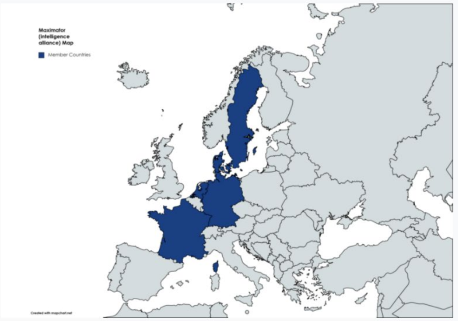
Towards a European Cryptographic Policy?

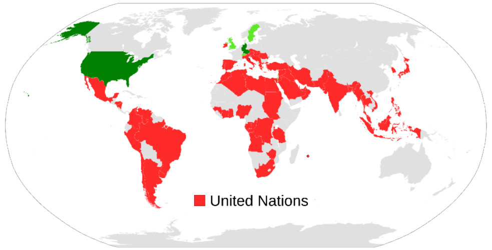
European Conference on PQC Migration
2-3 December 2025

Bart Preneel, COSIC, KU Leuven

Maximator

Maximator	
 Members shown in blue	
Type	Intelligence alliance
Members	Denmark France Germany Netherlands Sweden
Establishment	1976; 49 years ago

Rubicon Thesaurus



HAGELIN-CRYPTOS

CRYPTO AG

Philips helped US spy on Turkey, ex-employee says

Daily Sabah TÜRKIYE
Published February 17,2020

SUBSCRIBE Google News

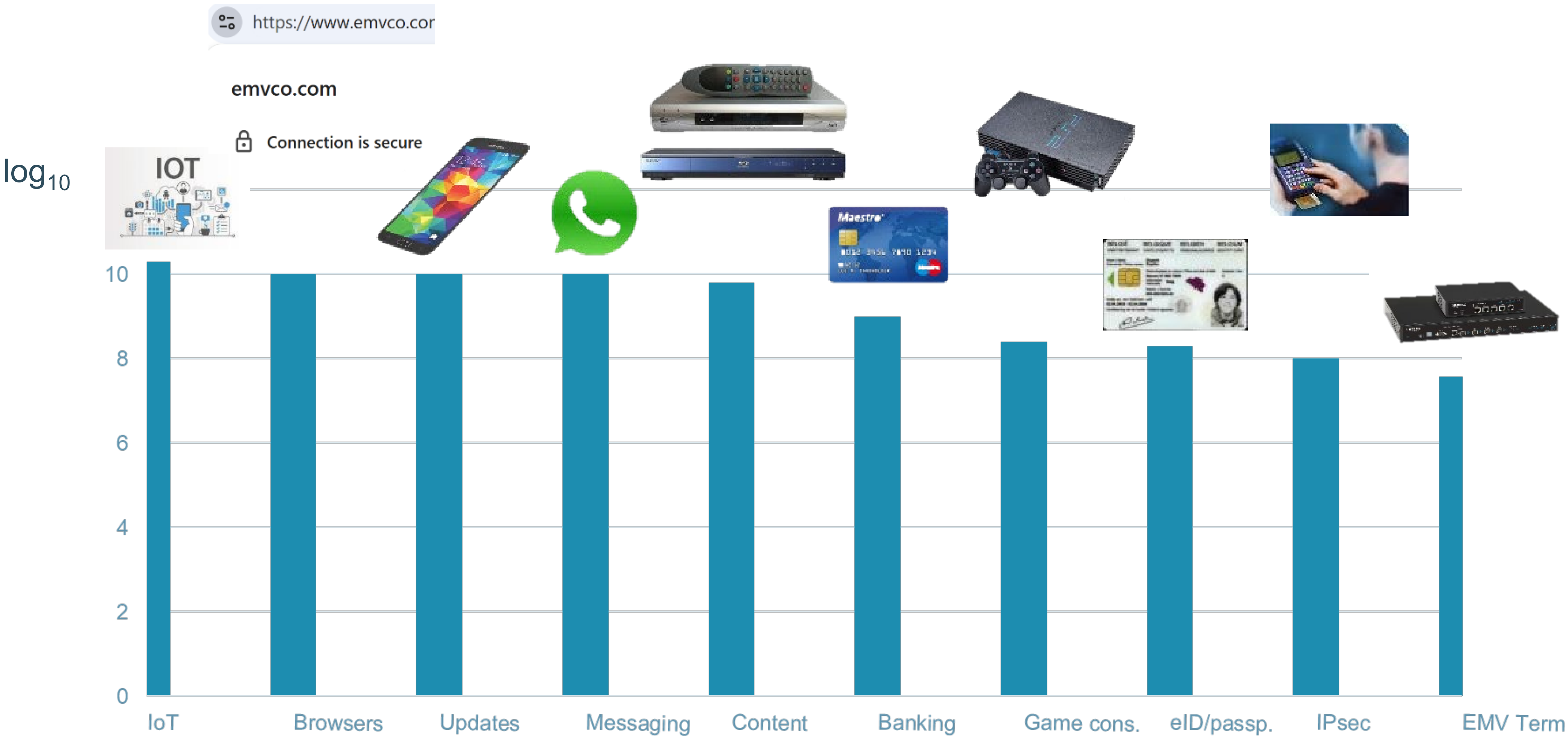
Reuters File Photo

Cryptography Timeline

kings, generals & diplomats	pre-1920	mechanical
wireless & commerce	1920-1960	electro-mechanical
