DES - Data Encryption Standard

Pro gradu -tutkielma
Ilkka Alanärä
Matemaattisten tieteiden tutkinto-ohjelma
Oulun yliopisto
Kevät 2020

Sisältö

Johdanto **2**

1 Data Encryption Standard **3**

2 Yksinkertaistettu DES-tyyppinen algoritmi **4**

3 DES-algoritmi **11**

4 Esimerkkisalaus ja salauksen purku **19**

4.1 Salausavaimet 19

4.2 Viestin salaus 22

4.3 Salauksen purku 46

5 DES:n murtaminen ja korvaaminen **47**

6 DES-algoritmin Python-koodi **49**

6.1 Alku- ja loppupermutaatio 49

6.2 DES-algoritmi 50

Lähdeluettelo **55**

Johdanto

Sähköisen tiedonvälityksen kehittyessä, 1970-luvulla, koettiin Yhdysvalloissa tarpeelliseksi kehittää salausmenetelmä, josta tulisi alan käytettävä kansallinen standardi. Vuonna 1973 silloinen National Bureau of Standards (NBS), josta myöhemmin tuli National Institute of Standards and Technology (NIST) julkaisi avoimen pyynnön uuden salausalgoritmin luonnista. Vuonna 1974 IBM lähetti tätä tarkoitusta varten algoritmin, jota se kutsui nimellä LUCIFER. NBS välitti algoritmin National Security Agencylle (NSA), joka tutki algoritmin. NSA teki algoritmiin muutamia muutoksia, mutta niiden jälkeen Data Encryption Standard eli DES oli syntynyt. NBS julkaisi DES:in avoimella käyttölisenssillä vuonna 1975 ja vuonna 1977 NBS teki siitä virallisesti kansallisen standardin.

Data Encryption Standard on ollut laajasti käytössä sähköisessä kaupankäynnissä, esimerkiksi pankkialalla. Yleisesti sitä käytettiin niin, että käyttäjät lähettivät tarvittavan salausavaimen käyttäen jotakin julkisen avaimen salausta, kuten esimerkiksi RSA:ta ja tämän jälkeen käyttivät DES:iä varsinaisen lähetettävän datan salaukseen. Näin saavutettiin erittäin nopea salauksen käyttö, ilman että turvallisuus juurikaan vaarantui.

Data Encryption Standardilla on hyvin tärkeä paikka osana modernien salausmenetelmien historiaa. DES:sta johdettu 3DES, eli kolminkertainen DES on ollut käytössä vielä pitkään tavallisen DES:n käytön loppumisen jälkeenkin ja DES:n seuraajaksi kehitetty AES käyttää monia samoja kryptografian rakennuspalikoita kuin DES:kin.

Tässä työssä tutustuttiin Data Encryption Standardin toimintaan ja käyttöön. Työn pääasiallisena lähteenä käytettiin teosta Introduction to Cryptography with Coding Theory[1].

1 Data Encryption Standard

DES on niin kutsuttu Feistel-salaus eli lohkosalain, joka käsittelee salattavaa selvätekstiä tietyn pituisina lohkoina. DES:in tapauksessa tuo lohkopituus on 64 bittiä. Tämänkaltaisen lohkosalauksen hyvä puoli on se, että salaus ja salauksen purku ovat hyvin samankaltaisia, jopa lähes identtisiä. Sen vuoksi, kun luodaan tämän kaltaista algoritmia, vaadittavan koodauksen määrä on hyvin vähäinen. Feistel-verkot kehitti alunperin Horst Feistel kun hän työskenteli IBM:llä kehittäessään LUCIFER-algoritmia.

Lohkosalaajien ongelmana voidaan pitää sitä, että hyvin harvoin lähetettävä selkoteksti saadaan sovitettua käytettävän lohkon pituuteen. Tässä tapauksessa siis 64 bittiin. Tämän vuoksi lohkosalaajille on kehitetty eri toimintatapoja. Yleisesti käytössä on viisi tapaa: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) sekä Counter (CTR). Tässä työssä ei kuitenkaan paneuduta näiden toimintatapojen yksityiskohtiin. Yleisesti voidaan kuitenkin sanoa, että jokainen näistä käyttää samaa salausta, mutta niihin on integroitu lisäominaisuuksia, jotka parantavat turvallisuutta tai esimerkiksi mahdollistavat salauksen purun aloituksen ennen kuin koko lohko on vastaanotettu.

2 Yksinkertaistettu DES-tyyppinen algoritmi

Ennen varsinaista DES-algoritmia tutustutaan saman tyyppiseen algoritmiin, jolla on monia samoja ominaisuuksia kuin DES:lla, mutta se on huomattavasti yksinkertaisempi. Kuten DES niin myöskin tämä algoritmi on tyypiltään lohkopohjainen salausmenetelmä. Koska jokainen lohko salataan erikseen, niin voimme olettaa, että lähetettävä viestimme mahtuu yhteen lohkoon.

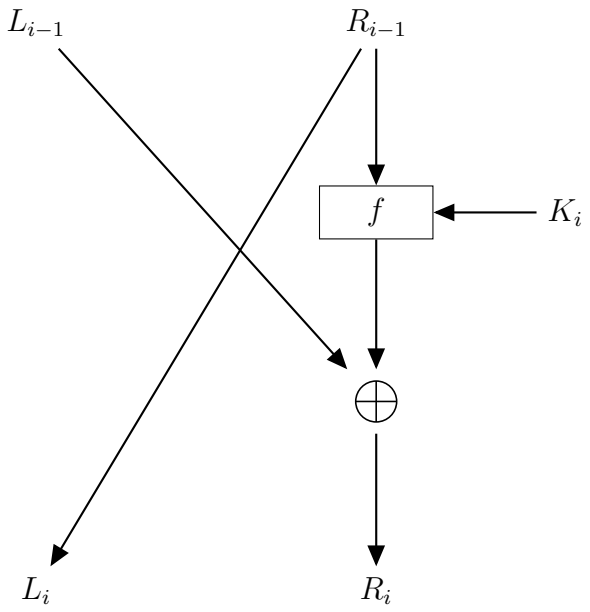
Selkokielinen viestimme m sisältää 12 bittiä ja se on kirjoitettu muodossa L_0R_0 siten, että L_0 sisältää ensimmäiset 6 bittiä ja R_0 loput 6 bittiä. Salausavaimessa K on 9 bittiä. Jokaisella kierroksella i algoritmi muuntaa syötteen $L_{i-1}R_{i-1}$ tulosteeksi L_iR_i käyttäen 8 bittistä salausavainta K_i, joka on johdettu avaimesta K.

Salauksen tärkein vaihe on funktio $f(R_{i-1}, K_i)$, joka ottaa syötteenä 6 bittisen merkkijonon R_{i-1} sekä 8 bittisen merkkijonon K_i ja tuottaa 6 bittisen tulosteen, joka kuvaillaan myöhemmässä vaiheessa.

Jokaisen kierroksen i tuloste määritellään seuraavasti

$$L_i = R_{i-1} \text{ ja } R_i = L_{i-1} \oplus f(R_{i-1}, K_i),$$

missä $\oplus$ on "poissulkeva tai", eli käytännössä bittikohtainen yhteenlasku mod 2. Tämä on esitetty Kuvassa 1. Kuvattua operaatiota toistetaan n kertaa, jolloin saadaan salattu viesti L_nR_n. Salauskierroksien määrä n on päätetty ennalta ja varsinaisessa DES-algoritmissä se on 16.



Kuva 1: Yksi kierros Feistel-pohjaisesta menetelmästä

Salatun viestin purkaminen aloitetaan kääntämällä L_nR_n toisinpäin jolloin saadaan R_nL_n. Seuraavaksi käytetään samaa menetelmää kuin edellä, mutta avaimia K_i käytetään käänteisessä järjestyksessä $K_n, \ldots, K_1$. Viestin avaaminen etenee siis seuraavasti: Ensimmäisen askeleen lähtöarvona käytetään merkkijonoa R_nL_n ja tulosteena saadaan

$$[L_n]\ [R_n \oplus f(L_n, K_n)].$$

Salausoperaation perusteella tiedämme, että $L_n = R_{n-1}$ ja $R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$, joten

$$\begin{aligned}
[L_n]\ [R_n \oplus f(L_n, K_n)] &= [R_{n-1}]\ [L_{n-1} \oplus f(R_{n-1}, K_n) \oplus f(L_n, K_n)] \\
&= [R_{n-1}]\ [L_{n-1} \oplus f(L_n, K_n) \oplus f(L_n, K_n)] \\
&= [R_{n-1}]\ [L_{n-1} \oplus 0] \\
&= [R_{n-1}]\ [L_{n-1}].
\end{aligned}$$

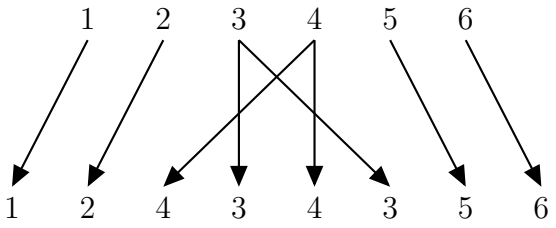
Vastaavasti toinen askel ottaa syötteenä merkkijonon $R_{n-1}L_{n-1}$ ja antaa tulosteena merkkijonon $R_{n-2}L_{n-2}$. Kun tätä jatketaan, niin huomataan, että

päädymme takaisin merkkijonoon R_0L_0 ja kun vielä vaihdamme siitä puolet keskenään niin saamme alkuperäisen selkokielisen viestin L_0R_0 kuten pitikin.

Salatun viestin avaaminen on käytännössä sama prosessi kuin viestin salaaminenkin, sillä erotuksella, että meidän pitää vaihtaa vasen ja oikea puoli keskenään ja käyttää avaimia K_i käänteisessä järjestyksessä. Näin ollen sekä lähettäjä, että vastaanottaja käyttävät yhteistä salausavainta ja he voivat käyttää samanlaista laitteistoa, kunhan vastaanottaja vaihtaa syötteen vasemman ja oikean puolen keskenään.

