**Question 1**

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?

|  |  |  |
| --- | --- | --- |
| Arthur: (na,ea)=(501,81) | d=(41) | Correcta |
| Zaphod: (nc,ec)=(38,17) | d=(17) | Correcta |
| Ford: (nb,eb)=(218,73) | d=(37) | Correcta |
| Trillian: (nd,ed)=(27977,21967) | d=(21103) | Correcta |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 2**

Els usuaris A i B es disposen a utilitzar el sistema RSA per intercanviar-se informació. L'usuari A ha escollit http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/8f3726bd3fd1279ae87ac2c5bd7101e3.png=913 i http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/12a5289ad024d525197e7e525c99e3cc.png=593 ; l'usuari B ha triat http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d3e275aa369c85150801206d94d949c5.png=793 i http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/7bc6bf5857ae3f04e2943abad2c87d3c.png=263 .   
L'usuari A desitja enviar la seva edat m=43 xifrada a B. Calculeu el criptograma c que l'usuari A enviarà a l'usuari B.

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 3**

Dos usuaris A i B s'intercanvien missatges amb el sistema de clau pública ElGamal, sobre un grup multiplicatiu http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/88674c2d26dc45342a87344ab8000f25.png. La clau privada de B és b=5. Quina és la clau pública de l'usuari B si http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/234aad638bc0d7928ab25a0110b084d7.png=161?

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 4**

Cosidereu el criptosistema ElGamal, del qual coneixem el fitxer públic calculat a partir de l'element http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/234aad638bc0d7928ab25a0110b084d7.png=74 de http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/4e4e9ec5405a733c00dd95a51907f2db.png. L'usuari A ha construït la seva clau pública com a http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/b25c8bdc27754e6970dc2b8dca54b86c.png. Si sabem que el parell http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/e6fbab9abe9c6661b12febf7764fefad.pngés el resultat de xifrar el missatge *m* amb la clau pública de l'usuari A. Quin és el missatge original *m*?

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 5**

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)=(7031, 1501). 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= 5813. 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

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 6**

Un usuari ha de respondre la pregunta d’una enquesta enviant la seva resposta xifrada amb la següent clau pública del criptosistema ElGamal (p,http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/234aad638bc0d7928ab25a0110b084d7.png,http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/351b11ddaefd51b64d36436d62556ba8.png)=(2663, 1004, 1197). 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 (615,2372). 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 una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. NO Correcta |  |
|  | b. SI Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 7**

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 (na, ea)=(1769, 1273) i la clau privada (na,da)=(1769,937). En Bob té la clau pública (nb, eb)=(323, 23) i la clau privada (nb,db)=(323,263).  
  
L'Alice envia el missatge m=36 signat a en Bob. Quina és la signatura de l'Alice sobre aquest missatge?

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 8**

Dos usuaris A i B, s'intercanvien missatges amb el sistema de clau pública ElGamal sobre el grup multiplicatiu http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/2b279d560ed264cc8bb08f86e234f826.pngamb http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/f5605293df278a907ad8b8e7206d793e.png. L'usuari A envia a B el missatge *m*=88. La clau privada de A és *a*=66 i la clau pública és http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/509dec7ea6306a94f23e5a09920ce6a0.png=13. Per tal d'enviar el missatge, A ha escollit a l'atzar *h=69.*   
  
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

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 9**

Dos usuaris A i B, s'intercanvien missatges amb el sistema de clau pública ElGamal sobre el grup multiplicatiu http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/c5d13d7ab57d52237319c0a13589c2ab.pngamb http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/234aad638bc0d7928ab25a0110b084d7.png=48. L'usuari A envia a B el missatge m= 130. La clau privada de A és a= 122 i la clau pública és http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/509dec7ea6306a94f23e5a09920ce6a0.png=4.   
  
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 almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d8ba3e78f2796165cd5e0a6608da9a5a.pngCorrecta |  |
|  | b. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/f9cbf1b3d30d3c364bf1c9e0847f1a81.pngCorrecta |  |
|  | c. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/1bbc27bb809e79889a69b3eacc2cd498.pngIncorrecta |  |
|  | d. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/8ee79100b2c2d6f3ebc07476b9494e95.pngIncorrecta |  |
|  | e. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/8851203039d133610fe209745f0d3ce1.pngIncorrecta |  |
|  | f. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/c5542f00b7fe1e203fca2d273cdb9d80.pngCorrecta |  |

Correcte

Punts d'aquesta tramesa: 1/1.

**Question 10**

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

Trieu almenys una resposta

|  |  |
| --- | --- |
|  | a. Calcular el hash d'un missatge m és un problema computacionalment difícil. Incorrecta |
|  | b. Donat el valor d'un missatge m, és difícil trobar el valor del hash h tal que H( m )=h. Incorrecta |
|  | c. La sortida de la funció té una longitud constant. Correcta |
|  | d. Donat el valor d'un hash h, és difícil trobar un missatge m tal que H(m)=h. Correcta |

Correcta

Punts d'aquesta tramesa: 1/1.