AES and NESSIE: Cryptographic algorithms for the 21st century

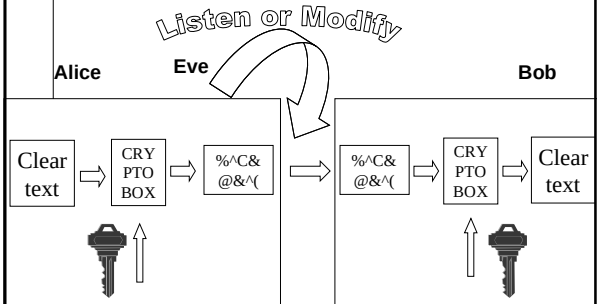
Bart Preneel
Katholieke Universiteit Leuven, COSIC
bart.preneel@esat.kuleuven.ac.be
http://www.esat.kuleuven.ac.be/~preneel

Agenda

- AES
- The NESSIE project

- Why?
- Status
- The future

Cryptology: basic principles

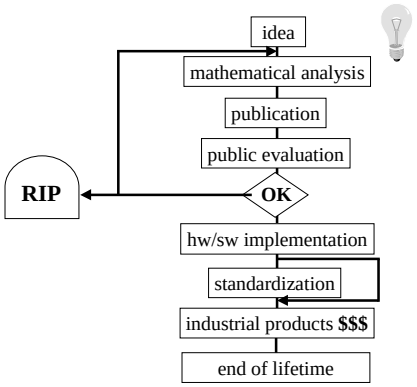


The Rotor machines (WW II)



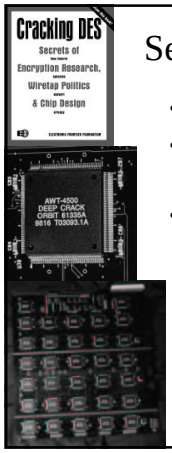


Life cycle of a cryptographic algorithm



Data Encryption Standard (1977)

- encrypts 64 plaintext bits under control of a 56-bit key
- 16 iterations of a relatively simple mapping
- designed by IBM together with NSA
- FIPS: US government standard for sensitive but unclassified data
- worldwide de facto standard since early 80ies
- surrounded by controversy



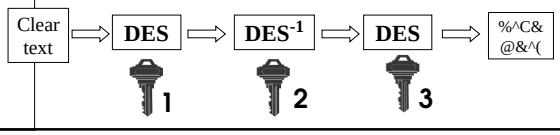
Security of DES (56-bit key)

- PC: trying 1 DES key: 0.25 μs
- Trying all keys on 4000 PCs:
  1 month: $2^{22} \times 2^{16} \times 2^{5} \times 2^{12} = 2^{55}$
- M. Wiener's estimate (1993):
  1,000,000 $ machine: 10 minutes in 2002

EFF Deep Crack (July 1999)
250,000 $ machine: 50 hours…

Solution to DES key length

- Moore's "law": speed of computers doubles every 18 months
  – key lengths need to grow in time
- Use new algorithms with longer keys
  – adding 1 key bits doubles the work for the attacker
- Or replace DES by triple-DES (168-bit key):



AES (Advanced Encryption Standard)

- open competition launched by US government (Sept. '97) to replace DES
- 128-bit block cipher with long key (128/192/256 bits)
- as strong as triple-DES, but more efficient
- royalty-free

A machine that cracks a DES key in 1 second would take 149 trillion years to crack a 128-bit key

15 AES Candidates (1st round - 1998)

- CAST-256 (Canada)
- Crypton (Korea)
- Deal (Canada)
- DFC (France)
- E2 (Japan)
- Frog (Costa Rica)
- HPC (USA)
- LOKI97 (Australia)
- Magenta (Germany)
- Mars (USA)
- RC6 (USA)
- Rijndael (Belgium)
- Safer+ (USA)
- Serpent (UK/IL/DK)
- Twofish (USA)

15 AES Candidates (1st round)

- CAST-256 (Canada)
- ~~Crypton (Korea)~~
- ~~Deal (Canada)~~
- ~~DFC (France)~~
- E2 (Japan)
- ~~Frog (Costa Rica)~~
- ~~HPC (USA)~~
- ~~LOKI97 (Australia)~~
- ~~Magenta (Germany)~~
- Mars (USA)
- RC6 (USA)
- Rijndael (Belgium)
- ~~Safer+ (USA)~~
- Serpent (UK/IL/DK)
- Twofish (USA)

