

Inici ► Cursos ► Semestre 20142 ► 142\_05\_601\_01 : Criptografia aula 1 ►  
Proves d'Avaluació Continuada (PACs) ► PAC-3

## NAVEGACIÓ PEL QÜESTIONARI

1 2 3 4 5

6 7 8 9 10

Acaba la revisió

**Començat el** Thursday, 30 April 2015, 07:00

**Estat** Acabat

**Completat el** Thursday, 30 April 2015, 07:51

**Temps emprat** 51 minuts 45 segons

**Qualificació** 9,00 sobre 10,00 (90%)

### Pregunta 1

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

L'Arthur, en Ford, en Zaphod i la Trillian s'han creat un parell de claus RSA cadascun i han publicat les seves claus públiques en un repositori. En Marvin ha aconseguit descobrir els valors privats  $d$  de tots ells, però no és capaç de saber de qui és cada clau (ser un robot té les seves limitacions).

Podries ajudar-lo unint les claus públiques amb les seves respectives claus privades?

Ford:  $(nb, eb) = (20687, 18103)$   $d = (2167)$  ✓

Zaphod:  $(nc, ec) = (28381, 6187)$   $d = (5123)$  ✓

Trillian:  $(nd, ed) = (749, 343)$   $d = (547)$  ✓

Arthur:  $(na, ea) = (45901, 19211)$   $d = (40899)$  ✓

La resposta correcta és: Ford:  $(nb, eb) = (20687, 18103)$  –  $d = (2167)$ , Zaphod:  $(nc, ec) = (28381, 6187)$  –  $d = (5123)$ , Trillian:  $(nd, ed) = (749, 343)$  –  $d = (547)$ , Arthur:  $(na, ea) = (45901, 19211)$  –  $d = (40899)$ .

### Pregunta 2

Correcte

Puntuació 1,00  
sobre 1,00

Marca la pregunta

Els usuaris A i B es disposen a utilitzar el sistema RSA per intercanviar-se informació. L'usuari A ha escollit  $n_A = 237$  i  $e_A = 59$ ; l'usuari B ha triat  $n_B = 9167$  i  $e_B = 6731$ .

L'usuari B ha rebut el criptograma  $c = 7060$  de l'usuari A que conté l'edat de l'usuari A. Desxifreu el contingut del missatge. Quants anys té l'usuari A?


Resposta:

46



**Pregunta 3**

Correcte

Puntuació 1,00  
sobre 1,00 Marca la  
pregunta

Dos usuaris A i B s'intercanvien missatges amb el sistema de clau pública ElGamal, sobre un grup multiplicatiu  $\mathbb{Z}_{109}^*$ . La clau privada de B és  $b=35$ . Quina és la clau pública de l'usuari B si  $\alpha=85$ ?


Resposta:



La resposta correcta és: 11

**Pregunta 4**

Correcte

Puntuació 1,00  
sobre 1,00 Marca la  
pregunta

Dos usuaris A i B s'intercanvien missatges amb el sistema de clau pública ElGamal, sobre un grup multiplicatiu  $\mathbb{Z}_{191}^*$ . L'usuari A envia el missatge  $m$ , que un cop xifrat queda representat pel parell  $(161, 173)$ . La clau privada de B és  $b=52$ . Quin és el missatge  $m$ ?


Resposta:



La resposta correcta és: 123

**Pregunta 5**

Correcte

Puntuació 1,00  
sobre 1,00 Marca la  
pregunta

Un usuari ha de respondre la pregunta d'una enquesta enviant la seva resposta xifrada amb la següent clau pública del criptosistema RSA  $(n,e)=(6497, 4021)$ . La resposta pot ser una de les següents: A, B, C i D. A l'escenari plantejat la pregunta i les respostes possibles són públiques, però les respostes dels usuaris han de ser secretes.

L'usuari envia el criptograma següent  $c= 6197$ . El criptograma correspon al xifrat amb la clau pública mencionada, del codi ASCII d'una de les opcions possibles. La taula següent mostra els codis ASCII de les opcions:

- A - 65
- B - 66
- C - 67
- D - 68

Pot un atacant sense conèixer la clau privada corresponent, deduir quin és el valor que l'usuari ha respost? En cas afirmatiu, responeu amb la resposta en clar enviada (A, B, C o D). En cas negatiu, responeu NO.

