- ✓ **Kryptoanalyysin menetelmiä**
- ✓ **Kryptografian menetelmien uusia sovelluksia**

# Kryptoanalyysin menetelmiä

Kryptoanalyysi tarkoittaa salakirjoituksen tai sen algoritmin murtamiseen tähtäävää toimintaa.

1. Ciphertext only -hyökkäys
2. Known/chosen plaintext -hyökkäys
3. Brute Force hyökkäys
4. Man in the Middle hyökkäys
5. Sanakirjahyökkäys - Dictionary attack
6. Takaportit
7. Replay -hyökkäys
8. Sivukanavahyökkäys - side channel attack
9. Päätelaitehyökkäys

## 1. Ciphertext only attack

- Analyytikolla on käytössään salakirjoitettuja viestejä

- Klassiset salakirjoitukset kuten Caesar tai Vigenere voidaan murtaa frekvenssianalyysillä, mikäli salattu viesti on riittävän pitkä.
- Moderneja salauksia voidaan yrittää murtaa Brute Force menetelmällä, mikäli salauksen avainpituus ei ole riittävä.

## 2. Known / chosen plaintext attack

- Analyytikolla on käytössään sekä alkuperäisiä viestejä, että niiden salakirjoituksia.

- Toisessa maailmansodassa liittoutuneet hyödynsivät saksalaisten vakiona pysyvää tapaa aloittaa (säätiedotukset alkoivat sanalla Wetter) tai lopettaa viestinsä (tietyissä viesteissä Heil Hitler)

*Wikipediassa on englanninkieliset artikkelit molemmista menetelmistä*

## 3. Brute force hyökkäys

Mikäli hyökkääjällä on käytössä riittävästi laskentatehoa, hän voivat murtaa salausavaimen käymällä läpi kaikki mahdolliset avaimet.

Metodilla voidaan murtaa salauksia, joissa avainpituus on reilusti alle 80 bittiä. Mm. DES – lohkosalaus, sekä GSM – salaus A5 voidaan murtaa Brute Forcella.

Minimiturvallisuuden takaavana avainpituutena pidetään käytännössä 128 bittiä.

## 4. Man in the middle attack:

Man in the Middle hyökkäyksessä kolmas osapuoli E tulee käyttäjien A ja B väliin esiintyen yhteyden toisena osapuolena molempiin suuntiin. E voi lukea dataa, sekä muuttaa sitä. CA -järjestelmän tarkoitus on estää väärien julkisten avainten levittäminen ja näiden avulla tapahtuvat hyökkäykset.

## 5. Sanakirjahyökkäys salasanatiivisteitä vastaan:

Analyytikolla on käytössään esim. 100 000 yleisimmän salasanan tiivisteet joille hän pyrkii löytämään vastineita kohteena olevan serverin salasanatiedostosta.

Vastatoimena sanakirjahyökkäykseen on salasanojen suolaus ennen tiivisteen laskemista tai shadow –tiedostot, joihin salasanatiivisteet tallennetaan

# 6. Takaportit

On olemassa salausalgoritmeja, joissa on ns. takaportti (backdoor). Se on tietoisesti algoritmiin jätetty turva-aukko, jota käyttäen sen laatija voi purkaa tiedon tai tietoliikenteen salaus.

Yleisesti uskotaan, että vakoiluorganisaatio NSA sai NIST:n hyväksymään takaportilla varustetun satunnaislukugeneraattorin Dual EC-DRBG kansainväliseen käyttöön v. 2006, sekä onnistui levittämään sen käyttöä eri tietoliikenneohjelmistoissa.

Asia tuli esiin Edwards Snowdenin paljastuksissa v. 2013 ja NIST faktisesti tunnusti takaportin olemassaolon vetäessään Dual EC-DRBG:n pois standardiensa joukosta huhtikuussa 2014.

USA:n standardointiviranomainen NIST, sekä sen johtavat tietoturvayritykset ovat menettäneet mainettaan em. skandaalin vuoksi. Tämä on näkynyt euroop-palaisten tietoturvayritysten liikevaihdon kasvuna.

