Tekstas, kurį galima skaityti nepanaudojus jokių specialių priemonių vadinamas paprastu tekstu. Metodas naudojatis paprastą tekstą ir paverčiantis jį į gausybę nieko bendro tarp savęs neturinčių simbolių vadinamas šifravimu. O toks tekstas - užšifruotu tekstu.

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. Šiame informacijos amžiuje kiekviena gauta informacijos delelytė gali būti panaudota prieš jus. Tai ypač aktualu konkurentams. Kam naudoti pinigus ir resursus, jei galima visą reikiamą informaciją gauti iš savo priešininkų. Šifravimas taip pat labai svarbi elektroninės komercijos dalis. Norint įgyti klientų pasitikėjimą turi būti užtikrintas jų duomenų saugumas.

Šifravimo algoritmas, tai matematinė funkcija naudojama šifravimo ir dešifravimo procese. Algoritmo veikimui reikalingas slaptažodis. Slaptažodis gali buti žodis, numeris, frazė, įvairūs simboliai. Tas pats tekstas užšifruotas skirtingais slaptažodžiais skirsis vienas nuo kito. Taigi viso užšifruoto teksto saugumas priklausys nuo pasirinkto algoritmo ir slaptažodžio slaptumo.

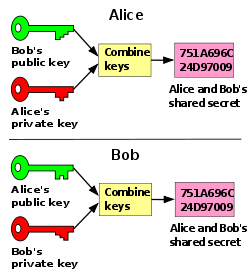
Gavėjas, norėdamas dešifruoti pranešimą, gali naudoti visiškai kitą algoritmą, negu naudojo žmogus šifruodamas informaciją. Taigi šifravimo ir dešifravimo raktai gali skirtis. Šiuo atveju yra išskiriamos dvi kriptosistemos: simetrinė ir asimetrinė.

Simetrinėse kriptosistemose šifravimo rakto žinojimas leidžia lengvai rasti dešifravimo raktą (neretai šie raktai yra vienodi). Todėl tokiose sistemose abu raktai turi būti laikomi paslaptyje. Taigi simetrinės kriptosistemos nėra itin saugios; jos gali būti naudingos tik tada, kai siuntėjas ir gavėjas yra tas pats asmuo. Tad šios sistemos dažniausiai yra naudingos tam tikros privačios informacijos išsaugojimui. Vienintelis tokio šifravimo privalumas ─ greitumas (informaciją galima greitai užšifruoti ir dešifruoti); naudojantis simetrine kriptografija, yra sutaupoma daug laiko.

Tuo tarpu asimetrinės kriptosistemos nėra tokios greitos, bet yra žymiai saugesnės. Jose šifravimo rakto žinojimas nepadės rasti dešifravimo rakto. Asimetrinėje sistemoje tik dešifravimo raktas turi būti laikomas paslaptyje, kitą raktą galaima paskelbti viešai. Taigi čia kiekvienas vartotojas turi du raktus, iš kurių vienas yra viešasis raktas, o kitas ─ privatusis raktas, arba slaptasis raktas. Kadangi viešasis raktas gali būti žinomas visiems, todėl asimetrinė kriptosistema dažnai vadinama viešojo rakto kriptosistema. Viešojo rakto kriptosistemą galima palyginti su pašto dėžute: kiekvienas žmogus gali mesti laiškus į jos vidų, tačiau dėžutę atidaryti, perskaityti gautus laiškus gali tik vienintelis žmogus ─ rakto turėtojas. Tad išsiųsti užšifruotą pranešimą, pasinaudojęs viešai paskelbta informacija, gali kiekvienas, o dešifruoti žinutę galima tik su slaptu raktu, kuris priklauso tik vienam žmogui ─ informacijos gavėjui.

Tačiau viešojo rakto kriptografija turi vieną didelę problemą. Tai ─ laikas, kurį sugaištame, kol sugalvojame šifravimo ir dešifravimo raktus. Be to, laikas, skirtas kompiuteriu apdoroti užšifravimo rezultatus, proporcingai didėja nuo žinutės ilgio. Pavyzdžiui, jei tam tikro ilgio pranešimą užšifruoti/dešifruoti trunka 10 sekundžių, tai keturis kartus ilgesnę žinutę dešifruoti prireiks šešiolika kartų daugiau laiko ─ 160 sekundžių. Tuo tarpu slaptas kriptografijos raktas yra greitas ir naudingas, nepriklausomai nuo žinutės ilgio.

