

**ECRYPT II**  
ITP@U^t  
<http://www.ecrypt.eu.org>

## Upgrading Cryptographic Algorithms for Network Security

Bart Preneel  
 COSIC, K.U.Leuven, Belgium  
 Bart.Preneel(at)esat.kuleuven.be  
<http://homes.esat.kuleuven.be/~preneel>  
 September 2009

1

## Information processing

the Internet of things, ubiquitous computing, pervasive computing, ambient intelligence ( $10^{12}$ )

Internet and mobile ( $10^9$ )

PCs and LANs ( $10^7$ )

mainframe ( $10^5$ )

mechanical processing ( $10^4$ )

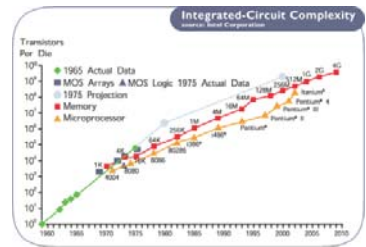
manual processing ( $10^2$ )

2

## Exponential growth

Ray Kurzweil, KurzweilAI.net

- Human brain:  $10^{14}$  ...  $10^{15}$  ops and  $10^{13}$  bits memory
- 2025: 1 computer can perform  $10^{16}$  ops ( $2^{53}$ )
- 2013:  $10^{13}$  RAM bits (1 Terabyte) cost 1000\$



3



4

## Context

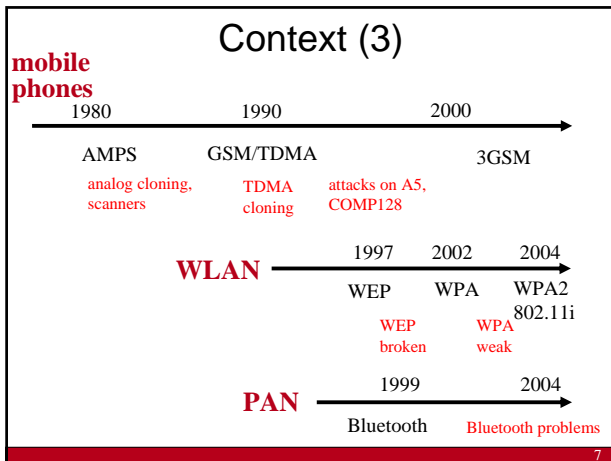
DES, RSA, DH, CBC-MAC	<b>HARDWARE</b>	70
Provable security (PKC), ZK, ElGamal, ECC, stream ciphers	Limited (govt+financial sector) DES, 3DES	80
MD4, MD5	<b>SOFTWARE</b>	90
Provable security (SKC)	GSM, PGP	
Key escrow	C libraries (RSA, DH)	
How to use RSA?	SSL/TLS, IPsec, SSH, S/MIME	
Alternatives to RSA	Java crypto libraries	
PKI	WLAN	
AES	<b>EVERYWHERE</b>	
ID-Based Crypto	Trusted computing, DRM, 3GPP, RFID, sensor nodes	

5

## Context (2)

1900	<b>wireless data</b>	1960	1980	1990	2000
	Vernam: OTP	rotor machines	LFSR		WLAN PAN 3GSM
1900	<b>wired data</b>	1960	1980	1990	2000
			block ciphers	X25	TLS SSH IPsec
1900	<b>wired voice</b>	1960	1980	1990	2000
		analog scramblers		STU	VoIP

6



### TLS 1.2 Data Encapsulation Options

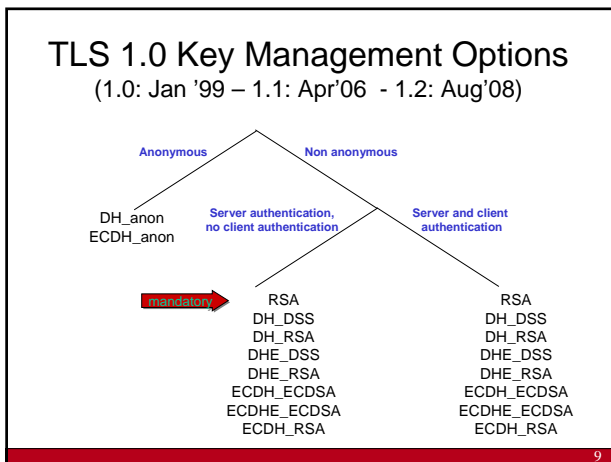
(1.0: Jan '99 – 1.1: Apr'06 - 1.2: Aug'08)

Integrity			
key size	128	160	160
algorithm options	AES-XCBC-MAC HMAC-MD5	HMAC-SHA	HMAC-SHA256

mandatory

Confidentiality			
key size	128	168	256
algorithm options	RC4 AES_CBC (AES_CTR) CAMELLIA_CBC SEED_CBC	3DES_EDE_CBC	AES_CBC CAMELLIA_CBC

mandatory



- ### TLS evolution
- 2002: AES
  - 2005: Camellia + PSK (pre-shared key variants)
  - 2006: ECC
  - 2008: PRF based on SHA-256

