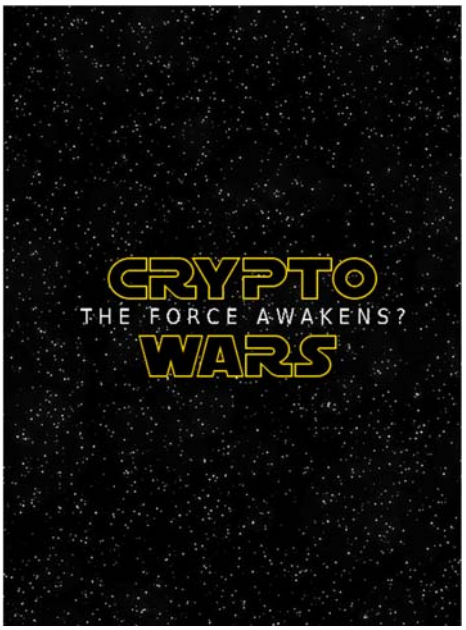


Why crypto regulation is doomed to fail

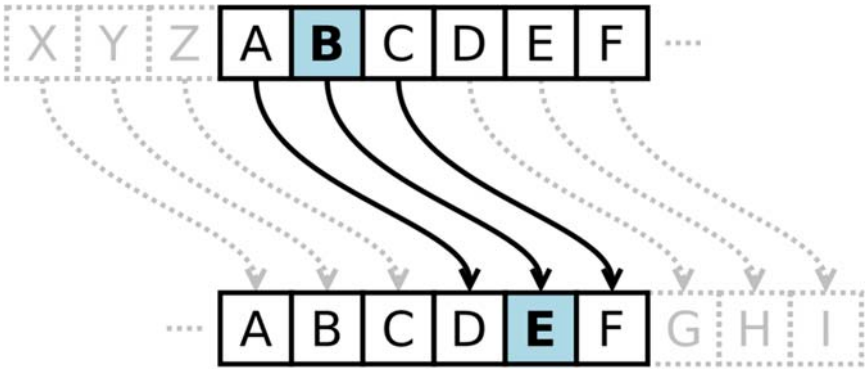
Marit Hansen
Data Protection Commissioner
Schleswig-Holstein

TEDxUniversityKiel, 3 December 2016

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

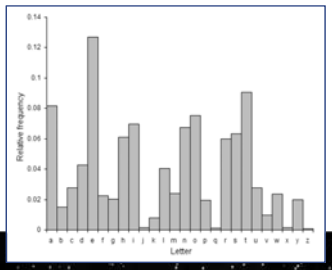
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

What is crypto?



Caesar cipher: shifting letters in the alphabet

Example:
`TEDxKielUniversity` → `WHGaNlhoXqlyhuvlwb`



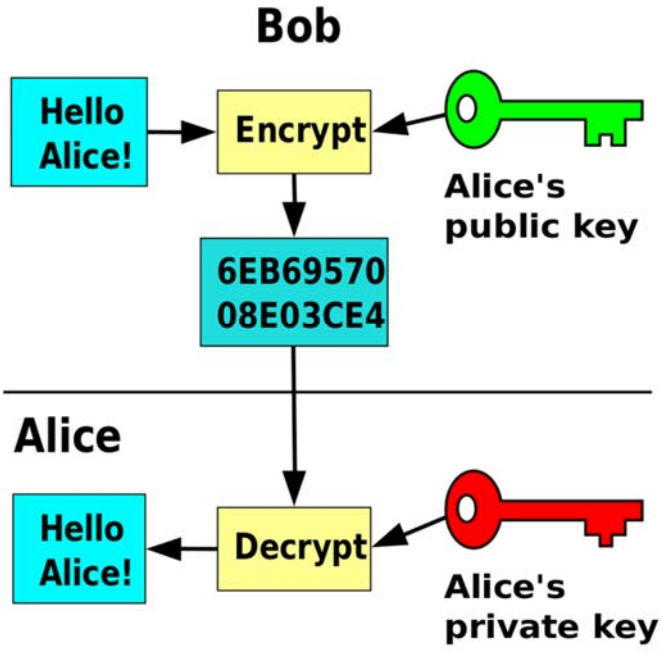
The authorised audience knows the key (“3”) for decryption.

Others may try to break the cipher.

Crypto is for spooks & politicians, isn’t it?

Reality: analysis by governments and companies

More advanced crypto



Alice has a pair of cryptographic keys: public key + private key.

Bob encrypts a message for Alice, using her public key.

