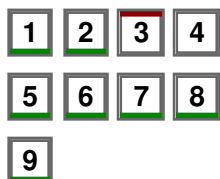


Inici ► Cursos ► Semestre 20142 ► 142_05_601_01 : Criptografia aula 1 ►
Proves d'Avaluació Continuada (PACs) ► PAC-4

NAVEGACIÓ PEL QÜESTIONARI



Acaba la revisió

Començat el Monday, 1 June 2015, 13:48

Estat Acabat

Completat el Monday, 1 June 2015, 13:57

Temps emprat 9 minuts

Qualificació 8,50 sobre 10,00 (85%)

Pregunta 1

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la
pregunta

Quins són els elements principals d'un certificat digital?

Trieu-ne una o més:

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

La resposta correcta és: La clau pública de l'usuari., L'identificador de l'usuari (subject)., L'identificador de l'autoritat de certificació (issuer)., La signatura del certificat realitzada per l'autoritat de certificació..

Pregunta 2

Correcte

Puntuació 1,00
sobre 1,00

▼ Marca la
pregunta

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

Trieu-ne una o més:

- ☐ a. Les claus públiques de totes les autoritats subordinades són les mateixes.
- ☐ b. L'autoritat de certificació arrel no pot signar certificats.
- ☐ c. Les autoritats de certificació subordinades tenen

15/06/15 14:30

un certificat autosignat.

- ☒ d. L'autoritat de certificació arrel té un certificat autosignat. <http://cv.uoc.edu/moodos/mod/quiz/review.php?attempt...> ✓
- ☒ e. El número de validacions necessàries per verificar un certificat d'un usuari dependrà de la seva situació a la jerarquia. ✓

La resposta correcta és: L'autoritat de certificació arrel té un certificat autosignat., El número de validacions necessàries per verificar un certificat d'un usuari dependrà de la seva situació a la jerarquia..

Pregunta 3

Incorrecte

Puntuació 0,00
sobre 1,00

🚩 Marca la
pregunta

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 : AB73899FB96772F

B -> J : 8840398AAFB6D96

J -> B : EEA39FC613BD438

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:

02333B01516D1AB9



La resposta correcta és: CD902FD3056CE81

15/06/15 14:30

Pregunta 4

Parcialment
correcte

Puntuació 0,50
sobre 1,00

🚩 Marca la
pregunta

Volem compartir el nombre secret 32 entre 10 usuaris utilitzant un esquema llindar (4 , 10) de compartició de secrets polinomial. Prenem com a valor per al mòdul el nombre primer 107 i el polinomi que utilitzarem serà el $32 + 74x + 67x^2 + 35x^3$

Selecciona quins dels següents fragments són correctes per repartir als usuaris.

Trieu-ne una o més:

- ☒ a. [109,86] ✖
- ☐ b. [95,62]
- ☒ c. [26,78] ✔
- ☒ d. [94,52] ✔

La resposta correcta és: [94,52], [26,78].

Pregunta 5

Correcte

Puntuació 2,00
sobre 2,00

🚩 Marca la
pregunta

Tenim un esquema llindar (5 , 7) de compartició de secrets polinomial i treballem als enters mòdul 907. Els fragments de 5 usuaris són els següents: [241,412], [719,239], [7,70], [760,767], [380,213]

Si és possible, calcula el valor del secret. En cas contrari escriu "NO" en la resposta.

Resposta:

290



La resposta correcta és: 290

Pregunta 6

Correcte

Puntuació 1,00
sobre 1,00

🚩 Marca la
pregunta

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=

(762C0843,10E107C1,B15DC4E9,757C6F0F,74F716F9,458E6F92,E3205AB3,8E7A8202,E74ADB15,80F822D7)

La segona vegada, després de rebre el nou repte, l'usuari anònim envia la TAI a <http://www.uoc.edu/moodos/mod/quiz/review.php?attempt...>

(6570CB75,10E107C1,A20107DF,757C6F0F,74F716F9,458E6F92,E3205AB3,8E7A8202,E74ADB15,A3A7E1E1)

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 $j = 1, \dots, K$ hi ha o bé el valor x_j o bé x_j' , 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:

135CC336



La resposta correcta és: 135CC336

Pregunta 7

Correcte

Puntuació 1,00
sobre 1,00

🚩 Marca la
pregunta

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 $k=12$

Trieu-ne una:

- ☐ a. 0.5
- ☒ b. $3.553 \cdot 10^{-15}$ ✓
- ☐ c. 0.0002441
- ☐ d. $8.674 \cdot 10^{-19}$
- ☐ e. $2.118 \cdot 10^{-22}$

La resposta correcta és: $3.553 \cdot 10^{-15}$.

Pregunta 8

Correcte

Puntuació 1,00
sobre 1,00

🚩 Marca la pregunta

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-ne una:


- ☐ a. Xifratge, Compresió, Signatura
- ☒ b. Signatura, Compresió, Xifratge ✓
- ☐ c. Signatura, Xifratge, Compresió
- ☐ d. Xifratge, Signatura, Compresió

La resposta correcta és: Signatura, Compresió, Xifratge.

Pregunta 9

Bitcoin és una moneda digital que utilitza protocols

Correcte

Puntuació 1,00
sobre 1,00 Marca la
pregunta

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

Trieu-ne una:

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

La resposta correcta és: Es fan servir identificadors aleatoris i un mateix usuari pot fer servir identificadors diferents a cada transacció.

Acaba la revisió

Heu entrat com Jose Vicente Gómez Jiménez (Sortida)
142_05_601_01 : Criptografia aula 1