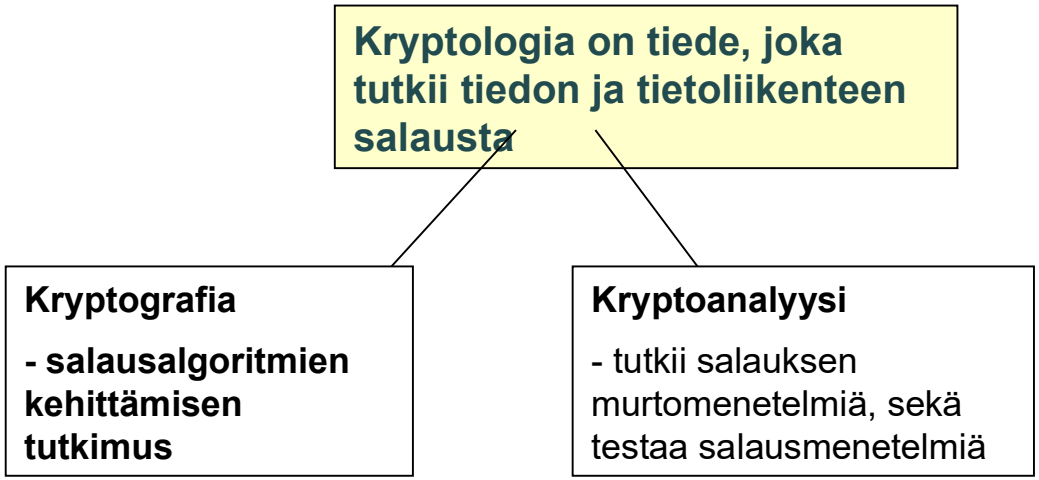
Suomenkielinen versio

Luku 1

Käsitteitä ja määritelmiä

Klassisia salauksia

Cryptology, Cryptography, Cryptoanalysis



Suomessa on kansainvälisestikin merkittävää alan teollisuutta. **SSH** on yleisesti käytetty salausohjelmisto, joka mahdollistaa tietojärjestelmän turvallisen etäkäytön. Sen on kehittänyt suomalainen Tatu Ylönen. SSH:n käyttäjiä ovat mm. EU, NASA ja USA:n armeija.

Internet Engineering Task Force (IETF) on määritellyt **tietoturvallisuuden palvelut** ao. listan mukaisesti. Listan palveluiden toteuttaminen edellyttää kryptografian menetelmiä.

Palvelu	Toteutuskeino
1. **Luottamuksellisuus ***	- tiedon ja viestien salaus
2. **Eheys ***	- tiivistefunktiot
3. **Autentikointi ***	- krytografinen autentikointi
4. **Kiistämättömyys ***	- digitaalinen allekirjoitus
5. **Pääsyn valvonta**	- jonkin verran edelleen salasanoilla tapahtuva. Yhä useammin käytössä ovat kryptografian todennusmenetelmät
6. **Käytettävyys**	

Terminology in english:

1.Confidentiality: Only those who are entitled to information can access to it

2.**Integrity**: Information is unchanged during transfer. Sender is authenticated

