http://www.ecrypt.eu.org

2012

The Cryptographic Year in Review

Prof. Bart Preneel
COSIC
KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be

24 October 2012

1

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 (layer 8)

2

Outline

- crypto algorithms
  - symmetric encryption
  - hash functions
  - public key crypto
  - padding attacks
- PKI
- hacks

3

AES update

- Rijndael algorithm designed in Belgium
- minor theoretical weaknesses in 2010/2011
- 2012: no news is good news
- 2255 implementations validated by NIST

- fast implementation:

fast implementation:	cycle per byte
bitsliced	7.60
2010 Intel Westmere	1.27
2011 Intel Sandy Bridge	0.64
2011 AMD Bulldozer	1.30
2012 Intel Ivy Bridge	0.64

4

GSM/DECT

- easy to break
  - tools are available to get traffic and key

Satellite telephones

- GMR-1 and GMR-2 broken
  - used by Thuraya and military

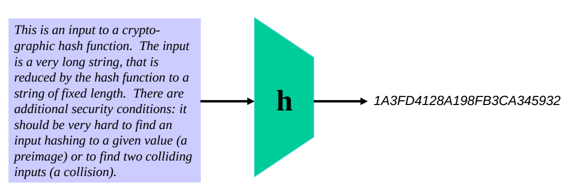
intercepting phone conversations is illegal

5

Hash functions

protect short hash value rather than long text

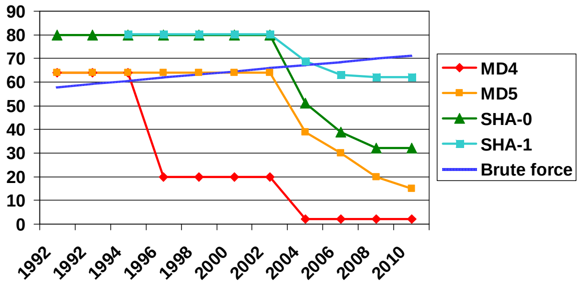
collision resistance
preimage resistance
2nd preimage resistance



6

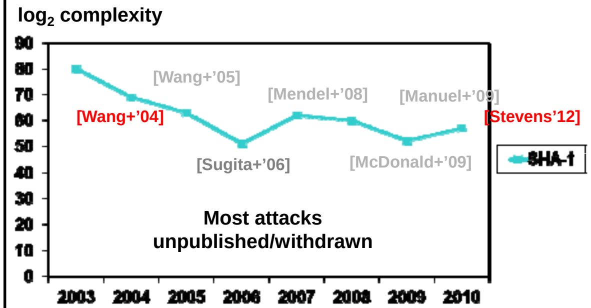
2004 Hash function crisis: the complexity of collision attacks

brute force: 4 million PCs or US$ 100K hardware (1 year)



7

SHA-1 designed by NIST (NSA) in '94



prediction: collision for SHA-1 in the next 12 months

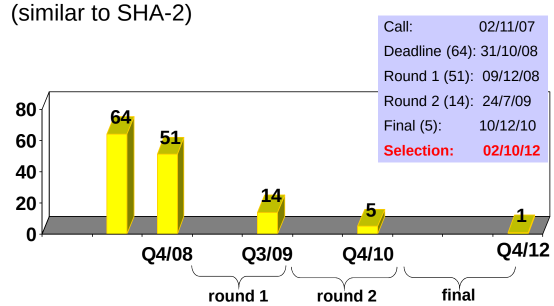
Alternatives to SHA-1

- RIPEMD-160 [BSI/KU Leuven 96]
  – still unbroken but output length too short for long term security
- SHA-2 [NIST/NSA 02]
  – seems to withstand attacks
  – some reservations

9

NIST AHS competition (SHA-3)

SHA-3: 224, 256, 384, and 512-bit message digests (similar to SHA-2)