### IKE Algorithm Selection

#### Mandatory Algorithms

Algorithm Type	IKE v1	IKE v2
<b>Payload Encryption</b>	DES-CBC	<b>3DES_CBC</b> (AES_128_CBC)
<b>Payload Integrity</b>	HMAC-MD5 HMAC-SHA1	HMAC-SHA1
<b>DH Group</b>	768 Bit	<b>1024</b> (2048) Bit
<b>Transfer Type 1 (Encryption)</b>	ENCR_DES_CBC	<b>ENCR_3DES</b> (ENCR_AES_128_CBC)
<b>Transfer Type 2 (PRF)</b>	PRF_HMAC_SHA1 [RFC2104]	PRF_HMAC_SHA1 [RFC2104]
<b>Transfer Type 3 (Integrity)</b>	AUTH_HMAC_SHA1_96 [RFC2404]	AUTH_HMAC_SHA1_96 [RFC2404]

Source: RFC 4384, April 07

- ### NSA Suite B (2005)
- (see also RFC 4869 – April 07)
- Block cipher: AES-CBC (128 + **256**-bit keys)
  - MAC algorithms: GMAC (128 + **256**-bit keys)
  - Authenticated encryption: AES-GCM (128 + **256**-bit keys)
  - Digital signatures: ECDSA (256 + **384**-bit prime moduli)
  - Key agreement: ECDH (256 + **384**-bit prime moduli)
  - Hashing: SHA-256 and **SHA-384**
- Note: NSA has licensed the rights to 26 patents held by Certicom Inc. covering a variety of elliptic curve technology.

### Implementations in embedded systems

Protocol: Wireless authentication protocol design

Algorithm: Embedded fingerprint matching algorithms, crypto algorithms

Architecture: Co-design, HW/SW, SOC

Micro-Architecture: co-processor design

Circuit: Circuit techniques to combat side channel analysis attacks

Technology aware solutions?

Slide credit: Prof. Ingrid Verbauwhede 13

### Disclaimer: cryptography ≠ security

- crypto is only a tiny piece of the security puzzle – but an important one
- most systems break elsewhere
  - incorrect requirements or specifications
  - implementation errors
  - application level
  - social engineering
- for intelligence, traffic analysis (SIGINT) is often much more important than cryptanalysis

14

[Adi Shamir '08] We are winning yesterday's information security battles, but we are losing the war. Security gets worse by a factor of 2 every year.

[Steve Kent '09] Current cryptography for network security is fine; if you need better performance, just throw in more hardware. The remaining challenge is high performance authentication for multicast

15

### Challenges for crypto

- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint

Performance

Cost Security

secure software and hardware implementations

Algorithm agility

16

### Outline

- Context
- Block ciphers
  - (Stream ciphers)
- Hash functions
  - (MAC algorithms and authenticated encryption)
- Public-key cryptology
  - (Protocols)
- Implementations issues
- Research challenges

17

### Block cipher

P1 P2 P3

block cipher block cipher block cipher

C1 C2 C3

- larger data units: 64...128 bits
- memoryless
- repeat simple operation (round) many times

18

## Block ciphers

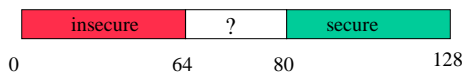
### 64-bit block

- 3-DES (112-168)
- IDEA (128)
- KASUMI (128 in 3G, 64 in 2G)
- MISTY1 (128)
- PRESENT (80-128)
- KATAN (80)

### 128-bit block

- AES (128-192-256)
- RC6
- CAMELLIA
- ...

Symmetric key lengths



19

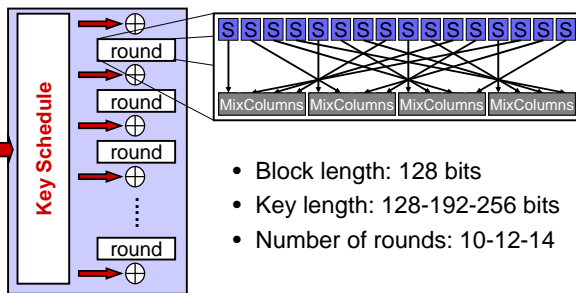
## AES (2001)

- open competition: 1997-2000
- FIPS 197 published on December 2001
- mandatory for sensitive US govt. information
- fast adoption in the market
  - ten thousands of products
  - NIST validation list: 1168 implementations
    - <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>
  - standardization: ISO, IETF, IEEE 802.11, ...
- slower adoption in financial sector
- mid 2003: AES-128 also for **classified** information and AES-192/-256 for **secret** and **top secret** information!