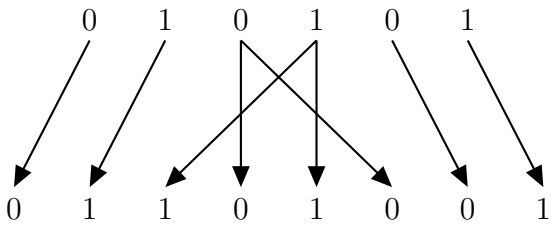
Perehdytään seuraavaksi funktioon f. Periaatteessa edellä kuvatut operaatiot voidaan suorittaa millä tahansa funktiolla f, mutta tietyt valinnat funktion luonnissa tekevät salauksesta turvallisemman. DES-algoritmissä käytettävä funktio on hyvin samantapainen kuin se mitä kuvataan seuraavaksi. Funktio rakentuu muutamasta osasta.

Ensimmäinen osa on laajennusfunktio. Laajennusfunktio ottaa 6 bittisen syötteen ja antaa 8 bittisen tulosteen. Tässä esimerkissä käytettävä laajentaja on annettu Kuvassa 2. Syötteen ensimmäisestä bitistä tulee tulosteen ensimmäinen bitti, kolmannesta bitistä tulee sekä neljäs, että kuudes bitti, ja niin edelleen.



Kuva 2: Laajennusfunktio E

Esimerkiksi syöte 010101 laajenee tulosteeksi 01101001 Kuvan 3 mukaisesti.



Kuva 3: Esimerkki laajennusfunktiosta

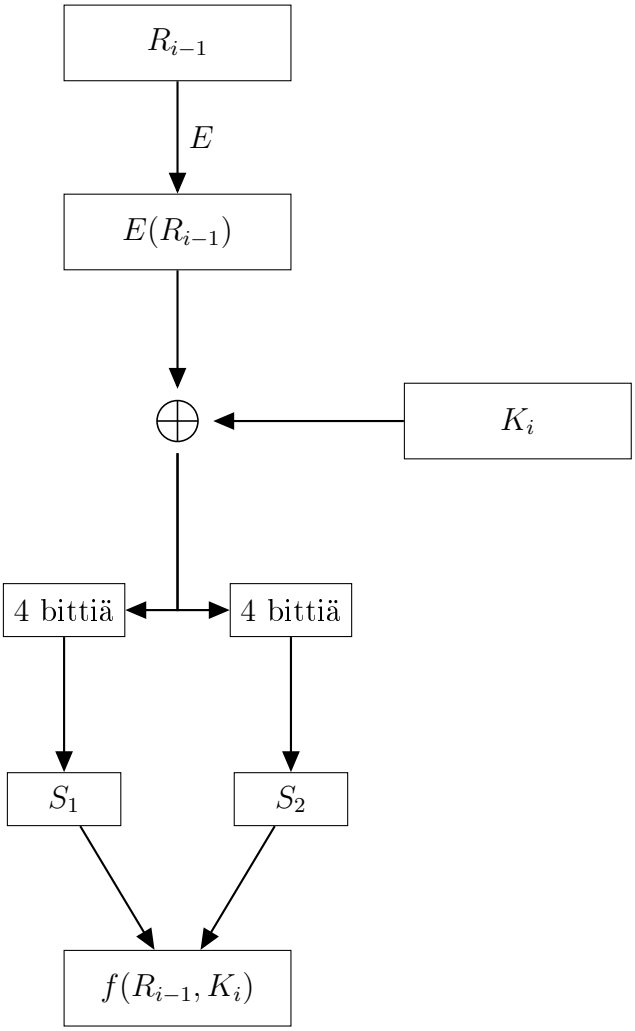
Pääkomponentteina funktiossa käytetään niin kutsuttuja S-laatikoita, joita tässä esimerkissä on kaksi. Ne on esitelty Taulukossa 1.

S_1	101	010	001	110	011	100	111	000
	001	100	110	010	000	111	101	011
S_2	100	000	110	101	111	001	011	010
	101	011	000	111	110	010	001	100

Taulukko 1: Esimerkkijärjestelmässä käytettävät S-laatikot

S-laatikon syöte koostuu neljästä bitistä. Ensimmäinen bitti määrää S-laatikon sisällä käytettävän rivin: 0 tarkoittaa ensimmäistä riviä ja 1 tarkoittaa toista riviä. Loput kolme bittiä määräävät käytettävän sarakkeen binäärinumerona: 000 tarkoittaa ensimmäistä saraketta, 001 toista, ... , 111 viimeistä saraketta. S-laatikon tulosteena saadaan syötettä vastaavan kohdan kolme bittiä. Esimerkiksi S_1-laatikon syöte 0011 viittaa ensimmäiseen riviin ja neljänteen sarakkeeseen, josta saadaan tulosteena 110.

Salausavain K koostuu yhdeksästä bitistä. Jokaisella salauksen kierroksella käytettävä salausavain K_i saadaan käyttämällä 8 bittiä salausavaimesta K siten, että aloitetaan aina i bitistä ja viimeisen bitin jälkeen siirrytään K:n ensimmäiseen bittiin. Esimerkiksi, jos $K = 001001111$, niin $K_5 = 01111001$, sillä viiden bitin jälkeen olemme käyttäneet viimeisen bitin K:sta ja loput kolme bittiä saamme jatkamalla K:n ensimmäisestä bitistä.



Kuva 4: Funktio $f(R_{i-1}, K_i)$

Nyt voimme määritellä funktion $f(R_{i-1}, K_i)$ seuraavasti. Syöte R_{i-1} koostuu kuuden bitin merkkijonosta. Laajennusfunktiota käytetään laajentamaan se kahdeksan bitin merkkijonoksi. Saatu kahdeksan bitin merkkijono ja K_i käsitellään aiemmin määritellyllä operaatiolla $\oplus$, jolloin tulosteena saadaan kahdeksan bittinen merkkijono. Saadun merkkijonon neljä ensimmäistä bittiä lähetetään S_1-laatikkoon ja loput neljä bittiä lähetetään S_2-laatikkoon. Kummastakin S-laatikosta saadaan tulosteena kolmen bitin merkkijono, jotka jälleen takaisin yhdistämällä saamme kuusi bittisen numeron, joka on

$f(R_{i-1}, K_i)$. Nämä tapahtumat on esitetty kaaviona Kuvassa 4.

Esimerkiksi, jos $i = 5$ ja $R_{i-1} = R_4 = 010101$, niin

$$E(R_{i-1}) = E(R_4) = E(010101) = 01101001$$

kuten Kuvassa 3 osoitettiin. Nyt jos $K_5 = 01111001$, kuten edellä, niin saadaan

$$\begin{array}{rr} & 01101001 \\ \oplus & 01111001 \\ \hline & 00010000 \end{array}$$

eli

$$E(R_4) \oplus K_5 = 01101001 \oplus 01111001 = 00010000.$$

Ensimmäiset neljä bittiä lähetetään S_1-laatikkoon ja loput neljä bittiä lähetetään S_2-laatikkoon. S_1-laatikkoon lähetetään bittijono 0001, joten sieltä valitaan ensimmäisen rivin toinen sarake,

S_1

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

joka antaa tulosteen 010. S_2-laatikkoon lähetetään bittijono 0000, joten sieltä valitaan ensimmäisen rivin ensimmäinen sarake,

S_2

100	000	110	101	111	001	011	010
101	011	000	111	110	010	001	100

joka antaa tulosteen 100. Kun nämä yhdistetään niin saadaan $f(R_4, K_5) = 010100$.

Nyt voimme kuvata, mitä yhdellä salauskierroksella tapahtuu. Mikäli syötteemme olisi esimerkiksi

$$L_4R_4 = 110011010101$$

ja $K_5 = 01111001$ kuten edelläkin, niin $R_4 = 010101$ kuten edellisessäkin esimerkissä ja siitä edelleen $f(R_4, K_5) = 010100$. Kun tämän ja bittijonon $L_4 = 110011$ välillä käytetään operaatiota $\oplus$, niin saadaan

$$\begin{array}{rr} & 010100 \\ \oplus & 110011 \\ \hline & 100111 \end{array}$$

eli

$$R_5 = L_4 \oplus f(R_4, K_5) = 010100 \oplus 110011 = 100111.$$

Lisäksi kun vielä tiedetään, että $L_5 = R_4$, niin saamme tulosteen

$$L_5 R_5 = 010101011000,$$

jota käytetään syötteenä seuraavalla kierroksella.

3 DES-algoritmi

Salattua viestiä kuvataan 64 bitin pituisilla jaksoilla. Salausavaimessa on 56 bittiä, mutta sitä kuvataan 64 bittisenä merkkijonona, sillä joka kahdeksas bitti on niin sanottu pariteetti-bitti. Pariteetti-bitit on järjestelty siten, että salausavaimen jokaisessa 8 bitin jaksossa on pariton määrä bitin arvoja 1. Pariteetti-bittien tarkoituksena on havaita mahdolliseet virheet salausavaimessa. Salauksen tulosteena saadaan 64 bittinen salattu viesti.

DES-algoritmi, joka esitellään kaaviona Kuvassa 5, alkaa 64 bitin pituisesta selkokielisestä viestistä m ja sisältää seuraavat kolme vaihetta:

1. Salattavan viestin m bitit permutoidaan muuttumattomalla alkupermutaatiolla IP, jotta saadaan $m_0 = IP(m)$. Tämän jälkeen m_0 jaetaan kahteen osaan siten, että L_0 sisältää m_0:n 32 ensimmäistä bittiä ja R_0 sen 32 viimeistä bittiä eli $m_0 = L_0R_0$.