10

Preliminary Cryptanalysis

Slide credit: Christophe De Cannière, KU Leuven

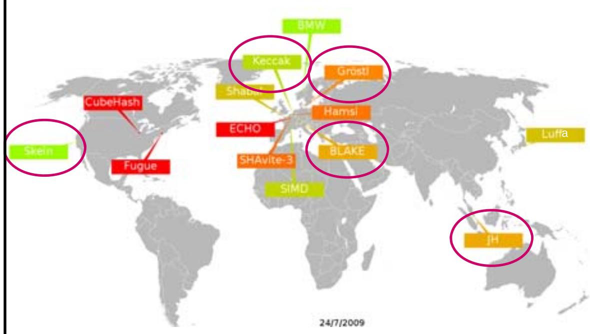
11

Round 2 Candidates

Slide credit: Christophe De Cannière, KU Leuven

12

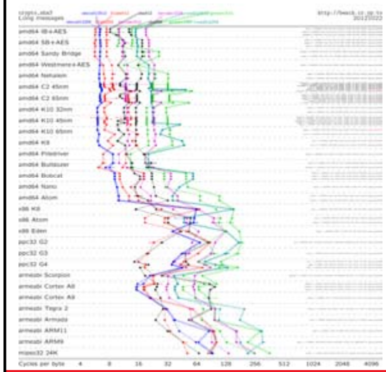
Finalists



Slide credit: Christophe De Cannière, KU Leuven

13

Software performance - eBash [Bernstein-Lange11]



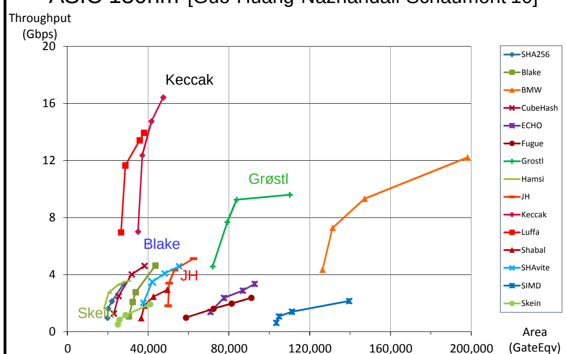
logarithmic scale

slower ⟶

⟵⟶ factor 4 in cycles/byte

14

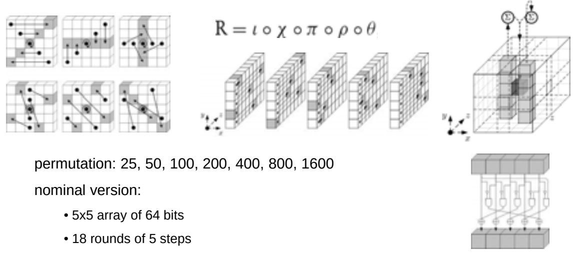
Hardware: post-place & route results for ASIC 130nm [Guo-Huang-Nazhandali-Schaumont'10]



Slide credit: Patrick Schaumont, Virginia Tech

15

Keccak



permutation: 25, 50, 100, 200, 400, 800, 1600

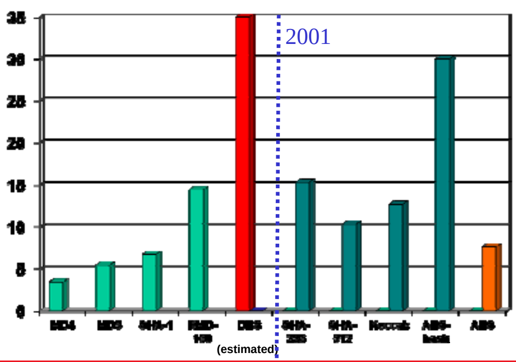
nominal version:

- 5x5 array of 64 bits
- 18 rounds of 5 steps

16

Performance of hash functions - Bernstein

(cycles/byte) Intel Core 2 Quad Q9550; 4 x 2833MHz (2008)



17

Public key crypto

"new" factorization record in January 2010: 768 bits

upgrade your RSA-1024 keys

- should have been done in 2010
- still lots of 512-bit keys around

increased "acceptance" of ECC

- example NSA Suite B in USA
- Certicom challenge: ECC2K-130: 1 year with 60 KEURO (a large effort is underway)
- limited commercial deployment outside government

18

Key lengths for confidentiality

http://www.ecrypt.eu.org

duration	symmetric	RSA	ECC
days/hours	50	512	100
3-4 years	73	1024	146
10-20 years	103	2048	206
30-50 years	141	4096	282

Assumptions: no quantum computers; no breakthroughs; limited budget

19

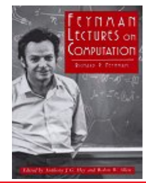
Quantum computers?

exponential parallelism

n coupled quantum bits ⇓ 2^n degrees of freedom !

Shor 1994: perfect for factoring

but: can a quantum computer be built?



20

If a large quantum computer can be built...

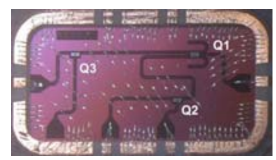
- all schemes based on factoring (such as RSA) will be insecure
- same for discrete log (Zp, ECC)
- symmetric key sizes: x2
- hash sizes: unchanged!

alternatives: postquantum crypto
- McEliece, NTRU,…
- so far it seems very hard to match performance of current systems while keeping the security level against conventional attacks

21

2001: 7-bit quantum computer factors 15
2007: two new 7-bit quantum computers
2012: 21 has been factored yesterday

2012: 10 to 15 years for a large quantum computer



Quantum Computing: An IBM Perspective

Steffen, M.; DiVincenzo, D. P.; Chow, J. M.; Theis, T. N.; Ketchen, M. B.

