KATHOLIEKE UNIVERSITEIT
LEUVEN

Trusted Cryptography

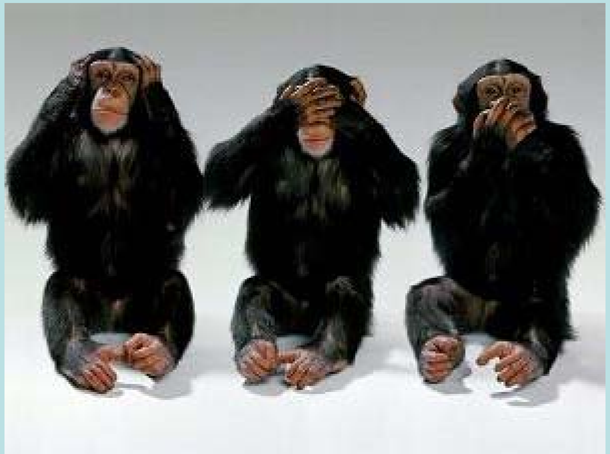
Vincent Rijmen

Overview

- Evolution of cryptography and security
- How to obtain trusted cryptography
- Green cryptography (with Justin Troutman), *IEEE Security & Privacy*, July/August 2009
- ~~Trusted computing~~

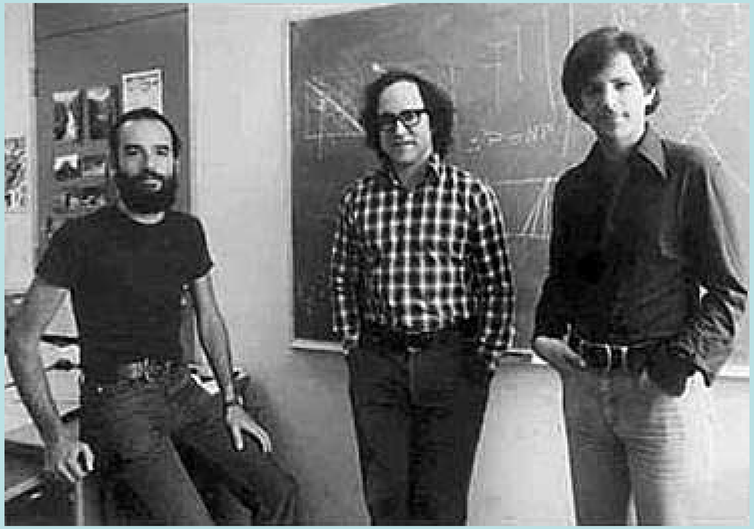