[Adi Shamir '07] AES may well be the last block cipher

20

## AES/Rijndael



- Block length: 128 bits
- Key length: 128-192-256 bits
- Number of rounds: 10-12-14

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

21

## AES implementations: efficient/compact

- SW: 7.6 cycles/byte on Core 2 or 110 Mbyte/s – bitsliced [Käsper-Schwabe'09]
- HW: 43 Gbit/s in 130 nm CMOS ['05]
- Intel (+AMD): new AES instruction: 0.75 cycles/byte ['09-'10]
- HW: most compact: 3600 gates
  - KATAN: 1054, PRESENT: 1570

22

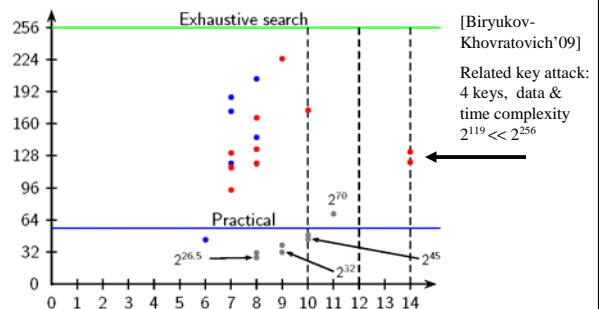
## AES: security

- Algebraic “attack”:
  - compact description of AES-128: 8000 quadratic equations with 1600 variables
  - is it hard to solve sets of non-linear Boolean equations?
  - no attack has been found that can exploit this structure (in spite of earlier claims)
- implementation level attack, e.g., cache timing, fault attacks
  - requires special countermeasures such as bitslice implementation or hardware
- [Biryukov+09] the key schedule of AES-256 is too lightweight: related key attacks
  - No implications on security of AES-128

23

## Related key attacks on AES-256

[Biryukov-Dunkelman-Keller-Khovratovich-Shamir'09]



Slide credit: Orr Dunkelman

24

### Block ciphers: Keeloq

- Microchip Inc algorithm, designed in the 1980s
- Allegedly used in 80% of the cars for car locks, car alarms
- Block cipher with 32-bit blocks, 64-bit keys and 528 simple rounds



25

### Block ciphers: Keeloq (2)

Leaked on the internet in 2006

[Bogdanov07] in some cases car key = Master key + Car ID  
[Bogdanov07], [Courtois-Bard-Wagner07] first cryptanalysis  
[Biham-Dunkelman-Indesteeghe-Keller-Preneel07]:

1 hour access to token ( $2^{16}$  known texts)

2 days of calculation on 50 PCs (10.000\$) -  $2^{44.5}$  encryptions

[Eisenbarth-Kasper-Moradi-Paar-Salmasizadeh-Manzuri Shalmani-Paar 08]

Side channel attack allows to recover master key

in 2010 cryptographers will drive expensive cars

26

### Block ciphers: conclusions

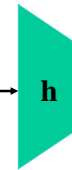
- Several mature block ciphers available
- Security well understood
  - in particular against statistical attacks (differential, linear) and structural attacks
  - algebraic attacks may be further developed
  - AES-256 is less robust than expected

27

### Hash functions

- MDC (manipulation detection code)
- Protect short hash value rather than long text
- collision resistance
- preimage resistance
- 2<sup>nd</sup> preimage resistance

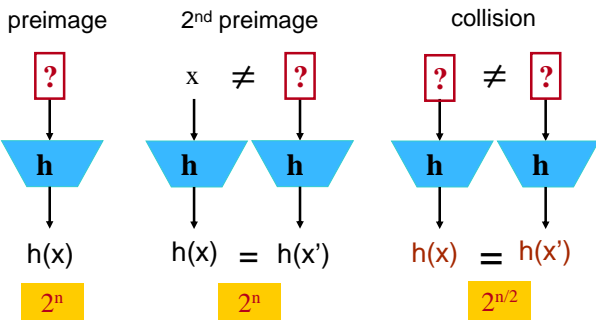
This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).



1A3FD4128A198FB3CA345932

28

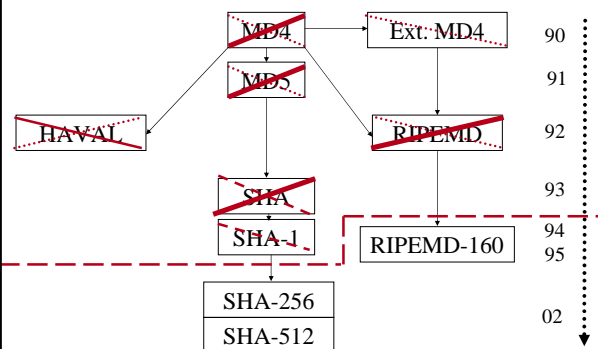
### Security requirements (n-bit result)



