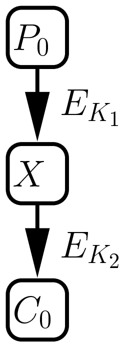
Kaksinkertainen salaus

- Tavoite: pitempi avain ja enemmän kierroksia, mutta vanha luotettava algoritmi.
- Ehdotus: salataan peräkkäin kahdella eri avaimella.

$$C = E_{K_2}(E_{K_1}(P)),$$
$$P = D_{K_1}(D_{K_2}(C)).$$



- **Huono ratkaisu!**

  Meet-in-the-middle-hyökkäyksen takia kaksinkertainen salaus vastaa avaimen pidentämistä 1 bitillä!

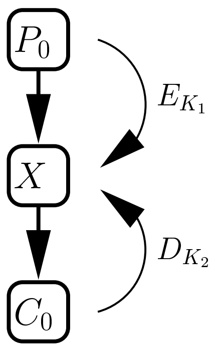
Meet-in-the-middle -hyökkäys

- Tarvitaan selväkieli-salakielipari P_0, C_0.

$$C_0 = E_{K_2}(E_{K_1}(P_0)).$$

Tällöin on olemassa jokin X s.e.

$$X = E_{K_1}(P_0),$$
$$X = D_{K_2}(C_0).$$



Salataan P_0 kaikilla mahdollisilla K_1 ja talletetaan tulokset. Joukossa on myös X. Jos avaimen pituus on n, joudutaan salaamaan 2^n kertaa.
Avataan C_0 kaikilla mahdollisilla avaimilla K_2 ja etsitään tulosta muistista. Kun avain on oikea, saadaan X ja se löytyy muistista.

On myös muita avaimia, joilla $C_0 = E_{K_2'}(E_{K_1'}(P_0))$. Löydetyt avaimet testataan toisen tunnetun parin P_1, C_1 avulla. Jos ei onnistu, jatketaan K_2:n hakua.

- Tarvitaan 2^{n+1} salausoperaatiota ja 2^n lohkoa muistia. (Esim. DES:illä $2^{56} * 8$ tavua.)

Kolminkertainen salaus

- Kaksi avainta (EDE-moodi):

$$C = E_{K_1}(D_{K_2}(E_{K_1}(P))),$$
$$P = D_{K_1}(E_{K_2}(D_{K_1}(C))).$$

- Jos $K_1 = K_2$, vastaa yksinkertaista salausta.
- Teoreettisia hyökkäyksiä:
  - 2^n valittua selväkieltä, 2^n lohkoa muistia, 2^{n+1} salausoperaatiota
  - p tunnettua selväkieltä, p lohkoa muistia, noin $2^{n+m}/p$ salausoperaatiota (n = avaimen pituus, m = lohkon pituus)

  Esim. 3DES:iä (112-bittinen avain) pidetään vahvana.
- Kolme avainta (EDE-moodi):

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P))),$$
$$P = D_{K_1}(E_{K_2}(D_{K_3}(C))).$$

- Hyökkäys: 2^{2*n} operaatiota, 2^n lohkoa muistia
- CBC-moodi ja muut toimintamoodit samoja kuin yksinkertaiselle salaukselle.

Differentiaalinen kryptoanalyysi (DES)

- Vaatii paljon tunnettua tai valittua selväkieltä.
- Toimii SP-verkkoa ja Feistel-salakirjoituksia vastaan.
- Käyttää hyväksi S-boksien pieniä, tilastollisia säännönmukaisuuksia.
- Voidaan torjua iteraatioiden määrää kasvattamalla (ainakin jos S-boksit satunnaisia ja aliavaimet toisistaan riippumattomia).
- Vaiheet:
  1. Etsitään sopivia karakteristisia differenssejä (käytetään tunnettuja).
  2. Salataan suuri määrä tunnettuja selväkielipareja, joiden erotus on karakteristinen differenssi.
  3. Kullekin parille tunnetaan tietyllä todennäköisyydellä differenssi kierroksen $n - 2$ jälkeen. Päätellään avain 2R-hyökkäyksellä.

Saranapuolen kautta sisään

- Useat nykyaikaiset salaukset ovat hyviä, eikä niitä pystytä ratkomaan kryptoanalyysin keinoin. Hyökkäykset ovat teoreettisia.
- Uuden tyyppisiä hyökkäyksiä:
  - mikropiirien suojausten murtaminen
  - differentiaalinen virheanalyysi
  - ajoitushyökkäys.
- Perinteiset hyökkäykset ovat perustuneet vain kerättyihin salakielisiin ja selväkielisiin sanomiin.

  Uudet hyökkäykset vaativat salaisen avaimen sisältävään laitteen fyysistä tutkimista tai manipulointia.
- Uhka älykorteille ja muille luotetuille laitteille, jotka annetaan hyökkääjän haltuun.

Mikropiirien suojausten murtaminen

- Hyökkäyksiä kehitetty kautta aikojen ammattimaisesti lähinnä maksu-TV-kortteja vastaan.

  Usein hyökkääjä tarvitsee useita kortteja rikottavaksi (joko vahinkojen tai suojausmekanismien takia).
- Hyökkäyksiä:
  - Virransyötön häiriöt tai fyysinen kosketus nollaavat pysyvän muistin bittejä helpommin kuin nostavat. Nollataan suurin (satunnaisesti valittu) osa avaimen biteistä ja selvitetään kokeilemalla jäljelle jääneet.
  - Muistipaikkoja voidaan rikkoa laserilla. Etsitään standardirakenteita mikroskoopilla ja rikotaan sopivat muistipaikat salausalgoritmin muuttamiseksi.
  - Lyhyet jännitepiikit ja liian nopeat kellotaajuudet voivat sekoittaa mikropiirin prosessorin. Ratkaisu: piirille oma kello ja teholähde.
  - Satunnaislukugeneraattorien häiritseminen tai vahingoittaminen.
  - Piirin suojauskerrosten poistaminen ja jännitemittaukset tai sähkömagneettisen kentän havainnointi.
- Yksinkertaiset hyökkäykset tepsivät halpoihin massavalmisteisiin kortteihin.

