

Enkriptatze perfektua: lagunek ere ezin ulertu



Espainiako Errege-erregina Katolikoek posta-trukearen isilpekotasuna bermatzeko testuen zifratze sistema bat ezarri zuten. Ezin esan arrakasta izan zuenik.

INGALATERRA, 1495. Espainiako Errege-erregina Katolikoek Rodrigo Gonzalez de la Puebla (c. 1450-1525) diplomazialaria bidali zuten Londresko gortera, Katalina Aragoikoaren –Isabel eta Fernandoren alaba– eta Ingalaterrako erregegai Arturoren arteko ezkontza negoziatzea.

De la Pueblaren ahaleginak sei urte geroago eman zuen fruitua. 1601ean ezkondu ziren Katalina eta Arturo, baina senarra handik bost hilabetera hil zen. Katalina hildakoaren anaiarekin ezkondu zen orduan, Henrike VIII.a guztiz ezagunarekin. Gerora, Katalinarengandik banantzeko, Eliza Katolikoarekin hautsi eta Eliza Anglikanoa sortuko zuen Henrikek, baina hori beste kontu bat da.

Errege-erregina Katolikoek eta haien diplomazialariek ezin zuten aurreikusi ondoren gertatuko zena, baina bazekiten halakoak gai arantzatsuak zirela, garrantzi handikoak, eta informazioa ahal zen neurrian ezkutan atxikitzea ezinbestekoa zela, etsaien begietatik urrun behintzat.

Errege-erreginak oso kezkatuta zeuden horrekin, Europa osoan zeuzkaten agenteei bidaltzen zizkieten mezuetako asko etsaiek bidean atzeman eta inolako arazorik gabe irakurtzen baitzituzten. Horregatik posta-trukean enkriptatze sistema bat ezartzeko agindua eman zuten. Zifratze sistema sinplea zen teoriarik, hitzak zenbaki erromatarrez ordeztu-

katzean zetzana. Praktikan, ordea, errege-erreginen espioitza zerbitzuak gehiegi korapilatu zuen metodoa. Hala, sistemaren helburu nagusia lortu zuten: etsaiek ezin zituzten mezuek irakurri. Baina arazo berri bat eragin zuten: mezuen hartzaileek ere ez, gehienetan.

Esaterako, “itsasoa” (*mar*) idazteko MCCCCLXXXVIII zenbakia erabiltzen zuten, baina “*en*” preposizioarako DCCCCLXVIII erabili behar zuten, eta “*el*” artikulurako DCCCXXXIX. Horrenbestez, besterik gabe “itsasoa” esateko DCCCCLXVIII DCCCXXXIX MCCCCLXXXVIII idatzi behar zuten.

Posta-trukea zeharo nahasi eta mantsotu zuen sistemak, “ez da ulertzen”, “ez du zentzurik”, “bidali mezu argiagoak” eta halakoetan denbora erruz galtzen baitzen.

Rodrigo Gonzalez de la Pueblak ez zuen nahi bere misioa gaitz-ulertuetan gal zedin. Horregatik, Katalina eta Arturoren arteko ezkontza negoziazioen berri emateko Errege-erregina Katolikoek idatzi zirenean, arazoari konponbide erabat eraginkorra eman zion: gutuna monarkek erabakitako sisteman zifratuta joan zen, baina harekin batera sistemak erabiltzen zituen kodeen liburuxka atxikita bidali zuen. Hala, edozein hartzaile mezua erraz transkribatzeko gai izango zen. Mezuek bidean atzematen zituzten etsaiek ere bai, jakina. ■

Arrastoak

Nondik datoz futboleko txartel hori eta gorriak?

KENNETH ASTON arbitro britainiarrari Ingalaterra eta Argentinaren arteko partida nahasia epaitzea egokitu zitzaion 1966ko Futboleko Munduko Kopan. Partida amaitu eta, etxean zegoenez –txapelketa Ingalaterran jokatu zen–, bere autoa gidatuz irten zen epailea estadiotik. Semaforo batean gelditu zenean, semaforoen kodea futbolari ere aplikatu zekiokeela bururatu zitzaion.

Hau da, kolore horia ez zen nahikoa izango arau-hauslea egotzeko, eta jokalaria ohartarazita geratuko zen; semaforo gorriak autoen ibilia geldiarazten duen moduan, txartel gorriak arau-hauslearen jokoa etengo zuen, eta zelaitik egotziko zuten berehala.

Handik gutxira ideia FIFA-ra helarazi zuen, eta federazioak hurrengo Munduko Kopan jarri zuen martxan Astonen txartel sistema. Txartel hori eta gorriak 1970eko Mexikoko Kopan erabili zituzten lehenengoz. ■



RONNIE McDONALD-CC BY