Resposta:




La resposta correcta és: A

**Pregunta 6**

Correcte

Puntuació 1,00  
sobre 1,00

 Marca la  
pregunta


Un usuari ha de respondre la pregunta d'una enquesta enviant la seva resposta xifrada amb la següent clau pública del criptosistema ElGamal  $(p, \alpha, \alpha^b) = (757, 631, 129)$ . La resposta pot ser una de les següents: A, B, C i D. A l'escenari plantejat la pregunta i les respostes possibles són públiques, però les respostes dels usuaris han de ser secretes.

L'usuari envia el criptograma següent (229,368). El criptograma correspon al xifrat amb la clau pública mencionada, del codi ASCII d'una de les opcions possibles. La taula següent mostra els codis ASCII de les opcions:

- A - 65
- B - 66
- C - 67
- D - 68

Pot un atacant, sense conèixer la clau privada corresponent i aprofitant el fet que coneix els possibles valors que poden ser xifrats, deduir quin és el valor que l'usuari ha respost?

Trieu-ne una:


- ☐ a. SI
- ☒ b. NO 

La resposta correcta és: NO.

**Pregunta 7**

Correcte

Puntuació 1,00  
sobre 1,00

 Marca la  
pregunta

Els usuaris Alice i Bob es disposen a utilitzar el sistema RSA per **signar** els missatges que s'envien. L'Alice té la clau pública  $(n_a, e_a) = (133, 11)$  i la clau privada  $(n_a, d_a) = (133, 59)$ . En Bob té la clau pública  $(n_b, e_b) = (943, 93)$  i la clau privada  $(n_b, d_b) = (943, 757)$ .

L'Alice envia el missatge  $m=103$  signat a en Bob. Quina és la signatura de l'Alice sobre aquest missatge?

Resposta:


31



La resposta correcta és: 31

**Pregunta 8**

Incorrecte

Puntuació 0,00  
sobre 1,00
 Marca la pregunta

Dos usuarios A i B s'intercanvien missatges amb el sistema de clau pública ElGamal sobre el grup multiplicatiu  $\mathbb{Z}_{191}^*$  amb  $\alpha = 173$ . L'usuari A envia a B el missatge  $m=138$ . La clau privada de A és  $a=165$  i la clau pública és  $\alpha^a=155$ . Per tal d'enviar el missatge, A ha escollit a l'atzar  $h=9$ .

Quina és la signatura  $[r,s]$  que rebrà B?

Nota: Respecteu el format indicat per a donar la solució. És a dir, doneu els dos valors en una llista:  $[r,s]$ .

Resposta:


(155,110)



La resposta correcta és: [179,27]

**Pregunta 9**

Correcte

Puntuació 1,00  
sobre 1,00
 Marca la pregunta

Dos usuarios A i B, s'intercanvien missatges amb el sistema de clau pública ElGamal sobre el grup multiplicatiu  $\mathbb{Z}_{173}^*$  amb  $\alpha=99$ . L'usuari A envia a B el missatge  $m=69$ . La clau privada de A és  $a=95$  i la clau pública és  $\alpha^a=141$ .

Quina (o quines) de les següents signatures són signatures vàlides del missatge  $m$  realitzades per l'usuari A?

Nota: Les signatures són parells de valors,  $[r,s]$ .

Trieu-ne una o més:

- ☐ a. [89,23]
- ☒ b. [18,145] ✓
- ☒ c. [171,72] ✓
- ☐ d. [48,110]
- ☐ e. [76,4]
- ☒ f. [30,113] ✓

La resposta correcta és: [171,72], [18,145], [30,113].

**Pregunta 10**

Correcte

Puntuació 1,00  
sobre 1,00
 Marca la pregunta

Les funcions hash són una de les primitives més utilitzades en criptografia. Quines afirmacions són certes sobre les funcions hash?

Trieu-ne una o més:

- ☒ a. Donat el valor d'un hash  $h$ , és difícil trobar un missatge  $m$  tal que  $H(m) = h$ . ✓
- ☐ b. Donat el valor d'un missatge  $m$ , és difícil trobar el valor del hash  $h$  tal que  $H(m) = h$ .
- ☐ c. La funció hash MD5 es considera actualment segura.
- ☒ d. La sortida de la funció té una longitud constant. ✓

La resposta correcta és: La sortida de la funció té una longitud constant.

Acaba la revisió

---

Heu entrat com Jose Vicente Gómez Jiménez (Sortida)  
142\_05\_601\_01 : Criptografia aula 1