····· too slow
——— some weakness

15 AES Candidates (1st round)

- ~~CAST-256 (Canada)~~
- ~~Crypton (Korea)~~
- ~~Deal (Canada)~~
- ~~DFC (France)~~
- ~~E2 (Japan)~~
- ~~Frog (Costa Rica)~~
- ~~HPC (USA)~~
- ~~LOKI97 (Australia)~~
- ~~Magenta (Germany)~~
- Mars (USA)
- RC6 (USA)
- Rijndael (Belgium)
- ~~Safer+ (USA)~~
- Serpent (UK/IL/DK)
- Twofish (USA)

····· too slow
——— some weakness
⟺ ∃ better alternatives

5 finalists [Aug. 1999]

- MARS', RC6, Rijndael, Serpent, Twofish
- Criteria:



security



performance



intellectual property



Security

- Limited cryptanalysis has been done during selection process
- Best known "attack"
  - MARS: 12 out of 32 rounds
  - RC6: 15..16 out of 20 rounds
  - Rijndael: 6..7 out of 10..14 rounds
  - Serpent: 9 out of 32 rounds
  - Twofish: 7..8 out of 16 rounds
- Some finalists are even "secure against unknown attacks"



Performance

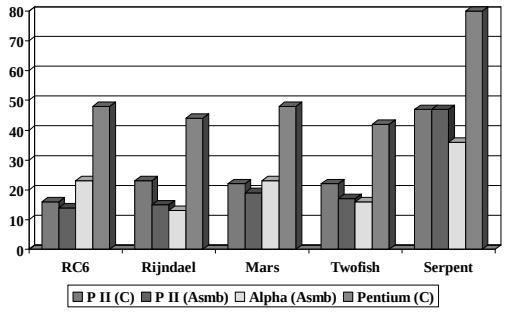
- Pentium Pro 200 MHz/Borland 5.0 reference platform/compiler
- Restricted environments
  - RAM requirements
  - Just in Time key schedule
  - resistance to side channel attacks (DPA)
- Hardware: NSA

Performance is very complex

- level of optimization
- encryption versus decryption
- memory usage
- number of blocks (key agility)
- security margin
- implementation attacks

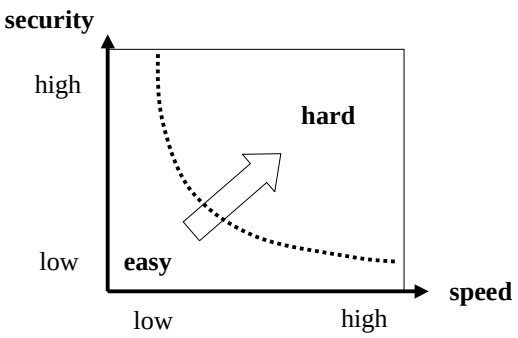


Software performance (cycles/byte)



Rijndael does 2-3x better for very short messages

Design trade-off





Intellectual property issues

- All submitters agree to waive intellectual property rights if their own algorithm is chosen
- Most submitters agree unconditionally to waive IP rights if someone else's is chosen
- In March 2000, a Japanese company has claimed IP on 4 of the 5 finalists
  - Rijndael does not use fixed rotations

And the winner is...Rijndael

- Joan Daemen (pronounced Yo'-ahn Dah'-mun)
- Vincent Rijmen (pronounced Rye'-mun).

Joan Daemen

PhD in COSIC in 1995

now at Proton World International

Vincent Rijmen

PhD in COSIC in 1997

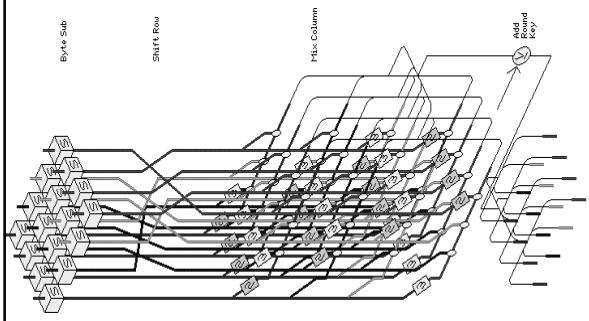
now at Cryptomathic



Rijndael

- history: Shark (1996) and Square (1997)
- security and efficiency through
  - simplicity
  - symmetry
  - modularity
- efficient on many platforms, including smart cards
- easier to protect against side channel attacks

Rijndael: 1 round



AES Status

- FIPS 197 published on 6 December 2001
- Revised FIPS on modes of operation
- Rijndael has more options than AES

- fast adoption in the market
  - early 2002, 74 products are using AES
  - standardization: ISO, IETF, …
- slower adoption in financial sector

NESSIE

New European Schemes for Signature, Integrity and Encryption

- EU Fifth Framework Program, IST
- 2000-2002
- http://www.cryptonessie.org

NESSIE goals

- put forward a portfolio of strong cryptographic primitives that have been obtained based on an OPEN call and an OPEN evaluation process
- deliver input to AES
- consensus building and dissemination
- strengthen European research and industry

