**Kas yra kriptografija?**

Kriptografija, tai mokslas naudojantis matematiką užšifruoti ir dešifruoti duomenims. Kriptografija leidžia saugoti ypač slaptą informaciją ir siųsti ją nesaugiais tinklais(kaip Internet), taigi jos negali perskaityti niekas kitas, kaip tik gavėjas.

Kriptografijos saugumui tikrinti yra naudojama kriptoanalizė. Paprasta kriptoanalizė, tai loginės kombinacijos, matematinių įrankių panaudojimas, kantrybė, pasiryžimas ir žinoma - sėkmė. Kripto analitikai dar kitaip vadinami atakuojančiaisiais.

SHA -1 ir SHA- 2 dalis tos pačios struktūros ir matematinė operacija , kaip jų pirmtakai - SHA- 0 ir MD5 . Tiek SHA- 0 ir MD5 jau neveikia. Tai yra viena iš pagrindinių priežasčių, kodėl SHA- 1 yra laikomas nesaugus ir yra palaipsniui nutraukiamas dėl SHA -2.

SHA-0: a Retronym kreipėsi į pradinės versijos 160 bitų maišos funkcija paskelbtas 1993 pagal pavadinimą "SHA". Jis netrukus buvo atšauktas ir pakeistas šiek tiek pataisytos versijos SHA-1.

     SHA-1: A 160 bitų maišos funkcija, kuri primena ankstesnę MD5 algoritmą. Tai buvo suprojektuotas Nacionalinio saugumo agentūros (NSA) dalyvauja skaitmeninio parašo algoritmą. Šifravimo trūkumai buvo atrastas SHA-1, o standartinis nebebuvo patvirtino dauguma kriptografinių naudojimo po 2010 m.

     SHA-2: iš dviejų panašių maišos funkcijų šeima, su skirtingų blokų dydžių, žinomas kaip SHA-256 ir SHA-512. Jie skiriasi žodis dydžio; SHA-256 naudoja 32 bitų žodžius, kur SHA-512 naudoja 64 bitų žodžius. Taip pat yra elektroniniai variantai kiekvienam standartui, žinomas kaip SHA-224, SHA-384, SHA-512/224 ir SHA-512/256. Tai taip pat buvo sukurta NSA.

     SHA-3: maišos funkcija anksčiau vadinta Keccak, pasirinko 2012 po viešo konkurso tarp ne NSI dizainerių. Jis palaiko tuos pačius maišos ilgio kaip SHA-2, ir jos vidaus struktūra labai skiriasi nuo SHA šeimos narių.

NIST paskelbė 2007 m konkursą gaminti naujos kartos NIST maišos funkcija: SHA- 3 .

Rakto stiprumas dar priklauso nuo jo dydžio. Dydis matuojamas bitais. Pvz.: 1028 bitų dydžio raktas skaitomas labai dideliu. Viešojo rakto kriptografijoje kuo didesnis raktas, tuo saugesni duomenys. Viešasis ir privatus raktai yra matematiškai susije. Nustatyti privatų raktą turint tik viešąjį yra begalo sunku, tačiau, tai įmanoma skyrus pakankamai laiko ir skaičiavimo resursų. Todėl svarbu parinkti teisingą dydį jūsų raktui. Taip pat reikia numatyti kas norės perskaityti Jūsų duomenis, ar labai jie tam pasiryžę, kiek laiko jie turi ir maždaug kokius resursus jie gali panaudoti. Raktai yra užšifruoti ir saugomi dvejuose failuose jūsų diske. Šie failai  
vadinami viešas žiedas raktams(angl. "public keyring") ir privatus žiedas raktams(angl. "private keyring"). Į viešą žiedą raktams galima dėti įvairių įmonių/žmonių viešuosius raktus. O į privatų žiedą - tik Jūsų privačius raktus. Jei prarasite savo privatų žiedą, nebegalėsite dešifruoti Jums skirtų duomenų.