# ZER DA MUTURRETIK MUTURRERA ENKRIPTATZEA ETA NOLA FUNTZIONATZEN DU?

Mutur-muturreko enkriptatzea da modurik seguruena Interneten modu pribatuan eta seguruan komunikatzeko. Elkarrizketa baten bi muturretan mezuak enkriptatuz, amaierako enkriptatzeari esker, erdian dagoen edonork komunikazio pribatuak irakurtzea eragozten du.

Duela gutxi arte, muturretik muturrera enkriptatzea (E2EE) teknologia adituen domeinu bakarra zen hura erabiltzeko behar ziren eragiketa korapilatsuengatik. Hala ere, azken aurrerapen teknologikoek muturreko enkriptatzea askoz errazagoa eta eskuragarriagoa bihurtu dute. Artikulu honetan, **muturretik muturrera enkriptatzea zer den azalduko dugu eta zer abantaila eskaintzen dituen ohiko enkriptatzearekin alderatuta.**

## ZER DA END-TO-END ENKRIPTATZEA (E2EE)?

E2EE erabiltzen duzunean mezu elektroniko bat edo norbaiti mezu bat bidaltzeko, sarea kontrolatzen duen inork ezin du zure mezuaren edukia ikusi, ez hackerrek, ez gobernuak, eta ezta zure komunikazioa errazten duen konpainiak (adibidez, ***ProtonMail)***.

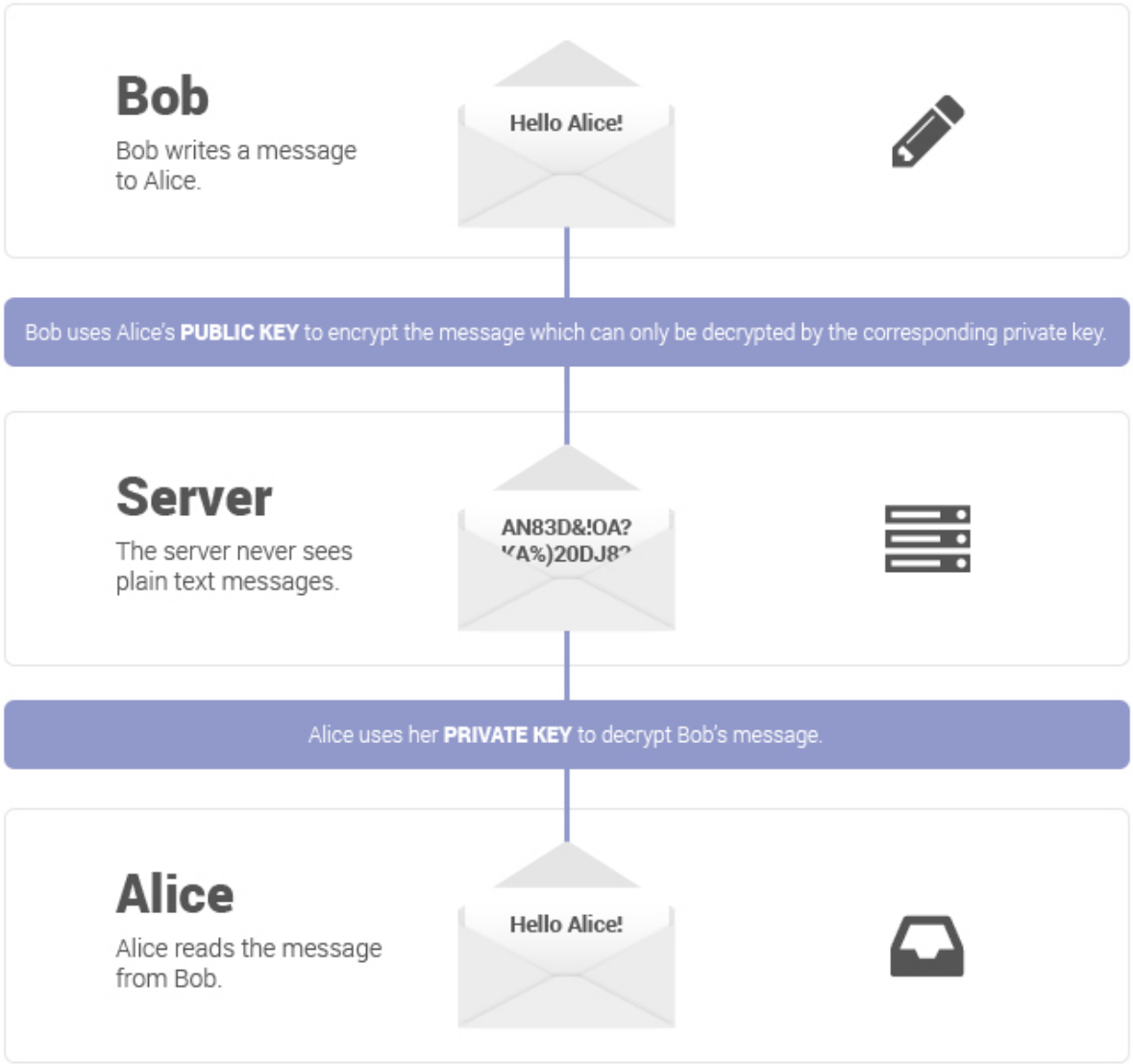
Enpresa gehienek dagoeneko erabiltzen duten enkriptatzetik desberdina da, zure gailuaren eta konpainiaren zerbitzarien artean igarotzen diren datuak soilik babesten dituena. Esaterako, E2EE eskaintzen ez duen zerbitzu bat erabiliz mezu elektroniko bat bidaltzen eta jasotzen duzunean, hala nola, Gmail edo Hotmail, enpresak zure mezuen edukia atzi dezake, enkriptatze-gakoak ere baititu. **E2EEk aukera hori ezabatzen du, zerbitzu-hornitzaileak ez baitu benetan deszifratzeko gakoa.** Horregatik, E2EE enkriptazio estandarra baino askoz indartsuagoa da.

