**Esitluse käsikiri**

**Algoritmid**

Algoritmid koosnevad reeglistikest, mis toodavad reeglitele vastavalt uue vastuse. Kui võtta näiteks tehe “1 + 2 = 3”, siis see koosneb kindlast liitmise reeglist - ühele arvule liidetakse teine. Samal põhimõttel töötavad ka algoritmid. Selleks, et saada endale näiteks parem parool või kasutajanimi, siis võib võtta näiteks valemi “eesnimi + sünniaasta 2 viimast numbrit = algoritm”. Seda või sarnast algoritmi saab kasutada omale turvalisema parooli või muu sarnase loomiseks.

Algoritmid on samm sammulised õpetused millegi tegemiseks. Algoritme saab kasutada ükskõik millise tegevuse kirjeldamiseks.

**Ajalugu**

1900 e.m.a

Esimesed teadaolevad tõendid krüptograafia kasutamise kohta leiti Egiptusest Khnumhotep II hauakambrist, mis on pärit aastast 1900 e.m.a.. Kuigi see ei olnud algselt mõeldud krüpteerimiseks, vaid pigem selleks, et muuta see tekst visuaalselt elegantsemaks, siis see on vanim tekst mida on sellisel viisil muudetud ning seetõttu arvestatakse seda, kui esimest krüpteerimist.

50-60 e.m.a

Caesari nihe on krüpteerimise viis, kus ühte tähte nihutati 3 koha võrra, see tähendab, kui oli vaja krüpteerida täht “A”, siis see võrdus krüpteerides tähega “D”, “B” asendati tähega “E” jne. Seda kasutas ta selleks, et saata sõnumeid oma sõjaväe kindralitele. Kahjuks ei olnud tema väljamõeldud krüpteerimis viis piisavalt turvaline ning pidevate kirjade saatmisega saadi peatselt koodi loogikale jälile ning kood murti.

16.saj

Vigenere krüpt oli väidetavalt esimene krüpteerimisvõtit kasutav krüptimis viis. Tervet sõnumit krüptiti mitmeid kordi üle ning seejärel lisati šifreerimistekst. (kuidas Enigma töötab on seletatud videos, mis on nimega “Kuidas Enigma töötab?” ). Nagu ka Caesari nihe, oli seda viisi liiga kerge lahti murda, aga erinevus on selles, et tähtsam oli murda lahti krüpteerimisvõti ning seetõttu läks selle krüpti lahtimurdmisega rohkem aega.

1939-1945

Sakslaste Enigma oli masin, mida kasutati Teises Maailmasõjas militaarsõnumite edastamiseks ning kaitsmiseks vaenlaste eest. Enigma kasutas kolme või isegi rohkemaid rootoreid, mis krüpteerisid teksti. **Rootor** on nn “salajane” võti mis on pööratud kettasse. Klahv kodeeris asendustabeli ja iga kord kui vajutati klahvi, siis sai see endale uue krüpteeritud väärtuse. Seda viisi kasutati kuni poolakad murdsid masina ning kõik tehnoloogia ning andmed edastati Briti krüptograafidele, kes selle masina lõplikult murdsid.

2001

AES on tõlkes Täiustatud Krüpteerimisstandard. See programm kasutab ühte võtit nii krüpteerimiseks kui ka dekrüpteerimiseks. AES kasutab aloritmi Rijndael. See töötleb 128-bitiseid andmeblokke.

2008

Aastal 2008 registreeriti Bitcoin ametlikult. Bitcoin on detsentraliseeritud digitaalne käibevahend ehk virtuaalraha ehk e-raha, millega saab kaubelda kogu maailmas.

**Krüpteerimise viisid**

Caesari nihe

Caesari nihe on krüptograafias üks lihtsamaid ja tuntumaid šifreerimismeetodeid. (Seda seletasime eelneval slaidil täpsemalt, seega pole uuesti vaja üle hakata rääkima)

Räsi ehk hash

Räsi ehk hash on suvaliste numbrite ja tähtede rida mida ei saa tagasi teha tavaliseks tekstiks. Hashi/räsi kasutatakse enamus veebilehtede salasõnade hoiustamisel. Hash/räsi tehakse algoritmi põhjal.

ID kaardiga krüpteerimine

Selle jaoks on vaja digidoc’i. DigiDoc´is koosneb faili krüpteerimine kahest etapist.

1. Kõigepealt krüpteeritakse fail sümmeetrilise algoritmiga, mille jaoks genereeritakse juhuslik võti (edaspidi transpordivõti).
2. Seejärel krüpteeritakse transpordivõti adressaadi avaliku võtmega, kasutades asümmeetrilist algoritmi. Kui adressaate on mitu, siis krüpteeritakse transpordivõti iga adressaadi avaliku võtmega eraldi.