3. **Authentication**: The sender is provably identified

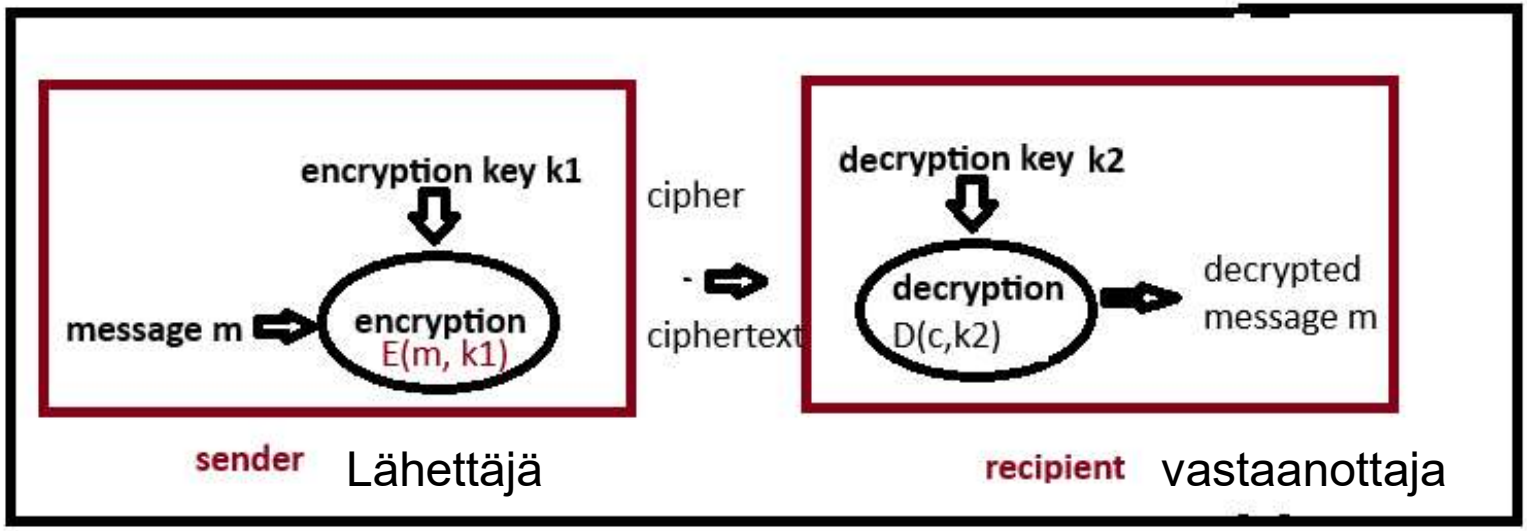
4. Non-repudiation: A communicating party cannot deny the contents of his/her messages or deny later having participated in the interaction.

Käsitteitä ja määritelmiä

Sisältöjä:

1. Diagrammiesitys viestien salauksesta
2. Symmetrinen ja asymmetrinen salaus
3. Kerckhoffin periaate
4. Avainavaruus, efektiivinen avainavaruus
5. Mathemaattisia käsitteitä

1. Diagrammi salauksesta



Viesti m (message or plaintext) salataan käyttäen salausfunktiota (encryption function) E(m, k1), jonka toinen argumentti on salausavain (encryption key) k1. Tuloksena saadaan salakirjoitus (cipher or ciphertext) c .

Salakirjoituksen purkuun (Decryption) käytetään purkufunktiota decryption function D(c, k2), jonka syötteinä ovat salakirjoitus c ja purkuavain (decryption key) k2. Tuloksena on alkuperäinen viesti m

2. SYMMETRINEN JA ASYMMETRINEN SALAUS

SYMMETRIC ENCRYPTION: **Salausavain k1 ja purkuavain k2 ovat samat.**

* Osapuolten täytyy sopia yhteydessä käytettävästä symmetrisestä avaimesta ennen istuntoa. (Avaimesta sovitaan turvallisesti käyttäen jotain avaimenvaihtoprotokollaa ”key exchange protocol” (esim. DH, RSA tai ECDHE)

ASYMMETRIC ENCRYPTION: **Salausavain k1 ja purkuavain k2 ovat erilaiset.**

- Yleisin muoto on ns. julkisen avaimen salaus (public key encryption PKI), jossa **jokaisella käyttäjällä on kaksi avainta** : **julkinen avain** , jolla käyttäjälle lähetetyt viestit salataan, ja sen parina **yksityinen avain**, jolla käyttäjä purkaa saamansa salatut viestit.

3. Kerckhoffin periaate

Kerckhoff principle:
"A cryptosystem should be secure even if all its details are public".
Only the key is secret.
(salausmenetelmän tulisi olla turvallinen vaikka sen kaikki yksityiskohdat olisivat julkisia, kunhan vain käytetty avain on salainen)

(Auguste Kerckhoff 1835 - 1903 was a Dutch linguistic and cryptographer)

Lähimenneisyydessä lohkosalaimen DES ja GSM – puhelujen salauksen algoritmeja yritettiin pitää salassa. Ne kuitenkin vuotivat julkisuuteen.

Nykyisten salaimien algoritmit ovat täysin julkisia noudattaen Kerckhoffin periaatetta.

4. Avainavaruus (key space)

Turvallinen salausjärjestelmä ei saa sisältää haavoittuvuuksia tai takaportteja.