finance	1960-1975	electronics
finance comms	1975-1990	VLSI
Internet GSM EMV	1990-2013	large-scale adoption
crypto-currencies messaging	2013-2025	mass adoption end-2-end
PQC	2025	ubiquitous

software

Public-key cryptography deployments ~ 60 B



KU LEUVEN

ETSI SAGE (1988)

Proprietary algorithms

- GSM: A5/1, A5/2
- GPRS: GEA1..2
- TETRA: TEA1..4
- DECT: DSC
- COMP-128-1..3

Public algorithms

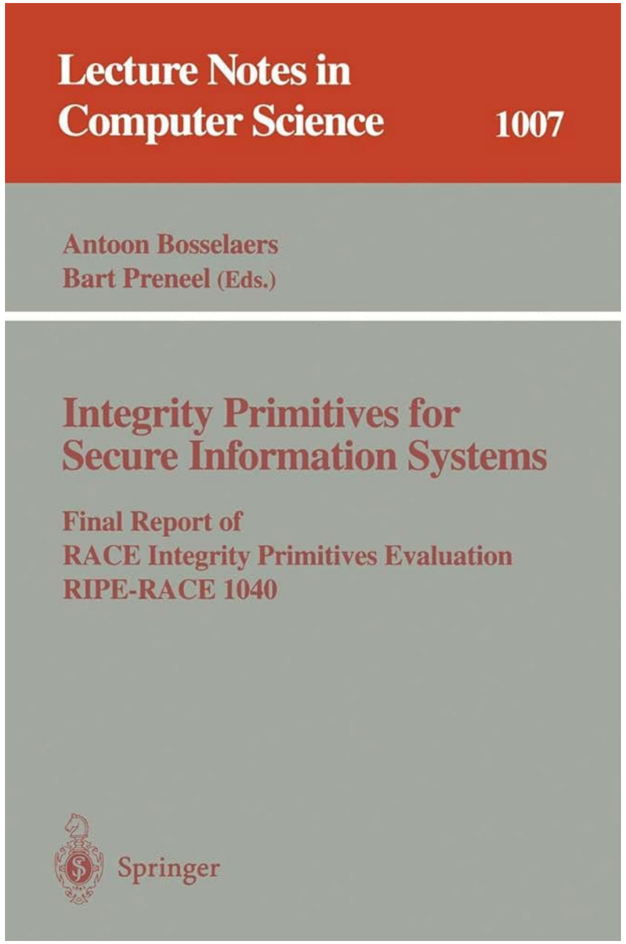
- KASUMI
- AES
- SNOW 3G
- ZUC
- MILENAGE (AES-based)
- Tuak (SHA-3-based)

https://www.ericsson.com/en/blog/2021/6/evolution-of-cryptographic-algorithms

RIPE (1988-1992)

- Restricted to integrity primitives

- Outcomes
  - Early cryptanalysis of MD4, MD5
  - RIPEMD-160
  - Polynomial hash (GMAC)



CWI

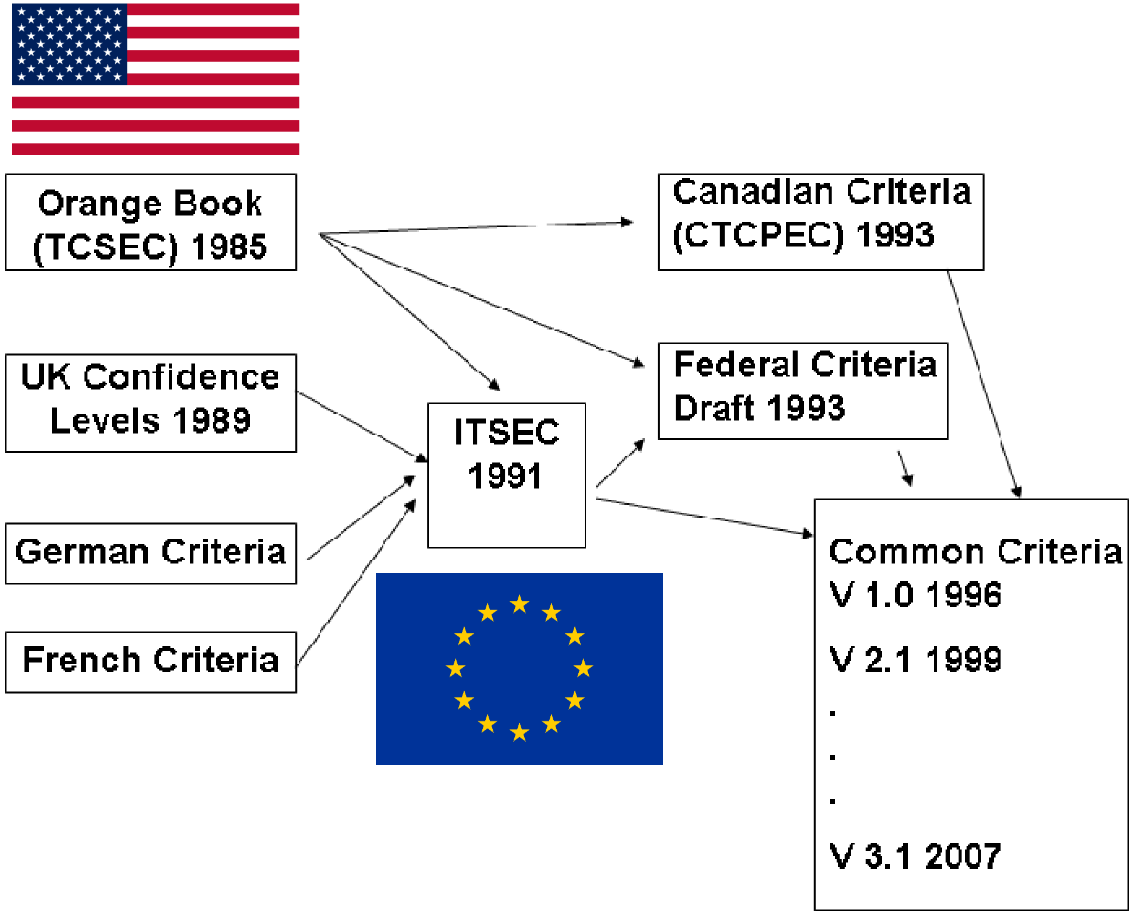
ITSEC (1991) and Common Criteria

Cryptographic algorithms: consult the appropriate national body

Requirements for Evidence

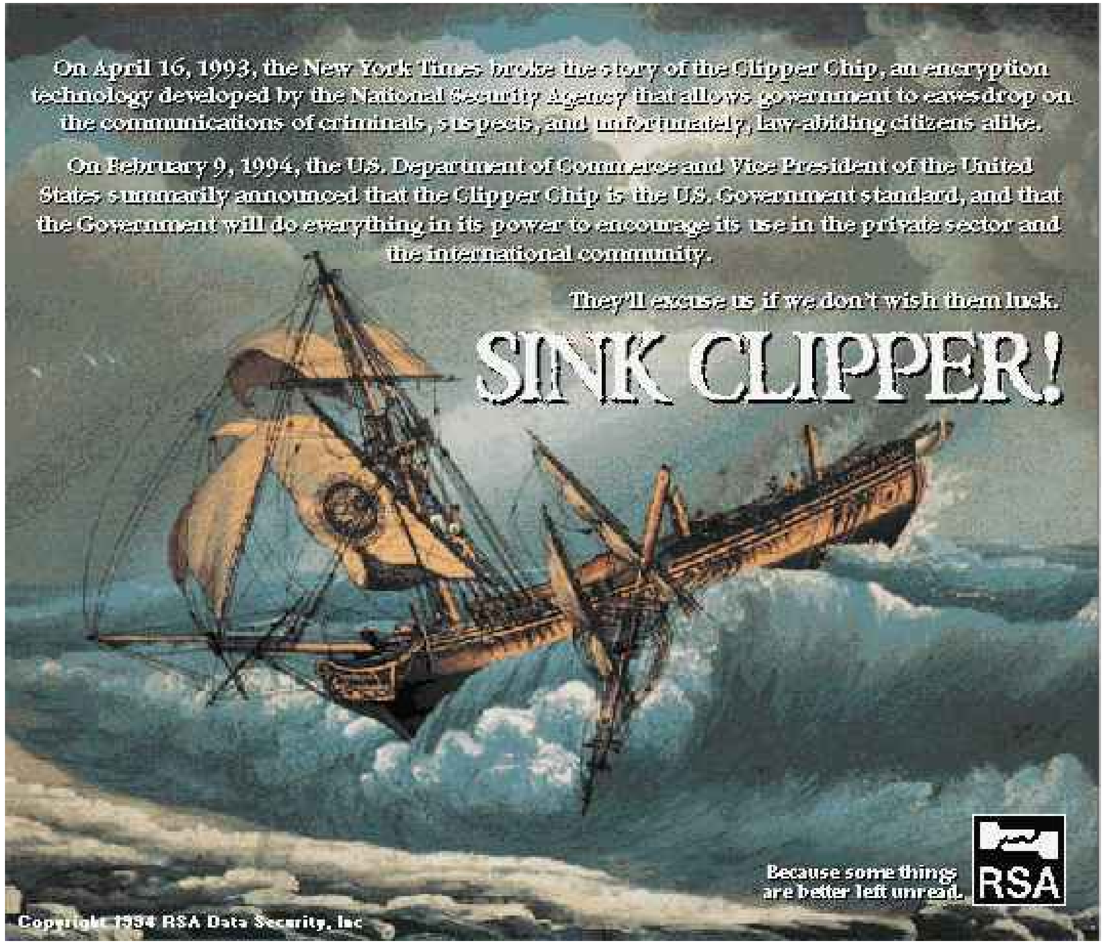
3.23 The strength of mechanisms analysis shall show that all critical mechanisms satisfy the claimed minimum strength of mechanisms rating, as defined in paragraphs 3.6 to 3.8: in the case of cryptographic mechanisms, this shall take the form of a statement of confirmation from the appropriate national body. Other analyses shall be performed using, at minimum, all the information given in figure 4 for the evaluation level in question.

1992: Creation of SOG-IS: Senior Officials Group, Information Systems Security



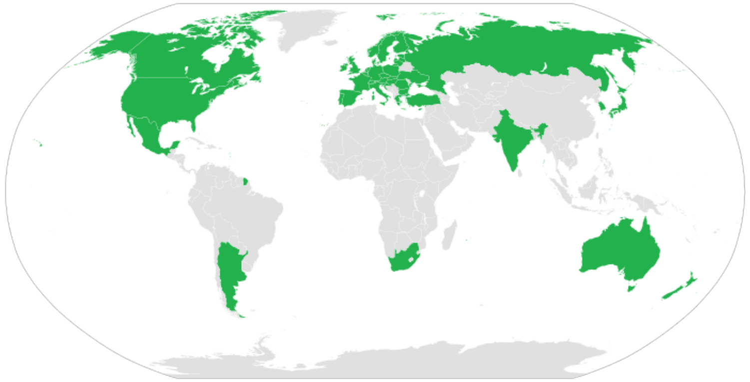
http://sogis.cc/

Clipper Chip (1993-1995)



Wassenaar arrangement
(12 July 1996)

- first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies
- Replacing Coordinating Committee for Multilateral Export Controls (CoCom)



Wassenaar Arrangement

on

Export Controls for Conventional Arms and Dual-Use Goods and Technologies

WASSENAAR ARRANGEMENT

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

'96-'97: EC draft proposal on the establishment of a Europe-wide network of Trusted Third Party Services (ETS) for certification by private services.