**Binaarsüsteem (see slaid on lisaks, siis kui aega jääb üle)**

Binaarsüsteem ehk kahendsüsteem on positsiooniline arvusüsteem, mille aluseks on arv2. Kahendloogikas öeldakse numbrimärgi “1” kohta "tõene" ja numbrimärgi 0 kohta "väär". Slaidi alumises vasakpoolses nurgas on tabel, kus on näidatud, mis viisil saadakse astendamise väärtused. Slaidi parempoolses osas on toodud näiteks, kuidas saadakse kahendsüsteemi abil arv 213. Tabeli esimesel real on märgitus astmed (20, 21 jne). Järgneval real on näidatud ära, mis väärtus vastab astmele(1, 2, 4 jne). Viimasel real on sümbolid (0 ja 1), mis näitavad kas see aste/astme väärtus on nn “tõene” või “väär”. Selleks, et saada teada, mis on lõplik arv, tuleb kõik tõesed astmed/astme väärtused kokku liita ning selle tulemusel saategi lõpp vastuse. Kahendsüsteemi põhiliseks kasutusalaks on arvutid ja enamasti lähtuvad arvutite ja muude elektroonikaseadmete mikrokiibid kahendloogikast. Vaatamata sellele ei ole see ainuvõimalik arvusüsteem arvuti sisesteks andmete vahetamiseks või säilitamiseks.

**Kus kasutatakse krüpteerimist?**

Tänapäeval on krüpteerimine põhiline viis digitaalsete andmete kaitsmiseks. Krüpteerimise abil kaitstakse telefonikõnesid pealtkuulamise eest ning meditsiiniandmeid ja ärisaladusi lekkimise eest. Muuhulgas kasutatakse krüpteerimist tasuliste telekanalite edastamisel, wifi võrgu kaitsmisel, HTTPS protokolli kasutavate veebilehtedega suhtlemisel, digiallkirjastamisel ja e-hääletamisel. Krüpteeritud ühenduse kasutamine on üks oluline meetod turvalise internetipanga teenuse pakkumisel.(*Tartu Ülikooli arvutiteaduse instituudi programmeerimise õpetamise töörühm 2015/16* )

**Kasutatud allikad**

* <https://access.redhat.com/blogs/766093/posts/1976023>
* <https://courses.cs.ut.ee/2016/eprogalused/Main/Silmaring-krypteerimine>
* <https://blog.storagecraft.com/5-common-encryption-algorithms/>
* <https://www.arvutikaitse.ee/arvutikaitse-algtoed/krupteerimine/>
* <https://www.cs.du.edu/~snarayan/crypt/vigenere.html>
* <https://learncryptography.com/tools/caesar-cipher>
* <http://www.counton.org/explorer/codebreaking/enigma-cipher.php>
* <https://et.wikipedia.org/wiki/Caesari_nihe>
* <https://www.id.ee/?id=30300>
* <https://penguindreams.org/blog/password-algorithms/>
* <https://en.wikipedia.org/wiki/Cryptographic_hash_function>
* <https://www.id.ee/?id=30300>
* <https://mirapic.com/abstract-matrix-binary-image-desktop-wallpaper-hd/>
* <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/polyalphabetic-cipher>
* <https://et.wikipedia.org/wiki/Kr%C3%BCptograafia>
* <https://et.wikipedia.org/wiki/%C5%A0ifreerimine>
* <https://www.google.com/search?rlz=1C1GCEA_enEE827EE827&ei=BQ9uXO7tDIadrgTjsJ-gDw&q=bitcoin&oq=bitcoin&gs_l=psy-ab.3..0i67l3j0j0i67l2j0l4.324864.326252..326818...0.0..0.132.766.1j6......0....1..gws-wiz.......0i71j0i131j0i131i67.zVoV2b2Ji7o>
* <https://et.wikipedia.org/wiki/T%C3%A4iustatud_kr%C3%BCpteerimisstandard>
* <https://www.google.com/search?q=Caesar+cipher&rlz=1C1GCEA_enEE827EE827&source=lnms&tbm=isch&sa=X&ved=0ahUKEwichq7Bt8rgAhVNtIsKHZtcBssQ_AUIDigB&biw=1600&bih=789#imgrc=U9ghdijQI_F4jM>:
* <https://www.google.com/search?rlz=1C1GCEA_enEE827EE827&biw=830&bih=766&tbm=isch&sa=1&ei=TW5tXNyCMMSBk74P9pOXwAE&q=enigma+machine&oq=enigma+ma&gs_l=img.3.0.0i19l10.2391.3534..4515...0.0..0.536.1017.2-2j5-1......1....1..gws-wiz-img.......0j0i30.SBrRhZmXdnU#imgrc=1nIN-mUIII2fDM>:
* <https://www.google.com/search?q=what+is+crypting&rlz=1C1GCEA_enEE827EE827&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjDxbPP7crgAhVy5KYKHYiCDWYQ_AUIDigB&biw=1600&bih=789#imgrc=824g8R3IVoqZ3M>:
* <https://www.google.com/search?rlz=1C1GCEA_enEE827EE827&biw=1600&bih=789&tbm=isch&sa=1&ei=1Z5tXKfVG62dmwXPk5SACg&q=cryptography+wifi&oq=cryptography+wifi&gs_l=img.3...5155.5968..6424...0.0..0.162.640.0j5......1....1..gws-wiz-img.......0i19j0i5i30i19j0i8i30i19.QmqwlOTortM#imgrc=hn4CFl_hlB9OlM>: