Cesar Kriptografia

Haitz Aldaraborda, Jon Mugica eta Iker Zaldua

2024.eko irailaren 15

1 Lehen Ariketa

Lehenengo ariketa honetan ondorengo mezu zifratua eskuratu da:

Jypwavnyhwof pz aol kpzjpwspul aoha ltivkplz aol wypujpwslz, tlhuz, huk tlaovkz mvy aol ayhuzmvythapvu vm khah pu vykly av opkl aolpy zlthuapj jvualua, wylclua aolpy buhbaovypglk bzl, vy wylclua aolpy buklaljalk tvkpmpjhapvu.

Hau deszifratzeko **"Brute Force"** ez erabiltzea eskatzen zen. Honen ondorioz, hizkien maiztasunaren araberako azterketa egitea proposatu da. Honen bidez, emandako zifratutako mezuan hizki bakoitzaren maiztasuna neurtu da. Neurketa hau egin ondoren, jakinik gure bukaerako mezua ingelesez egongo dela, maiztasun handieneko hizkia ingelesean gehien erabiltzen diren hizkiak direla suposatuko da. Honela, aldaketa hau egin dela suposasutz, mezua deszifratuko da. Ingelesean gehien erabiltzen diren hizkiak *"a", "e"* eta *"i"* hizkiak dira. Hauek dira lortu diren emaitzak:

A hizkia gaitik aldaturik: Ynelpkcnwldu eo pda zeoyelheja pdwp aixkzeao pda lnejyelhao, iawjo, wjz iapdkzo bkn pda pnwjobkniwpekj kb zwpw ej knzan pk deza pdaen oaiwjpey ykjpajp, lnarajp pdaen qjwqpdknevaz qoa, kn lnarajp pdaen qjzapaypaz ikzebeywpekj. E hizkia gaitik aldaturik: Ynelpkcnwldu eo pda zeoyelheja pdwp aixkzeao pda lnejyelhao, iawjo, wjz iapdkzo bkn pda pnwjobkniwpekj kb zwpw ej knzan pk deza pdaen oaiwjpey ykjpajp, lnarajp pdaen qjwqpdknevaz qoa, kn lnarajp pdaen qjzapaypaz ikzebeywpekj. I hizkia gaitik aldaturik: Criptography is the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Ikus daitekeenez, *"i"* hizkiarekiko egin da **"Cesar zifraketa"**.

2 Bigarren Ariketa

Bigarrengo ariketa honetan **"Brute Force"** metodoa erabiltzea eskatzen da. Ondorengoa da deszifratu beharreko mezua:

Tfewzuvekzrczkp zj ivjvimzex rlkyfizqvu ivjkiztkzfej fe zewfidrkzfe rttvjj reu uzjtcfjliv, zetcluzex dvrej wfi gifkvtkzex gvijferc gizmrtp reu gifgizvkrip zewfidrkzfe. Zekvxizkp zj xlriuzex rxrzejk zdgifgvi zewfidrkzfe dfuzwztrkzfe fi uvjkiltkzfe, reu zetcluvj vejlizex zewfidrkzfe efe-ivgluzrkzfe reu rlkyvekztzkp. Rmrzcrszczkp zj vejlizex kzdvcp reu ivczrscv rttvjj kf reu ljv fw zewfidrkzfe.

Egindako kodearen bitartez, zifratutako mezuaz eta ASCII taulaz baliatuz, aukera guztiak probatzen dira. Aukera egokia aurkitzeko, eskeinitako hiztegia erabiltzen da. Deszifratutako mezua hiztegiarekin konparatzen da, eta gutxienez sei hitz aurkitzerakoan, ontzat emango da deszifratutako mezua.

Honakoa da, emaitzatzat hartzen den deszifratutako testua:

Hau da deszifratutako mezua 9-ko desplazamenduarekin: Confidentiality is reserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is guarding against improper information modification or destruction, and includes ensuring information nonPrepudiation and authenticity. Availability is ensuring timely and reliable access to and use of information.

3 Cesar zifraketarekiko ondorioak

Cesar zifraketa ikusi ondoren ikus daiteke ez dela enkriptazio metodo fidagarri bat. Kode egokiarekin eta denbora nahikoarekin, azkar deszifra daiteke metodo hau erabili duen mezu zifratu bat. Zifraketa metodo hau ez litzake modu profesional batean erabili beharko eta ezta ere dokumentu garrantzitsu bat zifratu nahiko balitz. Metodo hau ona izan daiteke kriptografia zer den gehiago ulertzeko eta baita gai honetako kodeak diseinatzeko.