Радни лист – B08
Цезар и Al-Kindi су први актери криптографије

Људи су одувек желели да заштите своје комуникације, било да је реч о војним наредбама, шпијунирању непријатеља, трговини или размени љубавних писама. У време Јулија Цезара мало је било писмених људи па је зато његов метод шифрирања, иако врло једноставан, био довољан за већину ситуација. Ово шифрирање, при крају Старог века, постаје истанчаније јер се, уместо једноставног померања места слова у азбуци, користи случајна мешавина слова (тј., користи кључна реч или кључна реченица). Могућности су огромне и није могуће, ако се не познаје кључ, испитивање свих могућих азбука. Ово шифрирање познато као « моно-алфабетска супституција » (једном слову у « реалној поруци » одговара једно и само једно слово « шифрираној поруци ») није откривено током 1000 година. Тек је Al-Kindi пронашавши метод (назван « анализа фреквенције ») успео да за неколико минута открије шифру. Al-Kindi, чије је право име Abu¯ Yu¯suf Ya'qu¯b ibn Isa¯q al-Kind¯ |, је једна од највећих арапских научника, аутор је више од 290 рукописа из астрономије, математике, медицине, филозофије … Док је Западна цивилизација, у IX веку, била у периоду мрачњаштва (опскурантизма), дотле је арапска наука доживљавала своје златно доба. Al-Kindi је запазио да се нека слова појављују много чешће па се у моно-алфабетском шифрирањем не модификује ова фреквенција слова. На пример, ако је са « e » шифрирано « L », онда ће « L » имати исту фреквенцију у шифрираној поруци као и слово « e » у реалној поруци. Знајући фреквенцију слова у неком језику веома лако се налази довољно дуг реална текст. Al-Kindi је постао први криптоаналист у историји. Требало је сачекати XV век па да Léon Battista Alberti открије шифрирање поли-алфабетском супституцијом, а затим и да га Blaise de Vigenère доведе до перфекције. Овај метод је отпоран на анализу фреквенције јер користи више азбука, и доминирао је наредна 3 века, све док Шарл Бебиџ (Charles Babbage) није успео да га доведе у питање. Од тада се наставља трка између криптографа (који су иновирали шифрирања) и криптоаналиста (који су покушавали да та шифрирања открију). Критографи су се механизовали а затим и информатизовали. Савремени криптографи су више математичари него лингвисти, али проблеми остају исти. Међутим, као што ћемо видети, походом интернета и дигитализације наших комуникација, ови проблеми добијају нову димензију:

• С једне стране, државе могу да пресретну сваку комуникацију (e-mail, телефон…) између две индивидуе, и покушавају да лимитирају употребу криптографије у циљу очувања сигурности (пре свега, шпијунирање терориста).

• С друге стране, грађани постају свесни важности очувања своје интимности, било да је реч о породичном животу, здрављу, политичком мишљењу, религиозним слободама, сексуалним оријентацијама … Како могу да искористе ове информације неодговорни појединци или недемократске владе?