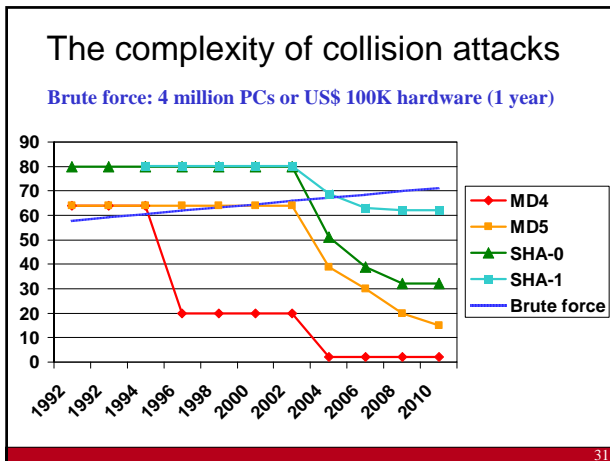
> 80% of all designs for collision resistant hash functions are broken

29

### MDx-type hash function history



30



### MD5

- Advice (RIPE since '92, RSA since '96): **stop using MD5**
- Largely ignored by industry (click on a cert...)
- Collisions for MD5
  - brute force ( $2^{64}$ ): 1M\$ 10 hours in '09
  - [Wang+'04] collision in 15 minutes on a PC
  - [Stevens+'09] collisions in milliseconds
- 2<sup>nd</sup> preimage:
  - $2^{123}$  [Asaki-Aoki'09]

### SHA-1

- SHA designed by NIST (NSA) in '93
- redesign after 2 years ('95) to SHA-1
- collisions for SHA-1
  - $2^{69}$  [Wang+'05] and  $2^{63}$  [Wang+'05 unpublished]
  - $2^{60}$  [Mendel+'08 - unpublished]
  - $2^{52}$  [McDonald+'08 - unpublished]
- preimages for 49/80 steps in  $2^{157}$  [DeCannière-Rechberger'08]

Prediction: collision for SHA-1 in the next 12-18 months

### Hash function attacks:

cryptographic **meltdown** yet with limited impact

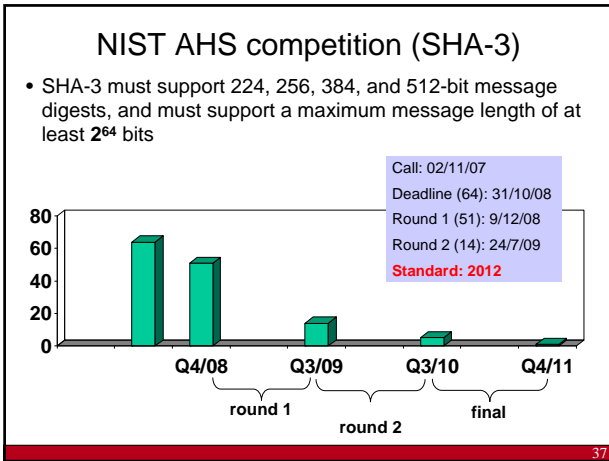
- collisions problematic for future
  - digital signatures for non-repudiation (cf. traffic tickets in Australia?)
- 2<sup>nd</sup> preimage:
  - MD2:  $2^{73}$  [Knudsen+09]
  - MD4:  $2^{102}$  [Leurent'08]
- RIPEMD-160 seems more secure than SHA-1 ☺
- use more recent standards (slower and larger)
  - SHA-2 (SHA-256, SHA-224, ...SHA-512)
  - SHA-3?

### Hash function attacks: impact (2)

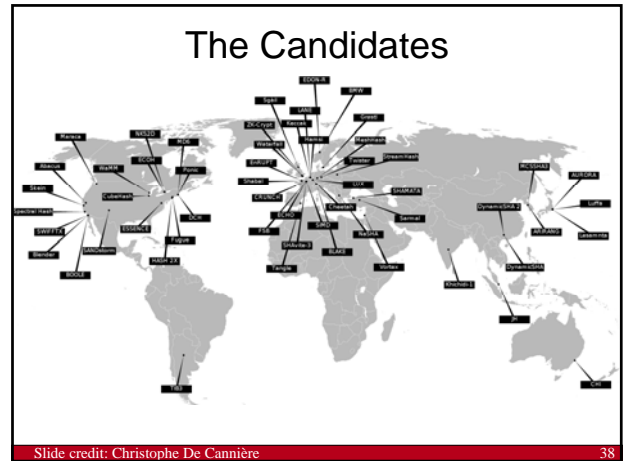
- TLS/SSL** has been designed for algorithm negotiation and flexible upgrades
  - ...but the negotiation algorithm uses MD5 || SHA-1
  - negotiation cannot be upgraded without changing the standard: TLS 1.1 -> 1.2
  - brings serious cost: no upgrade until there is an economic attack
- HMAC**
  - HMAC-MD4:  $2^{72}$  chosen plaintexts &  $2^{77}$  time
  - HMAC-MD5:  $2^{51}$  chosen plaintexts &  $2^{100}$  time in a related key setting
  - HMAC-SHA-1 seems fine for now