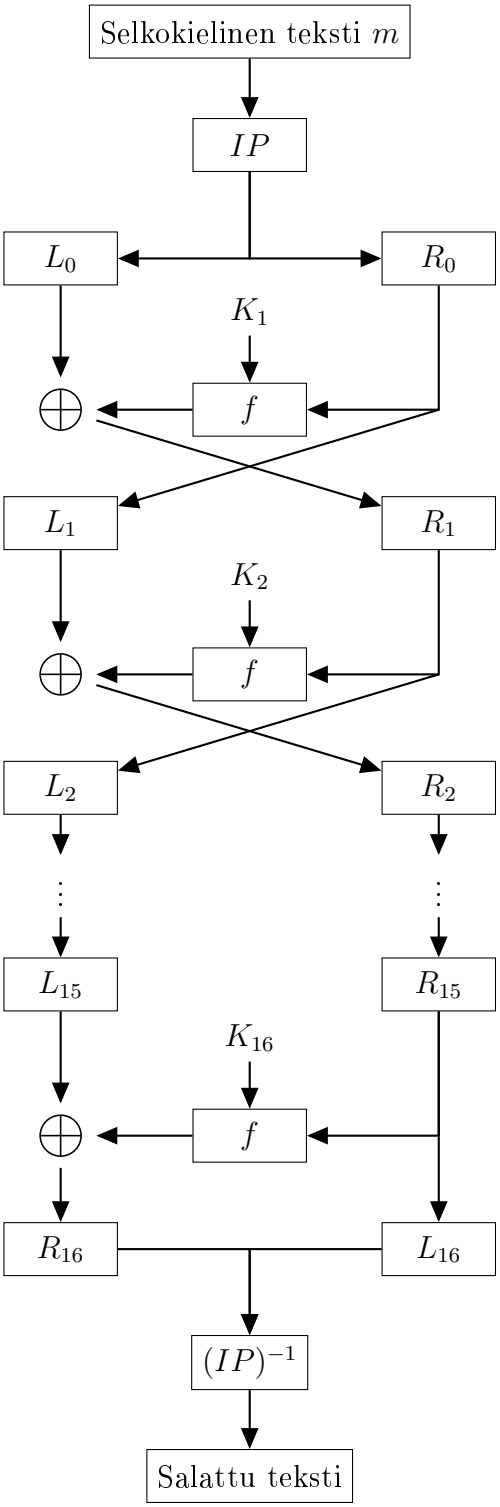
2. Kaikilla $1 \leq i \leq 16$

$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i),$$

   missä K_i on 48 bittinen merkkijono, joka on johdettu salausavaimesta K ja f on funktio, jota käsitellään hieman myöhemmin.

3. Vaihdetaan vasen ja oikea puoli keskenään, jotta saadaan $R_{16}L_{16}$. Suoritetaan vielä alkupermutaatio käänteisesti, jonka jälkeen saadaan salattu viesti $c = (IP)^{-1}(R_{16}L_{16})$.

Salatun viestin avaaminen tapahtuu täsmälleen samalla tavalla, mutta avaimia $K_1, ..., K_{16}$ käytetään käänteisessä järjestyksessä. Tämä toimii täsmälleen samaan tapaan kuin Luvussa 2 käsitelty yksinkertaistettu algoritmi, tosin sillä erotuksella, että puolten vaihto, joka kuvattiin DES-algoritmin vaiheessa 3, aiheuttaa sen, ettei yksinkertaisessa algoritmissa vaadittua puolten vaihtoa tarvitse erikseen tehdä salausta purettaessa.



Kuva 5: DES-algoritmi

Seuraavaksi käsitellään jokaista vaihetta hieman tarkemmin. Alkupermutaatiolla ei vaikuta olevan mitään vaikutusta itse salaukseen, vaan arvellaan, että se luotiin parantamaan algoritmin latautumistehokkuutta 1970-luvulla käytössä olleille mikrosiruille. Alkupermutaatio käyttää kiinteätä kaaviota, joka on kuvattu Taulukossa 2.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Taulukko 2: Alkupermutaatio IP

Tällä tarkoitetaan sitä, että selkokielisen viestin m bitistä 58 tulee m_0:n ensimmäinen bitti, m:n bitistä 50 tulee m_0:n toinen bitti, ja niin edelleen.

Funktio $f(R_{i-1}, K_i)$, jonka tapahtumat on esitetty kaaviona Kuvassa 6, voidaan jakaa useampaan eri vaiheeseen:

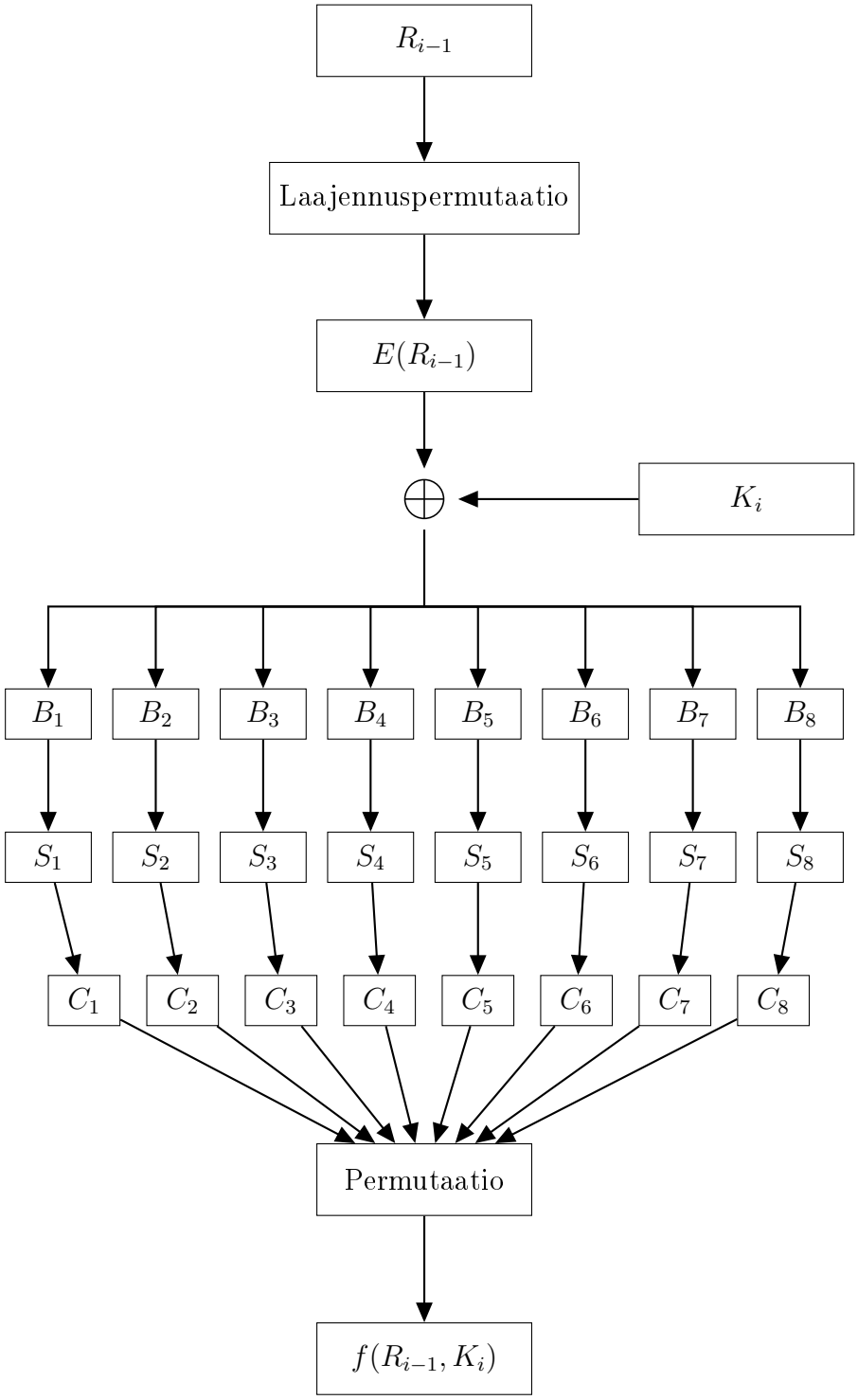
1. Aluksi R_{i-1} laajennetaan laajennuspermutaatiolla $E(R_{i-1})$ 48 bitin merkkijonoksi Taulukon 3 mukaisesti.

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Taulukko 3: Laajennuspermutaatio

   Tämä tarkoittaa sitä, että laajennuspermutaation $E(R_{i-1})$ ensimmäinen bitti on merkkijonon R_{i-1} bitti 32, laajennuspermutaation $E(R_{i-1})$ toinen bitti on merkkijonon R_{i-1} bitti 1, ja niin edelleen.

2. Lasketaan operaatio $E(R_{i-1}) \oplus K_i$, jossa on 48 bittiä ja jaetaan se 6 bitin pätkiinB_j: $B_1B_2 \cdots B_8$.



Kuva 6: DES-funktio $f(R_{i-1}, K_i)$

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Taulukko 4: S-laatikot $1-4$

3. DES käyttää kahdeksaa yksikertaisessa algoritmissa kuvaillun kaltaista S-laatikkoa. Jokainen 6 bitin merkkijono B_j toimii syötteenä laatikolle S_j. Kirjoitetaan B_j muodossa $B_j = b_1b_2b_3b_4b_5b_6$. Syötteen B_j ensimmäinen bitti b_1 sekä viimeinen bitti b_6 muodostavat merkkijonon b_1b_6, joka kertoo S-laatikossa käytettävän rivin. Bittien b_2, b_3, b_4 ja b_5 muodostama merkkijono $b_2b_3b_4b_5$ kertoo käytettävän sarakkeen. DES-algoritmissä käytettävät S-laatikot löytyvät Taulukoista 4 ja 5. Esimerkiksi, jos $B_3 = 001001$, niin käytämme laatikkoa S_3. Siitä valitsemme rivin 01, joka on toinen rivi, sillä 00 tarkoittaa ensimmäistä riviä. 0110 tarkoittaa saraketta 7, sillä binääriluku 0110 vasta lukua 6 ja ensimmäiseen sarakkeeseen viitataan luvulla 0, eli seitsemäs sarake vastaa lukua 6. Laatikosta S_3 saamme toiselta riviltä sarakkeesta seitsemän luvun 6, joka vastaa binäärilukua 0110. Näin ollen tässä tilanteessa S_3-laatikon

tuloste on $0110 = C_3$. Tähän tapaan saamme kahdeksan neljän bitin pituista merkkijonoa $C_1, C_2, \ldots, C_8$.

