***INTENT 1***

**Exercici 1**

Esteu preparant uns petits reptes de criptoanàlisi per a un concurs on es dóna un missatge xifrat als concursants i n'han d'esbrinar el corresponent text en clar. Atès que us toca crear la prova de nivell 1, heu decidit penjar un missatge xifrat amb el criptosistema de substitució de Cèsar amb un valor de clau arbitrari. Donat el missatge en clar ONTHESECURITYOFPUBLICKEYPROTOCOLS i la clau k=13 . Quin és el missatge xifrat que donareu als concursants com a primer text a criptoanalitzar?  
Nota: El text en clar és un text en anglès codificat amb un alfabet de 26 caràcters.

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. CBHVSGSQIFWHMCTDIPZWQYSMDFCHCQCZG Incorrecta |  |
|  | b. AZFTQEQOGDUFKARBGNXUOWQKBDAFAOAXE Incorrecta |  |
|  | c. LKQEBPBZROFQVLCMRYIFZHBVMOLQLZLIP Incorrecta |  |
|  | d. BAGURFRPHEVGLBSCHOYVPXRLCEBGBPBYF Correcta |  |
|  | e. MLRFCQCASPGRWMDNSZJGAICWNPMRMAMJQ Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Exercici 2**

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

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. MGNAURTI Correcta |  |
|  | b. GNIRATMA Incorrecta |  |
|  | c. TMIAGTRT Incorrecta |  |
|  | d. AAAAAAAA Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Exercici 3**

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

|  |  |  |
| --- | --- | --- |
| Cèsar | Clau=3 | Correcta |
| Vernam | Segona Guerra Mundial | Correcta |
| Beale | Declaració Independència dels Estats Units d'Amèrica | Correcta |
| Vigenère | Tabula Recta | Correcta |

Correcta

Punts d'aquesta tramesa: 1/1.

**Exercici 4**

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

Trieu una resposta.

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

Correcta

Punts d'aquesta tramesa: 2/2.

**Exercici 5**

Els criptosistemes de substitució simple són susceptibles a atacs amb text en clar conegut?

Trieu una resposta.

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

Correcta

Punts d'aquesta tramesa: 2/2.

**Exercici 6**

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 almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. H(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.pngH(M) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d8132101939a53e74b58c34a4c7b1467.pngH(C) Correcta |  |
|  | b. H(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.pngH(M|C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d8132101939a53e74b58c34a4c7b1467.pngH(C|M) Correcta |  |
|  | c. I(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.png0 Correcta |  |
|  | d. H(C) < H(C|M) Incorrecta |  |
|  | e. H(M) > H(M|C) Incorrecta |  |
|  | f. H(M) < H(M|C) Incorrecta |  |

Si M i C són variables independents, aleshores la informació mútua, I(M,C), és 0. D'altra banda, H(M|C)=H(M) ja que C no aporta cap informació sobre M. De la mateixa manera, H(C|M)=H(C) ja que el coneixement de M no aporta informació sobre C.  
  
Tenint en compte aquestes propietats, aleshores podem veure com   
H(M,C)=H(M)+H(C)=H(M)+H(C)+I(M,C)=H(M|C)+H(C|M)=H(M|C)+H(C|M)+I(M,C)

Parcialment correcte

Punts d'aquesta tramesa: 1.33/2.

**Exercici 7**

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 | Correcta |
| H(M) | Es queda igual | Correcta |
| H(M|C) | Baixa | Correcta |

Saber que l'últim bit del text xifrat és el contrari que el primer del text en clar fa que H(M|C) disminueixi, ja que una vegada sabem C, la incertesa que ens queda sobre  
M és menor (ja en sabem un bit).  
Aquest coneixement, però, no afecta H(M), que segueix sent igual. Tenint en compte que el criptoanalista coneix el sistema de xifratge, H(M|K,C) serà sempre 0, ja que donats un missatge xifrat i una clau, el criptoanalista sap quin és el missatge en clar, i per tant no té incertesa sobre aquest missatge. En conseqüència, H(M|K,C) tampoc varia amb el nou coneixement.

Correcta

Punts d'aquesta tramesa: 1/1.

***INTENT 2***

**Question 1**

Esteu preparant uns petits reptes de criptoanàlisi per a un concurs on es dóna un missatge xifrat als concursants i n'han d'esbrinar el corresponent text en clar. Atès que us toca crear la prova de nivell 1, heu decidit penjar un missatge xifrat amb el criptosistema de substitució de Cèsar amb un valor de clau arbitrari. Donat el missatge en clar NEWDIRECTIONSINCRYPTOGRAPHY i la clau k=14 . Quin és el missatge xifrat que donareu als concursants com a primer text a criptoanalitzar?  
  
