Criptografia i Seguretat
Curs 2022

1 de Juny 2022
Segon Parcial

Nom i Cognoms: SERGI GARRIGA MAS

NIU: 1606989

Puntuació: Exercicis 1-10: 1 punt
Duració: 110 minuts.

Les classes de problemes: Ajuden molt ☒ Ajuden ☐ No ajuden ☐
Hores de preparació:
Gràcies per contestar aquestes preguntes que no tindran cap impacte en l'avaluació.

1. Detalleu els passos que seguirien dos usuaris l'Alícia i el Bernardo per establir una clau de **sessió simètrica** si utilitzessin el protocol de **Diffie-Hellman** amb els següents tres punts de partida:
   a. Només l'usuari Alícia coneix el secret a
   b. Només l'usuari Bernardo coneix el secret b
   c. L'Alícia i el Bernardo comparteixen el nombre primer p i l'element generador g.

a) Alicia envia a Bern $g^a \bmod p$. Bernaldo fa $(g^a)^b \bmod n = \boxed{k}$

b) Bern envia a Alicia $g^b \bmod p$. Alicia fa $(g^b)^a \bmod n = \boxed{k}$

c) Ambdós tenen la mateixa clau: poden començar

2. L'Alícia i en Bernardo es volen comunicar **de manera confidencial i autèntica** fent servir un sistema basat en criptografia asimètrica. **Descriu** com enviarà un missatge l'Alícia dirigit al Bernardo.

(A) $E_{PubB}(m)$, $E_{priv_A}h(m)$ (B)

3. A TOR, el protocol per **anonimitzar** les comunicacions permet al node Alícia romandre anònim quan contacta un altre node. Per aquesta finalitat, es fa servir una variació del protocol Diffie-Hellman (DH). En aquesta variació de DH, l'Alícia envia el primer missatge de DH xifrat amb la clau pública del node TOR amb el que es vol crear la clau simètrica. El missatge que contesta el node TOR en qüestió ve acompanyat amb un **hash de la clau** que s'ha creat amb DH. **Raoneu** com pot ajudar aquest hash a prevenir un atac en el que algú vulgui impersonar el node TOR.

DF-Hellman autenticat.

$E_{K_{pubB}}(g^b \bmod n)$

$g^b \bmod n, h(k)$

amb $h(k)$ demostrem que tenim la clau sense enviar-la.

4. M.A.R., una agencia d'espionatge, ha interceptat un **missatge xifrat** amb el sistema **RSA** i sap que la longitud de les claus utilitzades és de 2048 bits. Aquest missatge prové de l'administració A i ha estat enviat cap a l'administració B. Com que la clau pública de l'administració B és coneguda ($KPub_B = (n, e)$), **expliqueu** els passos que seguiria aquesta agencia d'espionatge per **desxifrar el missatge** si disposen d'un supercomputador capaç de realitzar qualsevol operació matemàtica amb nombres de 2048 bits en menys de 10 minuts.

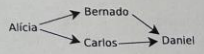
Mirar RSA. Com es genera claus + xifrat i desxifrat.

$pq \rightarrow \phi(n) \rightarrow (p-1)(q$

5. Un usuari es connecta al servidor online del banc de CiS (`www.bancdecis.com`). Per a que aquest servidor sigui segur es fan servir **certificats per autenticar-lo**. El certificat que rep l'usuari té com a **identitat** "www.bancdecis.com". El certificat està **signat** per una CA la qual l'usuari **la considera de confiança**. **Raona** què haurà de provar el servidor "Banc de CiS" per convèncer l'usuari que la conversa és **autèntica**.

L'usuari: per enviar un missatge encriptat amb la clau pública del certificat al servidori, en el cas que ho pugui desencriptar, serà autèntic.

6. Al proper diagrama es veu diferents certificats d'un **sistema distribuït** de signatura de claus. La notació A->B vol dir que A **ha signat el certificat** de B. En aquest sistema una **clau és vàlida** si s'ha signat personalment, si s'ha signat amb una clau de **total confiança**, o bé, si ha estat signat per **dos claus** de confiança marginal.



