



# ARCADE LAND



**TeduSa**  
FESTIVAL



**7 A 11 AGOSTO 2025**

**PLAYA DE CULLERA**

ACT OF  
RAGE -  
AFROJACK  
- ALESSO -  
AMBER  
BROOS  
ARMIN  
VAN  
BUUREN -  
ART OF  
FIGHTERS  
- BEN  
SIMS  
BRENDA  
SERNA -  
CARL  
CRAIG -  
CHARLOTT  
E DE  
WITTE  
CRISTIAN  
VARELA -  
D-BLOCK &  
S-TEFAN -  
DENNIS  
CRUZ  
DEXPHASE  
- DJ PEPO -  
DUAL  
DAMAGE -  
DYEN  
EDU  
IMBERNON  
-  
ENDYMION  
- FATIMA  
HAJJI  
FEDDE LE  
GRAND -  
HARDWELL  
- HÉCTOR  
OAKS  
JAMIE  
JONES -  
KLANGKUE  
NSTLER -  
KREWELLA  
LA LUNA  
LIVE -  
LAIDBACK  
LUKE -  
LEE ANN  
ROBERTS  
LILLY  
PALMER -  
LUCIANO -  
MANDY

CS 2021

104355 – Criptografia i Seguretat

## Examen Parcial 2

Nom:

NIU:

- Cada resposta ha de ser degudament justificada (de manera breu i concisa).
- No es pot tenir cap dispositiu electrònic i/o de comunicació (telèfon mòbil, smartwatch, tablet, calculadora, etc.) durant la realització de l'examen. Tal com indica la guia docent, tenir d'un d'aquests dispositius durant l'examen (estigui encès o apagat) comporta una qualificació de zero sense possibilitat de recuperació.

1. Definim una funció hash  $H^1$  com:

$$H^1(x) = x + 4 \pmod{10}$$

on  $x \in \mathbb{N}$ .

- i. és una funció hash criptogràfica? per què?
  - ii. construïm un arbre de Merkle (binari) pel conjunt de nombres  $\{2, 20, 101, 58\}$ . Quina serà l'arrel?
2. Suposem que els usuaris  $A$  i  $B$  volen acordar secretament un valor  $K_{AB}$  i per fer-ho utilitzen el protocol de Diffie-Hellman. Suposant que utilitzen com a paràmetres públics els valors  $p = 137$  i  $\alpha = 5$ , i que  $A$  té com a valor secret  $a = 4$  i  $B$  té com a valor secret  $b = 10$ , descriu el protocol indicant els diferents passos que realitzaran i calculeu el valor final  $k$  que compartiran.
  3. L'Alice i en Bob utilitzen un esquema de signatura digital ElGamal amb paràmetres  $\mathbb{Z}_{113}$  i  $\alpha = 3$  per autenticar els seus missatges. L'Alice té com a clau privada el valor  $SK_A = 6$  i en Bernat  $SK_B = 12$ .
    1. L'Alice ha rebut el missatge  $m = 8$  i la signatura (sense utilitzar cap funció hash)  $(r, s) = (12, 8)$ . Pot estar segura l'Alice que el missatge l'ha rebut del Bob?. Comproveu-ho.
  4. Demostreu que en un criptosistema RSA amb  $n = 35$  els exponents ( $e$  i  $d$ ) de cada parells de claus pública i privada són els mateixos. Es a dir, que sempre tindrem que  $e = d$ .
  5. En una PKI, l'entitat emissora de certificats envia el certificat al sol·licitant que el podrà verificar amb la clau pública de l'entitat emissora. Aquest certificat digital emés per l'entitat conté la clau pública del sol·licitant, la identitat, la data de validesa i està signat amb la seva clau privada.
    - i. Què vol dir "la seva clau privada"? la del sol·licitant? la de l'entitat emissora?
    - ii. Els altres usuaris de la PKI el poden verificar aquest certificat? En cas afirmatiu, com ho farien?
    - iii. El sol·licitant guarda el seu certificat digital al seu ordinador. L'ha de guardar en secret (xifrada o amb un password)? Què pot passar si li fan una còpia d'aquest certificat, en el cas que no l'hagi guardat de manera secreta?
  6. Alice i Bob volen intercanviar-se missatges de manera confidencial i garantint l'autenticitat fent servir RSA i amb signatura digital basada en la funció hash  $H$ . Les claus públiques de Alice i Bob són respectivament:  $PK_A = (e_A, n_A) = (171, 391)$  i  $PK_B = (27, 517)$ , on  $391 = 23 * 17$ , i  $517 = 47 * 11$ . (Justifiqueu totes les respostes).

