Aantekeningen Cyber 2

Kerchoff's law (1)

The enemy knows the system

- Betekenis voor cryptografie
  De veiligheid van een cryptosysteem mag niet afhangen van
  De geheimhouding van het systeem/algoritme zelf. Het enige
  Geheim mag een $\underline{sleutel}$ *zijn van beperkte omvang*
  - Motivatie:
    1. Sleutels zijn eenvoudiger te verversen dan systemen/algoritmes
    2. Vaak moeten systemen ivm stadardisatie worden gepubliceerd (bijv.)

Kirchoffs law (2)

- Opmerking:
  Je zou denken dat het meest veilig is om en de sleutel en de methode geheim te houfen maar vanwege punt 4 is dat niet het geval Toch komt dit vaaak voor. Eeen bekende term hiervoor is security by obscurity

Chiper -only attack: Frequentie-analyse

Je kijkt hierbij naar de meest gebruikte letters om zo de encryptie te decrypten.

Onkraakbaar: One Time Pad (OTP)

- Een eerste stap naar digitale cryptografie

Computional secrecy

- Perfect secrecy is dus niet bruikbaar, maar wat doen we
- Computional secrecy
  - Realistische sleutellenge
  - Niet "Onkraakbaar" maar er is veel computerkracht nodig om de sleutel te vinden en/of de plain tekst te vinden

Principes van computional secrecy

- **Algortime is niet geheim** (alleen de sleutel)
- **Voldoende grote sleutel** (tegen BFA, in 2019: L>>80 bit)
- **Confusion** = Ingewikkelde relatie tussen sleutel en cyphertext. Elke verandering van de sleutel (zelfs maar 1 bit) leidt gemiddeld to veranfering van 50% van de cyphertext

DES (Data Encryption Standard)

- USA federale cryptografische standaard (NIST/NBS: FIPS 46-2, 1976)
- Voortkomend uit IBM's Lucifer, aangepast door de NSA
- Blokversleuteling met 64 bits in datablokken

Cryptoanalyse op DES

- Goede bescherming tegen een differentiële aanvallen (waarschijnlijk invloed NS op de substitutieboxen

AES (Advanced Encryption Standard)

- Opvolger van DES en 3 Des
- De belangrijkste standardisatie van symmetrische encryptie