Tällöin murtoa yrittävälle jää parhaaksi vaihtoehdoksi **Brute Force attack**: avaimen etsiminen käymällä läpi kaikki mahdolliset avainvaihtoehdot.

Tärkein tekijä brute force menetelmää vastaan on **mahdollisten avainten lukumäärä**, jota kutsutaan nimellä avainavaruus ,**key space**. Avainavaruutta mitataan yleensä bitteinä (**bits)**.

Ehdoton teoreettinen minimi brute force hyökkäystä vastaan on 80 bittiä, jolloin mahdollisia avaimia on $2^{80} = 1.2*10^{24}$ kpl

Key space includes all keys from 00...0 to 11...1 (80 bit binary numbers)

Käytännön turvallinen minimi avainavaruudelle on 128 bittiä.

Efektiivinen avainavaruus

Useimmille salausalgoritmeille on kehitetty menetelmiä, joilla avain voidaan löytää jonkin verran vähemmällä määrällä hakuja kuin **teoreettisen avainavaruuden** perusteella voisi olettaa.

Effective key space means the average number of steps needed to break the key using best known methods of cryptanalysis. Efektiivinen avainavaruus on siis keskimääräinen kokeiltavien avainten määrä, joka tarvitaan salauksen murtamiseen käyttäen parhaimpia tunnettuja menetelmiä. Hyvässä algoritmissa efektiivinen ja teoreettinen avainavaruus ovat lähes samansuuruiset.

Most common symmetric cipher is AES	
AES128	key space 128 bits, effective 126.1
AES256	key space 256 bits, effective 254.4
In some older algorithms difference is bigger	
DES	key space 64 bits, effective 54
3DES	key space 168 bits, effective 112

Avainavaruutta voidaan käyttää myös salasanojen turvallisuuden arviointiin.

80 bitin minimiä $2^{80} = 1.2 \cdot 10^{24}$ voi käyttää myös laskettaessa salasanojen turvallisuutta Brute Force – hyökkäyksiä vastaan
Seuraavassa esimerkkejä:

1. Salasanan pituus = 8 (engl. aakkosto). Ei eroa pienten ja isojen kirjainten välillä (=26 characters)
   Salasana-avaruus = $26^8 = 2 \cdot 10^{11}$ turvaton

2. Salasanan pituus = 11 (engl. aakkosto). , pienet ja isot kirjaimet + numerot 0…9: (= 62 characters)
   Salasana-avaruus = $62^{11} = 5 \cdot 10^{19}$ turvaton

3. Salasanan pituus = 13 (engl. aakkosto). , pienet ja isot kirjaimet + numerot 0…9: + kymmenen erikoismerkkiä: (=72 characters)
   Salasana-avaruus $72^{13} = 1.4 \cdot 10^{24}$ ylittää turvarajan 80 bittiä

5. Matemaattisia käsitteitä

HARD PROBLEM

= matemaattinen ongelma, joka on **vaikea**, **monimutkainen ja hidas ratkaista**. Usein salausalgoritmien turvallisuus perustuu johonkin tunnettuun ”hard problem” -ongelmaan . Esim. RSA algoritmin turvallisuus perustuu suurten kokonaislukujen tekijöihin jaon vaikeuteen. Diffie-Hellman avaimen vaihtoprotokollan taustalla on Diskreetin Logaritmin Probleema (DLP).

ONE WAY FUNCTION - YKSISUUNTAINEN FUNKTIO

= funktio y = f(x), jolla y voidaan laskea nopeasti, kun x on annettu, mutta jonka käänteis-funktio, x:n ratkaiseminen kun y tunnetaan, on vaikeaa tai mahdotonta ilman jotain lisätietoa

BACKDOOR - TAKAOVI

= Lisätieto , joka mahdollistaa yksisuuntaisen funktion käänteisfunktion laskemisen.

