***INTENT 1***

**Question 1**

Quins són els elements principals d'un certificat digital?

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. La clau privada de l'usuari Incorrecta |  |
|  | b. La signatura del certificat realitzada per l'autoritat de certificació. Correcta |  |
|  | c. La clau privada de l'autoritat de certificació. Incorrecta |  |
|  | d. La clau pública de l'usuari. Correcta |  |
|  | e. La clau pública de l'autoritat de certificació. Incorrecta |  |
|  | f. L'identificador de l'autoritat de certificació (issuer). Correcta |  |
|  | g. L'identificador de l'usuari (subject). Correcta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 2**

Indiqueu quines de les següents afirmacions són certes en relació a un model de confiança jeràrquic:

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. Les autoritats de certificació subordinades tenen un certificat autosignat. Incorrecta |  |
|  | b. L'autoritat de certificació arrel no pot signar certificats. Incorrecta |  |
|  | c. Les claus públiques de totes les autoritats subordinades són les mateixes. Incorrecta |  |
|  | d. El número de validacions necessàries per verificar un certificat d'un usuari dependrà de la seva situació a la jerarquia. Correcta |  |
|  | e. L'autoritat de certificació arrel té un certificat autosignat. Correcta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 3**

El protocol de tres passos de Shamir permet establir una comunicació segura entre dues persones sense cap intercanvi de claus previ. Tot i que es pot fer servir Vernam com a funció de xifratge per a executar aquest protocol (ja que té les propietats requerides), el seu ús no n'és gens recomanable.   
  
En Julian i en Bradley fan servir el protocol de tres passos de Shamir amb Vernam per tal d'enviar-se un missatge M de forma segura (o això creuen). La NSA, fent ús de la xarxa ECHELON, aconsegueix interceptar els 3 missatges intercanviats:  
  
J -> B : 0CA8DA9EDA91259  
B -> J : 6E0F343099E699A  
J -> B : F49598EE860B843  
  
Els analistes de la NSA no tarden gaire en descobrir el missatge M que en Julian ha enviat a en Bradley. Però no cal disposar de tot el poder de còmput de la NSA per trobar aquest missatge, no? Quin és el missatge que ha enviat en Julian a en Bradley amb l'execució del protocol de 3 passos de Shamir?  
  
Nota: Els valors mostrats són cadenes hexadecimals. Entreu el valor del missatge M també com a una cadena de valors hexadecimals, per exemple 8A5EF0 (feu servir majúscules per a les lletres).

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 4**

Volem compartir el nombre secret 23 entre 10 usuaris utilitzant un esquema llindar (4 , 10 ) de compartició de secrets polinomial. Prenem com a valor per al mòdul el nombre primer 61 i el polinomi que utilitzarem serà  
el 23 + 22 x + 29 x2 + 14 x3  
  
Selecciona quins dels següents fragments són correctes per repartir als usuaris.

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/91a130170997bd6d0b7ca315e3f74815.pngCorrecta |  |
|  | b. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/c87b13853b4c27fe506b24bd191f7a2d.pngCorrecta |  |
|  | c. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/a20a1fe6c83b8f2e3ac6fc0c7cbc26d9.pngIncorrecta |  |
|  | d. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/b1d91fe084fd7b19dcdbbc8cf9ee996a.pngIncorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 5**

Tenim un esquema llindar (4 , 5 ) de compartició de secrets polinomial i treballem als enters mòdul 1657. Els fragments de 5 usuaris són els següents: http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/50ac70430d92b20745c71da00a24b8d2.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/dd8927dec89845b8933b0ba1489c7581.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d831abd8e7d81c87b407901c9974753c.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d609feda73ae1649143bb986993351be.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/1e0445711914848268e055b6bdaa4f20.png  
  
Si és possible, calcula el valor del secret. En cas contrari escriu "NO" en la resposta.

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 6**

Un dels problemes que cal afrontar quan es dissenya un esquema de diners electrònics és el control de la despesa múltiple, és a dir, com s'evita que els usuaris facin servir un mateix "bitllet" varies vegades. Una de les possibles solucions és incorporar tires d'identificació aleatòries (TAIs) sobre els bitllets, de tal manera que si un usuari fa servir el mateix bitllet dues vegades, aleshores es pugui descobrir la identitat d'aquest usuari.  
  