Quantum physics provides an intriguing basis for achieving computational power to address certain categories of mathematical problems that are completely intractable with machine computation as we know it today. We present a brief overview of the current theoretical and experimental works in the emerging field of quantum computing. The implementation of a functioning quantum computer poses tremendous scientific and technological challenges, but current rates of progress suggest that these challenges will be substantively addressed over the next ten years. We provide a sketch of a quantum computing system based on superconducting circuits, which are the current focus of our research. A realistic vision emerges concerning the form of a future scalable fault-tolerant quantum computer.

22

Problematic public keys (1/3)

[Lenstra-Hughes+ Crypto 12]

11.7 million openly accessible public keys (TLS/PGP)
6.4 million distinct RSA moduli
rest: ElGamal/DSA (50/50) and 1 ECDSA

- 1.1% of RSA keys occur in >1 certificate

- easy to factor: 0.2% of RSA keys
  - 12,000 keys!
  - 40% have valid certs

[Heninger+ Usenix Sec. 12]

12 million openly accessible public keys (5.8 TLS/6.2 SSH)
23 million hosts (12.8/10.2)

1%: 512-bit RSA keys

- 5.6% of TLS hosts share public keys
- 5.2% default manufacturer keys
- 0.34% have by accident the same key

- easy to factor: 0.5% of TLS hosts and 0.03% of SSH hosts
- DSA key recovery: 1.6% of DSA hosts

23

Problematic public keys (2/3)

- low entropy during key generation
- RSA keys easy to factor, because they form pairs like: n = p.q and n' = p'.q so gcd(n,n')=q
- DSA keys: reuse of randomness during signing or weak key generation

- why ???

- embedded systems
  - routers, server management cards, network security devices
- key generation at first boot

RSA versus DSA

Ron was wrong, Whit is right or vice versa?

24

Problematic public keys (3/3)

ethical problem: how to report this?

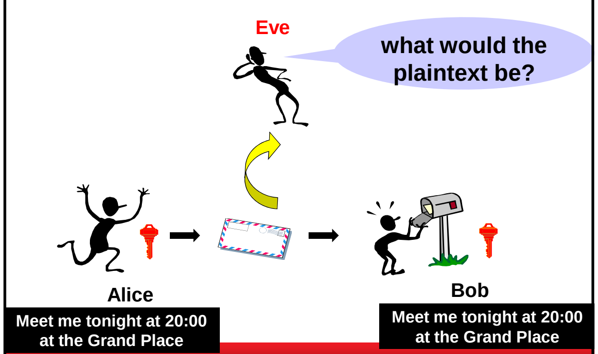
details:

Lenstra, Hughes, Augier, Bos, Kleinjung, Wachter, "Ron was wrong, Whit is right" http://print.iacr.org/2012/064.pdf, *or with as title* "Public keys," Crypto 2012.

Heninger, Durumeric, Wustrow, Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices," Usenix Security 2012, https://www.usenix.org/conference/usenixsecurity12/tech-schedule/technical-sessions

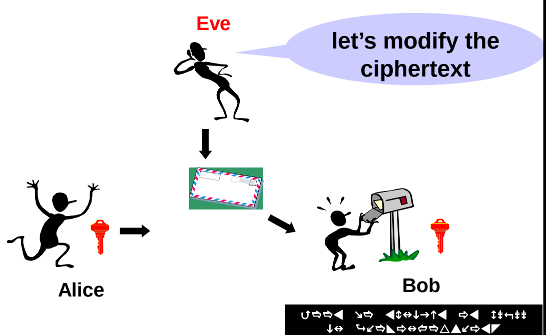
25

Reaction attack (aka padding attack)