### Hash function attacks: impact (3)

- MD5 considered harmful today** [Sotirov-Stevens-Appelbaum-Lenstra-Molnar-Osvik-de Weger '08]
  - request user certificate; by special collision this results in a fake CA certificate
    - need to predict serial number + validity period
  - Impact is a rogue CA with certificates that are trusted by all common browsers
- 6 CAs have issued certificates signed with MD5 in 2008:
  - Rapid SSL, Free SSL (free trial certificates offered by RapidSSL), TC TrustCenter AG, RSA Data Security, Verisign.co.jp

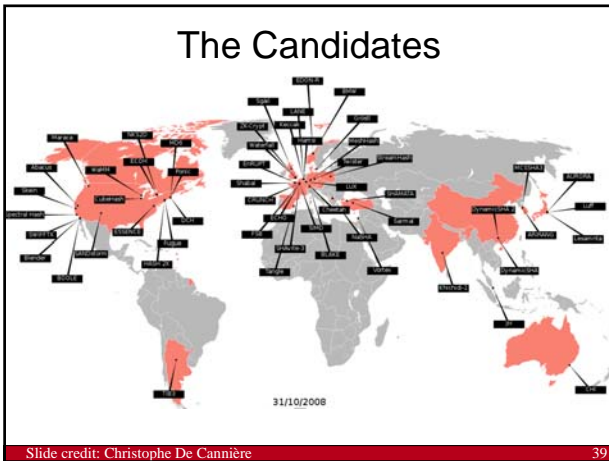


37



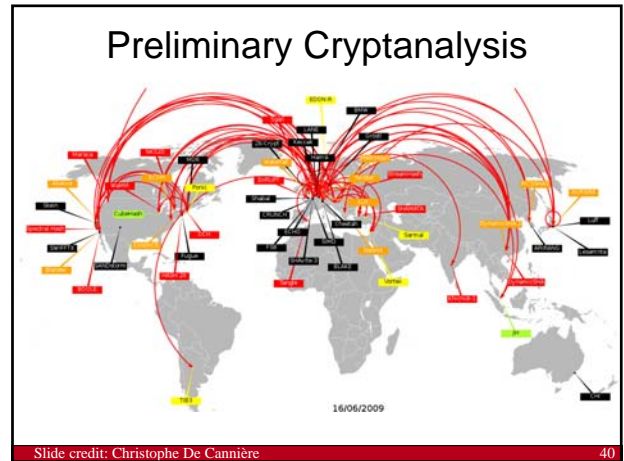
Slide credit: Christophe De Cannière

38



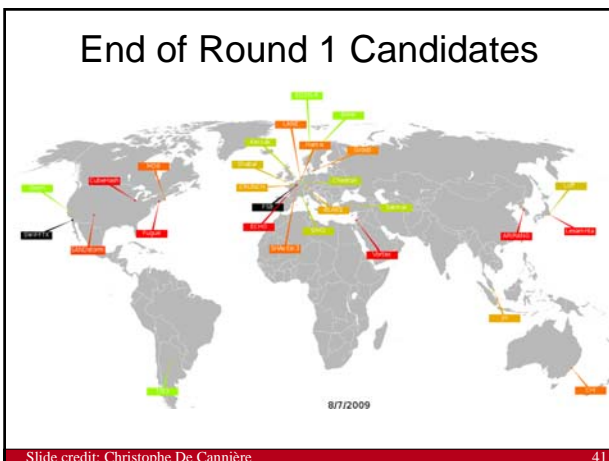
Slide credit: Christophe De Cannière

39



Slide credit: Christophe De Cannière

40



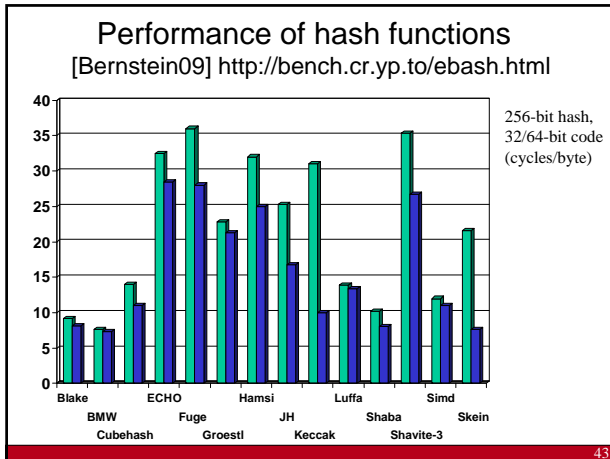
Slide credit: Christophe De Cannière

41



Slide credit: Christophe De Cannière

42



43

## Hash functions: conclusions

- Cryptographic meltdown but fortunately implications so far limited
- Designers often too optimistic (usually need 2x more rounds)
- Other weaknesses have been identified in general approach to construction hash functions
- Today, our understanding has improved substantially, so probably it will take a while before we have a SHA-4 competition

