OULUN AMMATTIKORKEAKOULU

Juuso Seppälä

Symmetrinen ja asymmetrinen salaus

Muinaisajoista nykypäivään

Symmetrinen ja asymmetrinen salaus

Muinaisajoista nykypäivään

Juuso Seppälä
Opinnäytetyö
Kevät 2024
Tietojenkäsittely
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittely

Tekijä: Juuso Seppälä
Opinnäytetyön nimi: Symmetrinen ja asymmetrinen salaus - Muinaisajoista nykypäivään
Työn ohjaaja: Minna Kamula
Työn valmistumislukukausi ja -vuosi: Kevät 2024
Sivumäärä: 47

Tämän työn tekstisisältö toimi johdatuksena ja pohjana salausmenetelmiä käsittelevälle verkkosivuprojektilleni, jonka työstäminen tulee jatkumaan tulevaisuudessa. Työn aihe on erittäin laaja, joten tekstisisältö pyrkii käsittelemään aihealueet tehokkaasti, mutta informatiivisesti.

Opinnäytetyön teoriasisältö johdattaa lukijan sekä symmetrisen että asymmetrisen salakirjoittamisen historiaan ja kehitykseen tarjoten tunnetuimpia esimerkkejä eri aikakausien salausmenetelmistä. Tekstissä mainitaan lyhyesti myös aiheeseen liittyviä käsitteitä ja avainteemoja. Työssä kuljetaan kronologisessa järjestyksessä, joka auttaa lukijaa hahmottamaan salakirjoitusmenetelmien kehityksen aikajanan selkeästi.

Teoriasisällössä ei pyritä keskittymään yksittäisiin salakirjoitusmenetelmiin ja algoritmeihin liian yksityiskohtaisesti, sillä varsinkin modernien salausmenetelmien kohdalla tämä tarkoittaisi sisältöä oman itsenäisen opinnäytetyön laajuudella. Sen sijaan tekstisisällössä keskitytään laajempaan näkökulmaan, mahdollistaen kokonaisvaltaisen katsauksen eri salausmenetelmiin.

Tekstin lopussa tarkastellaan verkkosivuprojektini tähänastista tilaa, sekä teknologioita sen takana.

Asiasanat: Kryptografia, kryptologia, salakirjoitus, salaus

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business information system

Author: Juuso Seppälä
Title of thesis: Symmetric and asymmetric encryption - From ancient times to the present day
Supervisor: Minna Kamula
Term and year when the thesis was submitted: Spring 2024
Number of pages: 47

The textual content of this thesis served as an introduction and foundation for a web project focusing on encryption methods, the development of which will continue in the future. The topic of this thesis is extensive, so the textual content aims to address the subject areas effectively yet informatively.

The theoretical content of this thesis guides the reader through the history and development of both symmetric and asymmetric cryptography, providing notable examples of encryption methods from different eras. The text also briefly mentions relevant concepts and key themes. The work follows a chronological order, aiding the reader in understanding the timeline of the development of encryption methods.

The theoretical content does not aim to delve too deeply into individual encryption methods and algorithms, especially for modern encryption, as this would imply content of the scope of an independent thesis. Instead, the textual content focuses on a broader perspective, enabling a comprehensive overview of various encryption methods.

At the end of the text, we will review the status of my web project and the technologies behind it.

Keywords: Cryptography, cryptology, cipher, encryption

SISÄLLYS

1 JOHDANTO

Opinnäytetyöni on kokonaisuus, joka koostuu niin teoriaosuudesta kuin käytännön osuudestakin. Työn päällimmäisenä tarkoituksena oli saada alkuun verkkosivuprojekti, jota voin tulevaisuudessa jatkokehittää. Projektin päämääränä on koota sivustolle keskitetysti erinäisiä salakirjoitusmenetelmiä läpi historian, lähtien yksinkertaisimmista klassisista salakirjoitusmenetelmistä.

Vaikkakin motiivi projektille on puhtaasti henkilökohtainen mielenkiinto aihetta kohtaan, responsiivinen ja käyttäjäystävällinen sivusto voisi tulevaisuudessa palvella vaikkapa eettisen hakkeroinnin tai geokätköilyn yhteisöjä. Edellä mainittujen yhteisöjen peleissä ja harjoituksissa, esimerkiksi CTF:ssä (Capture the flag), on satunnaisesti käytetty helppoja salakirjoitusmenetelmiä viestien salaamiseksi, sekä interaktiivisuuden ja mielenkiinnon lisäämiseksi.

Ottaen huomioon aiemman melko vähäisen tietämykseni kryptografiasta, oli teoriaosuudella merkittävä rooli luoda pohja ja ymmärrys aiheeseen. Aiheesta lukeminen ja kirjoittaminen syvensivät tietämystäni salakirjoittamisen monimutkaisista käsitteistä sekä tekniikoista. Toisaalta tähän työhön kokoamani aineisto voi toimia myös tämän työn lukijoille hyvänä aiheeseen johdattelevana tietopakettina.

Teoriaosuus käy läpi salauksen terminologiaa ja avainteemoja, minkä jälkeen siirrytään melko pian salakirjoittamisen historian maailmaan, alkaen muinaisen Egyptin hieroglyfeista. Tekstin edetessä tarkastellaan historian tunnetuimpia klassisia salakirjoitusmenetelmiä, jotka muokkasivat kryptografian maailmaa omalla tavallaan. Tekstin loppupuolella käydään myös läpi nykypäivän tunnetuimpia symmetrisiä ja asymmetrisiä salausmenetelmiä. Aiheen laajuuden vuoksi tekstissä ei pyritä käsittelemään yksittäisiä salakirjoitusmenetelmiä liian yksityiskohtaisesti. Sen sijaan sisältö on tiivistetty tehokkaaseen, mutta informatiiviseen kokonaisuuteen.

Työn aihe keskittyy keskeisimpiin symmetrisiin ja asymmetrisiin salausmenetelmiin, jotka muodostavat vain pienen osan laajasta kryptografian kentästä. Kryptografia on historian saatossa palvellut monia tarkoitusperiä, kuten salaperäisyyden lisääminen uskonnollisissa yhteyksissä, sotaviestinnän ja valtiosalaisuuksien turvaaminen, kuin myös yksilöiden yksityisyyden suojaaminen. Nykypäivän digitaalisessa maailmassa kryptografialla on keskeinen rooli tietoturvan

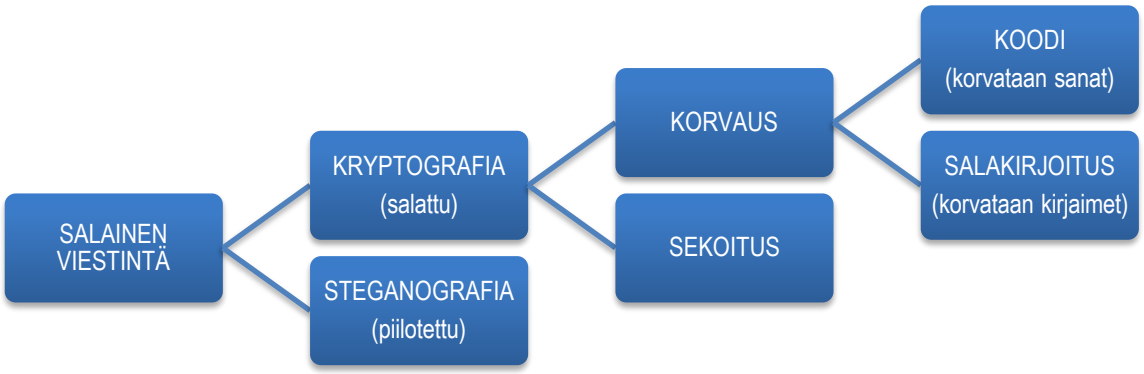
ylläpitämisessä, online-transaktioiden suojaamisessa ja yksityisyyden varmistamisessa. Täten aiheesta innostuneita kannustan tutustumaan kryptografian maailmaan syvemmin. Henkilökohtaisesti toivon, että teoriaosuus kykenee tarjoamaan selkeän ja informatiivisen näkökulman salakirjoitusten maailmaan tuoden lisäarvoa niille, jotka syventyvät opinnäytetyöhöni.

2 MIKÄ IHMEEN KRYPTOGRAFIA?

Kryptografiaan ja siihen sidoksissa oleviin termeihin liittyy usein väärinymmärryksiä siitä, mitä ne oikeastaan tarkoittavat. Jotkin määritelmät saattavat vaikuttaa monimutkaisemmilta kuin on tarpeellista ja eivät siten aina tarjoa riittävää käsitystä aiheesta. Yksinkertaisimmillaan kryptografia tarkoittaa tutkimusta, kuinka muokata viestejä niin, ettei ulkopuolinen viestin sieppaaja kykene lukemaan viestiä ilman oikeanlaista algoritmia ja avainta. (Easttom 2022, luku 1, ”What is Cryptography?”.)

On hyvä huomioida, että kryptografia ja kryptologia eivät myöskään ole synonyymejä, vaikka usein ihmiset sekoittavat nämä käsitteet keskenään. Jopa monet tekstikirjat sekoittavat käsitteet keskenään. Kryptologia on kryptografiaa kattavampi käsite, joka kattaa viimeiseksi mainitun lisäksi myös kryptoanalyysin. Kryptoanalyysilla sen sijaan viitataan menetelmiin ja periaatteisiin, joilla viestin salaus kyetään purkamaan tietämättä avainta. (Easttom 2022, luku 1, ”What is Cryptography?”.)

Kuviossa 1 havainnollistetaan salaisen viestinnän päähaarat, joita tarkastelemme lisää tulevissa kappaleissa.



Kuvio 1. Salakirjoituksen taito ja sen päähaarat (Singh 1999, 57). Kuvion ulkoasua on muokattu tarkemman selkeyden saavuttamiseksi.

2.1 Kryptografiaa ja mystiikkaa Egyptissä

Kryptografian historia on hyvin vanha, ja sitä voidaankin pitää lähes yhtä iäkkäänä kuin itse kirjoitustaitoa. Varhaisimpia esimerkkejä, joissa viitteitä kryptografiaan todistetusti voidaan havaita, sijoittuu noin 4000 vuoden taakse Egyptiin, jolloin sekä elämästä että saavutuksista kertovia hieroglyfejä käytettiin koristamaan kuolleiden hallitsijoiden ja kuninkaiden hautoja. Kyseisiä hieroglyfejä tarkoituksenmukaisesti muunneltiin kryptiseen muotoon, mutta ei välttämättä elämäntarinan tai tiedon salaamiseksi, vaan tarinan sisällön muuttamiseksi vetovoimaisempaan muotoon. Myös tuolloin Mesopotamian kulttuurit olivat omaksuneet samankaltaisia kryptografisia menetelmiä kuin egyptiläiset, eroavaisuutena tietenkin kulttuureille tyypillinen nuolenpääkirjoitus. (D'Agapeyeff 1939; Cohen 1990.)

2.2 Salauskirjoitusmenetelmät: Korvaus- ja sekoitusmenetelmät

Ensimmäiset merkittävät salakirjoitusmenetelmät olivat korvaussalakirjoituksia. Tässä menetelmässä jokainen selväkielen kirjain korvataan toisella kirjaimella jonkin tietyn algoritmin mukaan. Korvaussalakirjoitustyyppejä on kahdenlaisia, sekä yksiaakkosisia että moniaakkosisia, mutta näihin perehdytään myöhemmin tässä tekstissä. (Easttom 2022, luku 1, ”Substitution Ciphers”.)

Sekoitussalakirjoitus sen sijaan tarjoaa toisen tavan salakirjoittaa viestejä. Tässä menetelmässä viestin merkkejä ja osia siirretään paikasta toiseen. Sekoitussalakirjoitus on historiallisesta näkökulmasta jäänyt hiukan taka-alalle verrattuna muihin salakirjoitusmenetelmiin, mutta ehkäpä tunnetuin niistä on antiikin Kreikassa käytetty Skytale, jota havainnoidaan kuvassa 1. Spartalaiset omaksuivat arviolta 500-luvulla eaa. salakirjoitusmenetelmän nimeltä Skytale, jota käytettiin salaiseen viestittämiseen sotajoukkojen välillä. Menetelmä koostui ohuesta papyrus-, pergamentti- tai nahkakaistaleesta, joka kiedottiin puisen sauvan ympärille. Salainen viesti kirjoitettiin sauvan pituutta pitkin, minkä jälkeen kaistale käärittiin pois. Jotta viesti voitiin lukea, kaistale oli kiedottava halkaisijaltaan ja muodoltaan samankaltaisen sauvan ympärille. Ilman oikeanlaista sauvaa viestin sisältö olisi ollut vaikea purkaa tuon ajan keinoin. (Easttom 2022, luku 1, ”Transposition Ciphers”; Cohen 1990.)

Kuva 1. Skytale (Wikimedia Commons, Skytale)

2.3 Sisarukset kryptografia ja steganografia

Kryptografia kehittyi samanaikaisesti erään toisen menetelmän kanssa, joka tunnetaan nimellä steganografia. Menetelmä yksinkertaisuudessaan tarkoittaa viestin kätkemistä, toisin kuin kryptografia, jonka tarkoitus ei ole piilottaa viestiä vaan sen merkitys. (Singh 1999, 22–23.)

Yksi varhaisimpia tunnettuja kuvauksia viestin kätkemisestä löytyy Herodotoksen *Historiateoksesta*. Teoksessa kerrotaan Kreikan ja Persian välisistä yhteenotoista, jotka sattuivat 500-luvulla eaa. Tekstissä Persiaan karkotettu Demeratos niminen kreikkalainen päättää varoittaa entisiä maanmiehiään persialaisten salakavalasta yllätyshyökkäyksestä. Saadakseen viestin perille maanmiehilleen paljastumatta, Demeratoksen oli kätkettävä viesti. Teos kuvaa Demeratoksen ottaneen kirjoitustaulun ja kaapineen siitä vahan pois. Tämän jälkeen hänen kerrotaan kaivertaneen viestinsä taulun puukansiin ja valaneen päälle sulaa vahaa, jottei tyhjä taulu herättäisi epäluuloa tienvartijoissa. (Singh 1999, 20–21.)