## 7. Replay attack: (replay hyökkäys)

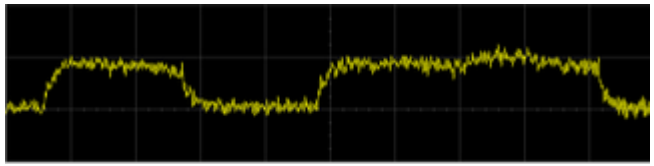
Hyökkääjä nappaa jonkin käyttäjän login – datan ja käyttää sitä myöhemmien kirjautuakseen järjestelmään.

Aikaleimojen ja datapakettien sarjanumerojen käyttö estää tätä hyökkäystä

*Auton etälukitusjärjestelmiin on kohdistettu replay -hyökkäyksiä. Auton avaimen lähettämä koodi on napattu ja sitä käytetty auton varastamiseen.*

## 8. Side channel attack (sivukanavahyökkäys):

Laitteisto mittaa prosessorista tulevan säteilyn silloin kun prosessori suorittaa esim. RSA – autentikointiin liittyvän laskun RES= $R^d$ mod n.
Yksityinen avain d yritetään määrittää prosessorisäteilyä analysoimalla.



An attempt to decode RSA key bits using power analysis. The left peak represents the CPU power variations during the step of the algorithm without multiplication, the right (broader) peak – step with multiplication, allowing to read bits 0, 1.

## 9. Päätelaitehyökkäykset

Turvallisimmastakaan tiedonsiirron salausalgoritmista ei ole hyötyä, mikäli hyökkääjä on vallannut jommankumman osapuolen päätelaitteen. Tietokoneen valtaaminen on eräs merkittävä kyberuhka yksityisille henkilöille ja yrityksille.

Valtiollisen toimijan ei aina tarvitse vallata päätelaitetta, vaan se voi myös pakottaa esim. Googlen tai Facebookin kaltaiset yritykset yhteistyöhön vedoten kansalliseen turvallisuuteen.

# NSA:n keinot salauksen murtamiseksi

Suurvaltojen keinoista tietoliikenteen salakuuntelemiseksi on tihkunut vain vähän tietoa. Julkiset asiakirjat mainitsevat, että mm. NSA:n toiminta pohjautuu lähinnä seuraaviin menetelmiin:

- Päätelaitehyökkäyksiin [1)]
- Postipalvelimien lähettämien pakettien peukalointiin
- Suhteisiin alan yritysten kanssa (Google, Facebook, RSA-lab,CA:t)
- Matemaattisiin menetelmiin [2)]

1) *Jos A:n ja B:n välistä tietoliikennesalausta ei voida murtaa, voidaan kaapata jompikumpi koneista A tai B, jolloin salauksella ei ole merkitystä.*

2) *Matemaattisten menetelmien arvellaan liittyvän mm. 1024 –bittisen RSA:n murtamiseen. Nykyisin vain 2048 bittistä RSA – avainta pidetään luotettavana.*

# Muita kryptografian sovelluksia

- Remote Keyless Entry  (RKE)
- Secret Sharing Systems
- Internet Voting

# REMOTE KEY ENTRY (RKE) OF CARS

**1. VARHAISISSA KAUKOSÄÄDINLUKOISSA** avain lähetti joka kerta saman signaalin.
Autovarkaille, jotka tunsivat taajuuden, ei signaalin tallentaminen nuuskivan laitteen muistiin ollut temppu eikä mikään.

* Kun omistaja poistui auton luota, varkaat aukaisivat auton ovet toistamalla tallennetun signaalin (ns. Replay Attack).

**2. TOISEN SUKUPOLVEN LUKOISSA** autonvalmistajat siirtyivät avaimiin, jotka käyttävät joka kerta eri avainkoodia. Ovet aukesivat tai sulkeutuivat kullakin avaimella vain kerran. Tyypillisesti virtalukossa oli kerrallaan 256 kertakäyttö-avainta, jotka tuotetaan esim. **HMAC** – funktiolla juoksevasta numerosta. Kun avaimen avaus tai lukituspainiketta painettiin, virtalukko vastaanotti signaalin, vertasi sitä listan avainkoodeihin, ja jos koodi oli listalla, ovi aukesi tai lukittui. Mikäli avaimen painikkeita painettiin kantaman ulkopuolella yli 256 kertaa, avainlistan avaimet loppuivat ja lukko ei enää auennut ilman merkkiliikkeen apua.