44

## Other symmetric primitives

- Stream ciphers:
  - eSTREAM (2004-2008) has resulted in substantial progress in low cost (Grain, Trivium) and high end (Salsa, HC-128)
- MAC algorithms
  - CBC-MAC: EMAC and CMAC ok
  - HMAC: ok with SHA-1
  - GCM (10.7 cycles/byte) and GMAC: ok if carefully implemented
  - UMAC: vulnerable to key recovery attacks
  - Authenticated encryption

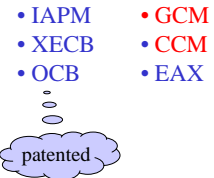
45

## Authenticated encryption

- Default modes: ECB/CBC/CFB/OFB and CTR
- Needed for network security, but only fully understood by crypto community around 2000 (too late)
- Standards have been selected recently:
  - CCM: CTR + CBC-MAC [NIST SP 800-38C]
  - GCM: CTR + GMAC [NIST SP 800-38D]
- Both are suboptimal

### Issues:

- associated data
- parallelizable
- on-line
- provable security



52

## Outline

- **Context**
- **Block ciphers**
- (Stream ciphers)
- **Hash functions**
- (MAC algorithms and authenticated encryption)
- **Public-key cryptology**
- (Protocols)
- **Implementations issues**
- **Research challenges**

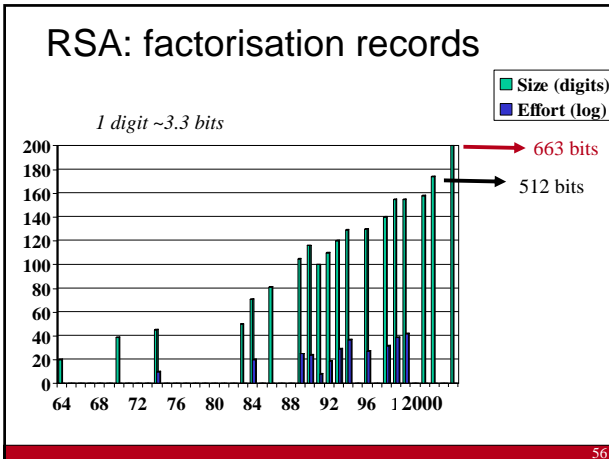
54

## RSA

- 2 large primes  $p$  and  $q$
- modulus  $n = p \cdot q$
- compute  $\lambda(n) = \text{lcm}(p-1, q-1)$
- choose  $e$  relatively prime w.r.t.  $\lambda(n)$
- compute  $d = e^{-1} \text{ mod } \lambda(n)$
- public key =  $(e, n)$
- private key =  $d$  of  $(p, q)$
- encryption:  $c = x^e \text{ mod } n$
- decryption:  $x = c^d \text{ mod } n$

- Is factoring hard?
- Is the RSA problem, i.e. inverting  $f(x) = x^e \text{ mod } n$  as hard as factoring?
- How to use RSA efficiently, that is, how to prove the forging a signature or learning any additional information on the plaintext from the ciphertext results in an *efficient* algorithm to solve the RSA problem
  - RSA KEM-DEM for encryption
  - RSA PSS for signature
- How to get rid of Random Oracle Model?

55



### Factorisation

- New record in May 2005: 663 bits (or 200 digits) using NFS
- New record in May 2007:  $2^{1039}-1$  (313 digits) using SNFS
- hardware factoring machine: **TWIRL** [TS'03] (The Weizmann Institute Relation Locator)
  - initial R&D cost of ~\$20M
  - 512-bit RSA keys can be factored with a device costing \$5K in about 10 minutes
  - 1024-bit RSA keys can be factored with a device costing \$10M in about 6 weeks
- ECRYPT statement on key lengths and parameters  
<http://www.ecrypt.eu.org>

768-bit factorization in 2009 and 896-bit factorization in 2012

57

### Key lengths for confidentiality

<http://www.ecrypt.eu.org>

duration	symmetric	RSA	ECC
days/hours	50	512	100
5 years	73	1024	146
10-20 years	103	2048	206
30-50 years	141	4096	282