Per a l'esquema descrit al Mòdul 8, quina és la probabilitat que un usuari faci servir un mateix bitllet 4 vegades i segueixi sent anònim si es fa servir un valor de k=15

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/43a3767ec9f6ce4848f11fcf19c27bc1.pngIncorrecta |  |
|  | b. 1 Incorrecta |  |
|  | c. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/e2729a8e00f789a1fcbf9265e67e4f49.pngCorrecta |  |
|  | d. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/a23308c73b736c68381588fdecd7b433.pngIncorrecta |  |
|  | e. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/1164989febf40087e8858550d76f3152.pngIncorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 7**

Un dels problemes que cal afrontar quan es dissenya un esquema de diners electrònics és el control de la despesa múltiple, és a dir, com s'evita que els usuaris facin servir un mateix "bitllet" varies vegades. Una de les possibles solucions és incorporar tires d'identificació aleatòries (TAIs) sobre els bitllets, de tal manera que si un usuari fa servir el mateix bitllet dues vegades, aleshores es pugui descobrir la identitat d'aquest usuari.  
  
Un usuari anònim ha sentit que rumors de que aquest sistema no funciona sempre i ha intentat fer servir un mateix bitllet dues vegades:  
  
http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/f974a3ec5bf381501e7b8fb9c9d395f9.pngLa primera vegada, després de rebre el repte, l'usuari anònim envia la TAI=  
La segona vegada, després de rebre el nou repte, l'usuari anònim envia la TAI=   
http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/5c7b656e2cb20c1d3e702d39c31f6fa0.png  
En els dos casos, el bitllet va ser acceptat ja que tant la signatura del banc sobre el bitllet com els valors de la funció hash mostrats eren correctes. Tenint en compte les TAIs que ha enviat l'usuari, pots saber quina és la identitat d'aquest usuari? En cas afirmatiu, responeu amb la identitat. En cas negatiu, responeu NO.   
  
Nota 1: La TAI és una llista de valors on a cada posició j = 1,...,K hi ha o bé el valor xj o bé xj', amb K el número de bits del repte.  
Nota 1: Trobareu una descripció del protocol de detecció de despesa múltiple al que es refereix la pregunta al Mòdul 8.  
Nota 2: Els valors de la TAI són cadenes hexadecimals. Introduïu la resposta també com a una cadena de caràcters hexadecimals, com ara per exemple, 8AB45E (feu servir majúscules per a les lletres).

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 8**

PGP (Pretty Good Privacy) és un programari creat als anys 90 que permet realitzar operacions criptogràfiques com ara xifrar, desxifrar, signar i verificar signatures. PGP es pot fer servir, entre d'altres usos, per enviar correus electrònics xifrats i signats.   
  
L'aparició de PGP va ser molt polèmica ja que, en aquells moments, l'exportació de software criptogràfic des dels EUA era considerat un delicte. Com es va intentar esquivar la normativa per exportar PGP?

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. Es van esperar uns quants anys fins que la normativa va canviar Incorrecta |  |
|  | b. Es distribuïa el codi font imprès en un llibre Correcta |  |
|  | c. Es van reduir les mides de les claus per sota els 40 bits Incorrecta |  |
|  | d. Es distribuïa dins d'un fitxer .zip Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 9**

Bitcoin és una moneda digital que utilitza protocols criptogràfics i una arquitectura P2P per permetre realitzar transaccions segures entre usuaris.   
  
Com s'evita la despesa múltiple amb Bitcoin?  
  
Nota: Podeu consultar la documentació de Bitcoin a [www.bitcoin.org/about.html](http://www.bitcoin.org/about.html)

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. Es fan servir timestamps i cadenes de blocs per tal que tots els usuaris reconeguin un sol ús de la moneda com a vàlid Correcta |  |
|  | b. S'afegeix una TAI (Tira d'Identificació Aleatòria) als blocs que permet reidentificar un usuari que ha fet servir una moneda més d'una vegada Incorrecta |  |
|  | c. Es fa ús d'un servidor que registra tots els usos de les monedes. Abans d'acceptar una moneda com a vàlida, el receptor contacta amb el servidor i comprova que no s'ha fet servir anteriorment. Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

***INTENT 2***

**Question 1**

Quins són els elements principals d'un certificat digital?