(a) Si sabem que l'Alícia té una **confiança marginal** en el Bernardo i en el Carlos, raona quines claus considerarà l'Alícia com a vàlides **especificant el tipus de validesa**.

Carlos → vàlid, signat personalment.
Bernaldo → " , "
Daniel → 1) Només firma per B o C → No vàlid
2) Firmat per B i C → vàlid

(b) I si l'Alícia té una **confiança marginal** només en el Bernardo?

Bernaldo → vàlid, signat personalment
Daniel → no vàlid, ja que només es firma per B, que te confiança marginal

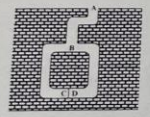
7. El **protocol de Shamir** entre dos nodes, A i B, funciona en tres etapes. **Primer**, A xifra un missatge amb la seva clau i envia el missatge xifrat a B ($E_{ka}(m)$). En la **següent etapa**, B xifra aquest missatge amb la seva clau i el torna a enviar a A ($E_{kb}(E_{ka}(m))$). En l'etapa **final**, A desxifra el segon missatge amb la seva clau i envia el resultat a B ($E_{kb}(m)$). D'aquesta manera, B pot desxifrar aquest últim missatge per obtenir el missatge original. **Raona** les implicacions que té que l'algoritme de xifra en aquest context sigui:

- (a) $E_k(m) = k \ xor \ m$

Fàcil d'interceptar

- (b) $E_k(m) = m^k \ mod \ p$ (donat un p, primer)

8. Alí Babá vol demostrar al Bertrand Russel que **sap les paraules màgiques** per obrir la porta que separa C de D.



Trobeu i expliqueu un protocol de coneixement nul que pugui implementar l'Alí Babá per aquest problema. **Raoneu** per què és de coneixement nul.

Fàcil, ho faig a casa.

9. L'Alícia ha trobat **dues claus públiques diferents** $pub1$ i $pub2$. Les dues claus pertanyen al Bernardo que té les seves corresponents claus privades. La primera clau ($pub1$) és una clau RSA (sistema de clau asimètrica no homomòrfic). La segona clau ($pub2$) és una clau Paillier (sistema de clau asimètrica homomòrfic). A més a més, l'Alícia ha trobat els següents dos missatges ($m1$ i $m2$):

- $m1 = Encrypt\_RSA_{pub1}(23)$
- $m2 = Encrypt\_Paillier_{pub2}(23)$

Fent servir les claus $pub1$ i $pub2$, $m1$ i $m2$ i l'operació $*$ de multiplicació, l'Alícia crea els **següents dos missatges** ($m3$ i $m4$):

- $m3 = Encrypt\_RSA_{pub1}(2) * m1$
- $m4 = Encrypt\_Paillier_{pub2}(2) * m2$

Raona quina informació obtindrà en Bernardo **desencriptant**, fent servir les seves claus privades, els missatges $m3$ i $m4$:

(a) $m3$

Horrible, bits random → no és homomòrtic i la criptosistema no té la qualitat d'operar

(b) $m4$

Homomòrtic $Ek(2 \cdot 23)$

10. L'Alícia i el Bernardo **volen jugar a cara i creu per telèfon**. Per aquest motiu, en Bernardo ha proposat que L'Alícia triarà un nombre (a) i el Bernardo triarà un altre nombre (b). Després s'intercanviaran els nombres triats per telèfon, de tal manera que **si** $a+b$ **es parell**, guanyarà Alícia i en cas contrari, guanyarà el Bernardo. L'Alícia sap molt de criptografia i li diu al Bernardo que aquest protocol no és segur ja que el primer en enviar el nombre per telèfon jugaria en desavantatge. L'Alícia proposa que s'enviïn abans un **compromís**. **A què es refereix** l'Alícia? **Com es pot implementar** per aquest cas en concret?