Myös italialaisen tiedemies Giovanni Portan tiedetään kuvanneen, kuinka viesti voidaan piilottaa kovaksi keitettyyn kananmunaan. Kuvauksessa ohjeistetaan sekoittamaan kolme senttilitraa alunaa kuuteen desilitraan etikkaa. Tästä syntyneellä musteella haluttu viesti kirjoitettiin kananmunan kuoreen. Kananmunan huokoisen kuoren ansiosta seos imeytyi kovettuneelle valkuaiselle, josta se voitiin lukea vain rikkomalla munan kuori. Hyvä esimerkki modernista steganografiasta voisi olla viestin piilottaminen tavallisen mediatiedoston, kuten kuvatiedoston

sisään, mikä tapahtuu koodaamalla viesti tiedoston bitteihin. (Singh 1999, 22–23; Dooley 2018, luku 1, kappale 1.2.)

3 YKSIAAKKOSINEN SALAKIRJOITUS

Yksiaakkosisessa korvaussalakirjoituksessa selväkielen tekstin jokainen kirjain korvataan aina salakirjoituksen vastaavalla kirjaimella tai symbolilla. Näin ollen esimerkiksi ennalta määritetyn algoritmin mukaan selväkielisen tekstin kirjain A voidaan korvata salakirjoituksessa kirjaimella K.

3.1 Polybiuksen neliö

Tunnettu kreikkalainen salakirjoitusmenetelmä tunnetaan nimellä Polybiuksen neliö. Menetelmässä aakkoston kaikki kirjaimet asetetaan 5x5 taulukkoon, jonka rivit ja sarakkeet ovat numeroitu. Yhtä kirjainta vastaa rivin ja sarakkeen muodostama lukupari. (Cohen 1990.)

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	w	x	y

Taulukko 1. Polybiuksen neliö

Taulukon 1 esimerkissä aloitetaan rivinumerolla, jonka perään lisätään sarakkeen numero. Nyt sanasta *”viesti”* voidaan muodostaa numerosarja 52, 24, 15, 44, 45, 24. On hyvä huomioida, että esimerkissä on noudatettu alkuperäistä 5x5 taulukkoa. Menetelmästä on lukusia muunnelmia, joissa kirjaimia voidaan sijoittaa taulukossa samaan soluun, tai korvata tyhjäksi jäävät solut niin numeroilla kuin muillakin merkeillä.

3.2 Atbash-salakirjoitus

Toisinaan Raamatun Vanhassa testamentissa voi törmätä tekstijaksoihin, jotka ovat kirjoitettu perinteisellä heprealaisella korvaussalakirjoituksella, Atbashilla. Tässä menetelmässä jokainen kirjain korvataan aakkoston käänteisellä kirjaimella. Suomenkielisessä tekstissä kirjain A

korvattaisiin kirjaimella Ö ja kirjain B korvattaisiin kirjaimella Ä ja niin edelleen. Havainnollistetaan edellä mainittua taulukossa 2. (Cohen 1990; Singh 1999, 50–51.)

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
Ö	Ä	Å	Z	Y	X	W	V	U	T
k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
S	R	Q	P	O	N	M	L	K	J
u	**v**	**w**	**x**	**y**	**z**	**å**	**ä**	**ö**	
I	H	G	F	E	D	C	B	A	

Taulukko 2. Atbash-salakirjoitus

Atbashin nimi muodostuu heprealaisen aakkoston ensimmäisestä kirjaimesta aleph, jonka jälkeen tulee viimeinen kirjain taw, sitten toinen kirjain beth, ja lopuksi toiseksi viimeinen kirjain shin. Atbashin tarkoitus ei todennäköisesti ole ollut tekstin merkityksen kätkeminen, vaan arvoituksellisuuden lisääminen. Esimerkkejä Atbashista voi löytää muun muassa *Jeremiaan kirjan* jakeista 25:26 ja 51:41, joissa sana ”Babylon” on korvattu sanalla ”Sesak”. Vaikka menetelmän oletettava tarkoitus olikin arvoituksellisuuden lisääminen, oli se merkityksellinen herättämään syvällistä mielenkiintoa kryptografiaan keskiajan Euroopassa, tuoden kryptografian takaisin länsimaisen sivistyksen pariin. (Singh 1999, 51.)

3.3 Caesarin salakirjoitus

Julius Caesarin on tiedetty käyttäneen useampaa salakirjoitusmenetelmää. Muun muassa Gallian sodan ajoilta löytyy merkintä, jossa viesti salattiin korvaamalla roomalaiset kirjaimet kreikkalasilla kirjaimilla. Kuitenkin Caesarin salakirjoituksesta puhuttaessa, tarkoitetaan korvaussalakirjoitusmenetelmää, joka on kuvattu yksityiskohtaisesti Suetoniuksen kirjoittamassa teoksessa *Rooman keisarien elämänkertoja*. Menetelmässä Caesar yksinkertaisesti vaihtoi viestin jokaisen kirjaimen toiseen kirjaimeen, joka on kolme kirjainta edempänä aakkosissa. (Singh 1999, 28–29.)

a	b	c	d	e	f	g	h	i	j
D	E	F	G	H	I	J	K	L	M
k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
N	O	P	Q	R	S	T	U	V	W
u	**v**	**w**	**x**	**y**	**z**	**å**	**ä**	**ö**	
X	Y	Z	Å	Ä	Ö	A	B	C	

Taulukko 3. Caesarin salakirjoituksen kirjainvastineet luvun kolme siirrolla.

Taulukkoa 3 hyödyntäen voidaan Caesarin tunnettu lausahdus ”Tulin, näin, voitin.” kääntää muotoon WXOLQ, QBLQ, YRLWLQ.

Salakirjoituksen algoritmia voidaan havainnollistaa myös matemaattisella kaavalla (kaava 1). Yleisesti ottaen muuttujalla C (Cipher) kuvataan salatun tekstin kirjaimen indeksiä aakkostossa, muuttujalla P (Plain text) selväkielisen tekstin kirjaimen indeksiä aakkostossa ja muuttujalla K avainta (Key), jolla tarkoitamme siirtolukua. Luku 29 kuvaa kirjainten lukumäärää suomen kielen aakkosissa. Merkinnällä $mod\ 29$ tarkoitetaan modulo 29-jakoa, jolla ilmaistaan jakojäännöstä jaettaessa luvulla 29.

$$C \equiv (P + K)\ mod\ 29 \qquad \textit{(Kaava 1.)}$$

Salauksen purkaminen kaavan 2 mukaan.

$$P \equiv (C - K)\ mod\ 29 \qquad \textit{(Kaava 2.)}$$

Kaavassa 3 havainnollistetaan Caesarin salakirjoitus luvun kolmen siirrolla.

$$C \equiv (P\ +\ 3)\ mod\ 29 \qquad \textit{(Kaava 3.)}$$

Havainnolistetaan kaavan 3 toiminnallisuus. Valitaan selväkielisen tekstin kirjaimeksi A, jonka indeksi aakkosissa on luku 1. Avain Caesarin salakirjoituksessa on luku 3. Asetetaan luvut, kuten kaavassa 4.

$$C \equiv (1 + 3)\ mod\ 29 \qquad \textit{(Kaava 4.)}$$

$$C \equiv 4\ mod\ 29 \qquad \textit{(Kaava 5.)}$$

Kaavan 5 lauseke antaa muuttujan C arvoksi luvun 4. Nyt huomaamme, että aakkosista löydämme indeksiluvulla 4 kirjaimen D. Saman tuloksen voimme havaita myös taulukosta 3, eli selväkielen kirjain A muuntuu kirjaimeksi D.

---

4 KRYPTOANALYYSIN KEHTO

Vuosisadan kestäneen vakauttamisen jälkeen 800-luvulla jaa., islamilainen sivilisaatio koki oman kulta-aikansa, jonka seurauksena taiteet ja tieteet kukoistivat yhtä lailla. Perinnöksi maailmalle tästä ajasta ovat jääneet muun muassa historian taidokkaimpia maalauksia, kaiverruksia ja kankaita. Sen sijaan islamilaisen tieteen jättämän perinnön voi havaita yhä niin arabiankielisissä sanoissa kuin modernin tieteen sanastossakin, kuten algebra, alkali ja zeniitti. Rikkaan, rauhallisen ja järjestäytyneen yhteiskunnan vakiinnuttaminen vaati tehokasta hallintoa, jonka työvoima tarvitsi turvallista viestintää. Tähän salakirjoitus oli oiva työkalu. Kryptografian voidaan osoittaa olleen laajassa ja jokapäiväisessä käytössä islamilaisessa yhteiskunnassa aina valtionsalaisuuksista verotusarkistoihin asti. (Singh 1999, 34–35.)

Arabioppineet eivät keskittyneet ainoastaan salaamaan tietoa, vaan osasivat myös ratkaista salausmenetelmiä. Tämän seurauksena syntyi uusi tieteenala, kryptoanalyysi, jonka päämääränä oli selvittää salattu viesti salakirjoituksen avainta tuntematta. Tämän tieteenalan harjoittajaa kutsutaan kryptoanalyytikoksi, jonka tehtävänä on löytää heikkouksia salausmenetelmistä, kun taas kryptografi pyrkii kehittämään uusia salakirjoitusmenetelmiä. Ajallaan nämä uuden tieteenalan, kryptoanalyysin, harjoittajat onnistuivatkin keksimään keinon murtaa yksiaakkosisen korvaussalakirjoituksen, menetelmän, joka oli pysynyt turvallisena satoja vuosia. (Singh 1999, 36.)

Arabioppineiden tutkiessa uskontekstien sanojen etymologiaa ja lauserakenteita, kiinnittivät he myös huomiota yksittäisten kirjainten esiintymistiheyteen tekstissä. Tämän kaltainen huomio johtikin kryptoanalyysin ensimmäiseen suureen läpimurtoon. Todistettavasti vanhin kuvaus salakirjoituksen murtamisesta on 900-luvulla jaa. Tässä teoksessa nimeltä *Käsikirjoitus salakielisten sanomien tulkitsemiseksi*, kryptoanalyysin järjestelmä on tiivistetty kahteen lyhyeen kappaleeseen. (Singh 1999, 38.)

Suomalaisaakkosilla demonstroituna, ensimmäiseksi on tutkittava pitkähköä jaksoa tavallista suomenkielistä tekstiä, ehkä useitakin, jotta voidaan määrittää aakkosten jokaisen kirjaimen esiintymistiheys. Suomen kielessä esimerkiksi kolme yleisintä kirjainta yleisimmästä alkaen ovat kirjaimet A, I ja T. Seuraavaksi tulisi tutkia salakirjoitusta ja määritellä jokaisen kirjaimen esiintymistiheys. Jos salakirjoituksen yleisin kirjain on esimerkiksi J, tuntuisi todennäköiseltä, että se on kirjaimen A vastine. Ja jos salakirjoituksen toiseksi yleisin kirjain olisi esimerkiksi kirjain P, se

olisi luultavasti kirjaimen I vastine, ja niin edelleen. Nimekseen menetelmä sai termin frekvenssianalyysi, joka todistaa, että on turhaa tarkistaa miljardeja mahdollisia avaimia. Sen sijaan salatun viestin voi paljastaa analysoimalla salakirjoituksen kirjainten esiintymistiheydet. Frekvenssianalyysin reseptiä ei kuitenkaan kannata soveltaa sokeasti, sillä esimerkiksi lyhyet tekstit yleisesti ottaen poikkeavat frekvenssiltään normaaleista frekvensseistä. Myös tekstit, joissa esimerkiksi on vältetty käyttämästä kielelle tyypillisiä kirjaimia, voi pilata salakirjoituksen murtoyrityksen. (Singh 1999, 40–42.)

Kamppailu kryptoanalyysia vastaan

Frekvenssianalyysin kehitys oli tehnyt yksiaakkosisen korvaussalakirjoituksen turvattomaksi ensin arabimaissa ja sitten Euroopassa. Tämä tarkoitti, että kryptografien oli löydettävä uusi ja turvallinen salakirjoitusmenetelmä, jota kryptoanalyytikot eivät kykenisi murtamaan. Kryptografit pyrkivätkin erinäisin keinoin parantamaan yksiaakkosista korvaussalakirjoitusta muun muassa lisäämällä salakirjoitukseen tyhjiä symboleja tai korvaamalla aakkoset esimerkiksi luvuilla lukujen 1-99 väliltä, jolloin tekstiin jäi noin 70 merkityksetöntä lukua. Joten toisin kuin viestin kaapannut ulkopuolinen taho, viestin oikea vastaanottaja saattoi jättää nämä symbolit ja luvut huomiotta. Viesteihin saatettiin myös kirjoittaa kirjoitusvirheen omaavia sanoja, mikä vaikeutti frekvenssianalyysin soveltamista. (Singh 1999, 75.)

Koodit ja koodikirjat

Toinen tapa parantaa salaisen viestinnän turvallisuutta oli koodisanojen käyttö, missä sekä kokonaisia sanoja että lauseita korvattiin kirjaimin, symbolein ja numeroin. Ensituntumalta tämä vaikutti olevan hyvä ratkaisu, sillä frekvenssianalyysi ei pure sanoihin, mutta koodisanojen käytöllä oli omat vakavat heikkoutensa. Käytännössä koodikirjat koostuivat tuhansista sanoista, jolloin koodisanaston laatiminen oli varsin työlästä ja kuljettaminen vaivalloista ympäri viestintäverkostoa. Lisäksi koodikirjan joutuminen vihollisen käsiin johti usein erittäin tuhoisiin seurauksiin. (Singh 1999, 56–57.)

