GSM ja 3G krüpteeringud mõlemad murtud

16 aastat tagasi - 19.01.2010 Autor: AM

Nii nagu hiljuti teatati GSM kürpteeringu lahtimurdmisest, langes äsja ka 3G krüpteering lahtimuukijate ees, kirjutab GSM Arena.

Artikkel GSM krüpteeringu lahtimuukimisest asub siin.

UMTSi krüpteerimisalgoritm KASUMI, mis võeti kasutusele keerukama MISTY1 asemel, murti lahti mõne tunniga ühel tavalisel arvutil. Seega pole võimalik reaalajas 3G seanssi lahti häkkida, kuid tegemist oli esimese, "toore" häkiga ja tegijad avaldasid arvamust, et algoritmi parandades saaks UMTSi krüpteering murtud tunduvalt kiiremini.

- Uudised