau pública d'una altra entitat de la que es coneix de manera fiable aquesta clau pública.

j) Els documents signats digitalment caduquen quan la clau utilitzada també caduca, de manera que cal tornar a signar-los.

k) Quan el GPG demana una clau a l'usuari per realitzar alguna operació de seguretat, està demanant la clau privada.

l) Quan es compra un domini, el gestor al que li contractes demana al responsable del top level domain una entrada a la seva base de dades amb un registre NS del domini registrat cap a un servidor de DNS autoritat administrat pel propi gestor.

m) El protocol HTTPS sempre garanteix la confidencialitat de la informació entre client i servidor a més de garantir l'autenticació de servidor però no de client.

n) La resolució de noms inversa que ofereix el servei de DNS només es pot demanar al teu proveïdor d'Internet sense que sigui possible contractar-la a un gestor de DNS qualsevol.

Exercici 2 [8 punts]. Respon **sí** o **no** i justifica si els següents mecanismes serveixen per autentificar, evitant l'atac de gravació, a un usuari A davant d'un usuari B. Considereu que si no es diu el contrari, la comunicació no està xifrada. Quan es parla de contrasenya, tant A com B la coneixen.

a) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge $H(m)$ com a prova de la seva identitat, on $H(m)$ és el resultat d'aplicar una funció de hash coneguda.

b) Usuari B envia un missatge aleatori m_1 a A. A retorna a B el missatge $H(m_1\|m_2)$ on m_2 és un missatge aleatori generat per A i $m_1\|m_2$ és la concatenació dels dos missatges. $H()$ és una funció de hash coneguda.

c) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge $K(m)$ que és el resultat d'aplicar una transformació a m on aquesta funció $K()$ de transformació només és coneguda per A i B.

d) Usuari B envia un missatge aleatori m_1 a A. A retorna a B el missatge $H(m_1\|m_2)$ on m_2 és un missatge fixe conegut només per A i per B. $H()$ és una funció de hash coneguda.

e) Usuari B espera la recepció d'un missatge c de A, on c és la contrasenya associada a A.

f) Usuari B espera la recepció d'un missatge m de A, on $m = KBp(c)$ és la contrasenya associada a A xifrada amb la clau pública de B.

g) Usuari B espera la recepció d'un missatge m de A, on $m = K(c)$ és la contrasenya associada a A xifrada amb una clau només coneguda per A i B.

h) Usuari B envia un missatge aleatori m_1 a A. A retorna a B el missatge $KBp(m_2)$ on m_2 és un missatge aleatori generat per A. La concatenació $K = m_1\|m_2$ és la clau de sessió d'un algoritme conegut de xifrat simètric. Usuari A envia $K(c)$ a B, on c és la contrasenya associada a A i coneguda per B.

Exercici 3 [2 punts]. Suposa que N persones volen comunicar-se entre elles fent servir claus simètriques. Totes les comunicacions entre qualsevol de 2 persones és visible per la resta de persones i cap d'aquesta la resta ha de poder descodificar la comunicació. Quin és el nombre de claus totals que calen en aquest sistema?

Exercici 4 [2 punts]. Suposa les mateixes N persones de l'exercici anterior amb les mateixes condicions, excepte que ara es fa servir clau pública i privada. En aquest cas, quants parells de claus calen en total?

Exercici 5 [2 punts]. Quina utilitat té la comanda systemctl? Descriu quins són els seus paràmetres típics.

Exercici 6 [2 punts]. Descriu de manera qualitativa quina serà la resposta de la comanda `dig @10.2.3.4 -t AAAA asi.cat`, definint el significat de cada paràmetre.

Exercici 7 [2 punts]. Descriu quina utilitat té la directiva VirtualHost en Apache.

Exercici 8 [6 punts]. Sigui el següent codi:

```
<!DOCTYPE HTML>
<html lang="ca">
  <head>
    <meta charset="UTF-8">
    <title>Examen ASI</title>
    <script>
      function load() {
          const xmlhttp;
          const objecte_div;
          objecte_div=document.getElementById("myDiv");
          xmlhttp=new XMLHttpRequest();
          xmlhttp.onload=function() {
              objecte_div.innerHTML=xmlhttp.responseText; }
          xmlhttp.open('GET','sensor/estat');
          xmlhttp.send(); }
      setInterval("load()",3000);
    </script>
  </head>
  <body>
    <div id="myDiv"> Bona Sort! </div>
  </body>
</html>
```

a) Descriu de manera general què fa aquest codi.

b) Descriu què són: xmlhttp, objecte_div, sensor/estat, mydiv

c) En el codi es fan servir Callbacks? Respon Sí o No. Tant en cas en un cas com un altre, justifica la resposta.

Exercici 9 [6 punts]. Quan es vol aplicar l'algoritme RSA, tingueu en compte que $p = 3$, $q = 11$ i $e = 3$. El mapa entre lletres i valors és el següent:

A:1, B:2, C:3, D:4, E:5, F:6, G:7, H:8, I:9, J:10, K:11, L:12, M:13, N:14, O:15, P:16, Q:17, R:18, S:19, T:20, U:21, V:22, W:23, X:24, Y:25, Z:26, _:27, Ç:28, Ñ:29, *:30, !:31, ?:32, +:33

a) Troba el valor més petit possible per d.

b) Quin són els parells de claus públic i privat?

c) En quina operació recau la fortalesa d'aquest algoritme per aplicar-lo a la seguretat?

d) Desxifreu INI_. [3 punts]

Exercici 10 [6 punts]. Un estudiant TIC espavilat vol patentar un mecanisme d'autentificació. El mecanisme generarà 6 dígits decimals que tindran una validesa durant 30 segons i serviran per a que B autentifiqui a A. El procediment és el següent:

- Originalment A i B pacten una clau k de manera segura.
- El *Epoch Time* o temps UNIX és el nombre de segons que han passat des de mitjanit de l'1 de gener de 1970. Generalment està codificat als rellotges de les màquines com un enter amb signe de 32 bits. Després de consultar aquest valor a la màquina, es fa una divisió entera per 100 obtenint el valor $t100$.
- La funció de Hash SHA-256, disponible a la majoria de sistemes Linux, genera una sortida de 256 bits. Amb aquesta funció es calcula el Hash del missatge format per la clau k seguida de $t100$. El resultat és el valor v.
- Es considera que v és un enter sense signe de 256 bits. Es crea la cadena de caràcters formada per la representació decimal d'aquest valor i es trunca aquesta cadena agafant els 6 caràcters menys significatius, obtenint vm.
- vm serà el valor que A envia a B com a contrasenya per poder ser autentificat.

a) Aquest mecanisme es pot considerar adequat per a que B autentifiqui a A? Resposta (S) o (N).

b) Justifica el perquè.

c) Si ho consideres necessari, proposa quines modificacions faries.