Alice decrypts the message, using her private key.

Crypto is available

Encrypting files or disks

Accessing web sites (passwords, credit card numbers, ...)

Exchanging confidential messages

How secure is today's crypto?

Open crypto algorithms quite secure.

Vulnerabilities:

Brute force (crypto)

Brute force (human)

Regulation

What is regulated? – Export control

- Restricting strong crypto: export controls
- Until 1997: U.S. Internet browser for export only offering short keys (40 bit RC4) (domestic keys: 128 bit length)
- 1997: 40 bit key length not secure, not fit for commercial purposes


c|net

REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

40-bit crypto proves no problem

A UC Berkeley grad student wins an international encryption contest by cracking a 40-bit algorithm in less than four hours.

Tech Industry

by CNET News staff

A graduate student at the University of California at Berkeley used a network of about 250 workstations to crack a 40-bit algorithm in less than four hours yesterday, a university professor told CNET today.

Today export regulation of cryptography only concerning a few states

What is regulated? – Back doors

Tailored Access Operations by the NSA:

"insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets"

Source: Snowden files


Bloomberg

Dear NSA, Thanks for Making Us All Insecure

David Meyer

September 6, 2013 — 11:35 AM EDT

Photograph by Mark Vikor/Getty Images

Similar: Locks when travelling to the U.S.

- Inspection of luggage by the U.S. Transportation Security Administration (TSA)
- Special TSA locks
- TSA agents use master keys

- Are the master keys in good hands?

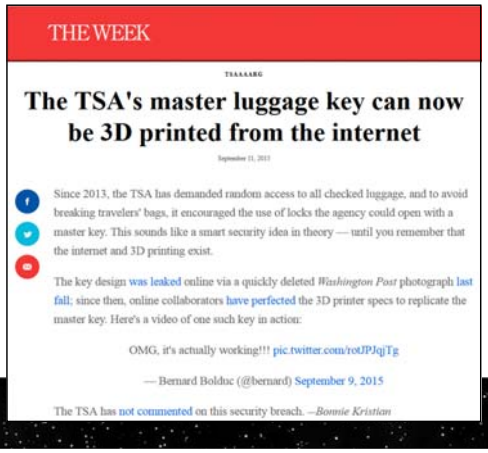

Photo: Willh26 (Wikipedia)

Similar: Locks when travelling to the U.S.

- Inspection of luggage by the U.S. Transportation Security Administration (TSA)
- Special TSA locks
- TSA agents use master keys

- Are the master keys in good hands?


Photo: Willh26 (Wikipedia)


THE WEEK

The TSA's master luggage key can now be 3D printed from the internet

Since 2013, the TSA has demanded random access to all checked luggage, and to avoid breaking travelers' bags, it encouraged the use of locks the agency could open with a master key. This sounds like a smart security idea in theory — until you remember that the internet and 3D printing exist.

The key design was leaked online via a quickly deleted *Washington Post* photograph last fall; since then, online collaborators have perfected the 3D printer specs to replicate the master key. Here's a video of one such key in action:

OMG, it's actually working!!! pic.twitter.com/rotJPJqjTg

— Bernard Bolduc (@bernard) September 9, 2015

The TSA has not commented on this security breach. —*Bonnie Kristian*

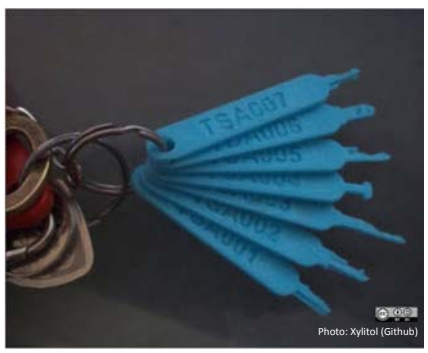


Photo: Xylitol (Github)

What is regulated? – Key escrow

Key escrow:
an organisation collects all keys to enable access to the clear text

Would you hand over your entire key ring for your apartment, work and car?

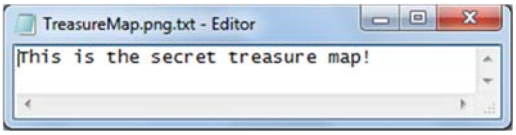
Similar: state can demand keys – else: jail
(e.g. UK Regulation of Investigatory Powers Act 2000 – without a court order)

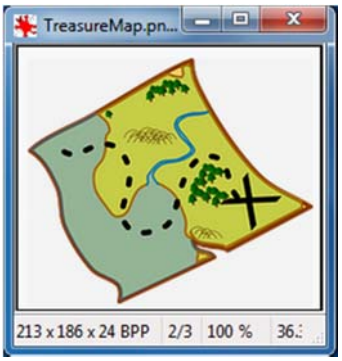
Circumvention by hiding

Can you see the treasure map?