- Although primarily meant for establishing an infrastructure for the use of public key encryption, the proposal might also try to address the legal access problem, e.g., through key recovery. […] The Report on the results of 1995 TTP projects said that key recovery systems "can potentially provide at least part of the answer to the problems raised by confidentiality functions." These "should be investigated as a matter of priority, in order to complete the picture of TTP functionality."

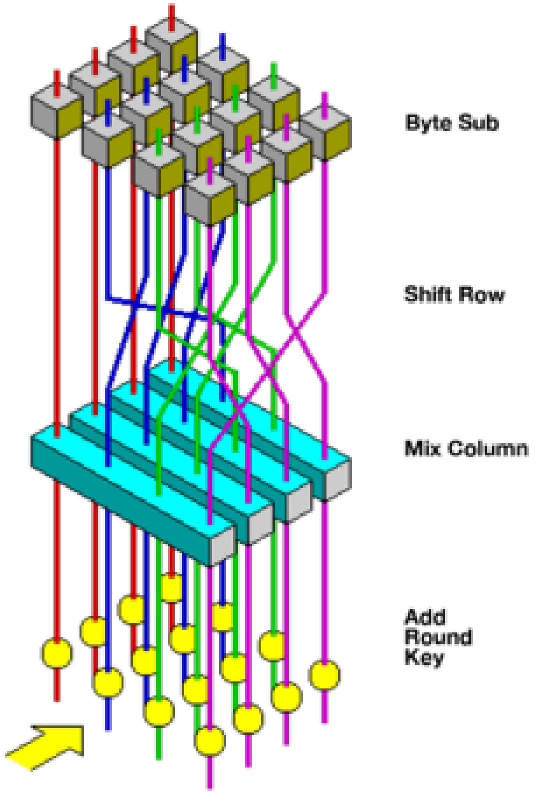
ETSI TS 102 176, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures, ETSI, Nov. 2004 (updated in 2005, 2007, 2011 and 2013)

- Need also encryption algorithm to protect signature keys, but this was removed at some stage

Selection of AES, FIPS 197 (1997-2000)

January 2000: US and Wassenaar export restrictions on encryption were revised (64-bit restriction removed)

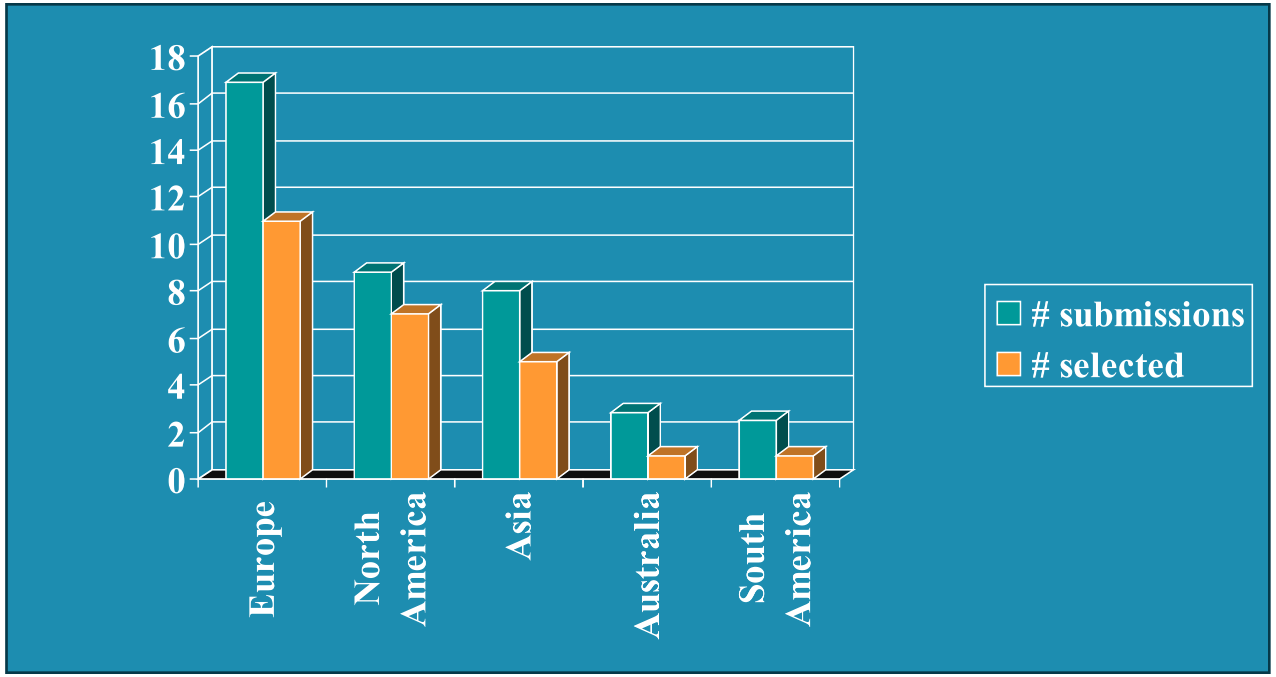
April 2000: Rijndael selected as winner of the AES competition