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. La signatura del certificat realitzada per l'autoritat de certificació. Correcta |  |
|  | b. La clau pública de l'usuari. Correcta |  |
|  | c. La clau privada de l'autoritat de certificació. Incorrecta |  |
|  | d. L'identificador de l'autoritat de certificació (issuer). Correcta |  |
|  | e. La clau privada de l'usuari Incorrecta |  |
|  | f. L'identificador de l'usuari (subject). Correcta |  |
|  | g. La clau pública de l'autoritat de certificació. Incorrecta |  |

Correcte

Punts d'aquesta tramesa: 1/1.

**Question 2**

Indiqueu quines de les següents afirmacions són certes en relació a un model de confiança jeràrquic:

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. Les claus públiques de totes les autoritats subordinades són les mateixes. Incorrecta |  |
|  | b. El número de validacions necessàries per verificar un certificat d'un usuari dependrà de la seva situació a la jerarquia. Correcta |  |
|  | c. Les autoritats de certificació subordinades tenen un certificat autosignat. Incorrecta |  |
|  | d. L'autoritat de certificació arrel té un certificat autosignat. Correcta |  |
|  | e. L'autoritat de certificació arrel no pot signar certificats. Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 3**

El protocol de tres passos de Shamir permet establir una comunicació segura entre dues persones sense cap intercanvi de claus previ. Tot i que es pot fer servir Vernam com a funció de xifratge per a executar aquest protocol (ja que té les propietats requerides), el seu ús no n'és gens recomanable.   
  
En Julian i en Bradley fan servir el protocol de tres passos de Shamir amb Vernam per tal d'enviar-se un missatge M de forma segura (o això creuen). La NSA, fent ús de la xarxa ECHELON, aconsegueix interceptar els 3 missatges intercanviats:  
  
J -> B : CB3AB6CD553B2F8  
B -> J : F648722FE2B6512  
J -> B : F6B9BA949C2DE09  
  
Els analistes de la NSA no tarden gaire en descobrir el missatge M que en Julian ha enviat a en Bradley. Però no cal disposar de tot el poder de còmput de la NSA per trobar aquest missatge, no? Quin és el missatge que ha enviat en Julian a en Bradley amb l'execució del protocol de 3 passos de Shamir?  
  
Nota: Els valors mostrats són cadenes hexadecimals. Entreu el valor del missatge M també com a una cadena de valors hexadecimals, per exemple 8A5EF0 (feu servir majúscules per a les lletres).

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 4**

Volem compartir el nombre secret 85 entre 10 usuaris utilitzant un esquema llindar (4 , 10 ) de compartició de secrets polinomial. Prenem com a valor per al mòdul el nombre primer 293 i el polinomi que utilitzarem serà  
el 85 + 163 x + 111 x2 + 254 x3  
  
Selecciona quins dels següents fragments són correctes per repartir als usuaris.

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/760ec0ce21ed53653138cdbabb33d250.pngCorrecta |  |
|  | b. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/7d785c2fc236362bc9bb16cd891fabb9.pngCorrecta |  |
|  | c. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/2f49187c528f149767e9bcd91f36de3e.pngIncorrecta |  |
|  | d. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/366c7b9f6c05ed123e8f6565f4150750.pngIncorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 5**

Tenim un esquema llindar (5 , 5 ) de compartició de secrets polinomial i treballem als enters mòdul 887. Els fragments de 5 usuaris són els següents: http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/8c3716e641aa584c6efb45ca652ae50d.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/cbd714164c03d33df6cc8bd1d5f88915.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d14d9ed608dade7338017160b8861f4f.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/21679d8612c4aaa349038c9025beedb7.png, http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/070e013bf64e41dc0ae2feef3d7d4d3e.png  
  
Si és possible, calcula el valor del secret. En cas contrari escriu "NO" en la resposta.

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 6**

Un dels problemes que cal afrontar quan es dissenya un esquema de diners electrònics és el control de la despesa múltiple, és a dir, com s'evita que els usuaris facin servir un mateix "bitllet" varies vegades. Una de les possibles solucions és incorporar tires d'identificació aleatòries (TAIs) sobre els bitllets, de tal manera que si un usuari fa servir el mateix bitllet dues vegades, aleshores es pugui descobrir la identitat d'aquest usuari.  
  