Raktai yra užšifruoti ir saugomi diske dvejuose failuose. Šie failai vadinami viešas žiedas raktams (public keyring) ir privatus žiedas raktams (private keyring). Į viešą žiedą raktams galima dėti įvairių įmonių/žmonių viešuosius raktus. O į privatų žiedą ─ tik asmens privačius raktus. Jei žmogus praranda savo privatų žiedą, nebegali dešifruoti jam skirtų duomenų.



Maišos algoritmai yra naudojami duomenims, esantiems sistemose su laisvu priėjimu, adresuoti. Maiša (angl. hashing). Tai yra matematinė transformacija, atliekama tam tikro ilgio simbolių eilutę verčiant į fiksuoto ilgio – dažniausiai trumpesnę – reikšmę. Ši reikšmė atstovauja originaliai eilutės reikšmei. Dažniausiai maiša naudojama duomenų įrašų duomenų bazėje indeksuoti ar ištraukti, nes taip operacija yra atliekama greičiau – surasti trumpesnę reikšmę yra mažiau sąnaudų reikalaujanti operacija, negu surasti originalią simbolių eilutę. Maiša taip pat naudojama ir kodavimo algoritmuose. Kriptografijoje maišos algoritmai priima tam tikrą duomenų kiekį, juos transformuoja ir grąžina fiksuoto dydžio simbolių eilutę. Tai yra vadinama maišos reikšme. Maišos reikšmė yra tiksli didesnio duomenų kiekio ar dokumento reprezentacija, tai yra tam tikras skaitmeninis pirštų antspaudas.

Plačią šifrų klasę sudarantys blokiniai šifrai veikia tokiu principu: atviras tekstas yra suskirstomas simbolių blokais, paskui sudaroma speciali funkcija, kuri susieja atviro teksto bloką su slaptu raktu. Taip gaunamas užšifruotas tekstas. Šiuolaikiniuose blokiniuose šifruose blokai yra pakankamai dideli: 64, 128 ir daugiau bitų. Sudarant blokinius šifrus yra naudojami keitimo bei perstatymo šifrai.

Secure Hash Algorithm (**SHA**). Saugus maišos algoritmas iš pranešimo, kuris yra mažesnis už 264 bitų, generuoja 160 bitų kodą. Šis kodas yra skaičiuojamas taip: pradinis tekstas suskirstomas į N blokų po 512 bitų (64 baitus); jei paskutiniame Mn bloke trūksta informacijos iki 512 bitų, bloko gale pridedamas 1 ir tiek 0, kad būtų užpildytas blokas paliekant 64 bitus pradinio teksto ilgio išsaugojimui bitais; naudojamos funkcijos f0, f1, … f79. Kiekviena funkcija operuoja trimis 32 bitų žodžiais B, C, D ir grąžina vieną 32 bitų žodį.

**SHA-1** (Secure Hash Algorithm) – dar vienas populiarus algoritmas, naudojamas įvairiose programose ir protokoluose. SHA-1 buvo laikomas pažeidžiamo MD5 algoritmo įpėdiniu, tačiau 2004 ir 2005 metais atrasti pažeidžiamumai daro šį algoritmą nerekomenduotinu. Yra sukurta saugesnių SHA-1 algoritmo variacijų (SHA-224, SHA-256, SHA-384, SHA-512). SHA-1 apskaičiuoja 160 bitų parašą.

**SHA-2** algoritmas - tai šeima is dviejų algoritmų (SHA-256 ir SHA-512). Jie skiriasi generuojamo bloko(žodžio) kodo dydžiu; SHA-256 naudoja 32 bitų žodius, o SHA-512 naudoja 64 bitų žodžius. Taip pat yra sukurtų ir sutrumpintų kiekvieno standarto versijų (SHA-224, SHA-384, SHA-512/224 ir SHA-512/256.

SHA-1 ir SHA-2 buvo sukurti Nacionlinės Saugumo Agenturos(NSA). **SHA-3** buvo sukurtas 2012 metais po viešo konkurso ne NSA dizainerių. Jis palaiko tuos pačius kaip ir SHA-2 maišos dydžius, tačiau jo vidinė sandara ganėtinai smarkiai skiriasi nuo kitų SHA šeimos algoritmų.