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NESSIE Project (2000-2003)

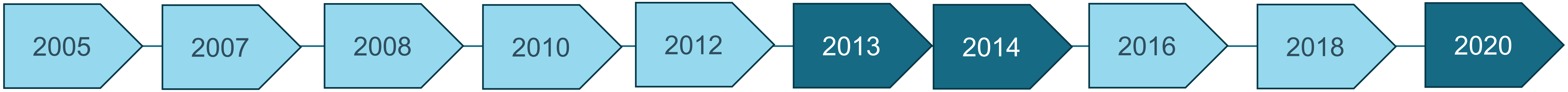
- Evaluation of cryptographic algorithms (including encryption)
- 39 submissions
- Portfolio with recommended algorithms
- Identified challenges with stream ciphers



ECRYPT (2004-2012, 2015-2018)
Key lengths, parameters and protocols

ECRYPT

ECRYPT CSA



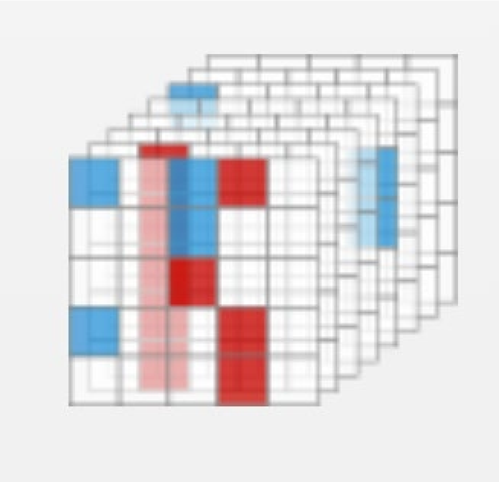
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

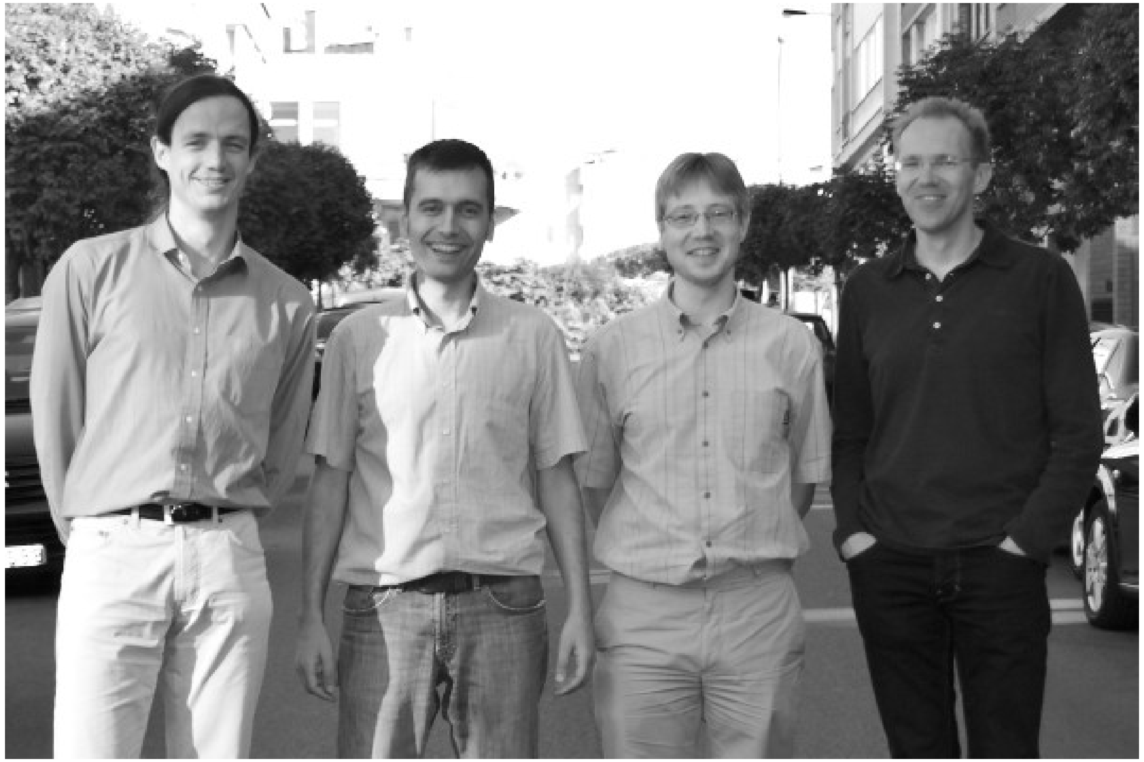
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Expanded to cryptographic protocols such as TLS