RSA:ssa purkuavaimen laskeminen julkisesta avaimesta on käytännössä mahdotona. Julkinen avain on suuri kokonaisluku. Kuitenkin **jos julkisen avaimen tekijät ovat tiedossa, purkuavaimen laskeminen on helppoa. Julkisen avaimen tekijöiden tunteminen on takaovi RSA:n murtamiseen.**

On olemassa esimerkkejä 2000- luvulta **tahallisista takaovista**, joita tiedusteluviranomaisest ovat saaneet ujutettua yleisesti käytettyihin algoritmeihin. (Tunnetuin tapaus on satunnaislukugeneraattori Dual_EC_DRBG, joka paljastui 2013)

Klassiset salaukset

Classical ciphers (cipher = encryption algorithm, encryption method)

Mono- and polyalphabetic ciphers

Eräitä klassisia salauksia:

1. Caesar salaus
 - frekvenssianalyysi
2. Affiini salaus
3. Hill cipher (Matrix cipher)
4. Enigma
5. Yksinkertainen substituutiosalaus
6. Vigeneren salaus
7. Autokey salaus
8. One Time Pad: ”the only unbreakable cipher”

Klassisten salausten luokitteluja

A) **Monoalphabetic cipher** on salaus, jossa viestin jokainen merkki salataan erikseen. Jokaisella merkillä on kiinteä, pysyvä kuvamerkki. Caesar salaus, affiini salaus ja yksinkertainen substituutio ovat esimerkkejä tästä tyypistä.

Frekvenssianalyysi on tehokkain keino murtaa em. salauksia.

B) **Polyaphabetic cipher** on salaus, jossa samalla viestin merkikkä voi olla useita eri kuvamerkkejä eri kohdissa viestiä. Vigenèren salaus on tätä tyyppiä. Frekvenssianalyysin tehokkuus murtomenetelmänä on heikompi tätä salaustyyppiä vastaan.

Salattavan yksikön pituuteen perustuva luokittelu

Monographic cipher on salaus, jossa salaus suoritetaan merkki kerrallaan
Polygraphic cipher on salaus, jossa viesti jaetaan usean merkin mittaisiin lohkoihin ja salausfunktio salaa viestin lohko kerrallaan. Nykyiset salaukset ovat tätä tyyppiä.

1. Caesar salaus

- Salaus perustuu aakkoston kiertoon. Salausavain on kierron suuruus

Viestin “AAMU” salakirjoitus on “NNZH” kuvan salauskiekon mukaan

Kiekko jäljittelee roomalaisten 2000 v sitten käyttämää kiekkoa

Avainavaruus = 25 (mahdollisten rotaatioiden lukumäärä käytettäessä engl. aakkostoa)

Caesar salaus on helposti murrettavissa
Brute Force:lla (kokeilemalla kaikkia 25 avainta)
Frekvenssianalyysillä murtaminen on vielä helpompaa .

Frekvenssianalyysi (kohteena monoalphabetic cipher)

Frekvenssianalyysi on yleinen tapa murtaa klassisia salauksia.
Tehokkaimmin se toimii, kun salaustyyppinä on monoalphabetic cipher.
(Frekvenssianalyysin variaatioita voidaan käyttää myös edistyneempiin salauksiin, kuten Enigma salauslaitteen salauksen murtamiseen)

Perinteinen frekvenssianalyysi (kun viestit ovat englanninkielisiä) hyödyntää taulukkoa englannin kielen kirjainten suhteellisista frekvensseistä teksteissä.

e	*t*	*a*	*o*	*n*	*i*	*s*	*r*	*h*
12.3	9.6	8.1	7.9	7.2	7.2	6.6	6.0	5.1

Kirjain **e** on selvästi yleisin kirjain englannin kielessä 12.3% osuudella.

Salakirjoituksen merkki, jolla on suurin frekvenssi on erittäin todennäköisesti merkin **e** kuvamerkki. (jos ei ole, t tai a tulevat kysymykseen)

Wikipediassa on myös muiden kielten merkkien yleisyystaukukot. Suomenkielisissä teksteissä 6 yleisintä merkkiä ovat järjestyksessä a, i , t , n , e , s

Esim. Caesar salauksen frekvenssianalyysi

Tarkastellaan seuraavaa salakirjoitusta.

```
cqnujcnbcvxernjkxdclahycxpajyqhrbwxfrwcqnjcnabrbcnuubjkxdcbnlxwmfxaumfjajwm
   cqnjccnvycbvjmnrwnwpujwmcxkajtnpnavjwnwrpvjlryqna
```

Lasketaan salakirjoituksen merkkien frekvenssit. Alla 6 yleisintä merkkiä

n : 15 , c : 14, j : 13 , w : 9 , a : 8 , x : 8 , ...

Merkillä n on suurin frekvenssi. Hypoteesi**:** n on kirjaimen e kuvamerkki**.** Rotaation määrä merkistä e merkkiin n on **9 , mikä on todennäköisesti salausavain.**

Testataan hypoteesi siirtämällä salakirjoituksen kirjaimia 9 pykälää vasemmalle Tuloksena on järkevä viesti, joten hypoteesi on oikea ja salakirjoitus murrettu.

```
thelatestmovieaboutcryptographyisnowintheatersistellsaboutsecondworldwarand
   theattemptsmadeinenglandtobrakegermanenigmacipher
```

2. Affiini salaus

1. Aakkoston merkit koodataan luvuiksi 0 – 25 ao. tapaan

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Salaus

2. Olkoon m = viestin merkki ja c = merkin m kuvamerkki. Salausavain on pari (a,b) of Z_{26}

Salauskaava : **$c = a\,m + b \pmod{26}$**

3. Lopuksi luvut c dekoodataan yo. taulukon avulla takaisin merkeiksi

Purkaminen

4. Ratkaistaan salauskaava m:n suhteen kertomalla se luvun a käänteisluvulla mod 26. Saadaan

Purkukaava: **$m = a^{-1}\,c - a^{-1}\,b \pmod{26}$**

5. Kaavassa m ja c ovat viestin ja sen salakirjoituksen merkkien koodeja

- Huom! Miten lasketaan luvun a käänteisluku?
- 1. Käytetään Extended Euclid algoritmiä
- 2. Kaavalla a^{-1} = a^(ϕ(26)-1) mod 26 = a^11 mod 26 (based on Euler's theorem)
- 3. WolframAlphalla voidaan laskea potenssia -1 käyttäen: a^-1 mod 26

Avainarvaruus affiinissa salauksessa on 26*ϕ(26) = 26*12 = 312
(vain sellaiset a:n arvot käyvät, joille gcd(a,26) = 1)

Esimerkki affiinista salauksesta

Salaa viesti ”kemi” kun avain on (a = 11 , b = 3)
1. Koodataan merkit viestiksi m = (10, 4 , 12 , 8)
2. Käytetään salauskaavaa:
c = (11*10 + 3 , 11*4 + 3, 11*12 + 3, 11*8 + 3) mod 26
= (9 , 21 , 5 , 13), joka dekoodattuna antaa ”jvfn”

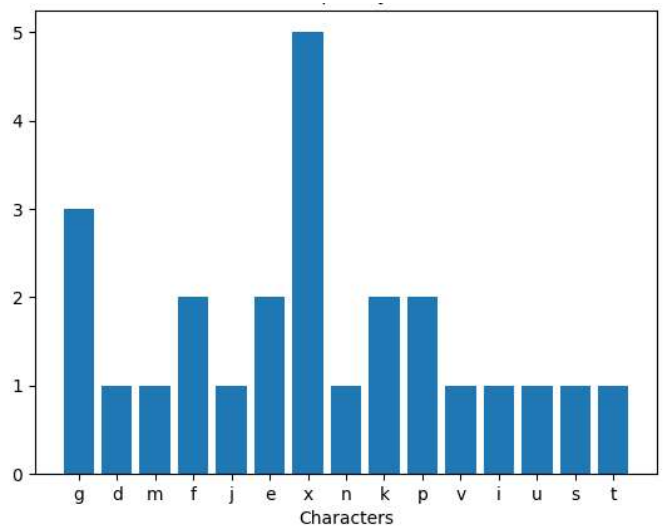
Purkaminen: $m = a^{-1} c - a^{-1} b \pmod{26}$
1. Lasketaan käänteisluku $a^{-1} = 11^{-1} \bmod 26 = 19$ *)WolframAlpha
2. Käytetään purkukaavaa
(19*9 – 19*3 , 19*21 – 19*3 , 19*5 – 19*3 , 19*13 – 19*3) mod 26 =
(10 , 4 , 12 , 8) , joka dekoodattuna on ”kemi”

***)WolframAlpha.com laskee käänteisluvun helposti: 11^-1 mod 26.**

Esim. affiinin salauksen frekvenssianalyysistä

Murretaan salakirj. ”gdmfjgexnxfgexkpvikxxupst”