- i. Perquè i com es fa servir una funció hash a les signatures digitals?
  - ii. Bob rep d'Alice ( $s = 165, c = 412$ ) on  $c$  és un missatge  $m$  xifrat i  $s$  la signatura del resum (*hash*) de  $m$ . És correcte la signatura del missatge enviada per Alice?
7. Denotem un certificat digital com  $A \rightarrow B$ , on  $A$  és l'emissor del certificat (*issuer*) i  $B$  el *subject*. Tenim dues PKIs jeràrquiques definides pels certificats següents:
1. PKI-1:  $CA_0 \rightarrow CA_0, CA_0 \rightarrow CA_1, CA_0 \rightarrow CA_2, CA_1 \rightarrow u_1, CA_1 \rightarrow u_2, CA_2 \rightarrow u_3$ .
  2. PKI-2:  $CA_{10} \rightarrow CA_{10}, CA_{10} \rightarrow CA_{11}, CA_{11} \rightarrow u_4, CA_{11} \rightarrow u_5$ .
- on  $CA_i$  denota una autoritat de certificació,  $u_i$  denota un usuari, i fem servir certificats autosignats per denotar les arrels de confiança de cada PKI.
- Ara volem fer servir el model de confiança conegut com a *Bridge CA* per tal de que les dues PKIs puguin interactuar entre elles, per això s'emeten els certificats següents:
- $CA_B \rightarrow CA_B, CA_B \rightarrow CA_0, CA_B \rightarrow CA_{10}$
- on  $CA_B$  denota la autoritat que fa de *bridge*.
- i. És correcta aquesta implementació de *Bridge CA*? En cas afirmatiu justifica la resposta i en cas negatiu digues amb quins certificats es podria implementar.
8. Respecte al protocol TLS 1.3, contesta breument pero de forma justificada les preguntes següents:
- i. TLS pot fer servir Diffie-Hellman per generar les claus de sessió. Com fa aquest protocol per evitar atacs de Person-in-the-middle (o man-in-the-middle)?
  - ii. Durant el handshake de TLS quan una de les part envia un missatge *Certificate* després ha d'enviar un missatge *CertificateVerify*. Per que cal enviar aquest segon missatge?

A continuació teniu taules de càlculs per poder realitzar els exercicis. No s'inclou la taula corresponent a l'exercici 4 pel qual podeu fer servir python o calculadora de forma excepcional (si fos un examen real sí que incorporariem la taula corresponent).

$5^4 \bmod 136 = 81$	$5^4 \bmod 137 = 77$	$4^5 \bmod 136 = 72$	$4^5 \bmod 137 = 65$
$10^5 \bmod 136 = 40$	$10^5 \bmod 137 = 127$	$5^{10} \bmod 136 = 9$	$5^{10} \bmod 137 = 128$
$77^4 \bmod 136 = 33$	$77^5 \bmod 136 = 93$	$77^4 \bmod 137 = 74$	$77^5 \bmod 137 = 81$
$77^{10} \bmod 136 = 81$	$77^{10} \bmod 137 = 122$	$72^4 \bmod 136 = 120$	$72^5 \bmod 136 = 72$
$72^4 \bmod 137 = 73$	$72^5 \bmod 137 = 50$	$128^4 \bmod 136 = 16$	$128^4 \bmod 137 = 122$
$128^{10} \bmod 136 = 64$	$128^{10} \bmod 137 = 4$		

$2^{12} \bmod 113 = 28$	$3^{12} \bmod 113 = 2$	$6^{12} \bmod 113 = 56$	$12^{12} \bmod 113 = 99$
$2^8 \bmod 113 = 30$	$3^8 \bmod 113 = 7$	$6^8 \bmod 113 = 97$	$12^8 \bmod 113 = 85$
$2^6 \bmod 113 = 64$	$3^6 \bmod 113 = 51$	$6^6 \bmod 113 = 100$	$12^6 \bmod 113 = 72$

$H(278) = 37$	$H(37) = 165$	$H(412) = 278$
$H(391) = 53$	$H(517) = 165$	

$171^{-1} \bmod 391 = 375$	$171^{-1} \bmod 460 = 191$	$171^{-1} \bmod 443 = 57$
$171^{-1} \bmod 352 = 35$	$171^{-1} \bmod 401 = 333$	$27^{-1} \bmod 391 = 29$
$27^{-1} \bmod 460 = 443$	$27^{-1} \bmod 443 = 361$	$27^{-1} \bmod 352 = 339$
$27^{-1} \bmod 401 = 104$		

$412^{383} \bmod 391 = 132$	$412^{171} \bmod 391 = 166$	$412^{375} \bmod 391 = 251$
$412^{27} \bmod 391 = 336$	$412^{443} \bmod 391 = 268$	$165^{383} \bmod 391 = 197$
$165^{171} \bmod 391 = 278$	$165^{375} \bmod 391 = 211$	$165^{27} \bmod 391 = 380$
$165^{443} \bmod 391 = 363$	$412^{383} \bmod 460 = 408$	$412^{171} \bmod 460 = 28$
$412^{375} \bmod 460 = 228$	$412^{27} \bmod 460 = 428$	$412^{443} \bmod 460 = 268$
$165^{383} \bmod 460 = 105$	$165^{171} \bmod 460 = 25$	$165^{375} \bmod 460 = 165$
$165^{27} \bmod 460 = 265$	$165^{443} \bmod 460 = 225$	$412^{383} \bmod 352 = 224$
$412^{171} \bmod 352 = 192$	$412^{375} \bmod 352 = 320$	$412^{27} \bmod 352 = 256$
$412^{443} \bmod 352 = 224$	$165^{383} \bmod 352 = 77$	$165^{171} \bmod 352 = 253$
$165^{375} \bmod 352 = 77$	$165^{27} \bmod 352 = 253$	$165^{443} \bmod 352 = 253$
$412^{383} \bmod 517 = 4$	$412^{171} \bmod 517 = 324$	$412^{375} \bmod 517 = 298$
$412^{27} \bmod 517 = 212$	$412^{443} \bmod 517 = 37$	$165^{383} \bmod 517 = 209$
$165^{171} \bmod 517 = 484$	$165^{375} \bmod 517 = 253$	$165^{27} \bmod 517 = 473$
$165^{443} \bmod 517 = 506$		