Selection of SHA-3, FIPS 202 (2008-2015)

2012: Keccak selected as winner of the SHA-3 competition





NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

2. *For the purposes of 5A002.a., 'described security algorithm' means any of the following:*

a. *A 'symmetric algorithm' employing a key length in excess of 56 bits, not including parity bits;*

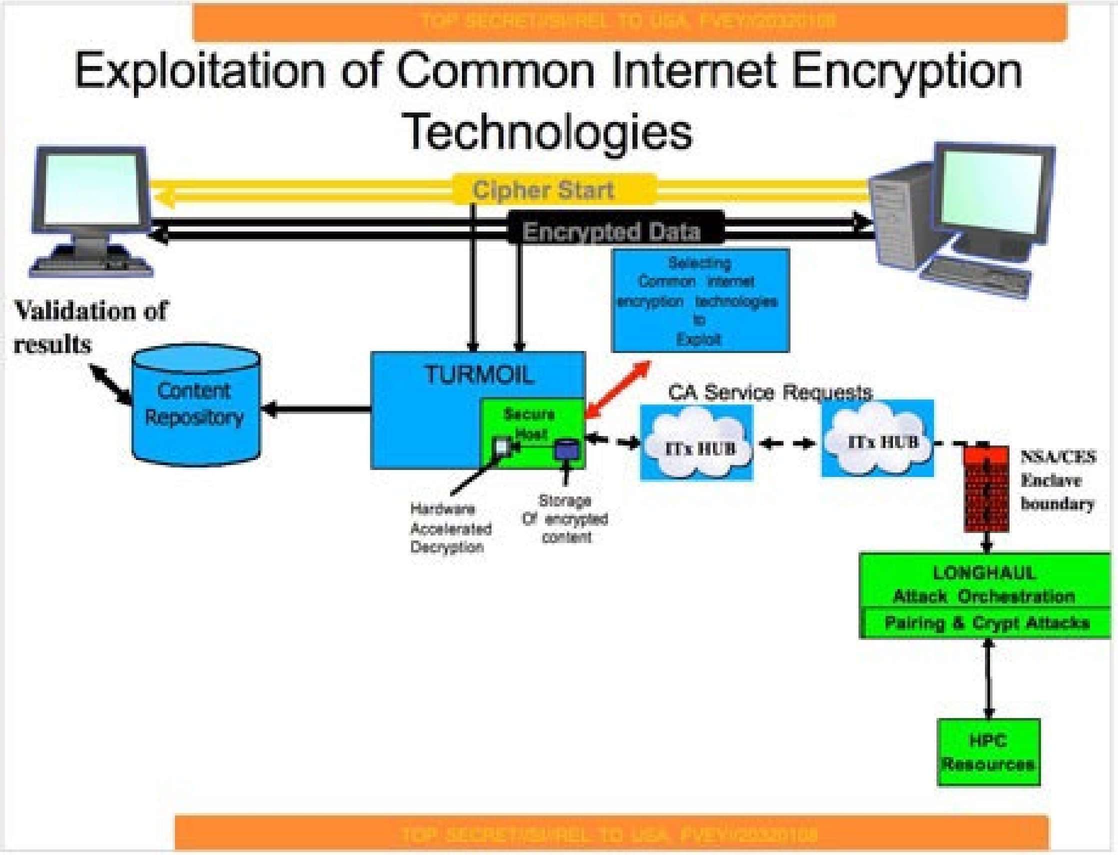
b. *An 'asymmetric algorithm' where the security of the algorithm is based on any of the following:*