S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Taulukko 5: S-laatikot $5 - 8$

4. Merkkijonot $C_1, \ldots, C_8$ yhdistetään ja näin saatu merkkijono $C_1C_2 \ldots C_8$ permutoidaan Taulukon 6 mukaisesti. Permutaatio käsitellään samoin kuin aiemmatkin, eli bitistä 16 tulee permutaation jälkeen ensimmäinen bitti, bitistä 7 tulee toinen bitti ja niin edelleen. Permutaation seurauksena saatava merkkijono on $f(R_{i-1}, K_i)$.

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Taulukko 6: Permutaatio

Käsitellään vielä miten jokaisella kierroksella tarvittavat salausavaimet K_i johdetaan avaimesta K. Salausavainta K kuvataan 64 bittisellä merkkijonolla, kuten aiemmin todettiin. Yhdellä kierroksella tarvittavan salausavaimen K_i saamiseksi suoritetaan seuraavat vaiheet:

1. Parillisuusbitit jätetään pois ja jäljelle jäävät 56 bittiä permutoidaan Taulukon 7 mukaisesti. Bitistä 57 tulee permutaation jälkeen ensimmäinen bitti, bitistä 49 tulee toinen bitti ja niin edelleen.

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Taulukko 7: Salausavaimen permutaatio

   Saatu tulos kirjoitetaan muotoon C_0D_0 siten, että merkkijonoissa C_0 ja D_0 on kummassakin 28 bittiä.

2. Kaikilla $1 \leq i \leq 16$

$$C_i = LS_i(C_{i-1}),$$
$$D_i = LS_i(D_{i-1}),$$

   missä LS_i tarkoittaa syötteen jokaisen bitin siirtoa yhdellä tai kahdella bittipaikalla vasemmalle Taulukon 8 mukaisesti.

Kierros	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Siirto	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Taulukko 8: Salausavaimen bittien siirtojen lukumäärä jokaisella kierroksella

3. 56 bittisestä merkkijonosta C_iD_i valitaan 48 bittiä Taulukon 9 mukaisesti ja tulosteena saadaan K_i.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Taulukko 9: Permutaatio $C_iD_i \rightarrow K_i$

Osoittautuu, että jokaista salausavaimen K bittiä käytetään noin 14 kertaa 16 salauskierroksen aikana.

4 Esimerkkisalaus ja salauksen purku

Ajatellaan tilanne, jossa haluamme lähettää DES:llä salatun viestin vastaanottajalle. Viestin selkokielinen sisältö $m = Maisteri$. Olemme jo aiemmin sopineet vastaanottajan kanssa yhteisestä salausavaimesta

$$K = 01010010\ 01100001\ 01101101\ 01100001$$
$$01110101\ 01110011\ 00100000\ 01010100.$$

Salausavaimen jokaisessa 8 bitin jaksossa on pariton määrä bitin arvoja 1, joten se toteuttaa salausavaimelle aiemmin mainitun tarkistusehdon.

4.1 Salausavaimet

Aloitetaan luomalla K:n pohjalta jokaisella salauskierroksella tarvittavat avaimet $K_1, \ldots, K_{16}$.

1. Parillisuusbitit, eli joka kahdeksas bitti, jätetään pois. Loput käsitellään Taulukossa 7 esitetyllä salausavaimen permutaatiolla, jolloin merkkijonoksi C_0D_0 saadaan

   $$C_0D_0 = 0000000\ 0101111\ 1101111\ 1101011$$
   $$0010000\ 1100101\ 0000000\ 1000001,$$

   josta edelleen

   $$C_0 = 0000000\ 0101111\ 1101111\ 1101011\ \textbf{ja}$$
   $$D_0 = 0010000\ 1100101\ 0000000\ 1000001.$$

2. Luodaan merkkijonot $C_1, \ldots, C_{16}$ kuten kohdassa 2 sivulla 17 määriteltiin eli seuraava C_i tai D_i saadaan aina edellisestä siirtämällä bittejä Taulukon 8 mukaisesti. Näin saadaan merkkijonot $C_1, \ldots, C_{16}$, jotka on kerätty Taulukkoon 10.

C_1	0000000 1011111 1011111 1010110
C_2	0000001 0111111 0111111 0101100
C_3	0000101 1111101 1111101 0110000
C_4	0010111 1110111 1110101 1000000
C_5	1011111 1011111 1010110 0000000
C_6	1111110 1111110 1011000 0000010
C_7	1111011 1111010 1100000 0001011
C_8	1101111 1101011 0000000 0101111
C_9	1011111 1010110 0000000 1011111
C_{10}	1111110 1011000 0000010 1111110
C_{11}	1111010 1100000 0001011 1111011
C_{12}	1101011 0000000 0101111 1101111
C_{13}	0101100 0000001 0111111 0111111
C_{14}	0110000 0000101 1111101 1111101
C_{15}	1000000 0010111 1110111 1110101
C_{16}	0000000 0101111 1101111 1101011

Taulukko 10: Merkkijonot $C_1, \ldots, C_{16}$

Sekä merkkijonot $D_1, \ldots, D_{16}$, jotka on kerätty Taulukkoon 11.

D_1	0100001 1001010 0000001 0000010
D_2	1000011 0010100 0000010 0000100
D_3	0001100 1010000 0001000 0010010
D_4	0110010 1000000 0100000 1001000
D_5	1001010 0000001 0000010 0100001
D_6	0101000 0000100 0001001 0000110
D_7	0100000 0010000 0100100 0011001
D_8	0000000 1000001 0010000 1100101
D_9	0000001 0000010 0100001 1001010
D_{10}	0000100 0001001 0000110 0101000
D_{11}	0010000 0100100 0011001 0100000
D_{12}	1000001 0010000 1100101 0000000
D_{13}	0000100 1000011 0010100 0000010
D_{14}	0010010 0001100 1010000 0001000
D_{15}	1001000 0110010 1000000 0100000
D_{16}	0010000 1100101 0000000 1000001

Taulukko 11: Merkkijonot $D_1, \ldots, D_{16}$

Kun nämä merkkijonot yhdistetään pareittain saadaan merkkijonot $C_1D_1, \ldots, C_{16}D_{16}$, joista esimerkkinä

$$\begin{aligned} C_1D_1 \ &= 0000000\ 1011111\ 1011111\ 1010110 \\ &\quad\ 0100001\ 1001010\ 0000001\ 0000010. \end{aligned}$$

3. Jokaisesta 56 bittisestä merkkijonosta C_iD_i valitaan 48 bittiä Taulukon 9 mukaisesti ja tulosteena saadaan K_i. Tämä toistetaan jokaiselle merkkijonolle $C_1D_1, \ldots, C_{16}D_{16}$, jolloin saadaan merkkijonot $K_1, \ldots, K_{16}$, eli salauksessa käytettävät avaimet. Salausavaimet $K_1, \ldots, K_{16}$ on koottu Taulukkoon12.

K_1	11110000 10110110 11001110 10000110 00000110 00000100
K_2	11100000 00111110 10110110 00000001 00010000 10000010
K_3	11110100 10111110 01110000 01000100 00100000 00100101
K_4	11000110 11110110 01110010 00100010 00001000 11001100
K_5	11101110 11010111 01010110 00000000 10010001 10010011
K_6	01101110 11010011 01001011 00000111 00000100 00100001
K_7	00101011 11010001 01111011 01001010 00001001 01000000
K_8	10101101 01001001 11011011 00000000 11000001 00011100
K_9	00011111 01010011 11011010 10000100 00001100 01001000
K_{10}	00111110 01011001 11001101 00001000 10110010 01010000
K_{11}	00011011 01101001 01001101 00110001 11000100 00100000
K_{12}	00001001 01101101 10111101 00001000 00001100 00000010
K_{13}	11010101 00101101 10101101 10001100 01100000 00010100
K_{14}	11010011 10101110 10100001 00100001 01000010 11000000
K_{15}	11011001 10111110 10100110 10010000 10000000 00000011
K_{16}	10100001 10101110 00101110 00110001 00000001 00011100

Taulukko 12: Salausavaimet $K_1, \ldots, K_{16}$

4.2 Viestin salaus

Esimerkkinä suoritettua DES-salausta varten kirjoitin Python-kielellä koodin, joka suoritti salauksen ja tulosti tarvittavan LaTeX-koodin. Kirjoittamani koodi koostuu kahdesta osasta, joista ensimmäinen suorittaa alkupermutaation ja toinen varsinaisen salauksen kierrokset 1-16. Nämä koodit löytyvät kohdista 6.1 ja 6.2.

Viestin lähettäjä ja vastaanottaja ovat sopineet ennakkoon jokaiselle kirjaimelle käytettävästä 8-bittisestä merkinnästä ja näiden avulla salattava viesti $m = Maisteri$ muunnetaan bittijonoksi seuraavasti:

M	01001101	t	01110100
a	01100001	e	01100101
i	01101001	r	01110010
s	01110011	i	01101001

Näin saadaan salattava viesti

$m = 01001101\ 01100001\ 01101001\ 01110011\ 01110100\ 01100101\ 01110010\ 01101001.$

Varsinaisessa salauksessa on kolme vaihetta:

1. Salaus aloitetaan alkupermutaatiolla IP, joka kuvailtiin sivulla 13 sekä Taulukossa 2. Näin saadaan m_0.

   $$\begin{aligned} m_0 &= IP(m) \\ &= 1111111101011000001100011010111100000000111111101000010101001000 \end{aligned}$$

   Kun m_0 jaetaan kahteen 32:n bitin osaan saadaan L_0 ja R_0, sillä $m_0 = L_0R_0$, kuten todettiin kohdassa 1 sivulla 11. Näin ollen saadaan

   $$\begin{aligned} L_0 &= 11111111010110000011000110101111 \text{ ja} \\ R_0 &= 00000000111111101000010101001000. \end{aligned}$$

2. Kaikilla $1 \leq i \leq 16$

   $$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i), \end{aligned}$$

   kuten todettiin kohdassa 2 sivulla 11. Käsitellään esimerkin omaisesti ensimmäinen kierros, eli kun $i = 1$. Suoraan määritelmän mukaan saadaan, että

   $$L_1 = R_0 = 00000000111111101000010101001000.$$

   Merkkijonon R_1 ratkaisu puolestaan vaatii useamman vaiheen:

(a) R_0 operoidaan laajennuspermutaatiolla, joka käsiteltiin kohdassa 1 sivulla 13. Näin saadaan 48 bittinen merkkijono

$$E(R_0) = 000000000001011111111101010000001010101001010000.$$

(b) Lasketaan operaatio $E(R_0) \oplus K_1$.

$$\begin{array}{rl} & 000000000001011111111101010000001010101001010000 \\ \oplus & 111100001011011011001110100001100000011000000100 \\ \hline & 111100001010000100110011110001101010110001010100 \end{array}$$

Saatu merkkijono jaetaan 6 bitin pätkiin $B_1, \ldots, B_8$.