Nomenklatuurit

1500-luvulta lähtien kryptografit suurelta osin tiedostivat koodien vakavat heikkoudet ja turvautuivatkin pääsääntöisesti käyttämään perinteisiä yksiaakkosisia salakirjoitusmenetelmiä ja nomenklatuurisalakirjoitusta. Nomenklatuurisalakirjoitus perustui perinteisen salakirjoituksen tavoin koodiaakkoston käyttöön, millä salattiin suurin osa viestistä. Tämän lisäksi nomenklatuurisalakirjoituksessa käytettiin koodisanoja korvaamaan joitakin tiettyjä sanoja tai lauseita. Koodisanojen käytöstä huolimatta nomenklatuurisalakirjoitus ei tuonut sen suurempaa turvaa verrattuna perinteisiin salakirjoituksiin, sillä usein frekvenssianalyysilla kyettiin tulkitsemaan suurin osa viestistä ja jäljelle jäävät koodisanat voitiin arvata asiayhteydestä. (Singh 1999, 56–57.)

Mustat kammiot

Yksiaakkosisen salakirjoituksen tie tuli lopulliseen päätökseensä 1700-luvulle siirryttäessä. Tuolloin kryptoanalyysi teollistui ja monet Euroopan mahtivaltiot muodostivat omia erikoisyksiköitään, jotka koostuivat usean kryptoanalyytikon muodostamista ryhmistä. Nämä niin kutsutut mustat kammiot kykenivät ratkaisemaan monimutkaisemmatkin yksiaakkosiset salakirjoitukset, ehkä kuuluisimpana näistä *Geheime Kabinets-Kanzlei* Wienissä. (Singh 1999, 93.)

5 MONIAAKKOSINEN SALAKIRJOITUS

Seuraava suuri edistysaskel kryptografialle oli moniaakkosisen korvaussalakirjoituksen synty, jolla kyettiin vaikeuttamaan frekvenssianalyysia. Moniaakkosisessa korvaussalakirjoituksessa käytetään useampaa kirjainkorvausta, mikä johtaa siihen, että selväkielisen tekstin kirjainvastine salatussa tekstissä vaihtelee.

Perustan moniaakkosisille salakirjoituksille loi 1400-luvulla firenzeläinen Leon Battista Alberti, joka kuvaili kirjoitelmissaan useamman koodiaakkoston käyttämistä salakirjoituksessa. Hän myös kehitti salakirjoituslevyn, jota emme kuitenkaan tässä tekstissä sen enempää käsittele. Saavutuksistaan huolimatta Alberti ei kyennyt elinaikanaan jalostamaan ajatuksistaan toimivaa salakirjoitusmenetelmää. Albertin kehitystyötä jatkoi kuitenkin hajanainen ryhmä ihmisiä, kuten *Tabula recta* nimisen taulukon kehittänyt Johannes Trithemius, sekä italialainen tiedemies Giovanni Porta. Edellä mainittujen henkilöiden saavutusten viitoittamana ranskalainen diplomaatti Blaise de Vigenère kehitti 1500-luvun lopulla ratkaisemattomaksi salakirjoitukseksi nimetyn salakirjoitusmenetelmän. (Singh 1999, 75–77, 84.)

Vigenèren salakirjoitus

Tässä salakirjoitusmenetelmässä turvaudutaan käyttämään yhtä montaa aakkostoa kuin yksittäisiä kirjaimia löytyy aakkosista. Esimerkiksi suomen kielen aakkosista puhuttaessa tämä tarkoittaisi 29 koodiaakkostoa, joista jokainen alkaa aina yhtä kirjainta edempää kuin edellinen aakkosto. Edellä mainittua havainnollistetaan taulukossa 4. (Singh 1999, 75–77, 84.)

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
27	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å
28	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä
29	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö

Taulukko 4. Vigenèren taulukko

Vigenèren salakirjoitusta tehtäessä laaditaan taulukko, kuten taulukko 4. Taulukon ylimmäisessä rivissä esitetään selväkielen aakkosto ja tämän alla 29 koodiaakkostoa. Ensimmäinen koodiaakkosto on kuin Caesarin salakirjoituksen yhden kirjaimen siirto. Sitä seuraavalla rivillä on Caesarin kahden kirjaimen siirto ja niin edelleen. Täten jokainen ylimmän rivin selväkielen kirjain voidaan koodata millä tahansa sen alapuolella olevalla koodiaakkostolla. Esimerkiksi, jos käyttäisimme koodiaakkoston numeroa kaksi, korvattaisiin selväkielen kirjain A koodiaakkoston kirjaimella C. Salakirjoituksen vahvistamiseksi Vigenèren salakirjoituksessa käytetään taulukon eri koodiaakkostoja selväkielisen viestin jokaisen kirjaimen kohdalla. Jotta salatun viestin

vastaanottaja tietää, mitä koodiaakkostoa yksittäisen kirjaimen kohdalla käytetään kulloinkin, tarvitaan jonkinlainen järjestelmä. Tämä voidaan toteuttaa käyttämällä avainsanaa, mitä demonstroidaan taulukossa 5. (Singh 1999, 79–80.)

S	A	L	A	I	S	U	U	S	S	A	L	A	I	S	U	U	S	S	A	L	A	I	S	U	U	S	S	A	L	A	I
t	**ä**	**m**	**ä**	**o**	**n**	**r**	**a**	**t**	**k**	**a**	**i**	**s**	**e**	**m**	**a**	**t**	**o**	**n**	**s**	**a**	**l**	**a**	**k**	**i**	**r**	**j**	**o**	**i**	**t**	**u**	**s**
I	Ä	X	Ä	W	C	I	U	I	Ö	A	T	S	M	B	U	K	D	C	S	L	L	I	Ö	Ö	I	Ä	D	I	B	U	Å

Taulukko 5. Vigenèren salakirjoitus. Keskirivillä selväkielinen viesti ja yllä avainsana ”SALAISUUS”, jota toistetaan koko viestin pituudelta. Alariville muodostuu teksti salatussa muodossa.

Havainnollistetaan menetelmää ottaen taulukon 5 ensimmäisestä sarakkeesta avainsanan kirjain S ja salatun viestin ensimmäinen kirjain I. Sijoitamme ne taulukkoon 4. Ensiksi etsimme rivin, joka alkaa kirjaimella S, joka näyttäisi olevan rivi luvulla 18. Tämän jälkeen haemme tuolta kyseiseltä riviltä kirjaimen I. Kun katsomme kyseisen sarakkeen ylintä riviä, eli selväkielen aakkostoa, huomaamme sen olevan kirjain T. Tämä täsmää taulukon 5 selväkielisen viestin kirjaimeen.

Vigenèren salakirjoituksen algoritmia havainnollistetaan kaavassa 6.

$$C_i \equiv (P_i + K_i)\ mod\ 29 \qquad \textit{(Kaava 6.)}$$

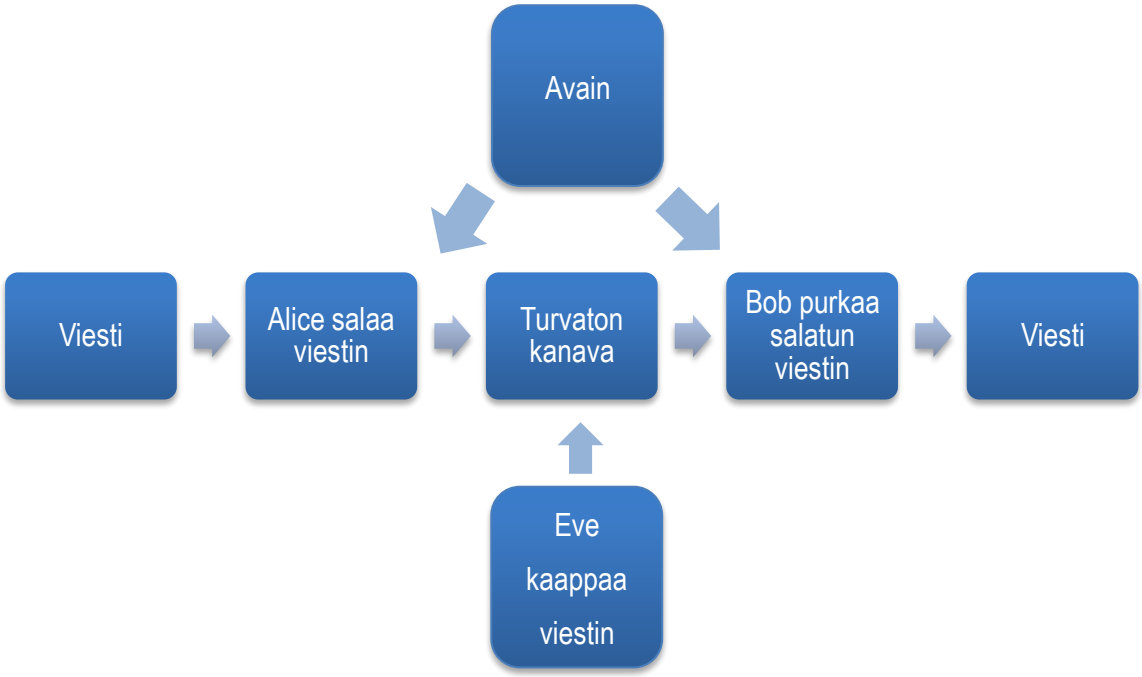
Kaavassa 6 muuttujalla C (Cipher) kuvataan salatun tekstin kirjaimen indeksiä aakkostossa, muuttujalla P (Plain text) selväkielisen tekstin kirjaimen indeksiä aakkostossa, sekä muuttujalla K avainta (Key), jolla tarkoitamme siirtolukua. Luku 29 kuvaa kirjainten lukumäärää suomen kielen aakkosissa ja merkinnällä $mod\ 29$ tarkoitetaan modulo 29-jakoa. Voimme siis huomata, että kaava mukailee hyvin pitkälti Caesarin salakirjoituksen algoritmia (kaava 1), johon tutustuimme aiemmin, mutta omaa yhden eroavaisuuden; muuttuja K muuttuu. Muuttuja i ilmaisee nykyisen avaimen, joka muodostuu nykyisestä selväkielisen tekstin kirjaimen indeksistä ja nykyisestä salatun tekstin kirjaimen indeksistä.

Vigenèren salakirjoituksessa useasti esiintyvä kirjain voi täten merkitä joka esiintymiskerralla eri selväkielen kirjainta, joka tekee kryptoanalyytikon työstä erittäin epävarmaa. Viestin lähettäjä ja vastaanottaja voivat keskenään sopia avainsanan luonteesta, mikä voi tarkoittaa jonkin tietyn

sanan tai sanyhdistelmän käyttöä. Tällä on mahdollista luoda salakirjoitukselle valtava määrä avaimia, jolloin kryptoanalyytikko ei kykene murtamaan salakirjoitusta tarkistamalla kaikkia avaimia. Vigenèren salakirjoituksen luotettavuudesta ja turvallisuudesta huolimatta, menetelmä mahdollisesti koettiin liian vaivalloiseksi käyttää, sillä sen käyttö yleistyi vasta lähes kaksi vuosisataa myöhemmin. (Singh 1999, 83–84.)

6 SYMMETRINEN SALAUS

Symmetrisellä salauksella tarkoitetaan salausta, jossa tiettyä avainta käytetään sekä viestin salaamiseen että salauksen purkuun. Kaikki aiemmissa kappaleissa mainitut klassiset korvaussalakirjoitukset ovat symmetrisiä salausmenetelmiä. Caesarin salauksessa luku kolme toimii avaimena, joka määrittää kuinka monta siirtoa aakkostossa suoritaan. Esimerkiksi Caesarin salakirjoituksessa kirjain A salauksen yhteydessä muuttuu kirjaimeksi D (taulukko 3). Tunnetuin tapa havainnollistaa symmetrisen salauksen toimintaa on kuvaus Alicesta, Bobista ja Evestä. (kuvio 2).

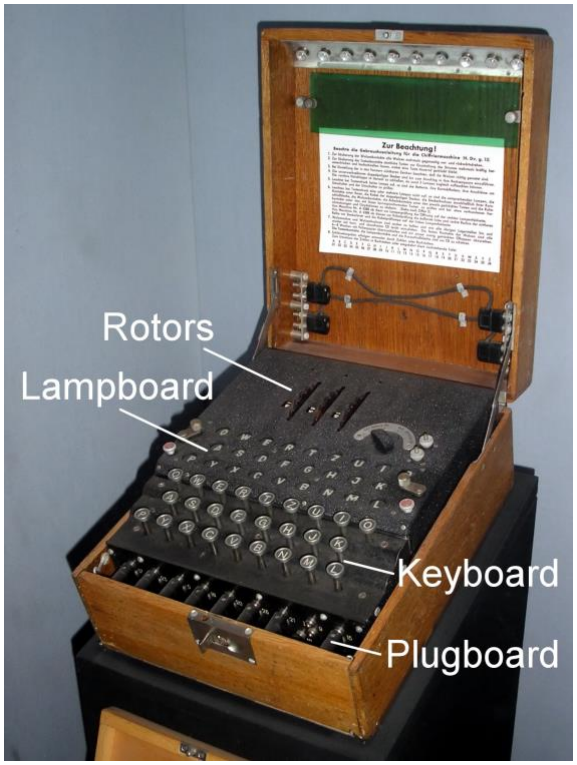


Kuvio 2. Alice, Bob ja Eve (symmetrinen salaus). (Dooley 2018, luku 11, kappale 11.1.). Kuvion ulkoasua ja tekstejä on muokattu tarkemman selkeyden saavuttamiseksi.