Per a l'esquema descrit al Mòdul 8, quina és la probabilitat que un usuari faci servir un mateix bitllet 5 vegades i segueixi sent anònim si es fa servir un valor de k=14

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. 1 Incorrecta |  |
|  | b. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/0c1c2f0b312e467073d494abac7097ee.pngIncorrecta |  |
|  | c. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/43a3767ec9f6ce4848f11fcf19c27bc1.pngCorrecta |  |
|  | d. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/870b94c2c9599cea64cdc16771f54930.pngIncorrecta |  |
|  | e. http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/98286385a0d6a02245ba1419fabe88f4.pngIncorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 7**

Un dels problemes que cal afrontar quan es dissenya un esquema de diners electrònics és el control de la despesa múltiple, és a dir, com s'evita que els usuaris facin servir un mateix "bitllet" varies vegades. Una de les possibles solucions és incorporar tires d'identificació aleatòries (TAIs) sobre els bitllets, de tal manera que si un usuari fa servir el mateix bitllet dues vegades, aleshores es pugui descobrir la identitat d'aquest usuari.  
  
Un usuari anònim ha sentit que rumors de que aquest sistema no funciona sempre i ha intentat fer servir un mateix bitllet dues vegades:  
  
La primera vegada, després de rebre el repte, l'usuari anònim envia la TAI=http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/089c0e1339972e543329be62c0839ddf.png  
La segona vegada, després de rebre el nou repte, l'usuari anònim envia la TAI=   
http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/23449f072bd5266f0e343ac880ce2deb.png

En els dos casos, el bitllet va ser acceptat ja que tant la signatura del banc sobre el bitllet com els valors de la funció hash mostrats eren correctes. Tenint en compte les TAIs que ha enviat l'usuari, pots saber quina és la identitat d'aquest usuari? En cas afirmatiu, responeu amb la identitat. En cas negatiu, responeu NO.   
  
Nota 1: La TAI és una llista de valors on a cada posició j = 1,...,K hi ha o bé el valor xj o bé xj', amb K el número de bits del repte.  
Nota 1: Trobareu una descripció del protocol de detecció de despesa múltiple al que es refereix la pregunta al Mòdul 8.  
Nota 2: Els valors de la TAI són cadenes hexadecimals. Introduïu la resposta també com a una cadena de caràcters hexadecimals, com ara per exemple, 8AB45E (feu servir majúscules per a les lletres).

Resposta

Correcta

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 8**

PGP (Pretty Good Privacy) és un programari creat als anys 90 que permet realitzar operacions criptogràfiques com ara xifrar, desxifrar, signar i verificar signatures. PGP es pot fer servir, entre d'altres usos, per enviar correus electrònics xifrats i signats.   
  
A més de permetre xifrar i signar missatges, PGP també permet comprimir-los per tal d'haver de transmetre la mínima quantitat de dades possible per la xarxa. Si es vol enviar un missatge xifrat, signat i comprimit, en quin ordre s'apliquen les funcions per defecte en PGP?

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. Xifratge, Compressió, Signatura Incorrecta |  |
|  | b. Signatura, Compressió, Xifratge Correcta |  |
|  | c. Signatura, Xifratge, Compressió Incorrecta |  |
|  | d. Xifratge, Signatura, Compressió Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 9**

Bitcoin és una moneda digital que utilitza protocols criptogràfics i una arquitectura P2P per permetre realitzar transaccions segures entre usuaris. Bitcoin fa servir certificats digitals en les seves transaccions (que permeten establir relacions entre identitats i claus públiques).  
  
Com s'aconsegueix mantenir l'anonimat de les transaccions en aquest cas?  
  
Nota: Podeu consultar la documentació de Bitcoin a [www.bitcoin.org/about.html](http://www.bitcoin.org/about.html)

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. Bitcoin no permet fer transaccions anònimes Incorrecta |  |
|  | b. Només la TTP (Trusted Third Party) coneix les identitats. La resta d'usuaris no poden saber quina identitat ha realitzat cada transacció. Incorrecta |  |
|  | c. Tots els certificats digitals que es fan servir relacionen una clau pública amb la identitat "AnonymousIdentity" Incorrecta |  |
|  | d. Es fan servir identificadors aleatoris i un mateix usuari pot fer servir identificadors diferents a cada transacció Correcta |  |

Correcta

Punts d'aquesta tramesa: 1/1.