$B_1 = 111100$	$B_2 = 001010$	$B_3 = 000100$	$B_4 = 110011$
$B_5 = 110001$	$B_6 = 101010$	$B_7 = 110001$	$B_8 = 010100$

(c) Jokainen B_i toimii syötteenä S-laatikolle S_i kuten kohdassa 3 sivulla 15 määriteltiin. Käsitellään näistä jokainen vuorollaan. $B_1 = 111100$ tarkoittaa S_1-laatikon riviä 10 eli 3 ja saraketta 1110 eli 15.

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-laatikosta tulosteena saadaan luku 5 eli binäärinä neljää bittiä käyttäen 0101. Tätä tulostetta merkitään $C_1 = 0101$. Käsitellään loput vastaavasti. $B_2 = 001010$ eli rivi 00 ja sarake 0101.

S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Joten tulosteena saadaan luku 11 eli binäärinä $1011 = C_2$. $B_3 = 000100$ eli rivi 00 ja sarake 0010.

S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Tulosteena saadaan 9 eli binäärinä 1001 = C_3. B_4 = 110011 eli rivi 11 ja sarake 1001.

S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Tulosteena saadaan 4 eli binäärinä 0100 = C_4. B_5 = 110001 eli rivi 11 ja sarake 1000.

S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Tulosteena saadaan 6 eli binäärinä 0110 = C_5. B_6 = 101010 eli rivi 10 ja sarake 0101.

S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Tulosteena saadaan 8 eli binäärinä 1000 = C_6. B_7 = 110001 eli rivi 11 ja sarake 1000.

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	(9)	5	0	15	14	2	3	12

Tulosteena saadaan 9 eli binäärinä $1001 = C_7$. $B_8 = 010100$ eli rivi 00 ja sarake 1010.

S_8	13	2	8	4	6	15	11	1	10	9	(3)	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tulosteena saadaan 3 eli binäärinä $0011 = C_8$.

(d) Saadut merkkijonot $C_1, \ldots, C_8$ yhdistetään merkkijonoksi

$$C_1C_2C_3C_4C_5C_6C_7C_8 = 0101\ 1011\ 1001\ 0100\ 0110\ 1000\ 1001\ 0011,$$

joka permutoidaan Taulukon 6 mukaisesti ja näin saadaan merkkijono

$$f(R_0, K_1) = 01010110000011101101100110000011.$$

Nyt voimme ratkaista operaation $R_1 = L_0 \oplus f(R_0, K_1)$:

$$\begin{array}{rl} & 11111111010110000011000110101111 \\ \oplus & 01010110000011101101100110000011 \\ \hline & 10101001010101101111010000010 1100 \end{array}.$$

joten $R_1 = 10101001010101101111010000010 1100$. Aiemmin määritimme, että $L_1 = 00000000111111101000010101001000$, joten olemme suorittaneet yhden kierroksen salausta ja voimme jatkaa saatujen arvojen avulla seuraavalle kierrokselle kunnes saamme ratkaistua parin $L_{16}R_{16}$.

Kierros 2, eli kun $i = 2$:

Edelliseltä kierrokselta meillä on

$$R_1 = 10101001010101101110100000101100,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_1) = 01010101001010101010110101110101000000101011001.$$

Käytettävä salausavain

$$K_2 = 11100000001111101011011000000001000100001000000 10$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_1) \oplus K_2 &= 10110101000101000001101101110100000100011101 1011 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 101101 \xrightarrow{S_1} 0001 = C_1 & B_2 &= 010001 \xrightarrow{S_2} 1100 = C_2 \\ B_3 &= 010000 \xrightarrow{S_3} 0001 = C_3 & B_4 &= 011011 \xrightarrow{S_4} 1010 = C_4 \\ B_5 &= 011101 \xrightarrow{S_5} 1000 = C_5 & B_6 &= 000001 \xrightarrow{S_6} 1010 = C_6 \\ B_7 &= 000111 \xrightarrow{S_7} 0111 = C_7 & B_8 &= 011011 \xrightarrow{S_8} 1110 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 00011100000110101000101001111110,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_1, K_2) = 00011111011110100000010001110010.$$

Seuraavaksi ratkaisemme operaation

$$R_2 = L_1 \oplus f(R_1, K_2) = 00011111100001001000000100111010.$$

Kun vielä muistamme, että

$$L_2 = R_1 = 10101001010101101110100000101100,$$

niin olemme ratkaisseet merkkijonot L_2 ja R_2, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 3, eli kun $i = 3$:

Edelliseltä kierrokselta meillä on

$$R_2 = 00011111100001001000000100111010,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_2) = 000011111111110000001001010000000010100111110100.$$

Käytettävä salausavain

$$K_3 = 111101001011111001110000010001000010000000100101$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_2) \oplus K_3 &= 111110110100001001111001000001000000100111010001 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 111110 \xrightarrow{S_1} 0001 = C_1 & \qquad B_2 &= 110100 \xrightarrow{S_2} 1100 = C_2 \\ B_3 &= 001001 \xrightarrow{S_3} 0011 = C_3 & \qquad B_4 &= 111001 \xrightarrow{S_4} 1100 = C_4 \\ B_5 &= 000001 \xrightarrow{S_5} 1110 = C_5 & \qquad B_6 &= 000000 \xrightarrow{S_6} 1100 = C_6 \\ B_7 &= 100111 \xrightarrow{S_7} 1000 = C_7 & \qquad B_8 &= 010001 \xrightarrow{S_8} 1100 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 00011100001111001110110010001100,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_2, K_3) = 00011101000011000001000011111111.$$

Seuraavaksi ratkaisemme operaation

$$R_3 = L_2 \oplus f(R_2, K_3) = 10110100010110101111100011010011.$$

Kun vielä muistamme, että

$$L_3 = R_2 = 00011111100001001000000100111010,$$

niin olemme ratkaisseet merkkijonot L_3 ja R_3, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 4, eli kun $i = 4$:

Edelliseltä kierrokselta meillä on

$$R_3 = 10110100010110101111100011010011,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_3) = 110110101000001011110101011111110001011010100111.$$

Käytettävä salausavain

$$K_4 = 110001101111011001110010001000100000100011001100$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_3) \oplus K_4 &= 000111000111010010000111010111010001111001101011 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$B_1 = 000111 \xrightarrow{S_1} 0100 = C_1 \qquad B_2 = 000111 \xrightarrow{S_2} 0111 = C_2$$
$$B_3 = 010010 \xrightarrow{S_3} 1101 = C_3 \qquad B_4 = 000111 \xrightarrow{S_4} 0101 = C_4$$
$$B_5 = 010111 \xrightarrow{S_5} 1010 = C_5 \qquad B_6 = 010001 \xrightarrow{S_6} 0110 = C_6$$
$$B_7 = 111001 \xrightarrow{S_7} 1110 = C_7 \qquad B_8 = 101011 \xrightarrow{S_8} 1010 = C_8 \quad .$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01000111110101011010011011101010,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_3, K_4) = 11001101001100111101010110011001.$$

Seuraavaksi ratkaisemme operaation

$$R_4 = L_3 \oplus f(R_3, K_4) = 11010010101101110101010010100011.$$

Kun vielä muistamme, että

$$L_4 = R_3 = 10110100010110101111100011010011,$$

niin olemme ratkaisseet merkkijonot L_4 ja R_4, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 5, eli kun $i = 5$:

Edelliseltä kierrokselta meillä on

$$R_4 = 11010010101101110101010010100011,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_4) = 111010100101010110101110101010100101010100000111.$$

Käytettävä salausavain

$$K_5 = 111011101101011101010110000000001001000110010011$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_4) \oplus K_5 &= 000001001000001011111000101010100000010010010100 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1 B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 000001 \xrightarrow{S_1} 0001 = C_1 & \qquad B_2 &= 001000 \xrightarrow{S_2} 0110 = C_2 \\ B_3 &= 001011 \xrightarrow{S_3} 0100 = C_3 & \qquad B_4 &= 111000 \xrightarrow{S_4} 0101 = C_4 \\ B_5 &= 101010 \xrightarrow{S_5} 1101 = C_5 & \qquad B_6 &= 100000 \xrightarrow{S_6} 1001 = C_6 \\ B_7 &= 010010 \xrightarrow{S_7} 1100 = C_7 & \qquad B_8 &= 010100 \xrightarrow{S_8} 0011 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 00010110010001011101100111000011,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_4, K_5) = 11110001000101110011100000010011.$$

Seuraavaksi ratkaisemme operaation

$$R_5 = L_4 \oplus f(R_4, K_5) = 01000101010011011100000011000000.$$

Kun vielä muistamme, että

$$L_5 = R_4 = 11010010101101110101010010100011,$$

niin olemme ratkaisseet merkkijonot L_5 ja R_5, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 6, eli kun $i = 6$:

Edelliseltä kierrokselta meillä on

$$R_5 = 01000101010011011100000011000000,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_5) = 001000001010101001011011111000000001011000000000.$$