Kuviossa 2 havainnollistetaan, kuinka Alice haluaa lähettää viestin Bobille. Ensin Alice salaa viestin käyttämällä avainta, jonka myös Bob tietää. Salattu viesti lähetetään turvattoman viestintäkanavan, esimerkiksi internetin, kautta Bobille. Eve kaappaa viestin sen kulkiessa turvatonta viestintäkanavaa pitkin, mutta ei kykene purkamaan salausta ilman avainta. Kun Bob saa vastaanotettua salatun viestin, hän purkaa sen käyttäen samaa avainta ja käänteistä algoritmia, jota Alice käytti.

6.1 Enigma

Symmetrisistä salausmenetelmistä puhuttaessa on mainittava salakirjoituslaite Enigma (kuva 2), joka toimi keskeisenä virstanpylväänä symmetristen salaustekniikoiden kehityksessä. Se oli elektromekaaninen laite, joka käytti roottoreita luomaan moniaakkosisia avainjärjestelmiä suorittaakseen sekä viestin salauksen että salauksen purkamisen. (Dooley 2018, luku 8, kappale 8.3).



Kuva 2. Enigma (Wikimedia Commons, Enigma)

Enigman toiminta

Enigman toiminta perustui pääasiassa roottoreihin, jotka mahdollistivat moniaakkosisen salauksen, sekä salauksen purkamisen. Salauksen käänteellisyys oli myös Enigman heikkous. Alun perin koneessa käytettiin kolmea roottoria, jotka olivat kiinteillä paikoilla, jolloin saatiin aikaan 17 576 sekoitettua aakkostoa. Myöhemmin kolme roottoria voitiin asettaa mihin tahansa järjestykseen, joka mahdollisti kuusi kolmen roottorin sarjaa. Tämä merkitsi, että käytettävissä oli 105456 sekoitettua aakkostoa. Tämän jälkeen saksalaiset lisäsivät koneisiin kaksi ylimääräistä roottoria, jolloin käyttäjä valitsi viidestä roottorista kolme, kasvattaen sekoitettujen aakkostojen määrän yli

miljoonaan. Sodan loppupuolella Saksan laivasto käytti Enigma-mallia, joka käytti neljää roottoria, mikä kasvatti aakkosvaihtoehtojen määrää merkittävästi. (Dooley 2018, luku 8, kappale 8.3.)

Roottoreiden lisäksi Enigmassa oli kiinteä puoliroottori, "heijastin" (*Umkehrwalze*), jossa kolmetoista sähköistä kontaktia toisella puolella roottoria oli yhdistetty vastaavien kolmentoista kontaktin kanssa. Tämä heijasti sähköisen signaalin ja sai sen kulkemaan takaisin roottoreiden läpi eri reittiä. (Dooley 2018, luku 8, kappale 8.3.)

Kaupallisesta Enigman versiosta poiketen, sotilasversio sisälsi liitinpöydän (*Steckerbrett*), joka mahdollisti 6–10 kirjainparin yhdistämisen toisiinsa, tuoden noin 150 biljoonaa lisäyhdistelmää jaksoon. Näppäimen painalluksella sähköinen signaali kulki siis roottoreiden, "heijastimen" ja liitinpöydän kautta, lopulta sytyttäen valon tietyn kirjaimen kohdalla. (Dooley 2018, luku 8, kappale 8.3.)

Koska Enigma esitti kirjaimet valotaulun kautta, laitteen tehokas käyttö vaati kahden tai kolmen henkilön yhteistyötä. Operaattoreiden tuli lukea selväkielinen viesti äänen, toisen kirjoittaessa ja ääneen ilmoittaessa valotauluun ilmestynyt salatun tekstin kirjain. Kolmas operaattori kirjoitti ylös salatun viestin, joka sitten lähetettiin eteenpäin morsettamalla. (Dooley 2018, luku 8, kappale 8.3.)

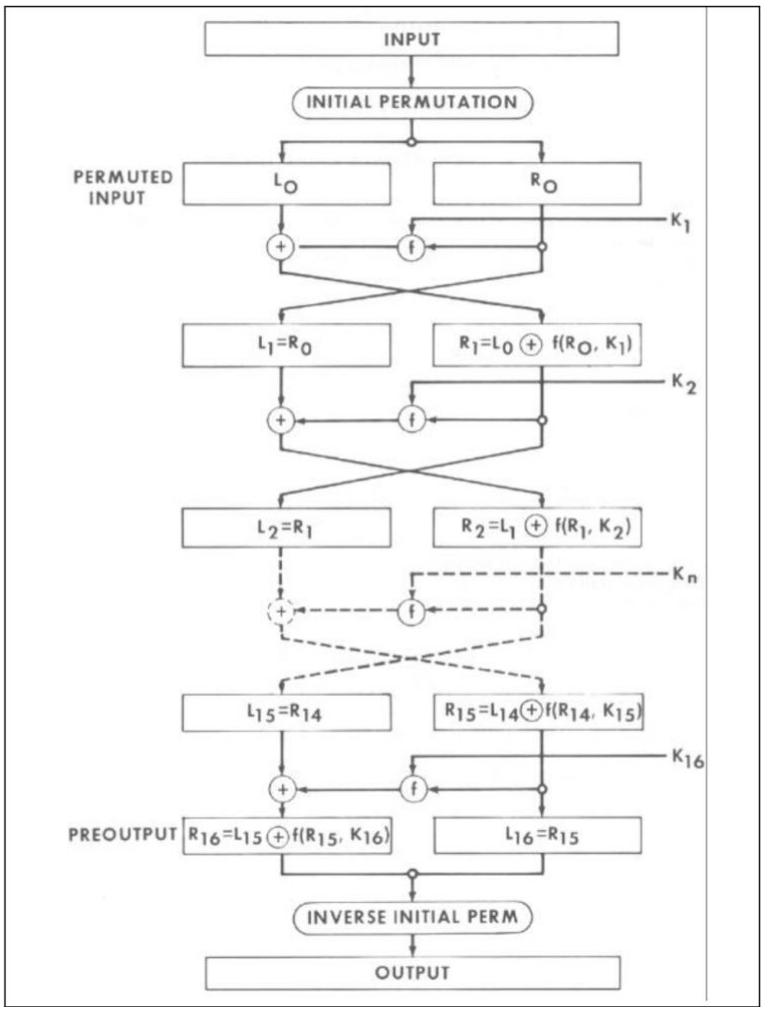
Enigman käytössä vaadittiin myös kahden erillisen avaimen käyttöä, joita kutsuttiin päiväavaimeksi ja viestiavaimeksi. Päiväavain jakautui viiteen osaan, joiden mukaan määriteltiin muun muassa roottoreiden asennot ja kääntöpisteet, liitinpöydän asetukset, sekä verkon tunniste. Edellä mainittu avain vaihtui kerran kuukaudessa. Viestiavain sen sijaan määritteli roottoreiden asetuksen kunkin yksittäisen viestin kohdalla. Tässä proseduurissa operaattori asetti päiväavaimen koneeseen ja valitsi kolme satunnaista kirjainta, jotka hän salakirjoitti Enigmalla. Nämä kolme kirjainta muodostavat viestiavaimen ja toimivat ensimmäisinä viestissä lähetettyinä kirjaimina. Viestiavain vaihtui jokaisessa viestissä, lisäten salauksen monimutkaisuutta. (Dooley 2018, luku 8, kappale 8.3.)

6.2 Data Encryption Standard (DES)

Alkujaan Horst Feistelin kehittelemä salausalgoritmi, jonka kehitystyön hän aloitti liityttyään IBM:n T. J. Watsonin tutkimuskeskukseen 1970-luvun alussa. Työn tuloksena syntyi järjestelmä Lucifer, joka erityisesti kehitettiin vastaamaan kasvaneeseen liiketoiminnan digitalisoitumiseen ja

finanssitransaktioiden kasvuun verkossa. Vuonna 1973 Yhdysvaltain kansallinen standardointivirasto National Bureau of Standards (NBS), haki salausalgoritmeja, jotka voisivat toimia liittovaltion standardina sekä soveltua valtion salaisuuksien salaamiseen. IBM tarjosi ratkaisuksi kehiteltyä Luciferia, joka osoittautui kilvassa ainoaksi hyväksyttäväksi ratkaisuksi. Salausalgoritmin muokattu versio otettiin käyttöön vuonna 1977 ja sai nimekseen nykyisen nimensä, Data Encryption Standard, tai lyhyemmin kutsuttuna DES. (Dooley 2018, luku 10, kappale 10.2.)

DES on symmetrinen lohkosalausalgoritmi ja se käyttää yhtä avainta sekä salaukseen että salauksen purkuun. Algoritmi toimii 64-bittisissä lohkoissa käyttäen 56-bittistä avainta. Algoritmi käsittelee jokaisen lohkon ytimessään, mitä kutsutaan kierrokseksi. Tämä toistuu 16 kertaa, kunnes tuloksena syntyy salattu teksti (kuva 3). Jokainen edellä mainituista kierroksista jakaa 64-bittisen lohkon kahteen 32-bittiseen lohkoon. Jokaisen jaon jälkeen toteutetaan Shannon-tyylinen korvaus-permutaatioverkko käyttäen osaa avaimesta, jota voidaan kutsua aliavaimeksi. Tämä tuottaa välivaiheen salatun tekstin, joka sitten palaa takaisin ja aloittaa uuden kierroksen. (Dooley 2018, luku 10, kappale 10.2.1.)



Kuva 3. DES:n kuusitoista kierrosta (FIPS 46-3, Data Encryption Standard (DES).)

Kuvasta 3 voidaan havainnoida, kuinka DES-algoritmiin tuleva 64-bittinen syöte menee alkuperäisen permutaation (IP) läpi, joka järjestää bitit uudelleen määrätyn permutaation avulla. Tämän jälkeen 64-bittinen lohko jaetaan kahteen 32-bittiseen puoliskoon, olkoot nämä nimillä OP (oikea puolisko) ja VP (vasen puolisko). Puoliskot matkaavat läpi kierroksen seuraavasti. Kierroksessa OP pysyy muuttumattomana, kun taas VP:lle tehdään muutoksia kierroksen aikana. Muuttumattomana pysynyt OP muuntuu seuraavalla kierroksella VP:ksi. Tämän jälkeen OP:n 32-bittiä asetetaan sekoitusfunktioon $f\,(Right, SKey)$, jossa Right on OP ja SKey on avainajastimen generoima aliavain. Sitten funktion tulos yhdistetään VP:n kanssa XOR-operaatiolla, mikä muodostaa OP:n syötteen seuraavalle kierrokselle, kun taas alkuperäinen OP muodostaa seuraavan kierroksen VP:n syötteen. 16 kierroksen jälkeen 64-bittinen tulos menee permutaation läpi, joka on alkuperäisen permutaation (IP) käänteinen versio. Nyt tuloksena saamme lopullisen salatun tekstin. (Dooley 2018, luku 10, kappale 10.2.1.)

DES oli aikanaan erittäin tehokas salausalgoritmi, mutta sisälsi kaksi merkittävää puutetta. Ensimmäisenä mainittakoon 56-bittisen avaimen lyhyys. Teoriassa tämä mahdollisti 2^{56} erilaista avainta, mikä aikanaan saatoi riittää tehokkaaseen salaukseen, mutta tietokoneiden laskentatehon kasvaessa, tietokoneet pystyivät murtamaan DES:n avaimen suhteellisen nopeasti. Alun perin DES:n edeltäjämalli Lucifer sisälsi 64-bittisen ja 128-bittisen avaimen, joka olisi tuonut huomattavaa suojaa, mutta väittämän mukaan National Security Agencyn (NSA) toiveesta avainta tuli lyhentää, koska vain heidän tietokoneillaan kyettiin tarvittaessa murtamaan DES:n avain. Väittämään tulee kuitenkin suhtautua varauksella, sillä sen on todettu olevan vain spekulaatiota, eikä tietoa ole vahvistettu. (Dooley 2018, luku 10, kappale 10.2.4.)

Toinen keskustelua herättänyt vika DES:ssä oli sen korvauslaatikoiden (S-boxes) suunnitellussa. Tälläkin kertaa epäilyt osoittivat kohti NSA:ta. Spekulaation mukaan NSA olisi vaatinut alkuperäisen Luciferin algoritmiin muutoksia, joita NSA olisi voinut hyödyntää takaportteina purkaakseen salauksia. Myös tällä kertaa todettakoon, että tämä väittämä ei ole saanut virallista vahvistusta. Ristiriitaisista vioistaan huolimatta DES oli aikanaan käytetyin tietokoneen salausalgoritmi, kunnes myöhemmin vuonna 2001 tuli vahvemman salausalgoritmin, Advanced Encryption Standardin (AES), syrjäyttämäksi. (Dooley 2018, luku 10, kappale 10.2.4.)

6.3 Advanced Encryption Standard (AES)

Vuonna 2000 belgialaisten kryptografien Joan Daemen ja Vincent Rijmen suunnittelema Rijndael nimeä kantava algoritmi valittiin seuraavaksi standardiksi ja julkaistiin nimellä Advanced Encryption Standard (AES) vuonna 2001. Tämä korvasi edellisen turvattomaksi luokitellun DES-algoritmin. (Dooley 2018, luku 10, kappale 10.3.)