NESSIE

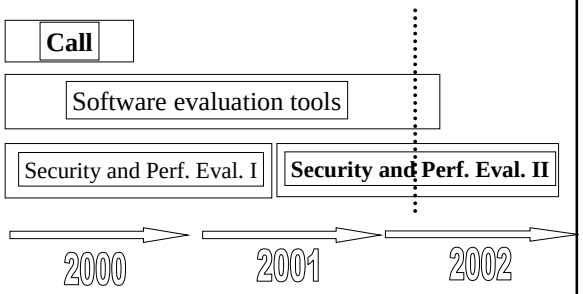


NESSIE partners

K.U.Leuven, B
ENS, F
RHUL, UK
SAG, D
Technion, IL
UiB, N
UCL, B



NESSIE timing



Related initiatives

- US: two calls for block cipher in 70ies, resulting in DES
- US: AES
  - http://www.nist.gov/aes
- Japan: CRYPTREC
  - http://www.ipa.go.jp/security
- Europe: RIPE (Race Integrity Primitives Evaluation) (1989-1992)

Primitives requested

+ evaluation methodologies

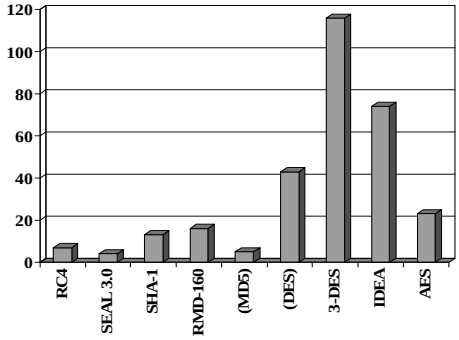
- block ciphers
- stream ciphers
- self-synchronizing stream ciphers
- MAC Algorithms
- collision-resistant hash functions
- one-way hash functions
- families of pseudo-random functions
- asymmetric encryption schemes
- asymmetric digital signature schemes
- asymmetric identification schemes

Why new primitives?

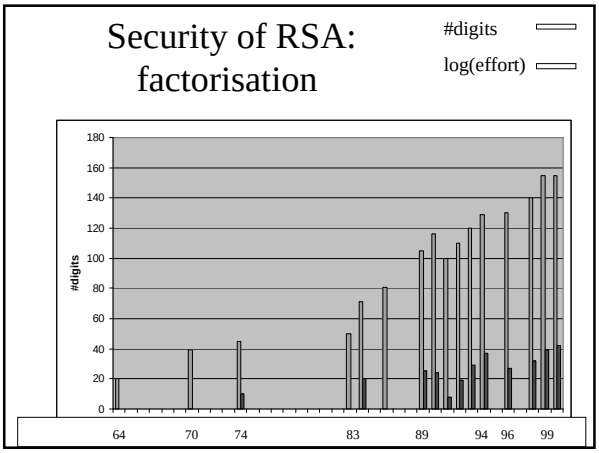
- Stream ciphers and MACs provide a better performance than block ciphers
- Need similar progress as for AES (higher security level and better performance)
  - Need new hash function for digital signatures
- Asymmetric schemes:
  - need for public key algorithms that are NOT based on factoring or algebraic number theory
  - how to use RSA?
- Side channel attacks

Performance reference data

(cycles/byte) Pentium



Security of RSA: factorisation



What about quantum computers?

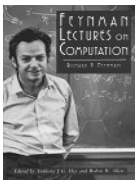
- exponential parallelism

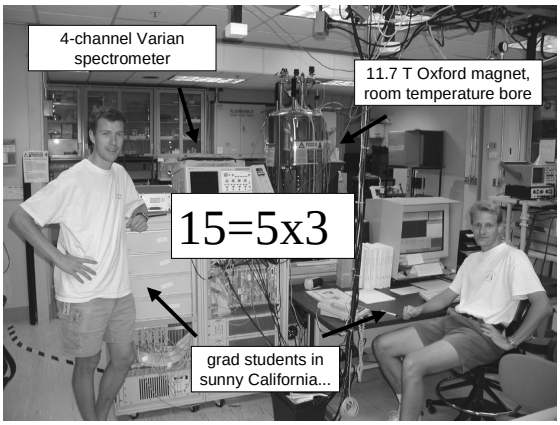
n coupled quantum bits

⇩

2^n degrees of freedom !

- Shor 1994: perfect for factoring
- But: can a quantum computer be built?