**Samy Kamkar** julkisti tietoturvatapahtuma Defconissa 2015 laitteen, jolla voi kaapata auton avainten kaukosäätimen lähettämän signaalin ja käyttää tätä oven avaamiseen jälkikäteen. Laite perustuu kolmeen eri radiolaitteeseen. Kaksi lähettää vahvaa häiriösignaalia kahdella tyypillisellä avainjärjestelmien käyttämällä taajuudella, mikä estää avaimen lähettämää signaalia päätymästä lukolle asti. Kolmas, herkästi viritetty radio, kaappaa lähetetyn signaalin ja tallentaa avainluvun muistiin.
Kun Kamkarin piilotetun laitteen lähellä painaa avausnappia, lukko ei reagoi. Todellisuudessa signaali ei häirinnän takia ikinä edes saavuta lukkoa, vaan päätyy laitteen muistiin.
Kuski painaa tällöin avaimen nappia uudelleen. Signaalia estetään jälleen saapumasta lukolle, uusi avain tallennetaan ja aiemmin kaapattu vanha avain lähetetään lukolle. Nyt lukko aukeaa ja laitteen muistiin jää yksi käyttämätön avauskoodi.

**3. Aikarajalliset avainkoodit**

Jotkin uusimmat automallit, kuten uudet Cadillacit, käyttävät lukkojärjestelmiä, joissa **avainkoodit ovat aikarajallisia**, ts. avain ja lukko generoivat uuden avainkoodin esim. puolen minuutin välein. Tällainen järjestelmä estää Kamkarin murtometodin.

# Kertakäyttösalasanalaitteet ”Password Tokens”


Laite tuottaa määrämittaisia ( esim. 6 – numeroisia) kertakäyttösalasanoja tietyn järjestelmän sisäänkirjautumista varten.

**Aikarajoitteinen malli:** Laite tuottaa uuden salasanan esim. joka minuutti. Laitteessa ja palvelussa, jota varten salasanoja generoidaan tulee olla synkronoidut kellot

**Laskurimalli:** Laite tuottaa uuden salasanan aina kun nappia painetaan. Laitteessa on laskuri, joka toimii syötteenä uuden salasanan generoinnissa.

# Kertakäyttösalasanat ja HMAC

Kertakäyttösalasanojen generointi perustuu HMAC funktioon, joka muodostaa laitteen SIM – avaimesta K ja laskurin arvosta C määrämittaisen tiivisteen. Laskurin tilalla syötteenä voi olla myös aika T.

$$HMAC(K, C) = sha(K \oplus opad || sha(K \oplus ipad || C)$$

Kuusinumeroinen kertakäyttösalasana saadaan 160-bitin HMAC arvosta Truncate – funktiolla, joka valitsee HMAC:stä määrätyn osan, josta muodostuu kertakäyttöavain.

Palvelin generoi samaa algoritmia käyttäen saman avainjonon. Käyttäjä pääsee paveluun, kun palvelin totetaa käyttäjän antaman kertakäyttöavaimen löytyvän palvelimen generoimalta listalta.

# Security Token laitteen turvallisuus

SHA tiivisteet toteuttavat hyvän tiivisteen vaatimukset. Tiivisteestä ei voi mitenkään päätellä sen syötettä, joka on SIM- avain + laskurin arvo.

Yhdestä salasanasta ei voi myöskään mitenkään laskea seuraavaa salasanaa.

Laitteen tulostamat avaimet R = Truncate(HMAC(K,C)) täyttävät tilastollisen satunnaisuuden vaatimukset.