Assumptions: no quantum computers; no breakthroughs; limited budget

58

- ### Protocols (1)
- key transport (email)
  - authenticated key agreement (TLS, SSH, GSM, UMTS)
  - time-stamping
  - notarisation
  - credentials (TPM)
  - anonymous communication
  - e-cash
  - voting
  - auctions
  - threshold cryptography
  - Identity based cryptography
  - robust networking (e.g., denial of service attacks, routing attacks)
- 62

### Protocols (2)

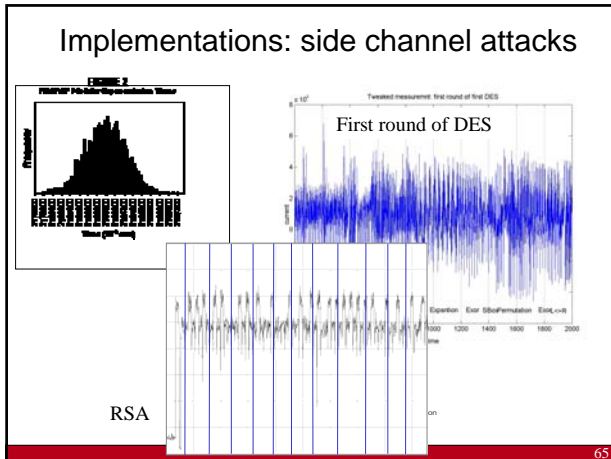
- multi-party computation
- threshold crypto
- privacy protecting data mining
- social and group crypto

decryption based on location and context  
distance bounding

“you can trust it because you don’t have to”

64





### Implementation attacks

Sun Tzu, The Art of War:  
In war, avoid what is strong and attack what is weak

- measure: time, power, electromagnetic radiation, sound
- introduce faults (even in CPUs – bug attacks)
- combine with statistical analysis and cryptanalysis
- software: API attacks

- major impact on implementation cost

L.R. Knudsen: "It is not cryptanalysis, it is vandalism"

66

### New side channel attack

#### Bug attack [Biham-Carmeli-Shamir'08]

- Introduce a bug in a multiplier such that it produces the wrong result for a single input pair
  - Example: Pentium FDIV bug '94
- Results in key recovery for RSA-CRT, ECC

- Requires no local access (as a fault attack); only needs chosen texts
- If 64x64: impossible to detect by testing
- Risk of outsourcing the manufacturing

68

### Implementation attacks (13 May '08)

#### Debian-OpenSSL incident

- Weak key generation:
  - only 32K keys
  - easy to generate all private keys
  - collisions
- Between 13-17 May:
  - 280 bad keys out of 40K (0.6%)
- Revocation problematic

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
MANDRIVA (SEE PC)	GIVES ROOT ACCESS IF ASKED IN SPEAKING VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ENOUGH WORDS FOR TREND
UBUNTU	THINKS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

69

### Implementation attacks: cold boot attack

- Why break cryptography? Go for the key, stupid!
- Data reminence in DRAMs
  - Lest We Remember: Cold Boot Attacks on Encryption Keys [Halderman-Schoen-Heninger-Clarkson-Paul- Calandrino-Feldman- Appelbaum-Felten'08]
  - Boot from USB device and dump RAM image
  - Works for AES, RSA,...
  - Products: BitLocker, FileVault, TrueCrypt, dm-crypt, loop-AES

5 sec    30 sec    60 sec    5 min

70

### Implementation attacks: cold boot attack countermeasures

- Overwrite keys in memory
- Shut down rather than sleep/hibernate
- Limit boot options (network, USB)
- resilient exposure cryptography (AONT)
- physical protection of DRAM
- encrypt in the disk controller
- new architecture
- Ineffective: trusted computing as implemented today

71

### Challenges for long term security

- cryptanalysis improves:
  - mathematical attacks A5/1, E0, MD5, SHA-1
  - implementation attacks
- computational power increases:
  - Moore's law
  - exponential progress with quantum computers?
- environment changes – new assumptions
  - packet switched networking
  - open networks
  - dynamic networks
  - untrusted nodes
  - ratio power CPU/memory size
  - outsourcing of data processing

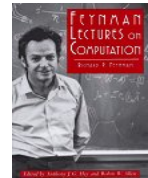
72

### New computational models: 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?



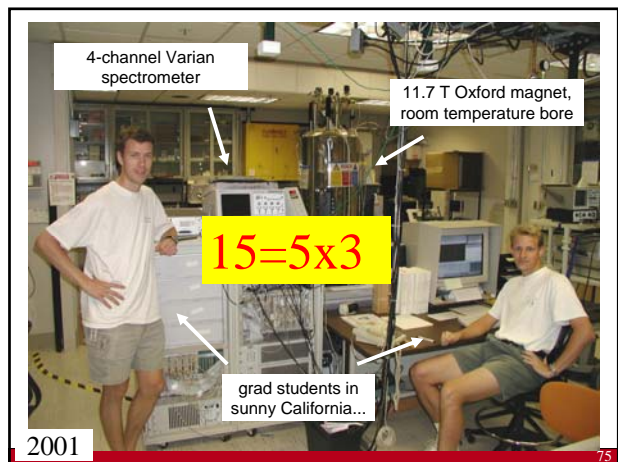
73

### If a large quantum computer can be built...

- All schemes based on factoring (such as RSA) will be insecure
- Same for discrete log (ECC)
- Symmetric key sizes: x2
- Hash sizes: x1.5
- Alternatives: McEliece, HFE, NTRU,...
- So far it seems very hard to match performance of current systems while keeping the security level against conventional attacks