Circumvention by hiding

Can you see the treasure map?



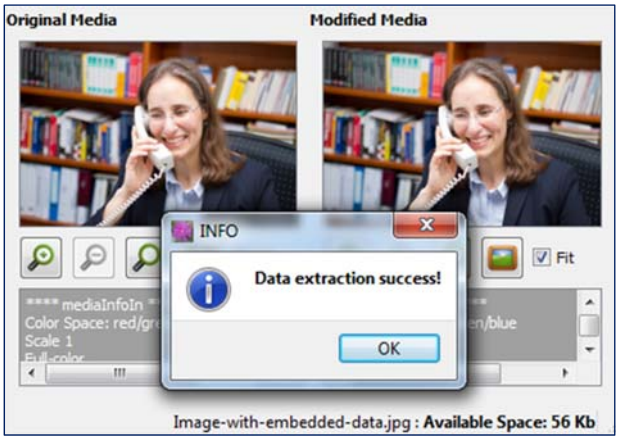


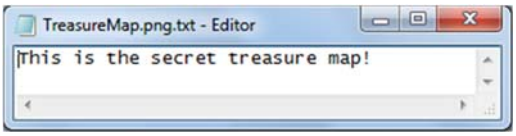
Only when using the right software.
The map is embedded in the picture on the left.

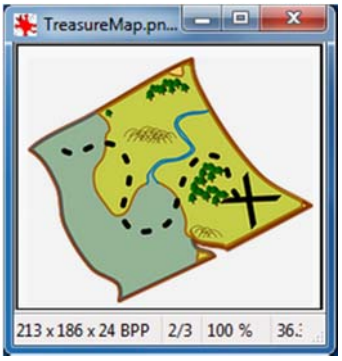
Steganography: hiding information in other information

Circumvention by hiding

Can you see the treasure map?







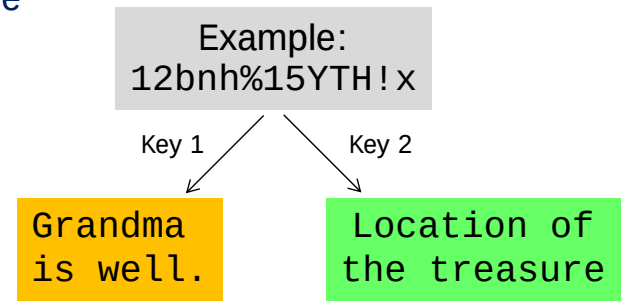
Only when using the right software.
The map is embedded in the picture on the left.

Steganography: hiding information in other information

Circumvention by crypto

Even with key escrow:

- Double encryption:
  additional key needed for 2nd encryption layer
- Clever encryption with two clear texts:
  key 1 shows innocent text,
  key 2 reveals the secret message



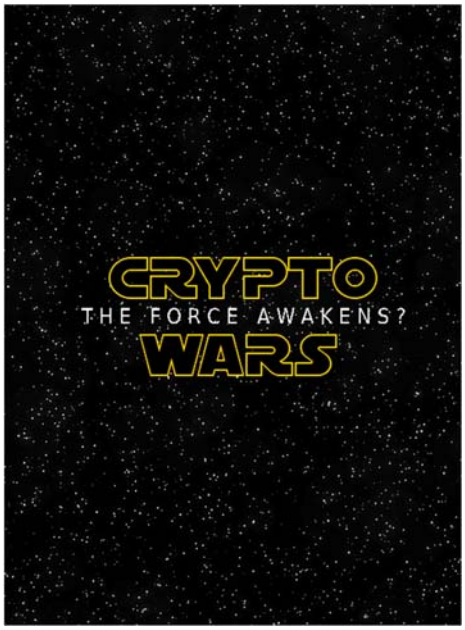
Does crypto regulation work?

Export control:
No – strong crypto is publicly available.

Back doors:
High risk!
Back doors can be used by criminals.

Key escrow:
High risk!
How to prevent misuse?
Circumvention possible!

Will we have strong crypto in the future?



- We need more, not less crypto
- Crypto = foundation of information society
- Try out crypto!
- Don’t know how?
  Attend crypto parties in your area!
- Then the force will awaken :-)