NAVEGACIÓ PEL QÜESTIONARI

1 2 3 4 5 6 7

Acaba la revisió

Començat el	Friday, 13 March 2015, 15:26
Estat	Acabat
Completat el	Friday, 13 March 2015, 15:55
Temps emprat	28 minuts 24 segons
Qualificació	**6,67** sobre 10,00 (**67**%)

Pregunta 1

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

Uns estudiants han trobat un *pendrive* abandonat a la facultat de lletres i han pogut recuperar un missatge xifrat el contingut del qual es mostra a continuació. Sabem que per xifrar el missatge s'ha fet servir un criptosistema de substitució de Cèsar amb un valor de clau arbitrari. Després d'estudiar el missatge durant uns minuts, els estudiants han descobert que la clau utilitzada ha estat k= 11 . Quin és el text en clar corresponent al missatge recuperat?

Missatge xifrat = CPUPHDVT

Nota: El text en clar és un text en anglès codificat amb un alfabet de 26 caràcters.

Trieu-ne una:

- a. FRIEDMAN
- b. FKASISKI
- c. REJEWSKI ✓
- d. CBABBAGE

Pregunta 2

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

Donat el text en clar CBABBAGE, seleccioneu tots els possibles textos xifrats que poden ser resultat de xifrar aquest text en clar amb un criptosistema de transposició.

Trieu-ne una o més:

- a. EGABCABC
- b. CCCCCCCC
- c. CAABBEGB ✓
- d. ABACEABA

Pregunta 3

Parcialment correcte

Puntuació 1,00 sobre 2,00

Marca la pregunta

Relaciona cadascun dels següents criptosistemes històrics amb el concepte o característica que millor els defineix.

Vernam — Tabula Recta ✗

Cèsar — Clau = 3 ✓

Vigenère — Segona Guerra Mundial ✗

Beale — Declaració d'Independència dels Estats Units d'Amèrica ✓

Pregunta 4

Correcte

Puntuació 2,00 sobre 2,00

Marca la pregunta

Un criptosistema de Vernam és vulnerable a atacs amb només text xifrat?

Trieu-ne una:

- a. Sí, sempre.
- b. No, mai. ✓
- c. Sí, si el criptoanalista disposa d'una capacitat il·limitada de càlcul.
- d. Sí, si el criptoanalista disposa d'un text prou llarg.

Pregunta 5

Incorrecte

Puntuació 0,00 sobre 2,00

Marca la pregunta

Els criptosistemes de substitució simple són susceptibles a atacs amb text xifrat escollit?

Trieu-ne una:

- a. Sí, sempre.
- b. No, mai.
- c. Sí, si disposem d'una capacitat de càlcul il·limitada.
- d. Sí, si el criptoanalista disposa d'un text prou llarg. ✗

Pregunta 6

Parcialment correcte

Puntuació 0,67 sobre 1,00

Marca la pregunta

Siguin M, C i K tres variables aleatòries discretes que poden prendre com a valors un conjunt de textos en clar, un conjunt de textos xifrats i un conjunt de claus en un criptosistema donat, respectivament. Si sabem que M i C són variables independents, marqueu les afirmacions que són **sempre** veritat.

Trieu-ne una o més:

- [ ] a. $H(M,C) = H(M) + H(C) + I(M,C)$
- [ ] b. $H(M) > H(M|C)$
- [ ] c. $H(C) < H(C|M)$
- [x] d. $H(C|M) = H(C)$ ✓
- [x] e. $I(M,C) = 0$ ✓
- [ ] f. $H(M) < H(M|C)$

Pregunta 7

Correcte

Puntuació 1,00 sobre 1,00

Marca la pregunta

Siguin M, C i K tres variables aleatòries discretes que poden prendre com a valors un conjunt de textos en clar, un conjunt de textos xifrats i un conjunt de claus en un criptosistema donat, respectivament. Suposem que hi ha un criptoanalista que està estudiant aquest criptosistema i que en coneix el seu funcionament (és a dir, donat un missatge en clar i una clau pot produir el text xifrat, i donat un missatge xifrat i una clau en pot obtenir el text en clar). Després d'uns dies de feina, el criptoanalista descobreix que l'últim bit del missatge xifrat és sempre diferent del primer bit del text en clar. És a dir, si el missatge xifrat acaba en un 1, voldrà dir que el text en clar comença en 0 i si, en canvi, el missatge xifrat acaba en 0, voldrà dir que el text en clar comença en 1. Quins canvis produeix aquest nou coneixement en l'entropia de M, la de M|C i la de M|K,C?

$H(M|K,C)$ Es queda igual. ✓

$H(M)$ Es queda igual. ✓

$H(M|C)$ Baixa. ✓

Acaba la revisió

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