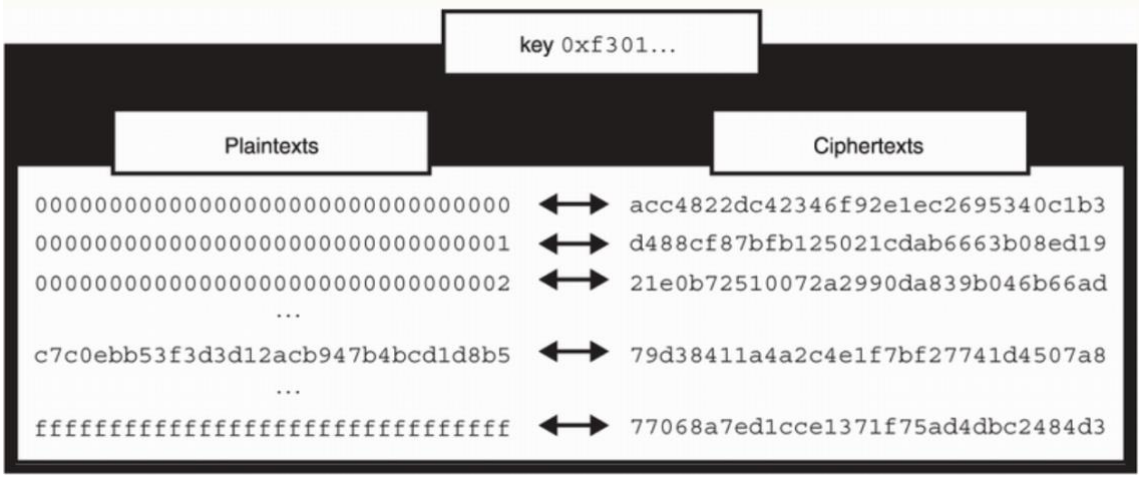
Käytännön esimerkkinä mainittakoon, että AES-salausalgoritmia käytetään laajalti suojaamaan tietoa erilaisissa sovelluksissa. Sitä käytetään jokapäiväisen nettiselailun yhteydessä, kuten verkkopankeissa, sähköpostipalveluissa, pilvipalveluissa ja salasanahallintaohjelmissa. (Wong 2021, luku 1, kappale 1.3.)

AES on myös erittäin yleinen menetelmä suojata tietoa ja tiedostoja ulkoisilla kiintolevyillä tai vaikkapa kannetavilla tietokoneilla.

Edeltäjänsä tavoin myös AES on symmetrinen lohkosalausalgoritmi käyttäen 128-bittistä lohkoa ja antaa käyttäjälle vapauden valita kolmesta avainkoosta, jotka ovat 128-bittiä (16-tavua), 192-bittiä (24-tavua) ja 265-bittiä (32-tavua). Avaimen pituus siis määrittää turvallisuuden tason. Tästä huolimatta suurin osa käyttämistämme sovelluksista tyytyy käyttämään 128-bittistä avainta, sillä se takaa riittävän turvallisuuden. Teoreettisesti tämä tarkoittaa, että AES-128:n murtaminen vaatisi noin 2^{128} murtoyritystä. Käytännössä tällaista lukua ei voida koskaan saavuttaa ja tämän kokoluokan hyökkäyksen toteutus vaatisi valtavan määrän resursseja. Toistaiseksi voidaan todeta AES-128:n olevan vielä turvallinen menetelmä, ellei ajansaatossa algoritmista löydetä muita kriittisiä heikkouksia (Dooley 2018, luku 10, kappale 10.3; Wong 2021, luku 4, kappale 4.2.1.)

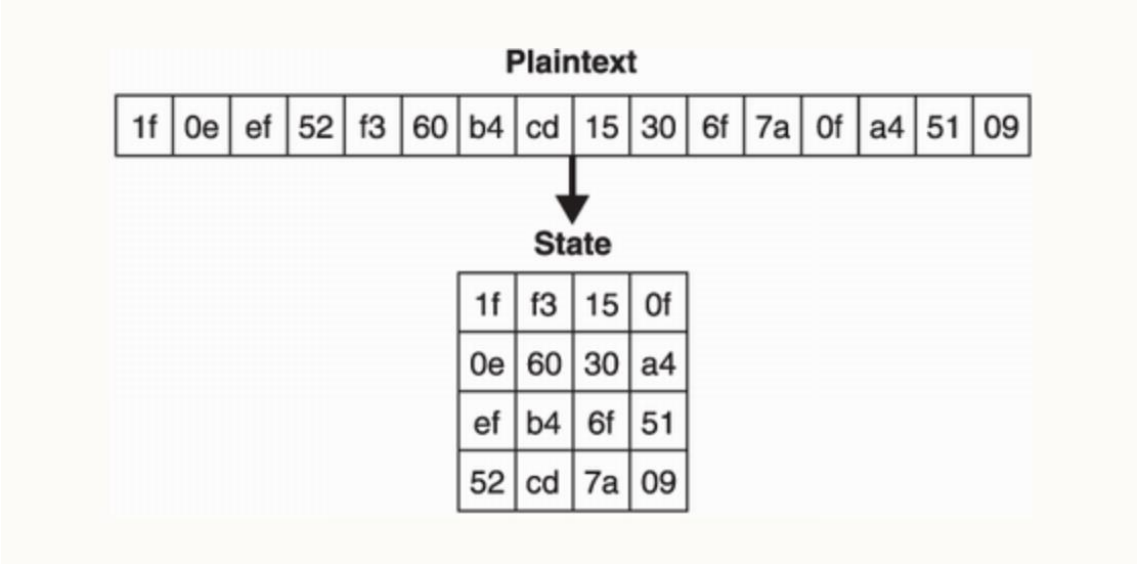
AES salakirjoittaa selväkielen tekstin 128-bittisinä lohkoina, sekä vastaavasti purkaa salauksen samalla kaavalla, mutta käänteisesti. Eli samaa avainta ja käänteistä algoritmia käyttäen, salakirjoituksen lohko muuntautuu selväkielen tekstiksi. (Wong 2021, luku 4, kappale 4.2.2.)

Kuten kuvassa 4 havainnollistetaan, lohkosalaus avaimen kanssa, voidaan ajatella permutaationa. Se kartoittaa ja vertaa kaikki mahdolliset selväkielen tekstit kaikkiin mahdollisiin salakirjoituksiin. Avaimen vaihtaminen muuttaa kartoituksen. Permutaatio on myös käänteinen, eli salakirjoitukselle löytyy aina kartta takaisin siihen vastaavaan selväkielen tekstiin. Tietenkin 128-bittisen lohkosalauksen kohdalla tämä tarkoittaisi 2^{128} kartoitusta, mikä on mahdottomuus vaadittavan tilan suhteen. Tähän kuitenkin AES:n kaltainen rakenne tuo ratkaisun. Se toimii kuin permutaatio ja on avaimen satunnaistama, toisin sanoen pseudosatunnainen permutaatio. (Wong 2021, luku 4, kappale 4.2.2.)



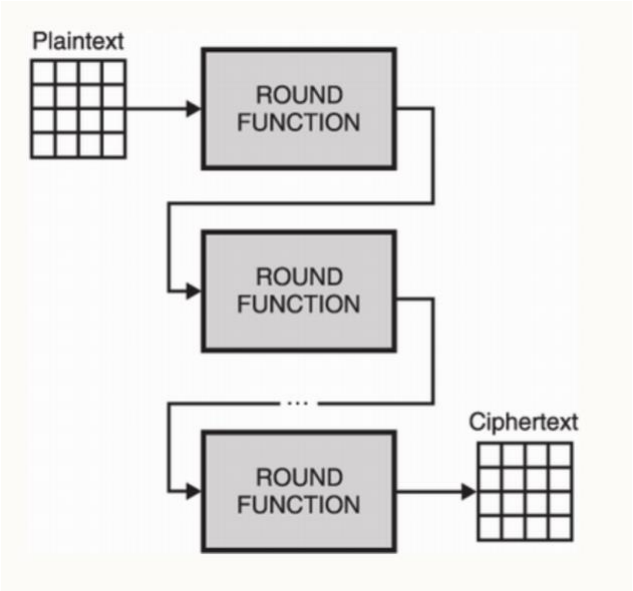
Kuva 4. Lohkosalaus avaimen kanssa voidaan ajatella permutaationa. (Wong 2021, luku 4, kappale 4.2.2.)

Salausprosessin yhteydessä AES näkee selväkielisen tekstin tilan (State) tavujen muodostamana 4x4 matriisina, kuten kuvassa 5 havainnoidaan. Kun 16-tavuinen selväkielinen teksti syötetään AES-algoritmiin, se muunnetaan 4x4 matriisiksi. Tämän jälkeen syntyvä tila salataan ja muunnetaan 16-tavuiseksi salakirjoitukseksi. Edellä mainitun tavoin AES pääpiirteisesti määritellään ja loppujen lopuksi AES toimii lähes samanlailla, kuin mikä tahansa muu samankaltainen lohkosalaus. (Wong 2021, luku 4, kappale 4.2.3.)



Kuva 5. AES matriisi (Wong 2021, luku 4, kappale 4.2.3.)

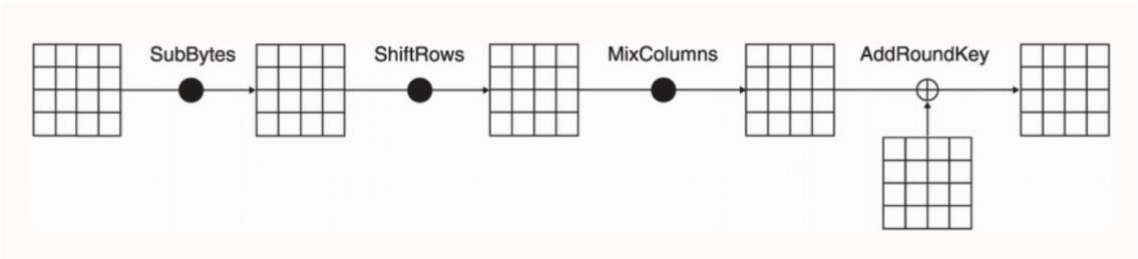
AES käyttää toiminnassaan kierrosfunktiota (Round function), joka salauksen yhteydessä iteroidaan useamman kerran, alkaen alkuperäisen syötteen kohdalla. Funktio käyttää useampaa argumenttia, kuten salausavainta (kuva 6). (Wong 2021, luku 4, kappale 4.2.3.)



Kuva 6. Yksinkertaistettu kuva salauksen kierrosfunktioista. (Wong 2021, luku 4, kappale 4.2.3.)

Jokainen kierrosfunktiokutsu muuntaa tavujen muodostamaa 4x4 matriisia edelleen ja lopulta muodostaa lopullisen salakirjoituksen. Jokaisessa kierroksessa käytetään eri kierrosavainta, joka johdetaan itse salauksen salausavaimesta. Edellä mainittua kutsutaan avaimen aikatauluttamiseksi, mikä on tyypillistä AES:n ja DES:n kaltaisille algoritmeille. Tämä mahdollistaa pienten muutosten syntymisen symmetrisen salausavaimen bitteihin, mikä antaa tuloksena täysin erilaisen salatun tekstin. Kyseinen toiminto perustuu diffuusion periaatteeseen, joka edistää salauksen turvallisuutta. (Wong 2021, luku 4, kappale 4.2.3.)

Kierrosfunktio (Round function) koostuu neljästä vaiheesta, joita kutsutaan alifunktioiksi: SubBytes, ShiftRows, MixColumns ja AddRoundKey (kuva 7). Ensimmäiset kolme alifunktiota ovat käänteisiä, ja niiden tuloksesta voidaan helposti selvittää alkuperäinen syöte. Sen sijaan viimeinen alifunktio, AddRoundKey, ei ole käänteinen. Se suorittaa XOR-operaation kierrosavaimen ja aiemminkin mainitun 4x4 matriisin (tila) välillä. Täten AddRoundKey-funktio tarvitsee kierrosavaimen, jotta tuloksesta voidaan palata alkuperäiseen syötteeseen. Käänteisyys on tärkeä, jotta salauksen purkaminen on mahdollista (Wong 2021, luku 4, kappale 4.2.3.)



Kuva 7. Kierrosfunktion vaiheet, eli alifunktiot. Jokainen funktio on käänteinen, mutta viimeinen funktiosta on käänteinen vain XOR-operaation avulla. Näkyy kuvassa ⊕ merkillä. (Wong 2021, luku 4, kappale 4.2.3.)

AES:n kierrosfunktion iteraatioiden määrällä on suuri merkitys salauksen tehokkuuteen. Monien iteraatioiden avulla salaus muuttaa selväkielisen tekstin joksikin, joka ei muistuta alkuperäistä selkokielistä tekstiä lainkaan. Pieninkin muutos selkokielisessä tekstissä tuottaa täysin erilaisen salatun tekstin. Tätä periaatetta kutsutaan lumivyöryefektiksi. (Wong 2021, luku 4, kappale 4.2.3.)

Symmetriset menetelmät

Symmetrisiä salauksia, kuten AES, voidaan vahvistaa erilaisin menetelmin. Perustavin salausmuoto turvallisuuden lisäämiseksi tunnetaan tilana, Electronic Codebook (ECB). Tässä tilassa viesti jaetaan lohkoihin, ja jokainen lohko salataan erikseen. Ongelma tässä menetelmässä ilmenee kuitenkin, kun käytetään samaa selväkielistä tekstiä: salakirjoitus pysyy identtisenä. Käytännössä tämä tarkoittaa sitä, että samanlaiset lohkot tuottavat aina saman salakirjoituksen, mikä mahdollistaa hyökkääjälle mahdollisuuden analysoida salausta ja päätellä salausavain. (Easttom 2015, luku 6, ”Symmetric Methods”, ”ECB”.)

Toinen tunnettu menetelmä, jota suositellaan käytettäväksi ECB:n sijaan on tila, Cipher-Block Chaining (CBC). Tässä menetelmässä jokainen selväkielen lohko käy läpi XOR-operaation edellisen salakirjoituslohkon kanssa ennen lopullista salausta. Täten lopullinen salakirjoitus sisältää merkittävästi enemmän satunnaisuutta. (Easttom 2015, luku 6, ”CBC”.)