Cryptography in the old days

Security in the old days



The 1970s and ‘80s

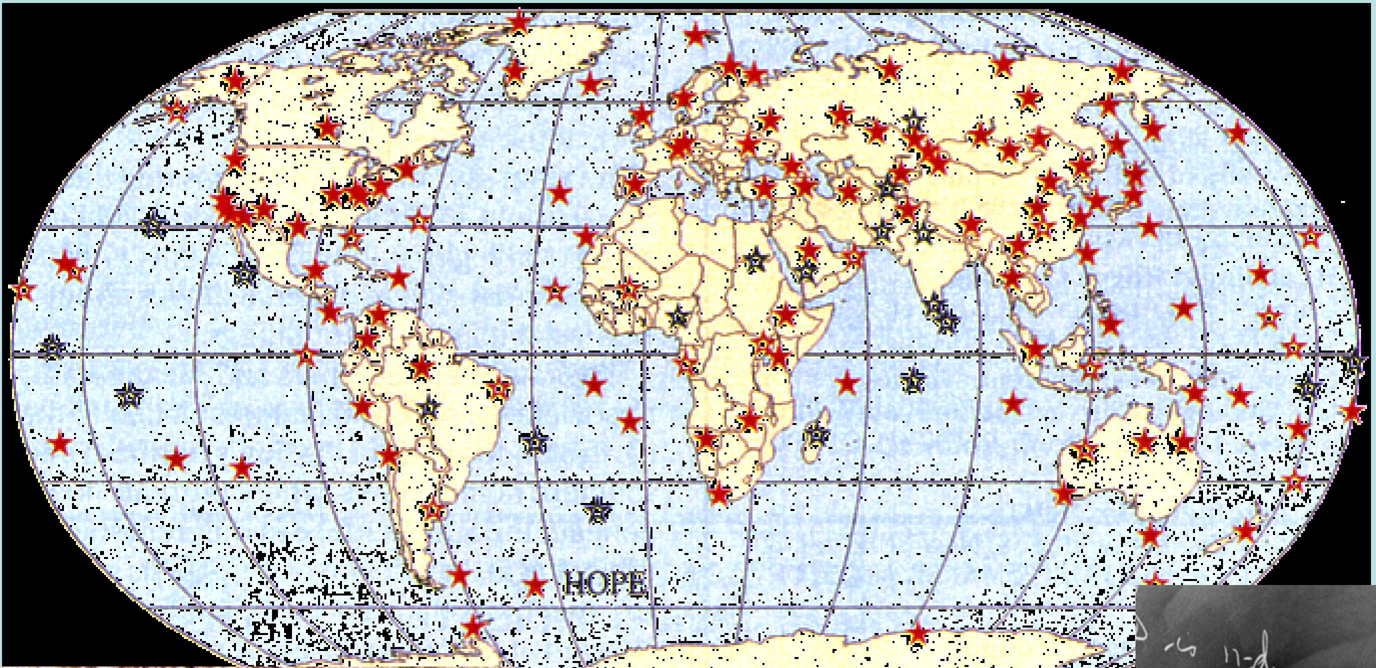
- Public (key) cryptography



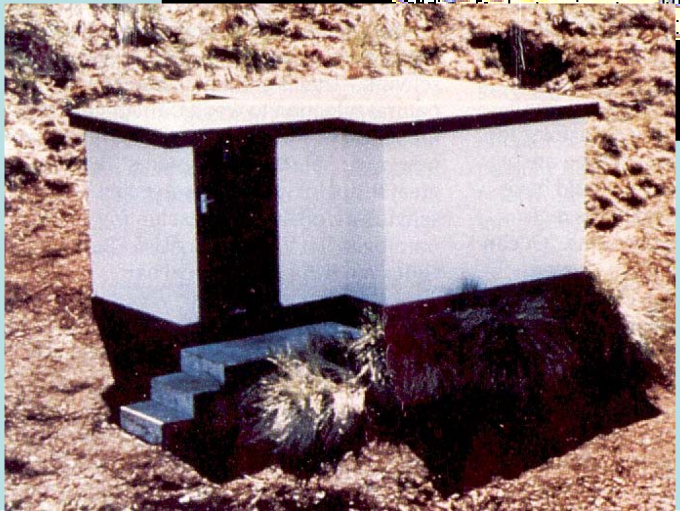
Cryptologic revolution

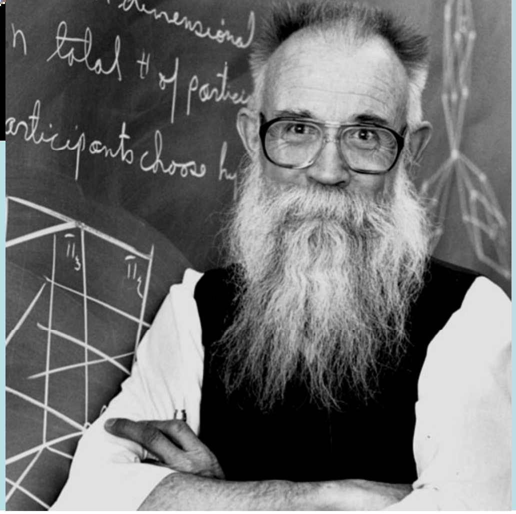
- Secure communication
- Key agreement & PKI
- Digital signatures
- Blind signatures
- Digital cash