Käytettävä salausavain

$$K_6 = 011011101101001101001011000001110000010000100001$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_5) \oplus K_6 &= 010011100111100100010000111001110001001000100001 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 010011 \xrightarrow{S_1} 0110 = C_1 & B_2 &= 100111 \xrightarrow{S_2} 0001 = C_2 \\ B_3 &= 100100 \xrightarrow{S_3} 0100 = C_3 & B_4 &= 010000 \xrightarrow{S_4} 0001 = C_4 \\ B_5 &= 111001 \xrightarrow{S_5} 1010 = C_5 & B_6 &= 110001 \xrightarrow{S_6} 1011 = C_6 \\ B_7 &= 001000 \xrightarrow{S_7} 1111 = C_7 & B_8 &= 100001 \xrightarrow{S_8} 0010 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01100001010000011010101111110010,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_5, K_6) = 10010011001100111110011010000001.$$

Seuraavaksi ratkaisemme operaation

$$R_6 = L_5 \oplus f(R_5, K_6) = 01000001100001001011001000100010.$$

Kun vielä muistamme, että

$$L_6 = R_5 = 01000101010011011100000011000000,$$

niin olemme ratkaisseet merkkijonot L_6 ja R_6, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 7, eli kun $i = 7$:

Edelliseltä kierrokselta meillä on

$$R_6 = 01000001100001001011001000100010,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_6) = 00100000001111000000100101011010010000010000010 0.$$

Käytettävä salausavain

$$K_7 = 00101011110100010111101101001010000010010100000 0$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_6) \oplus K_7 &= 00001011111011010111001000010000010010000100010 0 \\ &= B_1 B_2 \ldots B_8. \end{aligned}$$

Saatu merkkijono $B_1 B_2 \ldots B_8$ jaetaan 6 bitin pätkiin $B_1, \ldots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$B_1 = 000010 \xrightarrow{S_1} 0100 = C_1 \qquad B_2 = 111110 \xrightarrow{S_2} 1111 = C_2$$

$$B_3 = 110101 \xrightarrow{S_3} 1110 = C_3 \qquad B_4 = 110010 \xrightarrow{S_4} 0001 = C_4$$

$$B_5 = 000100 \xrightarrow{S_5} 0100 = C_5 \qquad B_6 = 000100 \xrightarrow{S_6} 1010 = C_6$$

$$B_7 = 100001 \xrightarrow{S_7} 0110 = C_7 \qquad B_8 = 000100 \xrightarrow{S_8} 1000 = C_8 \quad .$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01001111111000010100101001101000,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_6, K_7) = 11011000001111011100010100010100.$$

Seuraavaksi ratkaisemme operaation

$$R_7 = L_6 \oplus f(R_6, K_7) = 10011101011100000000010111010100.$$

Kun vielä muistamme, että

$$L_7 = R_6 = 01000001100001001011001000100010,$$

niin olemme ratkaisseet merkkijonot L_7 ja R_7, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 8, eli kun $i = 8$:

Edelliseltä kierrokselta meillä on

$$R_7 = 10011101011100000000010111010100,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_7) = 01001111101010111010000000000000101111101010 1001.$$

Käytettävä salausavain

$$K_8 = 10101101010010011101101100000000110000010001 1100$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_7) \oplus K_8 &= 11100010111000100111101100000000011111111011 0101 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$B_1 = 111000 \xrightarrow{S_1} 0011 = C_1 \qquad B_2 = 101110 \xrightarrow{S_2} 0001 = C_2$$
$$B_3 = 001001 \xrightarrow{S_3} 0011 = C_3 \qquad B_4 = 111011 \xrightarrow{S_4} 0111 = C_4$$
$$B_5 = 000000 \xrightarrow{S_5} 0010 = C_5 \qquad B_6 = 000111 \xrightarrow{S_6} 0010 = C_6$$
$$B_7 = 111110 \xrightarrow{S_7} 0010 = C_7 \qquad B_8 = 110101 \xrightarrow{S_8} 1001 = C_8 \quad .$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 00110001001101110010001000101001,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_7, K_8) = 10001100011000000101111010000110.$$

Seuraavaksi ratkaisemme operaation

$$R_8 = L_7 \oplus f(R_7, K_8) = 11001101111001001110110010100100.$$

Kun vielä muistamme, että

$$L_8 = R_7 = 10011101011100000000010111010100,$$

niin olemme ratkaisseet merkkijonot L_8 ja R_8, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 9, eli kun $i = 9$:

Edelliseltä kierrokselta meillä on

$$R_8 = 11001101111001001110110010100100,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_8) = 01100101101111110000100101110101100101010000 1001.$$

Käytettävä salausavain

$$K_9 = 000111110101001111011010100010000001100010010000$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_8) \oplus K_9 &= 011110101110110011010011111100011001100101000001 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1 B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 011110 \xrightarrow{S_1} 0111 = C_1 & B_2 &= 101110 \xrightarrow{S_2} 0001 = C_2 \\ B_3 &= 110011 \xrightarrow{S_3} 1111 = C_3 & B_4 &= 010011 \xrightarrow{S_4} 0111 = C_4 \\ B_5 &= 111100 \xrightarrow{S_5} 0001 = C_5 & B_6 &= 011001 \xrightarrow{S_6} 0001 = C_6 \\ B_7 &= 100101 \xrightarrow{S_7} 1101 = C_7 & B_8 &= 000001 \xrightarrow{S_8} 0001 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01110001111101110001000111010001,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_8, K_9) = 10100110010100011111101100000111.$$

Seuraavaksi ratkaisemme operaation

$$R_9 = L_8 \oplus f(R_8, K_9) = 00111011001000011111111011010011.$$

Kun vielä muistamme, että

$$L_9 = R_8 = 11001101111001001110110010100100,$$

niin olemme ratkaisseet merkkijonot L_9 ja R_9, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 10, eli kun $i = 10$:

Edelliseltä kierrokselta meillä on

$$R_9 = 00111011001000011111111011010011,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_9) = 100111110110100100000011111111111101011010100110.$$

Käytettävä salausavain

$$K_{10} = 001111100101100111001101000010001011001001010000$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_9) \oplus K_{10} &= 101000010011000011001110111101110110010011110110 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 101000 \xrightarrow{S_1} 1101 = C_1 & B_2 &= 010011 \xrightarrow{S_2} 0001 = C_2 \\ B_3 &= 000011 \xrightarrow{S_3} 0111 = C_3 & B_4 &= 001110 \xrightarrow{S_4} 1010 = C_4 \\ B_5 &= 111101 \xrightarrow{S_5} 0101 = C_5 & B_6 &= 110110 \xrightarrow{S_6} 1010 = C_6 \\ B_7 &= 010011 \xrightarrow{S_7} 0011 = C_7 & B_8 &= 110110 \xrightarrow{S_8} 1101 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 11010001011110100101101000111101,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_9, K_{10}) = 00111110111001011100110001100110.$$

Seuraavaksi ratkaisemme operaation

$$R_{10} = L_9 \oplus f(R_9, K_{10}) = 11110011000000010010000011000010.$$

Kun vielä muistamme, että

$$L_{10} = R_9 = 00111011001000011111111011010011,$$

niin olemme ratkaisseet merkkijonot L_{10} ja R_{10}, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 11, eli kun $i = 11$:

Edelliseltä kierrokselta meillä on

$$R_{10} = 11110011000000010010000011000010,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_{10}) = 011110100110100000000010100100000001011000000101.$$

Käytettävä salausavain

$$K_{11} = 000110110110100101001101001100011100010000100000$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_{10}) \oplus K_{11} &= 011000010000000101001111101000011101001000100101 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 011000 \xrightarrow{S_1} 0101 = C_1 & \qquad B_2 &= 010000 \xrightarrow{S_2} 1001 = C_2 \\ B_3 &= 000101 \xrightarrow{S_3} 0001 = C_3 & \qquad B_4 &= 001111 \xrightarrow{S_4} 0011 = C_4 \\ B_5 &= 101000 \xrightarrow{S_5} 1010 = C_5 & \qquad B_6 &= 011101 \xrightarrow{S_6} 0011 = C_6 \\ B_7 &= 001000 \xrightarrow{S_7} 1111 = C_7 & \qquad B_8 &= 100101 \xrightarrow{S_8} 1110 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01011001000100111010001111111110,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_{10}, K_{11}) = 10001111011110101110010010100011.$$

Seuraavaksi ratkaisemme operaation

$$R_{11} = L_{10} \oplus f(R_{10}, K_{11}) = 10110100010110110001101001110000.$$

Kun vielä muistamme, että

$$L_{11} = R_{10} = 11110011000000010010000011000010,$$

niin olemme ratkaisseet merkkijonot L_{11} ja R_{11}, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 12, eli kun $i = 12$:

Edelliseltä kierrokselta meillä on

$$R_{11} = 10110100010110110001101001110000,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_{11}) = 01011010100000101111011010001111010000111010000 1.$$

Käytettävä salausavain

$$K_{12} = 000010010110110110111101000010000000110000000010$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_{11}) \oplus K_{12} &= 010100111110111101001011100001110100111110100011 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$B_1 = 010100 \xrightarrow{S_1} 0110 = C_1 \qquad B_2 = 111110 \xrightarrow{S_2} 1111 = C_2$$
$$B_3 = 111101 \xrightarrow{S_3} 0010 = C_3 \qquad B_4 = 001011 \xrightarrow{S_4} 1111 = C_4$$
$$B_5 = 100001 \xrightarrow{S_5} 1011 = C_5 \qquad B_6 = 110100 \xrightarrow{S_6} 0100 = C_6$$
$$B_7 = 111110 \xrightarrow{S_7} 0010 = C_7 \qquad B_8 = 100011 \xrightarrow{S_8} 0001 = C_8 \quad .$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01101111001011111011010000100001,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_{11}, K_{12}) = 11100001010010001101111011011100.$$

Seuraavaksi ratkaisemme operaation

$$R_{12} = L_{11} \oplus f(R_{11}, K_{12}) = 00010010010010011111111000011110.$$

Kun vielä muistamme, että

$$L_{12} = R_{11} = 10110100010110110001101001110000,$$

niin olemme ratkaisseet merkkijonot L_{12} ja R_{12}, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 13, eli kun $i = 13$:

Edelliseltä kierrokselta meillä on

$$R_{12} = 00010010010010011111111000011110,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_{12}) = 000010100100001001010011111111111100000011111100.$$

Käytettävä salausavain

$$K_{13} = 110101010010110110101101100011000110000000010100$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_{12}) \oplus K_{13} &= 110111110110111111111100111001110100000111010 00 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1 B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 110111 \xrightarrow{S_1} 1110 = C_1 & B_2 &= 110110 \xrightarrow{S_2} 0110 = C_2 \\ B_3 &= 111111 \xrightarrow{S_3} 1100 = C_3 & B_4 &= 111110 \xrightarrow{S_4} 0100 = C_4 \\ B_5 &= 011100 \xrightarrow{S_5} 1110 = C_5 & B_6 &= 111010 \xrightarrow{S_6} 1101 = C_6 \\ B_7 &= 000011 \xrightarrow{S_7} 0001 = C_7 & B_8 &= 101000 \xrightarrow{S_8} 1001 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 11100110110001001110110100011001,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_{12}, K_{13}) = 01011011100001011011101110011000.$$

Seuraavaksi ratkaisemme operaation

$$R_{13} = L_{12} \oplus f(R_{12}, K_{13}) = 11101111110111101010000111101000.$$

Kun vielä muistamme, että

$$L_{13} = R_{12} = 00010010010010011111111000011110,$$

niin olemme ratkaisseet merkkijonot L_{13} ja R_{13}, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 14, eli kun $i = 14$:

Edelliseltä kierrokselta meillä on

$$R_{13} = 11101111110111101010000111101000,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_{13}) = 011101011111111011111101010100000011111101010001.$$

Käytettävä salausavain

$$K_{14} = 110100111010111010100001001000010100001011000000$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_{13}) \oplus K_{14} &= 101001100101000001011100011100010111110110010001 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 101001 \xrightarrow{S_1} 0100 = C_1 & B_2 &= 100101 \xrightarrow{S_2} 1010 = C_2 \\ B_3 &= 000001 \xrightarrow{S_3} 1101 = C_3 & B_4 &= 011100 \xrightarrow{S_4} 0100 = C_4 \\ B_5 &= 011100 \xrightarrow{S_5} 1110 = C_5 & B_6 &= 010111 \xrightarrow{S_6} 1110 = C_6 \\ B_7 &= 110110 \xrightarrow{S_7} 1000 = C_7 & B_8 &= 010001 \xrightarrow{S_8} 1100 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01001010110101001110111010001100,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_{13}, K_{14}) = 01011101001011011001000110101001.$$

Seuraavaksi ratkaisemme operaation

$$R_{14} = L_{13} \oplus f(R_{13}, K_{14}) = 01001111011001000110111110110111.$$

Kun vielä muistamme, että

$$L_{14} = R_{13} = 11101111110111101010000111101000,$$

niin olemme ratkaisseet merkkijonot L_{14} ja R_{14}, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 15, eli kun $i = 15$:

Edelliseltä kierrokselta meillä on

$$R_{14} = 01001111011001000110111110110111,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_{14}) = 10100101111010110000100000110101111111010110101110.$$

Käytettävä salausavain

$$K_{15} = 11011001101111101010011010010000100000000000011$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_{14}) \oplus K_{15} &= 01111100010101011010111010100101011111010110101101 \\ &= B_1B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$\begin{aligned} B_1 &= 011111 \xrightarrow{S_1} 1000 = C_1 & \qquad B_2 &= 000101 \xrightarrow{S_2} 0100 = C_2 \\ B_3 &= 010110 \xrightarrow{S_3} 0111 = C_3 & \qquad B_4 &= 101110 \xrightarrow{S_4} 1101 = C_4 \\ B_5 &= 101001 \xrightarrow{S_5} 0001 = C_5 & \qquad B_6 &= 010111 \xrightarrow{S_6} 1110 = C_6 \\ B_7 &= 110110 \xrightarrow{S_7} 1000 = C_7 & \qquad B_8 &= 101101 \xrightarrow{S_8} 1000 = C_8 \quad . \end{aligned}$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 10000100011111010001111010001000,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_{14}, K_{15}) = 10111100101000010001000001011101.$$

Seuraavaksi ratkaisemme operaation

$$R_{15} = L_{14} \oplus f(R_{14}, K_{15}) = 01010011011111111011000110110101.$$

Kun vielä muistamme, että

$$L_{15} = R_{14} = 01001111011001000110111110110111,$$

niin olemme ratkaisseet merkkijonot L_{15} ja R_{15}, joiden avulla jatkamme seuraavalle salauskierrokselle.

Kierros 16, eli kun $i = 16$:

Edelliseltä kierrokselta meillä on

$$R_{15} = 01010011011111111011000110110101,$$

joka operoidaan kohdassa 1 sivulla 13 käsitellyllä laajennuspermutaatiolla. Laajennuspermutaatiolla saadaan

$$E(R_{15}) = 10101010011010111111111111011010001111011010101010.$$

Käytettävä salausavain

$$K_{16} = 101000011010111000101110001100010000000100011100$$

poimitaan Taulukosta 12 ja tämän jälkeen lasketaan operaatio

$$\begin{aligned} E(R_{15}) \oplus K_{16} &= 000010111100010111010001111010110011110010110110 \\ &= B_1 B_2 \dots B_8. \end{aligned}$$

Saatu merkkijono $B_1B_2 \dots B_8$ jaetaan 6 bitin pätkiin $B_1, \dots, B_8$. Merkkijonojen B_i sekä laatikoiden S_i avulla saamme muodostettua merkkijonot C_i aivan kuten kierroksella 1. Merkkijonot muodostuvat seuraavasti:

$$B_1 = 000010 \xrightarrow{S_1} 0100 = C_1 \qquad B_2 = 111100 \xrightarrow{S_2} 0010 = C_2$$
$$B_3 = 010111 \xrightarrow{S_3} 1110 = C_3 \qquad B_4 = 010001 \xrightarrow{S_4} 0100 = C_4$$
$$B_5 = 111010 \xrightarrow{S_5} 0011 = C_5 \qquad B_6 = 110011 \xrightarrow{S_6} 1110 = C_6$$
$$B_7 = 110010 \xrightarrow{S_7} 1111 = C_7 \qquad B_8 = 110110 \xrightarrow{S_8} 1101 = C_8 \quad .$$

Nämä yhdistämällä saadaan

$$C_1 \dots C_8 = 01000010111001000011111011111101,$$

josta edelleen Taulukon 6 mukaisella permutaatiolla

$$f(R_{15}, K_{16}) = 01111010001100011001110110101101.$$

Seuraavaksi ratkaisemme operaation

$$R_{16} = L_{15} \oplus f(R_{15}, K_{16}) = 00110101010101011111001000011010.$$

Kun vielä muistamme, että

$$L_{16} = R_{15} = 01010011011111111011000110110101,$$

niin olemme ratkaisseet merkkijonot L_{16} ja R_{16}.

3. Vaihdamme vasemman ja oikean puolen ja yhdistämme ne, jolloin saamme merkkijonon $R_{16}L_{16}$. Kun vielä suoritamme sille käänteisesti alkupermutaation IP, niin saamme salatun viestin c.

$$\begin{aligned} c &= (IP)^{-1}(R_{16}L_{16}) \\ &= 11111010101001010111001000100001111111110110111010110100000001110, \end{aligned}$$

joka voidaan lähettää vastaanottajalle.

4.3 Salauksen purku

Salauksen purku tapahtuu vastaavasti kuin varsinainen salaus. Ainoa ero on, että salausavaimia K_i käytetään päinvastaisessa järjestyksessä. Kierroksella 1 avainta K_{16}, kierroksella 2 avainta K_{15} ja niin edelleen. Tämän toimivuus voidaan helposti osoittaa. Ensimmäisen purkuaskeleen syötteenä toimii $R_{16}L_{16}$. Sen avulla saadaan tulosteet L_{16} ja $R_{16} \oplus f(L_{16}, K_{16})$. Salauksen pohjalta tiedämme, että $L_{16} = R_{15}$ ja että $R_{16} = L_{15} \oplus f(R_{15}, K_{16})$. Näin saamme tulosteet muotoon R_{15} ja $L_{15} \oplus f(R_{15}, K_{16}) \oplus f(L_{16}, K_{16})$. Kun vielä hyödynnämme uudelleen tietoa, että $L_{16} = R_{15}$, niin tulosteet saadaan muotoon R_{15} ja $L_{15} \oplus f(R_{15}, K_{16}) \oplus f(R_{15}, K_{16})$. Koska $f(R_{15}, K_{16}) \oplus f(R_{15}, K_{16})$ on aina 0, niin tulosteet saadaan muotoon R_{15} ja L_{15}. Kun jatkamme vastaavasti kaikki 16 kierrosta, niin olemme palanneet lähtöarvoihin R_0 ja L_0. Kun nämä vielä käännetään ja yhdistetään kuten salauksenkin viimeisessä vaiheessa, niin saamme merkkijonon L_0R_0. Kun suoritamme sille vielä käänteisesti alkupermutaation IP, niin olemme saaneet alkuperäisen viestin m.

5 DES:n murtaminen ja korvaaminen

Alusta lähiten DES:in huonona puolena on pidetty salausavaimen pituutta, joka on vain 56 bittiä. Lisäksi NSA:n rooli salauksen kehittelyssä on aiheuttanut huolta mahdollisista takaporteista. Jo vuonna 1977, vain muutamia kuukausia DES:n julkaisun jälkeen, Whitfield Diffie ja Martin Hellman julkaisivat artikkelin, jossa he arvioivat voivansa rakentaa 20 miljoonalla dollarilla tietokoneen, joka kykenisi murtamaan DES-salauksen.