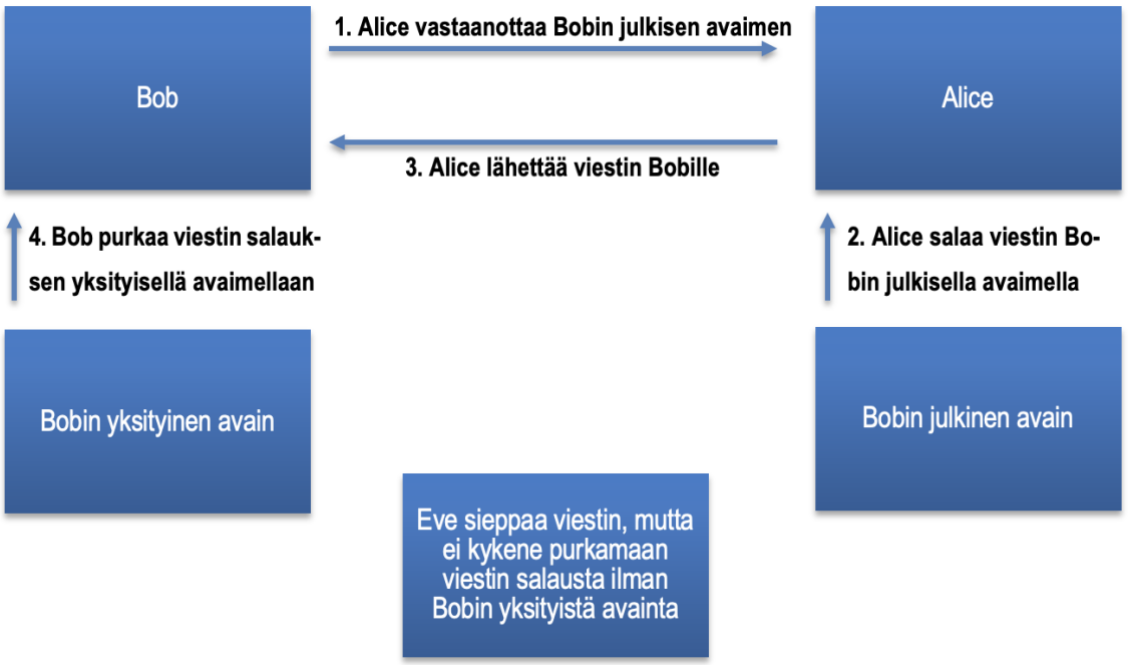
Ainoa ongelma CBC-tilassa liittyy ensimmäiseen lohkoon. Ensimmäiselle selväkielen tekstin lohkolle ei ole edeltävää salakirjoituksen lohkoa, jonka kanssa XOR-operaatio voitaisiin suorittaa. Yleistä on lisätä ensimmäiseen lohkoon alustusvektori (IV), jotta selväkielen lohkolla on jotain, jonka kanssa suorittaa XOR-operaatio. Alustusvektori (IV) on käytännössä pseudosatunnainen numero, samankaltainen kuin salausavain. Yleensä IV:tä käytetään vain kerran, joten sitä kutsutaan kertakäyttönumeroksi (nonce). (Easttom 2015, luku 6, ”CBC”.)

7 ASYMMETRINEN SALAUS

Symmetrisen salaukseen liittyy varteenotettava ongelma, sillä viestin salaaminen ja salauksen purku toteutetaan samalla avaimella. Käytännössä tämä tarkoittaa, että viestin lähettäjä ja viestin vastaanottaja turvautuvat saman avaimen käyttöön, jolloin avain tulee jakaa turvallisesti osapuolten kesken. Avaimen jakaminen kahden osapuolen kesken voi olla verrattain helppoa, mutta kun osapuolten verkosto kasvaa kymmeniin tai jopa satoihin, voi avaimen jakaminen vaikeutua huomattavasti. Tähän ongelmaan kuitenkin löytyy ratkaisu, nimittäin julkinen avainsalaus. Edellisestä voidaan käyttää myös termiä asymmetrinen salaus, sillä se koostuu kahdesta erilaisesta avaimesta, joten salaus on epäsymmetrinen. (Dooley 2018, luku 11, ”Abstract”; Easttom 2015, luku 10, ”What Is Asymmetric Cryptography?”.)

Asymmetrinen salaus ratkaisee ongelman matemaattisesti jakamalla salausavaimen kahteen osaan; julkinen avain ja yksityinen avain. Julkinen avain julkaistaan kaikkien viestinlähettäjien kesken, kun taas yksityinen avain pidetään salassa. Yksityisen avaimen avulla vastaanottaja voi purkaa salakirjoituksen, joka on salattu edellä mainitulla julkisella avaimella. (Dooley 2018, luku 11, ”Abstract”.)

Kuvio 3 havainnollistaa, kuinka Alice saa Bobin julkisen avaimen ja käyttää sitä salatakseen Bobille lähetettävän viestin. Jos Eve onnistuu sieppaamaan viestin ja saa käsiinsä Bobin julkisen avaimen, se ei haittaa, koska kyseinen avain ei pysty purkamaan viestin salausta. Vain Bobin yksityinen avain kykenee siihen. Jos Bob haluaa sen sijaan vastata Alicelle, on prosessi käänteinen. Eli Bob vastaanottaa Alicen julkisen avaimen, salaa viestin sillä ja lähettää viestin. Viestin saatuaan, Alice purkaa viestin salauksen omalla yksityisellä avaimellaan. Täten, niin kauan kuin yksityiset avaimet pysyvät ulkopuolisilta salassa, viestintä voidaan suorittaa turvallisesti, vaikka julkiset avaimet olisivatkin ulkopuolisten tiedossa.



Kuvio 3. Alice, Bobille ja Eve (asymmetrista salaus). (Easttom 2015, luku 10, "What Is Asymmetric Cryptography?"). Kuvion ulkoasua ja tekstejä on muokattu tarkemman selkeyden saavuttamiseksi.

RSA-salausalgoritmi

RSA-salaus on yksi vanhimmista, mutta yhä laajalti käytetyimmistä julkisen avaimen salausjärjestelmistä. Sen nimi muodostuu sen luojien, Rivestin, Shamirin ja Adlemanin sukunimistä. He esittelivät algoritmin vuonna 1977 työskennellessään Massachusetts Institute of Technologyssä. RSA:ta hyödynnetään muun muassa suojaamaan yhteyksiä selaimissa, pilvi- ja sähköpostipalveluissa, chat-sovelluksissa ja P2P-järjestelmissä. (Klusaitė Laura 2022, "RSA encryption definition", "Where is RSA encryption used?".)

Algoritmi käyttää julkista avainta viestin salaukseen ja yksityistä avainta sen purkamiseen. RSA-salausalgoritmin matematiikka sisältää yksisuuntaisen funktion, jonka laskeminen on helppoa, mutta sen kumoaminen on haastavaa. Tämä tekee RSA:sta turvallisen salausalgoritmin, joka on käytännössä mahdoton murrettavaksi "Brute force" -hyökkäyksin. (Klusaitė Laura 2022, "RSA encryption definition".)

Tästä huolimatta RSA:n ikä alkaa jo näkyä nykypäivänä, joten turvallisuuden maksimoimiseksi sitä yleensä käytetään yhdessä muiden salausmenetelmien, kuten AES:n, kanssa. Käytännössä RSA:ta voitaisiin käyttää symmetrisen salauksen, yksityisen avaimen salaamiseen, jolloin avain

saataisiin jaettua turvallisesti, symmetrisen salauksen suojatessa itse arkaluonteista dataa. Eli pääsääntöisesti RSA:lla luodaan turvallinen yhteys ja itse tiedon suojaamiseen käytetään resurssitehokkaampia, turvallisempia ja nopeampia salausmenetelmiä, kuten AES-algoritmi. (Klusaitė Laura 2022, “Where is RSA encryption used?”.)

RSA-matematiikkaa: avainparin luonti ja viestin salaaminen

Julkisen avaimen ja yksityisen avaimen parin luomiseksi aloitetaan generoimalla kaksi alkulukua, p ja q, jotka ovat suunnilleen samankokoisia. Lukujen tulee muodostaa haluttu koko, kuten esimerkiksi 2048-bittiä tai 4096-bittiä. Tämän jälkeen lasketaan muuttuja n kaavan 7 mukaan.

$$n = pq \qquad \textit{(Kaava 7.)}$$

Seuraavaksi käytetään Eulerin totienttifunktiota, jolla saamme muuttujan m kaavan 8 mukaan.

$$m = (p - 1)(q - 1) \qquad \textit{(Kaava 8.)}$$

Valitaan uusi muuttuja e niin, että seuraavat ehdot ovat tosia (kaava 9).

$$1 < e < m \; ja \; gcd(m, e) = 1 \qquad \textit{(Kaava 9.)}$$

Kaavassa 9 $gcd(x, y)$ (Greatest Common Divisor) merkitsee lukujen suurinta yhteistä jakajaa.

Seuraavaksi lasketaan muuttuja d tietyin ehdoin (kaava 10).

$$de \; (mod \; m) \equiv 1 \qquad \textit{(Kaava 10.)}$$

Muuttujat e ja n muodostavat julkisen avaimen (e, n). Viesti salataan julkisella avaimella kaavan 11 mukaan.

$$C \equiv M^e \ (mod\ n) \qquad \textit{(Kaava 11.)}$$

Kaavassa 11 muuttuja C ilmaisee salattua viestiä ja muuttuja M alkuperäistä viestiä.

Salauksen purkamisessa yksityistä avainta käyttäen toimitaan kaavan 12 mukaisesti. Kaavassa samat muuttujat M ja C kuin kaavassa 11. Muuttujat d ja n muodostavat yksityisen avaimen (d, n).

$$M \equiv C^d \ (mod\ n) \qquad \textit{(Kaava 12.)}$$

(Easttom 2015, luku 10, “The RSA Algorithm”; “Asymmetric Cryptography: The RSA algorithm”.)

8 PROJEKTI

Opinnäytetyöni on kokonaisuus, joka koostuu kahdesta eri osasta. Työ koostuu siis teoriaosuudesta, jonka tavoitteena oli luoda perustietämys kryptografiasta ja sen kehityksestä, sekä käytännön osuudesta, jossa sovellan oppimaani. Käytännön osuus konkretisoitui verkkosivuprojektiksi, jonka avulla pääsin sekä haastamaan ongelmanratkaisutaitojani että toteuttamaan itseäni mielenkiintoisen aiheen parissa.

Projekti itsessään on verkkosivusto, jonne on tarkoitus kerätä erinäisiä salausmenetelmiä, alkaen alkeellisemmista salakirjoitusmenetelmistä ja mahdollisesti edeten tulevaisuudessa monimutkaisempiin toiminnallisuuksiin. Sivusto on rakennettu hyödyntäen web-kehityksessä vakiintuneita ja ajanmukaisia teknologioita, kuten HTML, CSS, JavaScript ja React. Projektissa on keskitytty toimivuuteen, käyttöliittymän käyttäjäläheisyyteen, responsiivisuuteen sekä esteettisyyteen.

Projektin innoittajina ovat toimineet sivustot, kuten https://www.dcode.fr ja https://www.boxentriq.com. Sivuston tarkoitus on olla puhtaasti leikkimielinen, sillä alkeellisten salausmenetelmien käyttäminen nykypäivänä on turvatonta luottamuksellisen tiedon salaamisessa. Kohdeyleisö ja tilanteet, joissa tällaisia menetelmiä ja työkaluja voidaan vielä nähdä käytettävän ovat esimerkiksi eettiseen hakkerointiin yhdistetyt harjoitukset, CTF:t (Capture the Flag), sekä geokätköily. Näissä harjoituksissa olen henkilökohtaisestikin törmännyt tehtäviin, jossa haluttu viesti on salattu esimerkiksi Caesarin salakirjoituksella salaperäisyyden, mielenkiinnon ja interaktiivisuuden toivossa. Eli mitä todennäköisemmin projektin käyttötilanteet saattaisivat erityisesti liittyä edellä mainittuihin CTF- ja geokätköilyharrastuksiin. On olennaista kuitenkin muistaa, että sivusto on vasta alkumetreillä, ja sen kehitystyö jatkuu edelleen opinnäytetyön päättymisen jälkeenkin.