   1. *Factorisation of integers in excess of 512 bits (e.g., RSA);*
   2. *Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or*
   3. *Discrete logarithms in a group other than mentioned in paragraph b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve); or*

c. *An 'asymmetric algorithm' where the security of the algorithm is based on any of the following:*

   1. *Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium);*
   2. *Finding isogenies between Supersingular elliptic curves (e.g., Supersingular Isogeny Key Encapsulation); or*
   3. *Decoding random codes (e.g., McEliece, Niederreiter).*

Snowden documents: Bullrun (2013)
Resulting in inquire at NIST about Dual-EC DRBG



NIST Cryptographic Standards and Guidelines Development Process

Report and Recommendations of the
Visiting Committee on Advanced Technology
of the National Institute of Standards and Technology

July 2014

https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

From ETSI to SOG-IS (2019)

- ETSI TS 119 312, Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites (2014-2019-2021-2023-2024)
  - From 2019: “In order to avoid duplicated effort, the assessment of the security of underlying cryptographic schemes is delegated to the SOG-IS document.”
- SOG-IS Crypto Working Group: "SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms“ (updated 2016-2018-2020-2023)
  - The SOG-IS Crypto WG offers technical support for the establishment of a *SOG-IS Crypto Evaluation Scheme*, i.e. a set of requirements and evaluation procedures related to cryptographic aspects of CC security evaluations of IT products and mutually agreed by SOG-IS participants.
- October ‘23: EUCC approved: EU Cybersecurity Certification Scheme on Common Criteria

European Cybersecurity Certification Group: Agreed Cryptographic Mechanisms

(v2.0 April 2025)

https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf

- **Good:** Adds lattice-based schemes Frodo-KEM and ML-KEM in hybrid mode
- **Bad:** Phasing out RSA-2048 (up to RSA-2999) for encryption by the end of 2025!
- **Ugly:** transparent process for public review is missing

National cryptography guidelines (examples)

- Bundesamt fur Sicherheit in der Informationstechnik. Technical Guideline TR02102-1, BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths" 2019-2025 (last version: 2025-1)
  - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

- ANSSI-pg-083 Guide Des Mécanismes Cryptographiques, Règles et Recommandations Concernant le Choix et le Dimensionnement des Mécanismes Cryptographiques, 2004-2020 (last version: 2020)
  - https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf

EU versus Member States on Cryptography

- Member States point to Art. 4 of the Lisbon treaty (national security)
- EU academia and industry
  - extensive expertise in cryptographic algorithms and protocols
  - play strong role in NIST open competitions (AES, SHA-3, PQC)
  - NIST processes have been criticized due to NSA involvement, but at least they have a transparent review and commenting process
- At EU level
  - only a cryptographic policy for (EU)CC
  - transparency is lacking – no or very limited input from academia and industry

ProtectEU Internal Security Strategy

(April 1, 2025)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0148

The Commission will:

- present a Roadmap setting out the way forward on lawful and effective access to data for law enforcement in 2025
- prepare an impact assessment in 2025 with a view to updating rules on data retention at EU level, as appropriate
- present a Technology Roadmap on encryption to identify and assess technological solutions to enable lawful access to data by law enforcement authorities in 2026

Recommendations

Involve industry and academia at EU level (from the beginning) in all cryptographic guidelines

At the very least offer sufficiently long period for public comments on all cryptographic guidelines

Create expert group with broad composition (academia/industry/ government)

https://health.ec.europa.eu/medical-devices-expert-panels/work-expert-panels_en

Develop a cryptographic strategy involving all the stakeholders

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: homes.esat.kuleuven.be/~preneel/

EMAIL: Bart.Preneel@esat.kuleuven.be

MASTODON: bpreneel@infosec.exchange

TWITTER: @bpreneel1

TELEPHONE: +32 16 321148

KU LEUVEN

ArenBerg Crypto BV

COSIC

Link to slides

https://homes.esat.kuleuven.be/~preneel/eu_crypto_policy_3dec25.pdf