Nota: El text en clar és un text en anglès codificat amb un alfabet de 26 caràcters.

Trieu una resposta.

|  |  |  |
| --- | --- | --- |
|  | a. LCUBGPCARGMLQGLAPWNRMEPYNFW Incorrecta |  |
|  | b. MDVCHQDBSHNMRHMBQXOSNFQZOGX Incorrecta |  |
|  | c. BSKRWFSQHWCBGWBQFMDHCUFODVM Correcta |  |
|  | d. ARJQVERPGVBAFVAPELCGBTENCUL Incorrecta |  |
|  | e. CTLSXGTRIXDCHXCRGNEIDVGPEWN Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 2**

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

Trieu almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. RRRRRRRR Incorrecta |  |
|  | b. JESRIJWJ Incorrecta |  |
|  | c. KRWEJEIS Correcta |  |
|  | d. IKSWRJER Incorrecta |  |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 3**

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

|  |  |  |
| --- | --- | --- |
| Cèsar | Substitució simple | Correcta |
| Vernam | Secret perfecte | Correcta |
| Vigenère | Kasiski | Correcta |
| Beale | Resistent a l'anàlisi de freqüències | Correcta |

Correcta

Punts d'aquesta tramesa: 1/1.

**Question 4**

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

Trieu una resposta.

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

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 5**

Els criptosistemes de substitució simple són susceptibles a atacs amb text en clar conegut?

Trieu una resposta.

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

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 6**

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 almenys una resposta

|  |  |  |
| --- | --- | --- |
|  | a. H(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.pngH(M|C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d8132101939a53e74b58c34a4c7b1467.pngH(C|M) Correcta |  |
|  | b. I(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.png0 Correcta |  |
|  | c. H(C) < H(C|M) Incorrecta |  |
|  | d. H(M|C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.pngH(C) Incorrecta |  |
|  | e. H(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.png0 Incorrecta |  |
|  | f. H(M,C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/821970ac8fea87234f395e06ad0e5d67.pngH(M) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d8132101939a53e74b58c34a4c7b1467.pngH(C) http://cv.uoc.edu/app/moodle19/filter/wiris/filter/wrs_showimage.php/d8132101939a53e74b58c34a4c7b1467.pngI(M,C) Correcta |  |

Si M i C són variables independents, aleshores la informació mútua, I(M,C), és 0. D'altra banda, H(M|C)=H(M) ja que C no aporta cap informació sobre M. De la mateixa manera, H(C|M)=H(C) ja que el coneixement de M no aporta informació sobre C.  
  
Tenint en compte aquestes propietats, aleshores podem veure com   
H(M,C)=H(M)+H(C)=H(M)+H(C)+I(M,C)=H(M|C)+H(C|M)=H(M|C)+H(C|M)+I(M,C)

Correcta

Punts d'aquesta tramesa: 2/2.

**Question 7**

Suposem que existeixen un conjunt de variables aleatòries discretes Xi que modelen cadascun dels escenaris plantejats. Ordeneu els següents escenaris segons el valor de l'entropia de cada Xi. Ordeneu-los de major a menor, és a dir, indiqueu amb un 1 l'escenari que té una entropia més gran i amb un 6 l'escenari que mostra una entropia més petita.

|  |  |  |
| --- | --- | --- |
| El llançament d'un dau. | 5 | Correcta |
| Fer una travessa (sense saber-ne res de futbol). | 4 | Correcta |
| Escollir un àtom de l'univers observable a l'atzar. | 2 | Correcta |
| Triar una clau de 512 bits. | 1 | Correcta |
| Triar una persona dels Estats Units a l'atzar. | 3 | Correcta |
| El llançament d'una moneda. | 6 | Correcta |

Si considerem que cadascuna de les variables aleatòries discretes pot prendre un nombre ni de valors diferents i que cadascun d'aquests valors és igual de probable, aleshores l'escenari amb més entropia serà aquell que tingui un ni més gran.   
  
Analitzem doncs els valors ni de cada escenari:

* El llançament d'una moneda pot tenir dos possibles resultats (cara o creu).
* El llançament d'un dau tradicional en pot tenir 6.
* Una travessa té unes 15 milions de configuracions possibles (315 = 14348907).
* La població estimada dels Estats Units és de 315 milions de persones (315469000 al 2012).
* S'estima que hi ha entre 1078 i 1082 àtoms a l'univers observable.
* Si treballem amb claus de 512 bits, hi ha 2512 possibles claus diferents. 2512 és un nombre molt més gran que 1082.

Correcta

Punts d'aquesta tramesa: 1/1.