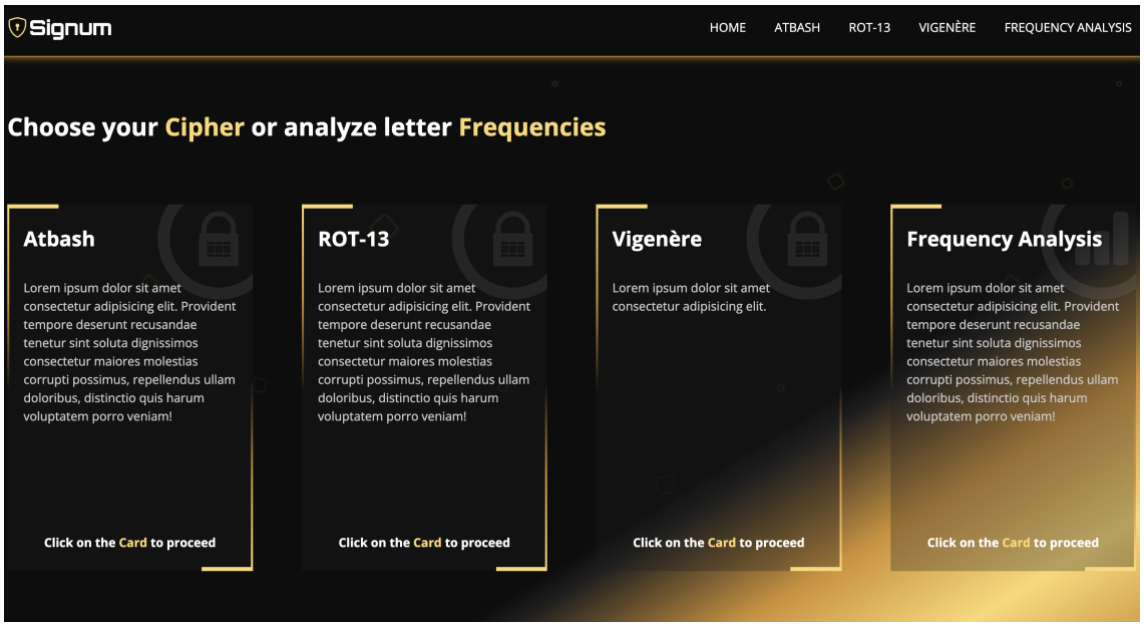
Projektin teemassa pyritään yhdistämään renessanssi moderniin ja digitaaliseen maailmaan. Tämä näkyy muun muassa projektin värimaailmassa, jossa korostuu renessanssiajan kullan kimallus, sekä mustan luoma salaperäisyys. Katsoin, että renessanssi toimii erinomaisena teemana, sillä siinä yhdistyvät aikakaudelle tyypillinen antiikin maailman ihannointi, sekä itse renessanssin tieteiden ja taiteiden kukoistus. Juuri näinä aikoina voidaan myös kryptografisten menetelmien

kokeneen suuria edistysaskeleita. Esimerkiksi Caesarin salakirjoitus edustaa hyvin antiikin ajan salausmenetelmiä, Vigenèren salakirjoituksen edustaessa renessanssia.

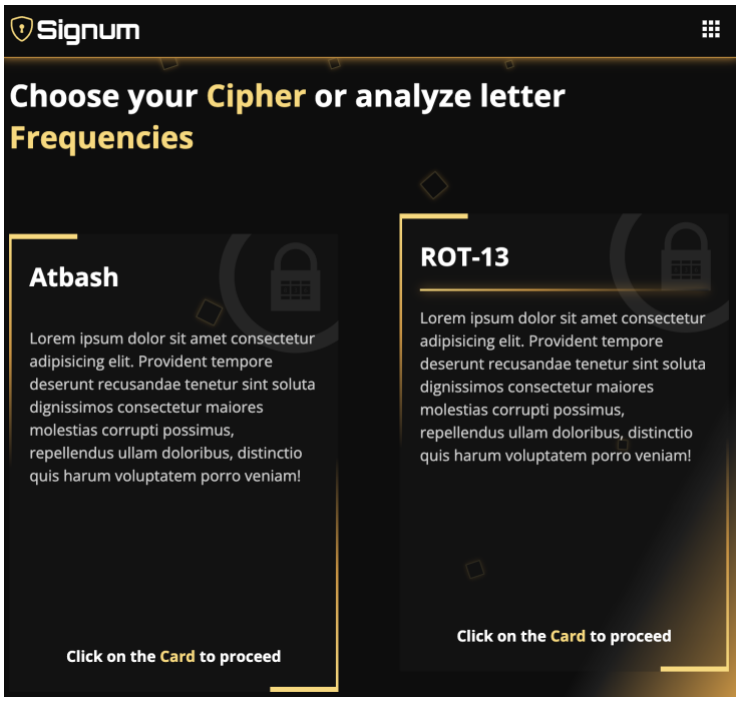
8.1 Responsiivinen sivusto

Projektissa pyrin myös tarjoamaan vaivattoman käyttökokemuksen, sekä halusin varmistaa, että sivustoa voi selata helposti missä tahansa tilanteessa, laitteesta riippumatta. Käyttömukavuus ja toimivuus pienemmillä näytöillä ovat erityisen tärkeitä esimerkiksi geokätköjä metsästettäessä.

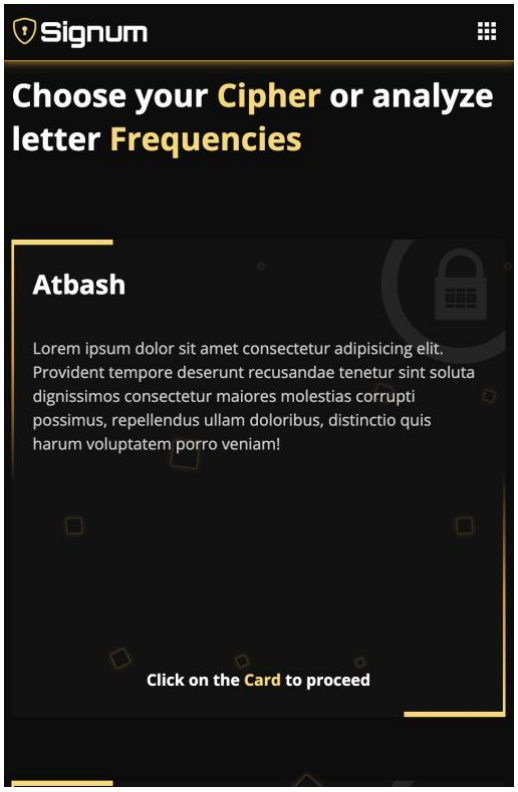
Kuvista 8, 9 ja 10 voidaan huomata, että kortit käyttävät toistaiseksi ”lorem ipsum” -täytetekstiä, mutta tulevaisuudessa kortteihin tulisi sisällyttää lyhyt informatiivinen teksti koskien kortin viittaamaa salausmenetelmää.



Kuva 8. Projektin työpöytänäkymä



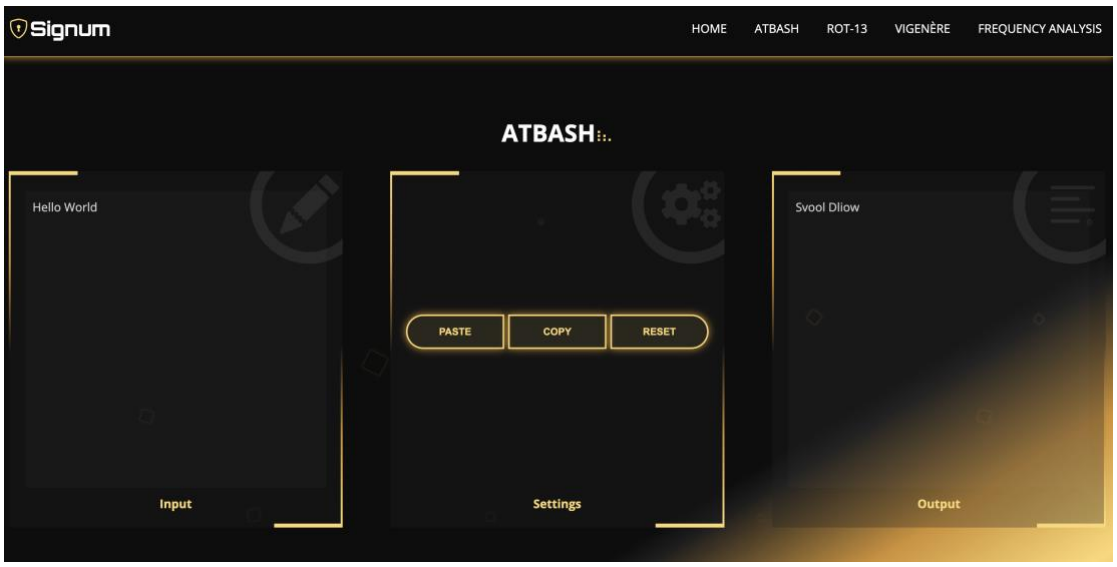
Kuva 9. Projektin tablettinäkymä



Kuva 10. Projektin mobiilinäkymä

8.2 Atbash sivustolla

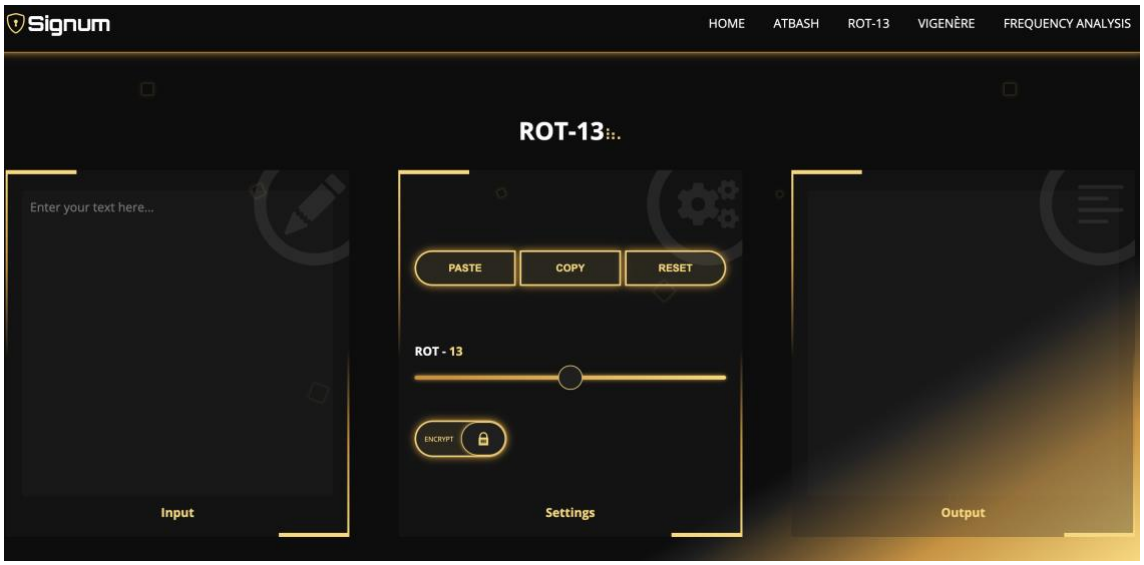
Kuva 11 sivuston Atbash-osiosta. Tässä melko yksinkertaisessa salakirjoituksessa syöteteksti generoituu tulostustekstiksi käyttäjän kirjoittaessa. Jos saadun tulostustekstin syöttää takaisin syötetekstiksi, uusi tulostusteksti on selväkielinen. Asetusikkunassa painikkeet, joilla voi sijoittaa syötetekstiksi sisältöä leikepöydältä, kopioida tulostusteksti leikepöydälle, sekä nollata asetukset ja sisältö.



Kuva 11. Atbash-salakirjoitus

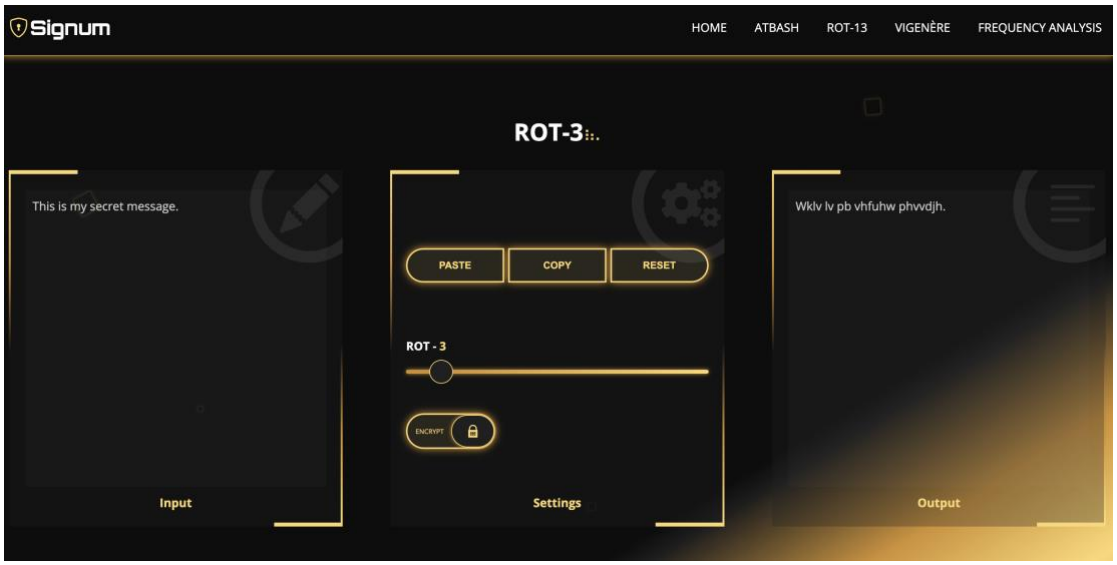
8.3 ROT-13 ja Caesarin salakirjoitus

ROT-13 (Rotate by 13 places) -salakirjoitusta (kuva 12) on käytetty usein verkkoyhteisöissä, foorumeilla ja sähköpostiviestinnässä, kun on haluttu salata viestin sisältöä. Tarkoitus on kuitenkin ollut vain pinnallinen ja leikkimielinen, vaikka esimerkiksi elokuvan juonipaljastusten välttämiseksi. Caesarin salakirjoitus toimii samalla algoritmilla, joten periaatteessa Caesarin salakirjoitus voidaan tulkita myös ROT-3:na.