Frekvenssianalyysi näyttää, että **x** ja **g** ovat yleisimmät salakirjoituksen merkit:



Hypoteesi E(e)=x ja E(t)=g antaa yhtälöt
a*4 + b ≡ 23 ja a*19 + b ≡ 6 (mod 26)
Vähennetään yhtälö (1) yhtälöstä (2)
15*a ≡ -17 ≡ 9 =>
a ≡ 15^{-1}*9 ≡ 7*9 ≡ **11** (mod 26)
Sijoitus a=11 yhtälöön (1) antaa
b ≡ 23-11*4 ≡ **5** (mod 26)

Testataan tulos (a,b) = (11,5)
Käänteisluku $a^{-1} \equiv 11^{-1} \equiv 19$.

Käytetään purkuun Moodlessa olevaa Excel taulukkoa (välilehti Affiini salaus).
Tuloksena on viesti.

”todaytheweatherisfreezing”

3. Hill Cipher (Matrix cipher)

Luonnollinen laajennus Affiinille salaukselle on Hill cipher (1929), jolla salataan merkkien sijasta uean merkin lohkoja. Samalla viesti merkillä voi olla useita kuvamerkkejä. **Hill cipher salaa käyttäen matriisien kertolaskua**.

Salataan lohko ”act” käyttäen matriisia ((G,Y,B),(N,Q,K),(U,R,P))

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

= ”poh”

Puretaan salakirjoitus käyttäen käänteismatriisia

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \pmod{26} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

Taking the previous example ciphertext of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

= ”act”

Hill cipher toteuttaa **Shannonin diffuusio-periaatetta**:

”Jokaisen salakirjoituksen merkin tulee riippua useista viestin merkeistä”

- Jos lohkon pituus on 4 , Hill cipher käyttää 4x4 matriiseja, j.n.e
- Avainavaruus 3x3 matriiseille on 26^9 = n. 10^{12}
-
- Saksan ensimmäiset Enigma salauslaitteet perustuivat Hill salauksen ideaan.

4. Enigma salauslaitteet

In World War II the Germans used Enigma encryption machine in communication with submarines.

The first computers were made in England for breaking the encrypted messages of Enigma. (”Tummy – machine”)

Videos: 15 min

https://www.youtube.com/watch?v=GBsfWSQVtYA Lorentz machine

https://www.youtube.com/watch?v=b4WBINgRMTY Tummy machine

Klassisten salausten aikakausi päättyi, kun tietokoneet ja tietokoneverkot keksittiin.
Modernit salausmenetelmtä otettiin käyttöön 1970 – luvulla.

5. Yksinkertainen substituutiosalaus

Salausavain on aakkoston satunnainen permutaatio **(a->k, b->z, c->q,…).**

Avainavaruus = permutaatioiden lkm = 26! = $4*10^{26}$. Brute force on siis käyttökelvoton. Frekvenssianalyysillä murtaminen on kohtuullisen helppoa ja on verrattavissa ristisanatehtävän ratkaisemiseen.

CIpher:

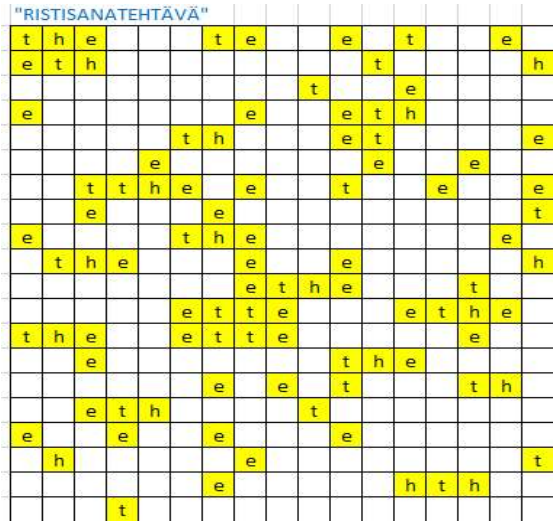
u	o	s	w	e	i	u	s	m	m	s	q	u	z	r	s	w
s	u	o	e	b	e	m	q	d	c	v	u	e	x	t	x	h
c	i	z	i	e	m	j	x	d	u	z	w	s	q	z	v	o
s	d	i	z	i	m	d	s	p	f	s	t	q	c	x	t	x
h	c	i	z	i	u	o	z	i	w	s	u	o	e	b	d	s
p	f	z	d	s	i	n	t	e	j	h	s	b	y	s	x	g
e	f	u	u	o	s	d	s	h	x	u	z	r	s	m	d	s
p	f	s	t	q	z	s	i	e	m	q	o	x	d	x	q	u
s	d	i	e	m	u	o	s	h	x	t	y	f	x	y	s	z
t	u	o	s	q	x	i	s	e	m	s	t	y	h	z	i	o
h	x	t	y	f	x	y	s	u	o	s	w	e	i	u	q	e
w	w	e	t	h	s	u	u	s	d	z	i	s	u	o	s	e
u	o	s	d	h	s	u	u	s	d	i	q	e	w	s	m	x
d	g	s	o	z	t	b	x	t	e	u	o	s	d	j	x	c
e	m	z	w	v	h	s	w	s	t	u	z	t	y	u	o	z
i	w	s	u	o	e	b	z	i	u	e	x	t	x	h	c	i
s	m	d	s	p	f	s	t	q	z	s	i	e	m	u	j	e
q	o	x	d	x	q	u	s	d	q	e	w	g	z	t	x	u
z	e	t	i	z	t	s	t	y	h	z	i	o	u	o	z	i
w	e	i	u	q	e	w	w	e	t							

Frequency analysis

Alla englanninkielen tekstin merkkien suht. frekvenssit

e	*t*	*a*	*o*	*n*	*i*	*s*	*r*	*h*
12.3	9.6	8.1	7.9	7.2	7.2	6.6	6.0	5.1

Initial phase of cryptanalysis



*) Oikeanpuolimmaisessa taulukossa osa viestin kirjaimista on jo ratkaistu perustuen siihen, että s on merkin e kuva ja u on merkin t kuva. Lisäksi englannin kielessä yhdistelmän t_e välikirjain on todennäköisimmin h. (esim. ”the”, ”these”, ”they”, ”them”, ….). Seuraava vaihe olisi etsiä salakirjoituksesta kolmen merkin yhdistelmiä, jotka vastaisivat sanaa and, joita englanninkielisessä tekstissä on yleensä useita.

5. Vigenèren salaus (alkuper. versio)

Blaise de Vigenère 1523 -1596 was a french linguistic and cryptographer

- Salausavaimena on salasana tai lause
- Koko avain saadaan laajentamalla salasana koko viestin mittaiseksi
- Salaus suoritetaan yhteenlaskemalla viestin merkki ja avaimen merkki joko perinteistä taulukkoa, tai koodattuna yhteenlaskulla mod 26.

- Vigenere salaus on haavoittuva, jos salasana on lyhyt. Preussilainen upseeri Kasiski keksi 1800-luvulla murtomenetelmän, joka perustuu 2-3 merkin mittaisten salakirjoituksen lohkojen frekvenssianalyysiin.

Perinteinen Vigenèren yhteenlaskutaulukko

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Salataan viesti “helsinki” kun salasana on “oulu”

H E L S I N K I

O U L U O U L U

==========

V Y W M W H V C

Avainavaruus on 25^{n}, missä n = salasanan pituus. Jos n = 20, avainavaruus = $9*10^{27}$, joka ylittää turvarajan Brute Force hyökkäystä vastaan.

6. Autokey cipher = parannettu Vigenèren salaus

- Master avaimena toimii salasana
- Viesti jaetaan salasanan mittaisiin lohkoihin
- 1. salauslohko saadaan lisäämällä 1. viestilohko salasanaan
- Seuraavien lohkojen salakirjoitus saadaan lisäämällä salattavaan viestilohkoon edellisen lohkon salakirjoitus
- Menettelystä voidaan käyttää nimeä CBC : ”cipher block chaining”.