Cryptology against nuclear arms



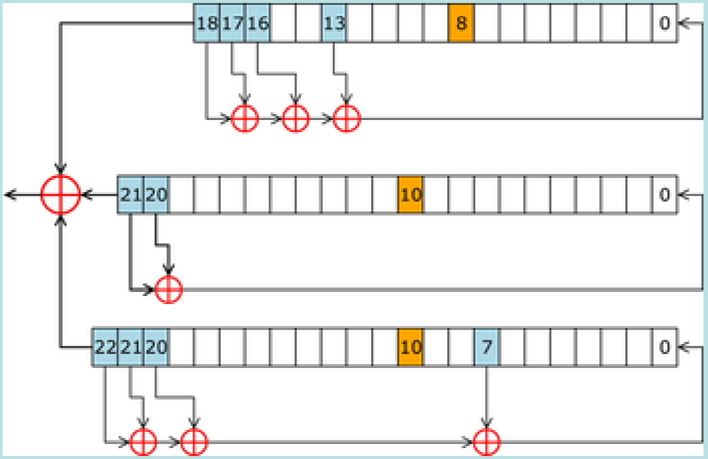
★ Installation in 97/98 ☆ Proposed

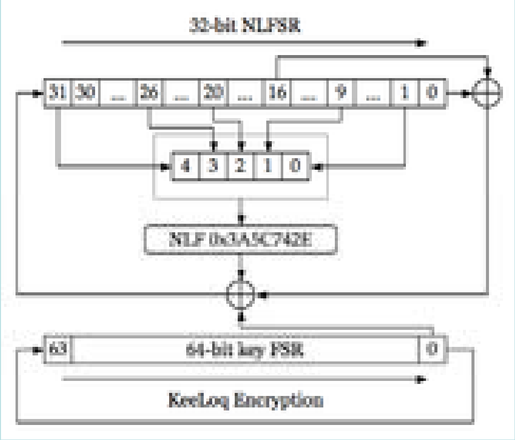


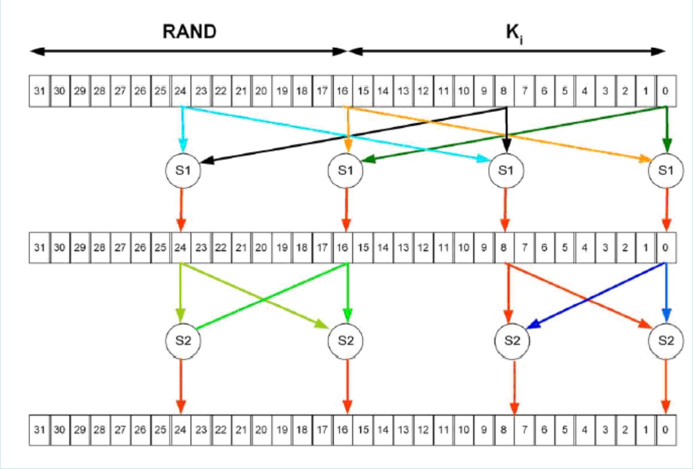


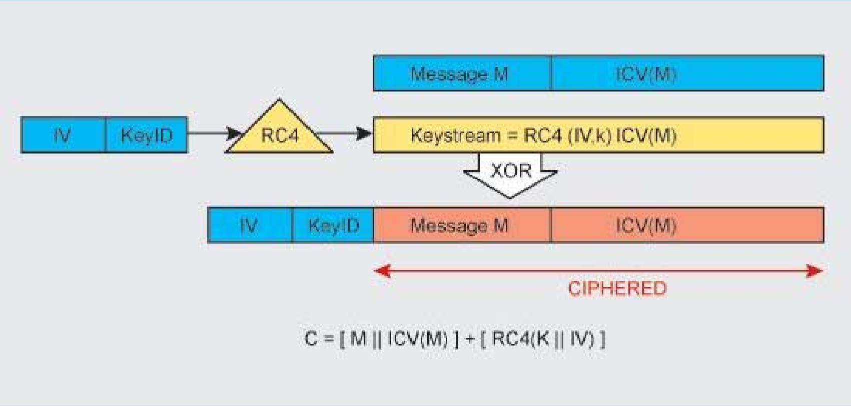
Modern Communication Networks

Modern cryptography








Message M
ICV(M)
IV
KeyID
RC4
Keystream = RC4 (IV,k) ICV(M)
XOR
IV
KeyID
Message M
ICV(M)
CIPHERED
C = [M || ICV(M)] + [RC4(K || IV)]

Industry myths

- We’ll first go to market, then we’ll add security
- Obscurity gives extra security
- Security is a very complex issue
- We have no room/money/time to add security
- We’ll never need to update (Hardcode everything)

Cases where the crypto works

VLN-07 950mAh 3.7V
CAUTION:
USE SPECIFIED CHARGER ONLY. DO NOT EXPOSE TO TEMPERATURES ABOVE 60°C/140°F. TO PREVENT INJURY OR BURNS, DO NOT ALLOW METAL OBJECTS TO CONTACT THE BATTERY TERMINALS. DO NOT DISASSEMBLE
Li-ion Battery