# Secret sharing scheme

**Secret sharing** sopii erinomaisesti erittäin luottamuksellisen ja tärkeän tiedon talletukseen, Esimerkkinä ovat 1) tärkeiden salausavainten turvatalletus 2) ydinohjusten laukaisukoodien säilytys 3) nimettömien pankkitilien käyttäminen (esim. Sveitsin pankeissa on sallittu nimettömiä tilejä)

**Periaate:** Avain, jolla pääsee arkaluonteiseen tietoon, on jaettu siten että sen osia on n:llä henkilöllä. Avain voidaan rekonstruoida, kun määrätty määrä henkilöitä, joilla on avaimen osia, käyttää avaintansa.

Esim. Suurvallan puolustusorganisaatiossa on 7 henkilöä, jolla on avaimet ohjusten laukaisukoodit sisältävään tiedostoon. Tiedosto voidaan avata, kun mikä tahansa kolmen henkilön osajoukko em. henkilöistä käyttää avaimiaan.

Esim. Sveitsiläisessä pankissa nimettömältä nmerotilitä voi suoritaa noston, kun kolme eri henkilöä, joista osa pankkivirkailijoita, käyttää avaimiaan. Nostajan ei tarvitse todistaa henkilöllisyyttään.

# Shamirin ”secret sharing scheme”

- Paraabelin $y = f(x) = a\,x^2 + b\,x + c$ määrittää yksikäsitteisesti kolme paraabelin eri pistettä.
- Esimerkiksi seitsemälle eri henkilölle annetaan avaimena kullekin eri ko. paraabelin piste (x,y).
- Kun ketkä tahansa kolme syöttää avaimensa järjestelmään, järjestelmä ratkaisee yhtälöparista paraabelin määrittelevät parametrit a, b ja c.
- Järjestelmässä suojattu salausavain on jonkin määrätyn paraabelin $y = a\,x^2 + b\,x + c$ pisteen y – koordinaatti: esimerkiksi f(10).
- Paraabelilla tarkoitetaan tässä diskreettiä paraabelia, joka koostuu kokonaislukupareista (x,y), jotka toteuttavat yhtälön $y = a\,x^2 + b\,x + c$ kun vakiot a,b ja c ovat kokonaislukuja ja laskutoimitukset on suoritetaan mod q, missä q on kokonaisluku.

# Laskuesimerkki Shamirin järjestelmästä

1. Diskretisoidun paraabelin modulus q = 113.
2. Seitsemälle henkilölle on annettu avaimina paraabelin pisteet:

{7,91} {49,41} {110,85} {51,49} {18,74} {58,87} {72,59}

3. Jaettu salaisuus K on paraabelin y –arvo, kun x = 10.

Henkilöt 1,3 ja 7 syöttävät avaimensa järjestelmään.
Avaimet ovat {7,91} , {110,85} ja } {72,59}

**Lasketaan paraabelin parametrit a, b ja c.**

Mathematica- ohjelmalla ratkaistu yhtälöryhmä:

```
Reduce[a * 7^2 + b * 7 + c == 91 ∧
  a * 110^2 + b * 110 + c == 85 ∧
  a * 72^2 + b * 72 + c == 59,  {a, b, c},
 Modulus → 113]
```

```
a == 45 && b == 24 && c == 91
```

Jaettu salaisuus **K** = **(45***$10^2$ + **24***10 + **91)** mod 113 = **85**

# Internet -äänestäminen

- **Net voting** tarkoittaa äänestämistä valtiollisissa vaaleissa Internetin kautta. Äänestäjä todistaa henkilöllisyytensä esim. tietokoneen lukulaitteeseen laitetutta sähköisellä henkilökortilla tai mobiilivarmenteella.

* **Viro edelläkävijänä.** Internetin kautta äänestäminen on ollut toistaiseksi laajassa käytössä vain Virossa, jossa äänestystapa on ollut mahdollinen viimeisen 10 vuoden ajan pidetyissä vaaleissa.

Suomalainen tietoturvaekspertti **Harri Hursti** muutaman muun tutkijan kanssa on kritisoinut Viron nettiäänestyksen turvallisuutta ao. linkin raportissa:
https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

Lainaus arviosta:
“As we have observed, the procedures Estonia has in place to guard against attack and ensure transparency offer insufficient protection. Based on our tests, we conclude that a state-level attacker, sophisticated criminal, or dishonest insider could defeat both the technological and procedural controls in order to manipulate election outcomes”