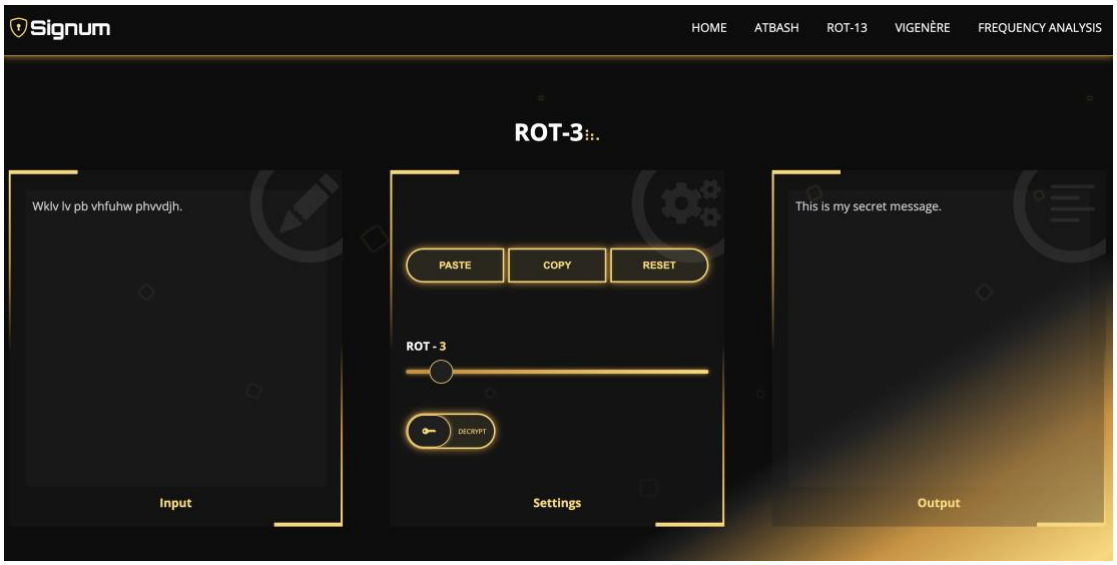
Kuva 12. ROT-13 -salakirjoitus

Kuvassa 13 salaus tehty ROT-3:lla. Kuten Atbash-osiossa, niin myös tässä osiossa teksti generoituu automaattisesti käyttäjän kirjoittaessa. Asetusikkunan liukusäätimellä valitaan haluttu rotaatio, tässä tapauksessa ROT-3. Leikepöytä- ja nollaustoiminnot ovat Atbash-osiostakin tutut.



Kuva 13. Viestin salaaminen (ROT-3)

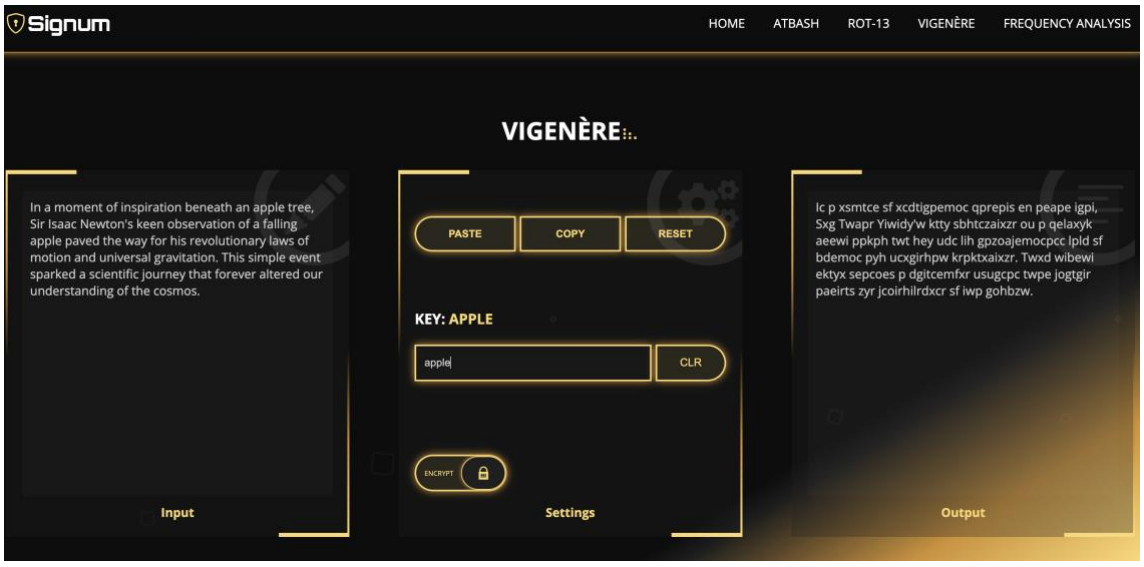
Demonstroidaan salatun tekstin purkaminen takaisin selväkieliseksi. Ensin salattu teksti syötetään syötetekstiksi, valitaan oikea rotaatio keskimmäisellä liukusäätimellä ja asetetaan alin liukusäädin “Decrypt” -asentoon (kuva 14).



Kuva 14. Viestin salauksen purkaminen (ROT-3)

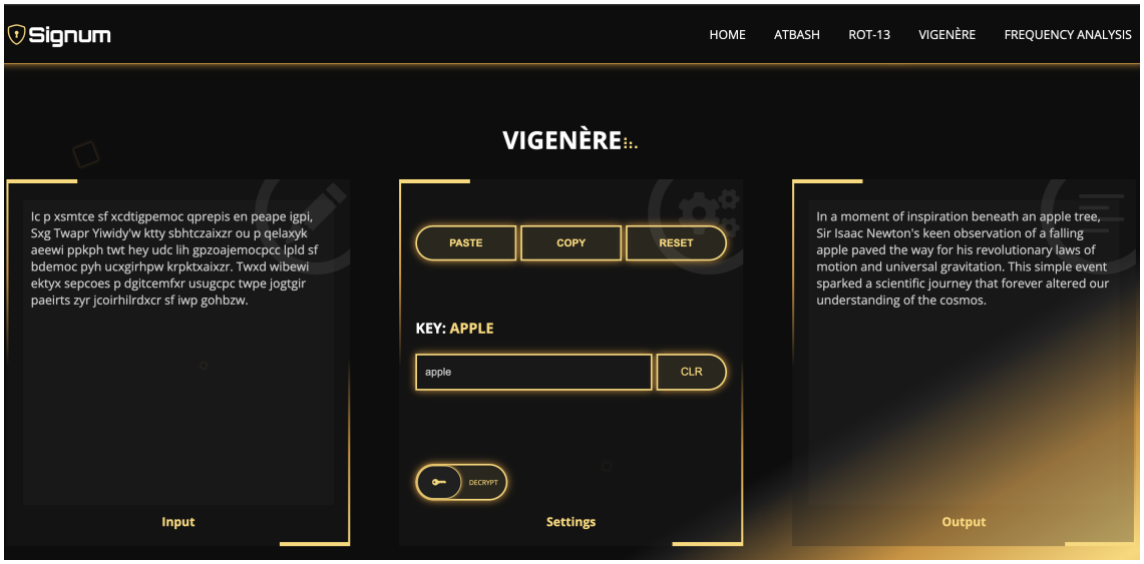
8.4 Vigenèren salakirjoitus sivustolla

Vigenèren salakirjoitusosiossa käyttäjä syöttää syötetekstin. Tämän jälkeen asetusikkunassa syötetään salausavain. Salausavainta syötettäessä, jokainen näppäinpainallus generoi salattua tulostustekstiä. Myös tässä osiossa asetusikkunan leikepöytä- ja nollauspainikkeet toimivat edellisistä osioista tutulla tavalla (kuva 15).



Kuva 15. Viestin salaaminen (Vigenèren salakirjoitus)

Salauksen purkaminen tapahtuu salausavaimen ja käänteisen algoritmin avulla. Eli syötetekstiksi asetetaan saatu salattu viesti. Tämän jälkeen syötetään salausavain ja asetetaan liukusäädin asentoon ”Decrypt” (kuva 16).



Kuva 16.Viestin salauksen purkaminen (Vigenèren salakirjoitus)

8.5 Sivuston jatkokehitys

Sivustolla on vielä paljon työtä tulevien toimintojen ja ominaisuuksien kehittämiseksi. Alle olen koonnut alustavaa listaa tulevista ominaisuuksista ja parannuksista.

- Frekvenssianalyysiosion loppuunsaattaminen
- Aakkosvalinta toimintoihin
- RSA-salausgeneraattori
- Sivuston ulkoasuun parannuksia

9 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyö kokonaisuudessaan toimi itselleni oppimismatkana kryptografian maailmaan ja erityisestin sen historiaan, mutta mikseipä työ voisi myös tarjota jotain hyödyllistä tietoa muille aiheesta kiinnostuneille. Lähtökohdat työlle juontavat juurensa hetkeen, kun pääsin tutustumaan Caesarin salakirjoitukseen leikkimielisen CTF-harjoituksen (Capture the Flag) parissa, jolloin jouduin purkamaan salatun viestin hyödyntäen verkosta löytyvää työkalua. Tuolloin koin, että kyseinen sivusto oli melko sekava, eikä mielestäni soveltunut hyvin mobiilikäyttöön, mikä voisi mahdollisesti olla tärkeää esimerkiksi geokätköilyssä. Täten halusin luoda jotain samanlaista ja konkreettista, mutta ottaen huomioon erilaiset käyttötarkoitukset.

Aiheesta kirjoittamisen koin olevan merkittävä osa oppimisprosessia, sekä tärkeää tiedon jäsentelemisen kannalta. Tämä antoikin perusteen tehdä kokonaisvaltaisen katsauksen aiheen historiaan ja kehitykseen, luoden pohjan perustietämykselle ja työn käytännön osuudelle. Haasteita teoriaosuudelle tuottivat muun muassa historiateosten melko rajallinen lukumäärä, monien lähteiden perustaessa tietonsa juuri näihin muutamaan kirjateokseen historian näkökulmasta. Lisäksi nämä jo melko iäkkäät klassikkoteokset kryptografian historiasta sortuivat ajoittain tarinankerronnan saattelemana käsittelemään aiheelle epäolennaisiakin asioita.

Rajallisen tietämykseni ansiosta päädyin myös aliarvioimaan sekä kryptografian että sen läheisten avainteemojen laajuuden aiheena, minkä vuoksi jouduin pohdiskelemaan aihetta ja sen rajausta uudelleen. Koska historian näkökulmasta merkittävimmät salausmenetelmät ovat symmetrisiä salausmenetelmiä ja asymmetrisen salauksen ollessa oleellinen jatkumo symmetriselle salaukselle, päätin rajata työn käsittelemään sekä symmetristen että asymmetristen salausmenetelmien historiaa ja kehitystä. Pääaiheen ohessa katsoin myös tärkeäksi käsitellä aiheelle läheisiä avainteemoja.

Pitääkseni työn teoriasisällön maltillisena, pyrin käymään läpi vain historian merkittävimpiä salausmenetelmiä eri ajanjaksoina. Eri salausmenetelmien kohdalla, etenkin modernien sellaisten kuten DES, AES ja RSA, pyrin pitämään asiasisällön informatiivisena, mutta pintapuoleisena, sillä näissä tapauksissa sisältöä olisi riittänyt jokaisen menetelmän kohdalla oman opinnäytetyön laajuudella.

Verkkosivuprojektia ehdin opinnäytetyön aikana työstämään muutaman salakirjoitusmenetelmän verran, kuten Atbash, ROT-13 ja Vigenèren salakirjoitus. Tämän lisäksi pääsin aloittamaan frekvenssianalyysiosion rakentamista. Sivustolle sain myös suunniteltua alustavaa ulkoasua ja responsiivista käyttöliittymää. Sivuston parissa on vielä paljon työstettävää tulevien toimintojen ja ominaisuuksien osalta, mutta tämän tiedostinkin alusta pitäen, eikä sivustoprojektia ollut tarkoitus saada valmiiksi opinnäytetyön aikana.

Kaiken kaikkiaan opinnäytetyö antoi erittäin monipuolisen annin itselleni mieleisen aiheen parissa. Teoriaosuuden laatiminen antoi hyvät eväät salausmenetelmien historiaan ja perusteisiin, mutta mikseipä aineisto voisi toimia myös hyvänä tietopakettina tuleville lukijoille, sekä aiheesta kiinnostuneille.

LÄHTEET

Asymmetric Cryptography: The RSA algorithm (with examples). Hakupäivä 1.12.2023
https://justcryptography.com/rsa-algorithm/

Cohen, Fred 1990. 2.1 - A Short History of Cryptography. Hakupäivä 7.6.2022
http://all.net/books/IP/Chap2-1.html

D'Agapeyeff Alexander 1939. Codes and Ciphers - A History of Cryptography. Read Books Ltd 2016. Hakupäivä 7.6.2022
https://books.google.fi/books?hl=en&lr=&id=Uab7DAAAQBAJ&oi=fnd&pg=PT7&dq=history+of+cryptography&ots=GF6dS2RCuR&sig=rm1IE74KFv3O9VZYO0VLJ5T9MyE&redir_esc=y#v=onepage&q&f=false

Dooley John F. 2018. History of Cryptography and Cryptoanalysis
https://link.springer.com/book/10.1007/978-3-319-90443-6

Easttom William 2015. Modern Cryptography: Applied Mathematics for Encryption and Information Security
https://www.oreilly.com/library/view/modern-cryptography-applied/9781259588099/

Easttom William 2022. Modern Cryptography: Applied Mathematics for Encryption and Information Security
https://link.springer.com/book/10.1007/978-3-031-12304-7

Klusaitė Laura 2022. What is RSA encryption, and how does it work? Hakupäivä 1.12.2023
https://nordvpn.com/fi/blog/rsa-encryption/

NIST (National Institute of Standards and Technology) 2005. Data Encryption Standard (DES). Hakupäivä 1.12.2023
https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf

Singh Simon 1999. Koodikirja: Salakirjoituksen historia muinaisesta Egyptistä kvanttitypografiaan

Wikimedia Commons. Enigma. Hakupäivä 1.12.2023
https://commons.wikimedia.org/wiki/File:EnigmaMachine.jpg

Wikimedia Commons. Skytale. Hakupäivä 1.12.2023
https://commons.wikimedia.org/wiki/File:Skytale.png

Wong David 2021. Real-world cryptography
https://learning.oreilly.com/library/view/real-world-cryptography/9781617296710/