DES:n jatkoa alan standardina arvioitiin uudelleen aina viiden vuoden välein. Vuoden 1987 arvioinnin yhteydessä NBS olisi halunnut parantaa DES:ia tai lopettaa sen kokonaan. Myös NSA oli halukas kehittämään uuden standardin, jonka se saisi suunnitella sisäisesti. Ajatus kuitenkin hylättiin, sillä Yhdysvaltalaiset suuryritykset eivät uskaltaneen olla ilman salausta sillä aikaa, kun uutta algoritmia olisi kehitelty. Tämän seurauksena DES:n asemaa standardina jatkettiin viidellä vuodella. Vuonna 1992 NIST, NBS:n uudelleen nimetty seuraaja, jatkoi DES:n serfiointia standardina, huolimatta ongelmista jotka oli tuotu esille jo vuoden 1987 tarkastuksessa.

DES oli alan vallitseva standardi yli 20 vuoden ajan, mutta viimeistään 1990-luvun loppupuolella se alkoi osoittaa ikääntymisen merkkejä. Internetin yleistyminen toi mahdolliseksi hajautetun laskennan käytön DES:in murtamiseen. 1997 RSA Data Security -yritys järjesti kilpailun, jonka tavoitteena oli murtaa DES:lla salattu viesti. Kilpailun palkintona oli 10000 dollaria. Viisi kuukautta kilpailun aloittamisen jälkeen Rocke Verser oli onnistunut murtamaan salauksen ja mikä tärkeintä tämä oli ensimmäinen kerta kun hajautettua laskentaa oli käytetty DES:iä vastaan. Rocke Verser oli luonut ohjelman, jonka avulla kuka tahansa saattoi osallistua omalla tietokoneelllaan DES:in murtamiseen internetyhteyttä käyttäen. Seuranneina vuosina DES murrettiin yhä nopeammin ja viimein vuonna 2000 NIST korvasi DES:in uudella standardilla, joka sai nimekseen Advanced Encryption Standard, AES.

Myös AES oli kilpailun tulos. Kryptografian merkittävimmät tekijät saivat kommentoitavakseen 15 kandidaattia, joista 5 valittiin finaalisteiksi ja niiden joukosta voittajaksi valittiin Rijndael-nimellä tullut algoritmi. Rijn-

dael oli lohkosalain, kuten DES:kin. Sitä voitiin käyttää eri toimintatavoilla, aivan kuten edeltäjäänsäkkin. Rijndael oli suunniteltu käyttämään salausavaimia, joiden pituus olisi 128, 192 tai 256 bittiä. Algoritmi sisältää 128 bitin salausavainta käytettäessä 10 salauskierrosta, 192 bitin avainta käytettäessä 12 kierrosta ja 256 bitin avaimella 14 kierrosta. Algoritmiin kuuluu myös S-laatikko kuten DES:ssa, mutta siitä poiketen laatikoita on vain yksi ja se on huomattavasti laajempi. Tämän lisäksi Rijndael sisältää myös bittien siirtoa, sekä sekoittamista.

AES algoritmi eri versioineen on edelleen laajalti käytössä pienemmän prioriteetin salauksissa, kuten esimerkiksi kotien lähiverkoissa, mutta sitä ei pidetä enää turvallisena vaihtoehtona tärkeämmän datan salaukseen.

6 DES-algoritmin Python-koodi

6.1 Alku- ja loppupermutaatio

```
AP = [58, 50, 42, 34, 26, 18, 10, 2, 60, 52, 44, 36, 28, 20, 12, 4,
      62, 54, 46, 38, 30, 22, 14, 6, 64, 56, 48, 40, 32, 24, 16, 8,
      57, 49, 41, 33, 25, 17, 9, 1, 59, 51, 43, 35, 27, 19, 11, 3,
      61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7]

RL = [0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1,
      1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1,
      0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1,
      1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1]

c = [1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0,
     1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0,
     1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1,
     1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1]

for i in range(64):
    c[(AP[i]-1)] = str(RL[i])

CC = ""
CC = CC.join(c)
print("c=" + CC)

m = "0100110101100000101101001011100110111010001100101011100100110100 1"
m0 = ""
for i in range(64):
    m0 += m[AP[i]-1]
print ("m0=" + m0)
```

6.2 DES-algoritmi

```
def int2bin(n):
    return int2bin(n >> 1) + [n & 1] if n > 1 else [1]

L = ["11111111010110000011000110101111"]
R = ["00000000111111101000010101001000"]

E = [32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9, 8, 9, 10, 11, 12, 13,
     12, 13, 14, 15, 16, 17, 16, 17, 18, 19, 20, 21, 20, 21, 22,
     23, 24, 25, 24, 25, 26, 27, 28, 29, 28, 29, 30, 31, 32, 1]

K = ["111100001011011011001110100001100000011000000100",
     "111000000011111010110110000000010001000010000010",
     "111101001011111001110000010001000010000000100101",
     "110001101111011001110010001000100000100011001100",
     "111011101101011101010110000000001001000110010011",
     "011011101101001101001011000001110000010000100001",
     "001010111101000101111011010010100000100101000000",
     "101011010100100111011011000000001100000100011100",
     "000111110101001111011010100001000000110001001000",
     "001111100101100111001101000010001011001001010000",
     "000110110110100101001101001100011100010000100000",
     "000010010110110110111101000010000000110000000010",
     "110101010010110110101101100011000110000000010100",
     "110100111010111010100001001000010100001011000000",
     "110110011011111010100110100100001000000000000011",
     "101000011010111000101110001100010000000100011100"]

S = [[[14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7],
    [0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8],
    [4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0],
```

```
    [15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13]],
    [[15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10],
    [3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5],
    [0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15],
    [13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9]],
    [[10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8],
    [13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1],
    [13, 6, 4, 9, 8, 15, 3, 0, 11, 1, 2, 12, 5, 10, 14, 7],
    [1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3, 11, 5, 2, 12]],
    [[7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15],
    [13, 8, 11, 5, 6, 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9],
    [10, 6, 9, 0, 12, 11, 7, 13, 15, 1, 3, 14, 5, 2, 8, 4],
    [3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11, 12, 7, 2, 14]],
    [[2, 12, 4, 1, 7, 10, 11, 6, 8, 5, 3, 15, 13, 0, 14, 9],
    [14, 11, 2, 12, 4, 7, 13, 1, 5, 0, 15, 10, 3, 9, 8, 6],
    [4, 2, 1, 11, 10, 13, 7, 8, 15, 9, 12, 5, 6, 3, 0, 14],
    [11, 8, 12, 7, 1, 14, 2, 13, 6, 15, 0, 9, 10, 4, 5, 3]],
    [[12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11],
    [10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8],
    [9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6],
    [4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13]],
    [[4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1],
    [13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6],
    [1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2],
    [6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12]],
    [[13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7],
    [1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2],
    [7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8],
    [2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11]]]

PE = [16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10,
```

```
      2, 8, 24, 14, 32, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25]

for kierros in range(16):
    print("\nKierros %d"%(kierros+1) +", eli kun $i=%d$."%(kierros+1))
    print("\\begin{align*}")
    print("R_{%d} & = "%kierros + R[kierros] + "\\\ ")

    ER = ""
    for x in E:
        ER += str(R[kierros][x-1])
    print ("E(R_{%d}) & = "%kierros + ER + "\\\ ")
    print ("K_{%d} & = "%(kierros+1) + K[kierros] + "\\\ ")

    ERK = ""
    for i in range(len(ER)):
        if ER[i] == str(K[kierros][i]):
            ERK += str(0)
        else:
            ERK += str(1)

    print("E(R_{%d})"%kierros + "\oplus K_{%d} & = "%(kierros+1)
          + ERK + "\\\ ")
    print("& =B_1B_2\\dots B_8")
    print("\\end{align*}")
    print("\\begin{align*}")

    B = []
    for i in range(8):
        B.append(str(ERK[i*6:i*6+6]))

    C1 = []
```

```
for i in range(8):
    Cl.append(int2bin(S[i][int(str(B[i][0]) +
    str(B[i][5]), 2)][int(B[i][1:5], 2)]))

for i in range(8):
    while len(Cl[i]) < 4:
        Cl[i].insert(0, 0)

C = []
for i in range(8):
    Cm = ""
    for j in range(4):
        Cm += str(Cl[i][j])
    C.append(Cm)

for i in range(4):
    for j in range(2):
        if j == 0:
            print("B_%d="%(i*2+j+1) + B[i*2+j] +
                  " \\xrightarrow{S_%d} "%(i*2+j+1) +
                  C[i*2+j] +  "=C_%d"%(i*2+j+1) + "\\qquad\qquad")
        elif i == 3 and j == 1:
            print("B_%d="%(i*2+j+1) + B[i*2+j] +
                   " \\xrightarrow{S_%d} "%(i*2+j+1) +
                   C[i*2+j] +  "=C_%d"%(i*2+j+1))
        else:
            print("B_%d="%(i*2+j+1) + B[i*2+j] +
                   " \\xrightarrow{S_%d} "%(i*2+j+1) +
                   C[i*2+j] +  "=C_%d"%(i*2+j+1) + "\\\ ")

print("\\end{align*}")
```

```
print("\\begin{align*}")

CC = ""
CC = CC.join(C)
print("C_1\\dots C_8 & =" + CC + "\\\ ")

FRK = ""
for x in PE:
    FRK += str(CC[x-1])
print ("f(R_{%d}"%kierros + ",K_{%d}) & ="%(kierros+1) +
       FRK + "\\\ ")

RU = ""
for i in range(32):
    if L[kierros][i] == FRK[i]:
        RU += str(0)
    else:
        RU += str(1)

print("R_{%d}= "%(kierros+1) + "L_{%d}\oplus "%kierros +
      "f(R_{%d}"%kierros + ",K_{%d}) & = "%(kierros+1) + RU + "\\\ ")
print("L_{%d}= "%(kierros+1) + "R_{%d} & ="%kierros + R[kierros])
print("\\end{align*}")

R.append(RU)
L.append(R[kierros])
```

Lähdeluettelo

[1] W. Trappe, L. Washington: *Introduction to Cryptography with Coding Theory*. Pearson Education, Inc. New Jersey, 2006.