Libe MORI CARRASCAL
UPV/EHUko Donostiako Informatika Fakultateko irakasle eta ikertzailea

Zer dela eta jasaten du kriptografia alorrak etengabeko aldaketa?

Historian zehar mezu sekretuak trukatzeko metodo ugari erabili dira. Kriptografia teknika matematiko ezberdinak erabiliz informazioa zifratzeko eta deszifratzeko zientzia da. Antzinako Egiptoko hieroglifiko misteriotsu batzuk dira kriptografiaren lehen hastapenak, baina ordutik asko aldatu da zientzia hau.

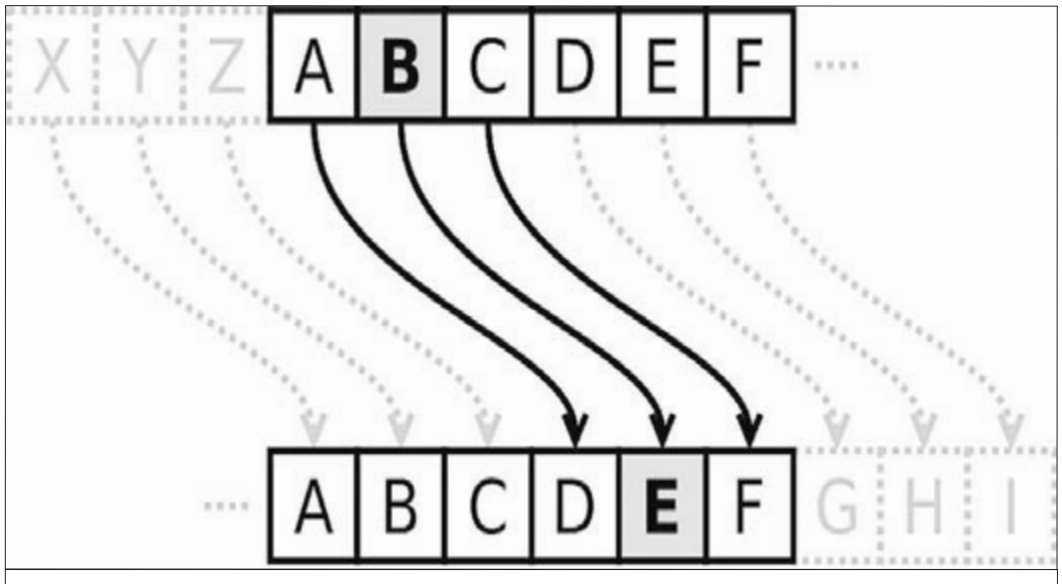
Julio Zesar enperadore erromatarrak bere jeneralekin komunikatzeko desplazamenduzko zifratze-sistema edo Zesarren zifratzea erabiltzen zuen. Zesarren zifratzea alfabetoa hainbat posizio eskuinera desplazatzean datza. Adibidez, hiru posizioko desplazamenduarekin A hizkia D bilakatzen da, B hizkia E eta Z hizkia C. Beraz,"BAI" hitza zifratzean, "EDL" bilakatzen da; "EZ", aldiz, "HC". Hiru posizioko desplazamenduarekin zifratutako mezu hau deszifratzen jakingo al zenuke? "CRULRQDN!"

Zenbat denbora behar izan duzu mezu hori deszifratzeko? Eta zifratzeko erabilitako desplazamendua zenbatekoa izan den jakingo ez bazenu, asmatuko al zenuke zein den jatorrizko mezua? Zenbat denbora beharko zenukeela uste duzu? Gaur egungo ordenagailu batek milisegundo bakar batzuk besterik ez lituzke beharko! Izan ere, latindar alfabetoan 27 hizki daudenez, alfabetoaren 26 desplazamendu ezberdin bakarrik dira posible. Edozein ordenagailuk ia bat-batean frogatu ditzake 26 aukerak eta, hiztegi bat erabilita, erraza da jatorrizko mezua zein den automatikoki identifikatzea. Aukera guztiak frogatzeari *brute force attack* deritzo.

Bigarren Mundu Gerran, Alemaniarrek Enigma makina erabili zuten. Makina honek barneko funtzionamendu elektriko mekaniko bati esker zifratu eta deszifratzen zituen mezuak. Makinak barnean bost errotoreko sistema bat zuen eta zifratzea errotore horien posizio aldakorraren araberakoa zen. Aliatuek, Alan Turing matematikariari esker, kodea apurtzea lortu zuten. Ondorioz, nazien mezu garrantzitsuak deszifratu ahal izan zituzten aliatuek. Naziek gerra galtzeko pisuzko arrazoitzat jotzen da Turing eta bere kideek egindako lana.

Gaur egun gehien erabiltzen den zifratze algoritmoa Advanced Encryption Standard (AES) da. Algoritmo hau guztiz irekia da, hau da, bere funtzionamenduaren azalpena edonorentzat eskuragarri dago. Mezu bat zifratzeko, 128, 196 edo 256 biteko luzera duen gako sekretu bat aukeratu behar da. Gako hau ezagutzen dutenek bakarrik deszifratu ahalko dute zifratutako mezua. AEBetako Gobernuak *top-secret* dokumentuak zifratzeko AES-256 algoritmoa erabili ohi du. Baina WhatsApp aplikazioak ere, AES-256 erabiltzen du mundu mailan egunero idazten diren mezu guztiak zifratzeko. Gakoa ezagutzen ez duen gaizkile batek WhatsApp mezuren bat deszifratu nahiko balu, 2256 gako posible guztiak frogatu beharko lituzke. Pelikuletan hackerrek segundo gutxi batzuetan egiten badute ere, errealitatean gure WhatsApp mezu bat deszifratzeko 1.000 milioi urte baino gehiago behar dira. Hau da, ezinezkoa da gaur egun AES-256 algoritmoa apurtzea gako sekretua seguru mantenduz gero.

Baina zer dela eta jasaten du kriptografia alorrak hainbesteko aldaketa? Zientzia eta teknologia alorretako aurrerakuntzen ondorioz, konputazio abiadura azkartuz doa. Hori dela eta, algoritmo bati *brute force attack* bat egitea azkarregia bilaka daiteke, eta ondorioz, algoritmoa ez da segurua izango. Zifratze algoritmoak seguruak diren bitartean erabili ohi dira, baina algoritmo baten ahulezia bat detektatzen denean, algoritmo berri seguruago batekin ordezkatzen da. •



Zesarren zifratzea alfabetoan hiru letrako desplazatzea egitean datza. GAUR8