2DES (MITM)

“Meet in the middle” erasoa bitartez, key2-ren aukera guztiak erabiliz testua zifratuko dugu eta mezu zifratuak taula batean gorde eta ordenatuko ditugu. Gero key1-eko aukera guztiak erabiliz mezu zifratuak deskodetu eta taulan dauden aukera guztiekin konparatzen ditugu, berdina den aukera bat aurkitzean key1 lortzen dugu eta key2 taulako posizio originala gorde duen k-index bektore bat erabili lortzen dugu. Azkenik emaitzak pantailaratzen ditugu. Segundu bat baino gutxiago behar du gakoaklortzeko.

2DES (Brute force)

Brute force bitartez gakoen aukera guztiak egiaztatu behar dira. Hau egiteko, bi for sortu ditugu, lehenengoan k2 gakoaren aukera guztiak egiaztatzeko 0 posizioan dauden bitak eguneratzen dira, eta k1 gakoan ezezagunak diren biteak 0ra jartzen ditugu. Bigarren for-aren barruan twodes funtzioari deitzen diogu, `"Can you "` mezua zifratzeko eta gero c1 mezu zifratuarekin konparatzen dugu, mezu zifratua eta twodes funtzioak hemandako emaitzak berdinak badira orduan begiztatik atera eta emaitzak pantailaratuko dira, konparazioa desberdina bada orduan k1 en beste aukera bat egiaztatzeko eguneratuko dugu. 52 segundu behar ditu gakoak aurkitzeko.

Ondorio nagusiak

2DES ez da zifratzeko teknika segurua, “meet in the middle” estrategia erabiliz mezuak deszifratzea nahiko azkarra da. 2DES brute force bitartez deszifratzeko aldiz gakoen aukera guztiak egiaztatu behar dira eta denbora asko beharko genuke, 2^112 aukera.