- When there is a business case, cryptography is deployed

Research myths

- A good model is a model that allows to prove theorems
- “Security” is what we can prove in our models

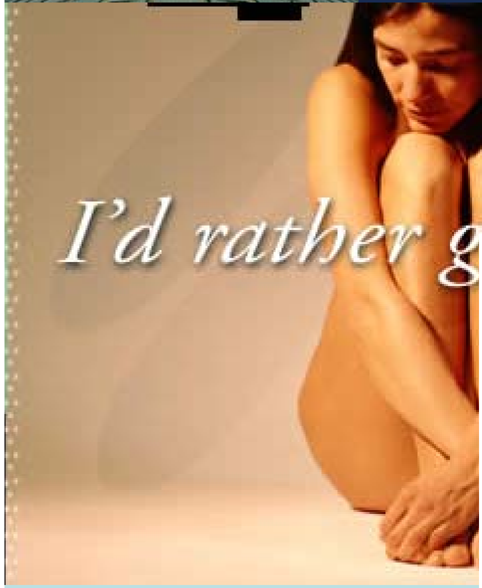
- Good research = apply well-known methods to well-known problems

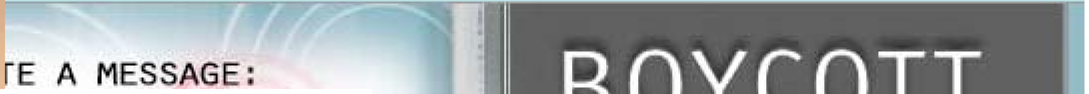
Evil cryptography

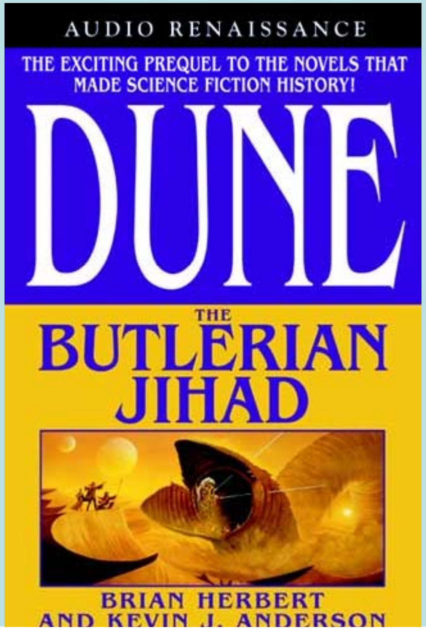
Malware writers discovered cryptography

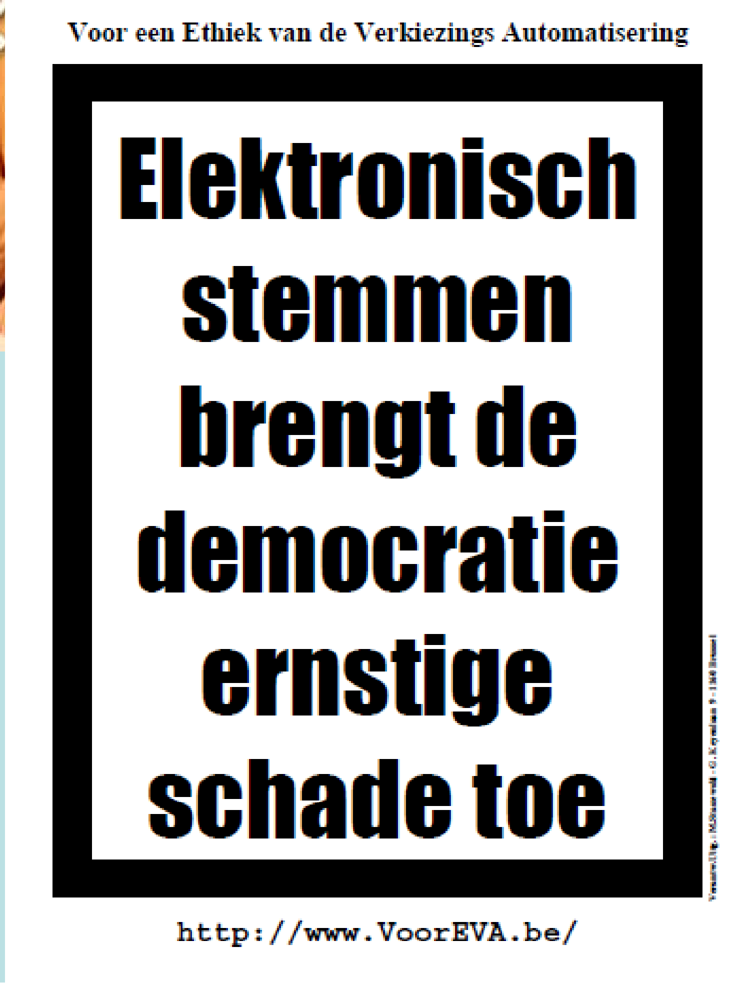
- To escape detection
- To cause reversible damage (extortion)
- To implement recovery after partial exposure