74



75

### News on 13 Sept. 2007

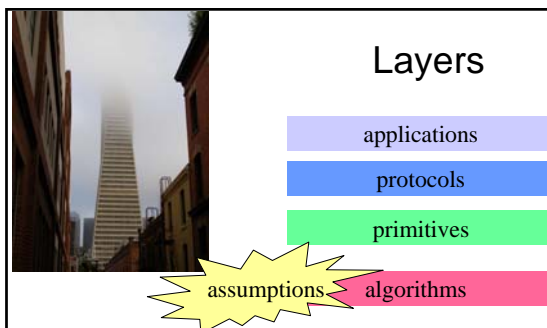
- "Two independent teams (led by Andrew White at the University of Queensland in Brisbane, Australia, and the other by Chao-Yang Lu of the University of Science and Technology of China, in Hefei) have implemented Shor's algorithm using rudimentary laser-based quantum computers"
- Both teams have managed to factor 15, again using special properties of the number

### News on 19 Dec. 2007

- optical quantum computer (team led by Daniel James, University of Toronto)
- factored 15

76

### Layers



Proofs: link security at different levels in a quantitative way

L.R. Knudsen:  
"If it is provably secure, it is probably not"

77

### Assumptions

research on **hard problems?**

James L. Massey:  
A hard problem is one that nobody works on

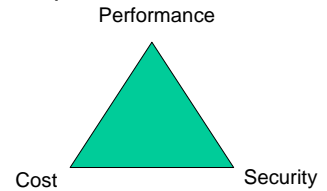
good lower bounds  
average versus worst case  
find new hard problems

### Challenges for crypto

- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint

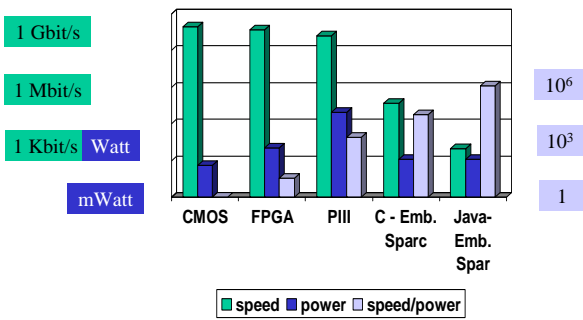
secure software and hardware implementations

algorithm agility

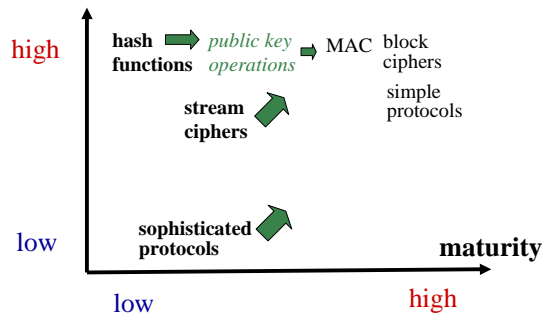


### The power challenge:

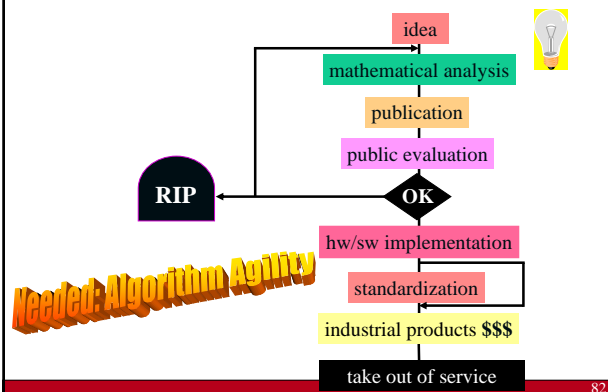
AES-128 speed/power for various platforms (Gb/Joule)



### demand in applications



### Life cycle of a cryptographic algorithm



### Conclusions

- The “crypto problem” is not solved
  - many challenging problems ahead...
  - make sure that you can upgrade your crypto algorithm and protocol
  - bring advanced cryptographic protocols to implementations

When will every network packet be protected with authenticated encryption?

When will everyone pay with e-cash?

Can we reconcile privacy, DRM and data mining?