## NOLA FUNTZIONATZEN DU MUTURREKO ENKRIPTATZEA?

E2EE nola funtzionatzen duen ulertzeko, diagrama bat ikusteak laguntzen du. Beheko adibidean, Bobek Aliceri agurtu nahi dio pribatuan. Alicek gako

publikoa eta pribatua ditu, matematikoki erlazionatutako bi enkriptazio-gako dira. Gako publikoa edonorekin parteka daiteke, baina Alicek bakarrik du gako pribatua.

Lehenik eta behin, Bob-ek Aliceren gako publikoa erabiltzen du mezua enkriptatzeko, eta “Kaixo Alice” testu zifratua deritzon zerbait bihurtuko du: karaktere nahastuak, itxuraz ausazkoak.



Bob-ek enkriptatutako mezu hau Internet publikoaren bidez bidaltzen du. Bide horretan, hainbat zerbitzarietatik pasa daiteke, erabiltzen ari diren posta elektronikoko zerbitzuarenak eta Interneteko zerbitzu hornitzaileak barne. Enpresa horiek mezua irakurtzen saiatuko diren arren (edo hirugarrenekin partekatzen ere), ezinezkoa zaie testu zifratua testu arrunt irakurgarri bihurtzea. Alicek bakarrik egin dezake hori bere gako pribatuarekin sarrera-ontzian sartzen denean, Alice baita bere gako pribaturako sarbidea duen pertsona bakarra. Alicek erantzun nahi duenean, prozesua errepikatu besterik ez du egiten, Bob-i bere mezua enkriptatzen Bob-en gako publikoa erabiliz.

# ENKRIPTAZIO-ZERBITZUEN ABANTAILAK

E2EEk hainbat abantaila ditu zerbitzu gehienek erabiltzen duten enkriptazio estandarraren aldean:

- **Zure datuak hacketatik babestuta mantentzen ditu.** E2EEk esan nahi du alderdi gutxiagok atzitu ditzaketela zifratu gabeko datuetara. Hacker-ek zure datuak gordetzen diren zerbitzariak arriskuan jartzen badituzte ere (adibidez, Yahoo posta-hackea), ezin dituzte zure datuak deszifratu, ez baitute deszifratze-gakorik.
- **Zure datuak pribatuak mantentzen ditu.** Gmail erabiltzen baduzu, Google-k zure mezu elektronikoetan jartzen dituzun xehetasun intimo guztiak ezagutu ditzake, eta zure mezu elektronikoak gorde ditzake ezabatu badituzu ere. E2EEk zure mezuak nork irakurtzen dituen kontrolatzen dizu.
- **Ona da demokraziarentzat.** Pertsona orok du pribatutasunerako eskubidea. E2EEk adierazpen askatasuna babesten du eta jazarturiko ekintzaile, disidente eta kazetariak beldurretik babesten ditu.

Hauek dira ProtonMail eraiki genuen arrazoiak. Posta elektronikoko hornitzaile seguru lehen eta handiena izanik, milioika erabiltzaile babesten ditugu egunero. Enkriptatzea muturreko enkriptatzea da gure ikuspegiaren ardatz teknologikoa Internet pribatuago eta seguruago baterako.