Consequences: Luddites in action






AUDIO RENAISSANCE
THE EXCITING PREQUEL TO THE NOVELS THAT MADE SCIENCE FICTION HISTORY!
DUNE
THE BUTLERIAN JIHAD
BRIAN HERBERT AND KEVIN J. ANDERSON



Voor een Ethiek van de Verkiezings Automatisering

Elektronisch stemmen brengt de democratie ernstige schade toe

http://www.VoorEVA.be/

Time for a change

Two proposals

1. Collaborative standard development
2. Best practice approach
   - Green cryptography

Example case: AES

January 1997: Announcement of initiative, Call for comments

September 1997: Call for algorithms

- Two evaluation rounds
- Three NIST conferences + 2 dedicated editions of Fast Software Encryption (FSE)
- Hundreds of papers, reports, notes, comments

October 2000: announcement of the winner

AES process: Remarkable facts

- NIST identified and approached the relevant academic community (also outside the USA!)
- NIST forced the industry to adopt 128-bit block length, at least 128-bit key length
- Cross-breeding of academic and industrial research
- Open process, many contributions

AES acceptance

- Original scope: sensitive data of the US government
- CNSS June 2003: AES for classified information, AES-192/256 for secret and top secret

- Included in ISO, IETF, IEEE standards
- 3GPP MILENAGE algorithm suite

- Software: ubiquitous
- More than 300 products certified by NIST

- EMV v4.2 (2008) still uses 2-key Triple-DES

Collaborative Standard Development

- Organize more competitions a la AES

- Invite the relevant people to contribute
- Get the industry and the academy on board
- Envision future requirements

- Advertise the development process
- Motivate submitters *and* reviewers
- Evaluate the evaluations

- Push the result

Green Cryptography: Recycling

- Limit the number of standards & standard solutions

1. Reuse of ideas that have proven their merits
2. Simplicity of implementations

- *Less is more* (Ludwig Mies van der Rohe)

Cryptographers’ Perspective

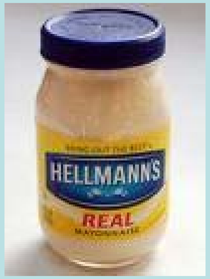
Recycle

- Design strategies
- Components
- Primitives

- Example: SHA-3 competition: Many candidates recycle parts/ideas of AES
  - Round 1: 17 AES-based candidates (out of 51)
  - Round 2:   6 AES-based candidates (out of 14)

Developers’ Perspective

- Welcome at the Diffie Mart



- Unless you absolutely cannot, use the standard

Example: Authenticated Encryption

- Encryption without authentication leads to weaknesses in almost all applications

- Bleichenbacher attacks on PKCS #1 (1998)
- Vaudenay attacks on SSL, IPsec (2002)

- Trend since 2000: combine encryption and authentication into one operation: Authenticated Encryption (AE)
  - NIST Special Publications SP 300-38X
  - ISO 19772:2009
  - RFCs

BitLocker Drive Encryption

- Uses AES ...
- ... In CBC mode
- ... Without authentication

- “No space to store authentication tags”
- Elephant diffuser

Cryptography is not DIY

- We don’t need better cryptography, we need better implementations

- Take a cryptographer on board
  - (And ask him to stick to standards)

To Open the Source or Not

- Openness has been the pulse of cryptographic design
- We should expect the same from its implementation

- Openness works in cryptography, because cryptographers to the design AND the analysis

- For implementations of cryptography, opening the source is *not sufficient* to attract cryptographers