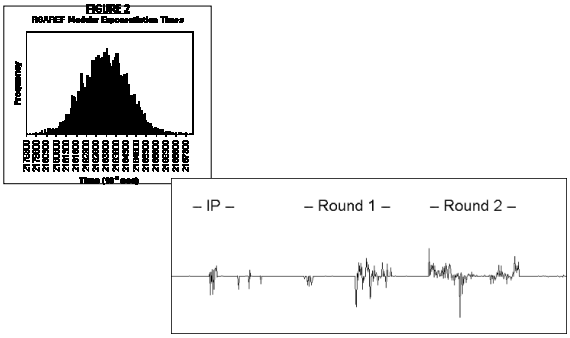




Insecure use of RSA

- RSA security assumption: extracting random e-th roots is hard (≠ factorisation)
- But… most standards do not rely on this specific assumption
  - 1998: PKCS v1 broken
  - 1999: ISO 9796-1:1991 broken
  - 2000: PCKS v2 (OAEP) has problems

Timing attacks and power analysis



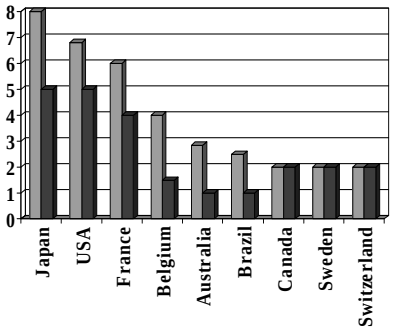
Results of NESSIE Call

43 submissions:

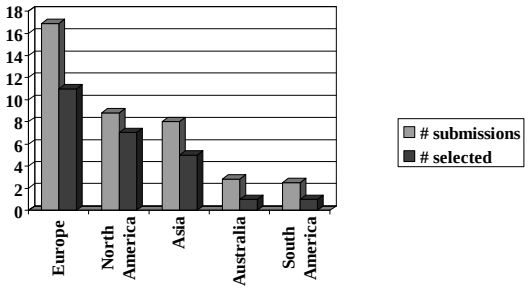
- 17 block ciphers
- 6 synchronous stream ciphers
- 3 hash & MAC
- 16 public-key primitives
- 1 identification scheme

24 submissions retained for phase II

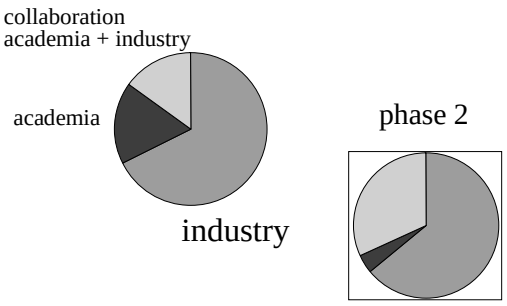
Submissions by country



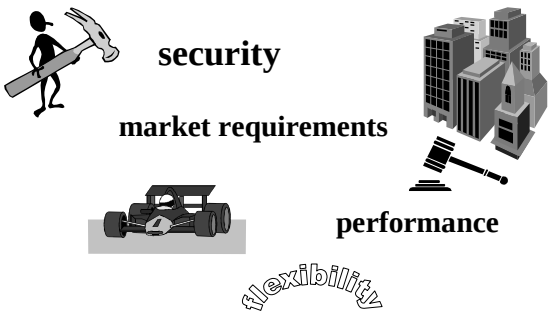
Submissions by region



Industry versus Academia



Selection criteria



NESSIE Project Industry Board

- provide guidance on: type of primitives, evaluation criteria, IPR issues,…
- technical input: performance evaluation,…
- standardisation strategy and consensus building
- meeting: twice per year
- 25 security vendors and users

IPR Status

- 10 in public domain
- 6 reasonable and non-discriminatory
- 2 reasonable and non-discriminatory + reciprocate
- 4 don't know yet

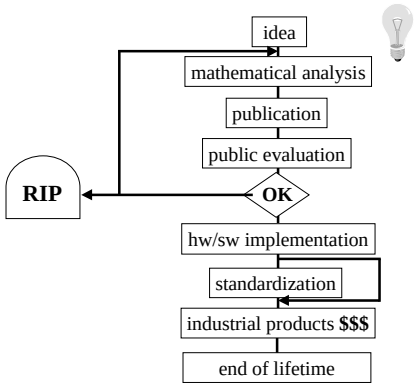
Standardization

- ISO/IEC JTC1/SC27
- P1363
- IETF
- Framework of European Directive: EESSI
  - CEN, ETSI

Conclusions

- AES: a European success story in the area of block ciphers
  - free for all
- NESSIE: European research on new cryptographic primitives with better security and performance
  - all 6 stream ciphers submitted have been broken
  - developing and validating new asymmetric primitives is a major challenge (proofs!)
  - IPR will be a key issue
- essential component of digital economy

Life cycle of a cryptographic algorithm



AES: http://www.nist.gov/aes

NESSIE: http://www.cryptonessie.org

The end