Salataan ”konferenssi” salasanalla ”lumi”

message	k	o	n	f	e	r	e	n	s	s	i
key	l	u	m	i	**v**	**i**	**z**	**n**	z	z	d
cipher	**v**	**i**	**z**	**n**	z	z	d	a	r	r	l

Puretaan salakirjoitus ”viznzzdaffl” salasanalla ”lumi”

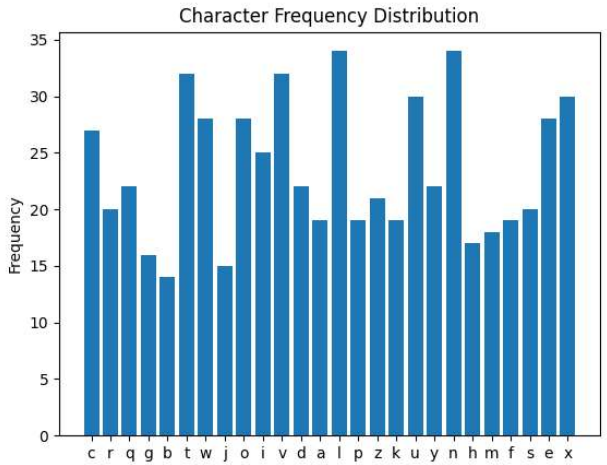
”vizn” – ”lumi” = ”konf”
”zzdz”-”vizn” = ”eren”
”rrl”-”zzs” = ”ssi”

Alkuperäisessä Vigeneren salauksessa laajennettu avain oli periodinen (salasanaa kopioimalla muodostettu). Tässä periodisuutta ei ole.

7. One Time Pad : ”the unbreakable cipher”

- Jos Vigeneren salauksessa avain on satunnainen, viestin mittainen merkkijono ja samaa avainta ei käytetä kahdesti, salaus on murtamaton. (myös kvanttitietokoneille)

- Tämä on ilmeistä, koska jokaista salakirjoitusta c ja jokaista saman pituista mahdollista viestiä m kohti, on olemassa avain j k olla m kuvautuu c:ksi. Ei ole mitään keinoa erottaa oikeaa viestiä muista mahdollisista viesteistä.



One Time Pad:n tuottaman salakirjoituksen frekvenssitaulukko on täysin satunnainen.

Turvallisten salausmenetelmien yksi vaatimus onkin se, että salakirjoituksien frekvenssianalyysi on täysin satunnainen eikä tuota mitään tietoa sen käyttäjälle

7. Binääriversio One Time Pad:sta on Vernam cipher

Vernam cipher (1919) oli käytössä kylmän sodan aikana Moskova- Washington kuuman linjan telex yhteyksissä.

Viesti m ja satunnainen viestin mittainen avain k ovat bittijonoja. Salauksessa viesti m ja avaimen k lasketaan yhteen XOR yhteenlaskua käyttäen. Salaus puretaan lisäämällä avain k salakirjoitukseen

XOR addition: 0 + 0 = 0, 1 + 1 = 0 , 1 + 0 = 1, 0 + 1 = 1

Encryption:

Message	1	0	1	1	0	0	1	0
Key	0	1	1	0	1	0	1	1
Cipher	1	1	0	1	1	0	0	1

Decryption:

Cipher	1	1	0	1	1	0	0	1
Key	0	1	1	0	1	0	1	1
Decrypted m	1	0	1	1	0	0	1	0

One Time Pad :n molemmat versiot vaativat, että osapuolilla on samanlaiset koodikirjat, jotka sisältävät pitkiä kertakäyttöavaimia. Tämä tekee niistä hankalia käyttää tietoverkoissa tapahtuvan massiivisen tiedonsiirron salauksessa.

Klassisten salausten perintö

Enigma salauslaitteen murtamisyritykset johtivat **ensimmäisten tietokoneiden keksimiseen** 2. maailmansodan loppupuolella.

Modernit kryptoalgoritmit alkoivat kehittyä sodan jälkeen tietokoneiden yleistyessä ja ensimmäisten tietoverkkojen ilmestyttyä hallintoon ja liike-elämään.

Modernit salausmenetelmät ovat kopioineet ideoita klassisista:
- avainavaruuden käsite
- Kerckhoffin periaate
- murtomenetelmät kuten frekvenssianalyysi

Amerikkalainen matemaatikko **Claude Shannon**, ”Informaatioteorian isä” loi modernin kryptografian perustan julkaisuissaan ”Mathematica Theory of Information” ja ”Communication Theory of Secrecy System” (molemmat 1948).