  Suojautumiseen on keinoja, mutta ne maksavat. Hyökkäykset kehittyvät, joten kortit on uusittava usein.

Differentiaalinen virheanalyysi

(*differential fault analysis*)

- Menetelmä julkisen avaimen salausten ratkaisemiseksi: Demillo ja Lipton 1996

  Salaisen avaimen salausten ratkaiseminen: Biham ja Shamir 1996, Anderson ja Kuhn 1996
- Hyökkäyksen tavoitteena on selvittää suojatulla mikropiirillä oleva salausavain.

  Säteilytetään mikropiiriä ionisoivalla säteilyllä tai mikroaalloilla, jotka aiheuttavat satunnaisia yhden bitin virheitä mikropiirin rekistereissä.

  Verrataan virheellisten salausten tuloksia ja päätellään avain.
- **DES**: Salataan sama selväkielinen sanoma virheettömästi ja useaan kertaan säiteilytyksessä. Verrataan salakielisiä sanomia.

  Jos vain muutama salakielen bitti muuttuu, tiedetään virheen tapahtuneen ennen tiettyä kierroksen 15 tai 16 S-boksia. Säteilytyksessä kääntynyt bitti on yksi kuudesta S-boksiin menevästä.

  Päätellään kuten differentiaalisen kryptoanalyysin 2R-hyökkäyksessä: Tunnetaan S-boksiin menevät arvot, jotka eroavat yhden bitin, ja boksista tulevien arvojen differenssi. Saadaan 6 avainbittiä. Pian koko viimeinen aliavain tunnetaan.

- Säteilyn aiheuttamat virheet eivät aina ole näin ideaalisia. Kerätään tilastoa mahdollisista avainbiteistä. DES-aliavaimen selvittämiseksi tarvitaan noin 200 toistoa.
- Viimeisen aliavaimen selvittyä on mahdollista ratkaista sitä edellinen aliavain jne. Näin voidaan ratkaista myös moninkertainen salaus.
- On mahdollista selvittää tuntemattomien salakirjoitusten rakennetta (S-boksien koot ja sisältö).
- Suojautumiseen käytetään virhetarkistuksia:
  - pariteettibitit
  - kaksi rinnakkaista prosessorin lohkoa, joiden tuloksia vertaillaan
  - tarkistuslaskelmat modulo jokin pieni luku.
- Keskeinen periaate: suojatun piirin murtamisen pitää olla kalliimpaa kuin siitä saatava hyöty.

  Yhdellä piirillä olevan tiedon paljastuminen ei saa haitata muita käyttäjiä. Ei yhteisiä salaisuuksia kaikille piireille!
- Hyökkäysten teoria tunnetaan, mutta käytännön toteutuksia ei julkistettu.

Ajoitushyökkäys

(*timing attack*)

- Paul Kocher 1995 (uudenlaisten hyökkäysten aallon aloittaja)
- Koskee **julkisen avaimen** algoritmeja, ei salaisen!
- Mitataan vasteaikoja älykortilta tai verkon yli.

  Kerätään ajoista tilastoa.

  Päätellään yhsityisen avaimen avaimen suuruus (tai muu ominaisuus) laskentaan kuluneen ajan perusteella. Eri algoritmeille kehitetty tarkkoja tilastollisia kaavoja.
- Hyökkäykseltä suojaudutaan antamalla vastaus vakioajassa tai lisäämällä laskenta-aikoihin satunnaisia viiveitä.

Hyvän salakirjoituksen ominaisuuksia

- Suurestakaan määrästä salakieltä ei ole mahdollista saada **mitään** tietoa selväkielisestä tekstistä. (Esim. toistoja ei saisi havaita.)
- Selväkielen redundanssi ei saa olla näkyvissä salakielessä. Salakielen tulee näyttää täysin satunnaiselta, eikä sitä voi muuksi todistaa ilman avainta.
- Salakielen on hyvä olla saman pituinen kuin selväkielinen sanoma. (Sanoman pituus paljastuu!)
- Kestää kaikki tunnetut hyökkäykset.
- Suurestakaan määrästä tunnettuja tai valittuja selväkieli-salakielipareja ei ole mahdollista selvittää avainta.
- Kaikkien avainten läpikäyminen (brute force) on tehokkain hyökkäys.

- Avaimen pituuden pitää olla riittävä ($>$ 80 bittiä).
- Ei heikkoja avaimia. Koko avainavauuden pitää olla tasavahva.
- Avaimet on valittava satunnaisesti ja tasaisesti tasaisesti koko avainavaruudesta.
- Algoritmin tuntemisesta ei ole apua ratkaisussa, jos avain ei ole tiedossa.
- Algoritmin suunnitteluperiaatteiden pitää olla julkisia tai siitä pitää helposti näkyä, ettei kätkettyjä takaportteja ole.
- Lohkosalauksessa yhdenkin bitin muutoksen selväkielessä lohkossa pitää aiheuttaa suuri muutos salakielessä. Keskimäärin puolet lohkon biteistä kääntyy.
- Salaus- ja avausfunktiot pitää voida vaihtaa keskenään turvallisuuden kärsimättä.
- Algoritmin pitää olla tehokkaasti toteutettavissa raudalla tai ohjelmallisesti.
- Algoritmin suoritusajan pitää olla vakio.