Kryptographie

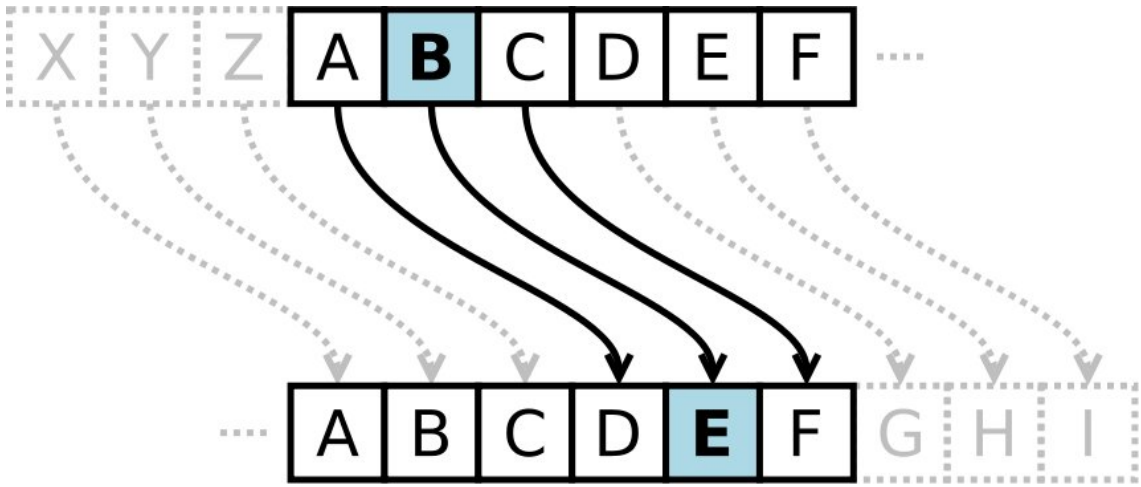
Matheschülerzirkel Augsburg

15. März 2014

http://xkcd.com/257/

Caesar-Verschlüsselung

- Verschlüsselung durch Rotation des Alphabets
- Beispielklartext: `Linux macht Spass!`
  Verschlüsselung: `OlqxA pdfkw Vsdvv!`

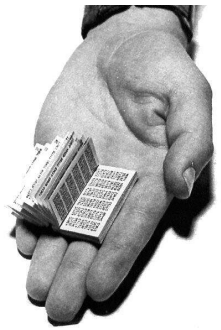


Monoalphabetische Substitution

- Verschlüsselung durch Verwendung eines Kunstalphabets
- Beispiel im Browser

Polyalphabetische Substitution

- Verschlüsselung durch Addition, Entschlüsselung durch Subtraktion eines geheimen Schlüssels
- Beispielklartext: `Linux macht Spass!`
  Schlüssel: `GeheimerSchluessel`
  Verschlüsselung: `RMUYf QRuJa MTSkW!`



Münzwurf über Telefon

- Kontext:
  Alice und Bob telefonieren.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

Münzwurf über Telefon

- Kontext:
  Alice und Bob telefonieren.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

1. Alice wählt Kopf, Bob wählt Zahl.
2. Alice wirft eine Münze.
3. Alice teilt Bob mit, dass die Münze Zahl anzeigt.
4. Bob muss die Aufgabe übernehmen.

Münzwurf über Telefon

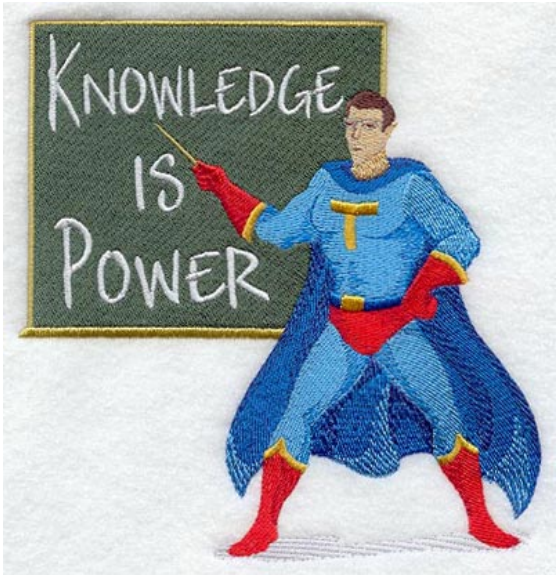
- Kontext:
  Alice und Bob telefonieren.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

1. Alice wählt Kopf, Bob wählt Zahl.
2. Alice wirft eine Münze.
3. Alice teilt Bob mit, dass die Münze Zahl anzeigt.
4. Bob muss die Aufgabe übernehmen.

- Offensichtlich: Alice kann betrügen!

Zero-Knowledge-Beweise

- Kontext:
  Alice möchte Bob davon überzeugen, dass sie ein bestimmtes Geheimnis kennt, ohne das Geheimnis preiszugeben.
- Illustration: Wo ist Waldo?



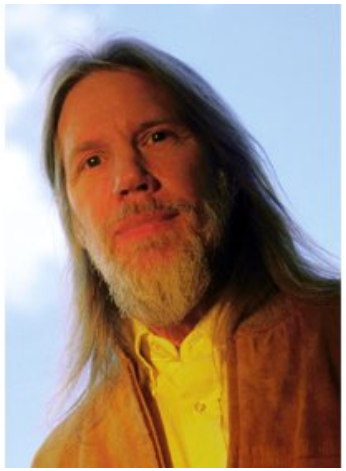
Zero-Knowledge-Beweise

- Kontext:
  Alice möchte Bob davon überzeugen, dass sie ein bestimmtes Geheimnis kennt, ohne das Geheimnis preiszugeben.
- Illustration: Wo ist Waldo?

- Variante: Alice und Bob möchten überprüfen, ob sie beide dasselbe Geheimnis kennen, ohne es preiszugeben.

Diffie–Hellman

- Kontext:
  Alice und Bob wollen ohne sonstige vorherige Absprachen ein gemeinsames Geheimnis ausmachen.



Bildquellen

- http://biblioragazzi.files.wordpress.com/2008/04/reference.jpg
- http://i34.tinypic.com/51ptu0.jpg
- http://imgs.xkcd.com/comics/code_talkers.png
- http://one-time-pad.tripod.com/otp.jpg
- http://upload.wikimedia.org/wikipedia/commons/2/2b/Caesar3.svg
- http://www.bryx.de/wp-content/uploads/2008/09/800px-zeichen_220svg.png
- http://www.cellphones.ca/news/upload/2008/09/knowledge1.jpg
- http://www.gpuri.com/images/213/21325.jpg
- http://www.hirt-institut.de/de/Media/Shop/CategoryTextMedia/hirt_motiv_ihre_ziele.jpg
- http://www.kveller.com/images/Article_images/wheres_waldo.jpg
- http://www.marketoracle.co.uk/images/coin-toss.jpg
- http://www.treachery.net/images/why_security_through_obscurity_isnt.jpg
- http://www.waleed-security.com/wp-content/uploads/2008/11/bruceab.jpg