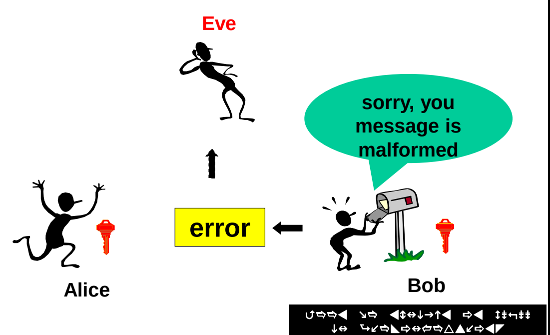
26

Reaction attack



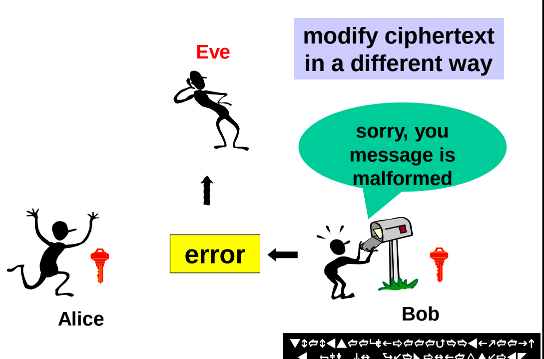
27

Reaction attack (attempt 1)



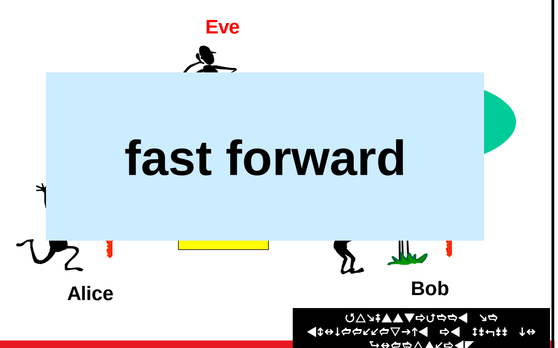
28

Reaction attack (attempt 2)



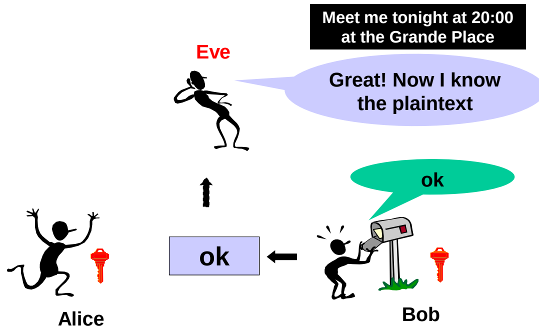
29

Reaction attack (attempt 3)



30

Reaction attack (attempt 1001)



31

Reaction attacks: well known

[Bleichenbacher 98] PKCS #1v1.5 – 1 million chosen ciphertexts (in practice 200,000)
[Klima-Pokorny-Rosa 03] 40% improvement
[Bardou–Focardi–Kawamoto-Simionato-Steel-Tsay 12]
- **reduced to about 10,000 chosen ciphertexts**

[Manger 01] OAEP PKCS #1v2 – a few 1000 chosen ciphertexts
[Bellare-Kohno-Namprempre 02]: SSH
[Vaudenay 02] SSL, IPsec, WTLS...
[Canvel-Hiltgen-Vaudenay-Vuagnoux 03]: SSL/TLS

Solution:
- don't send error messages (bad engineering practice)
- KEM/DEM schemes and symmetric authenticated encryption

32

"Efficient padding oracle attacks on cryptographic hardware" (PKCS#11 devices)

[Bardou+ 12] most attacks take less than 100 milliseconds

Device	PKCS#1v1.5		CBC pad	
	token	session	token	session
Aladdin eTokenPro				
Feitian ePass 2000	OK	OK	N/A	N/A
Feitian ePass 3003	OK	OK	N/A	N/A
Gemalto Cyberflex		N/A	N/A	N/A
RSA Securid 800		N/A	N/A	N/A
Safenet iKey 2032			N/A	N/A
SATA dKey	OK	OK	OK	OK
Siemens CardOS		(89 secs)	N/A	N/A

33

Outline

- crypto algorithms
  - symmetric encryption
  - hash functions
  - public key crypto
  - padding attacks
- PKI
- hacks

34

Analogies

the biology analogy

the car analogy

cars have brakes so they can go *fast*

hidden assumption:
you never drive downhill

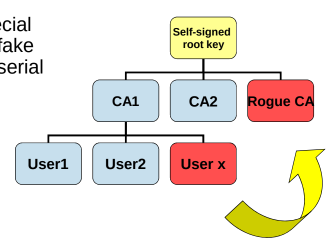
35

2008 Rogue CA attack

[Sotirov-Stevens-Appelbaum-Lenstra-Molnar-Osvik-de Weger '08]

request user cert; by special collision this results in a fake CA cert (need to predict serial number + validity period)

impact: rogue CA that can issue certs that are trusted by all 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

36

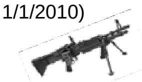
Flame (successor of Stuxnet/Duqu)

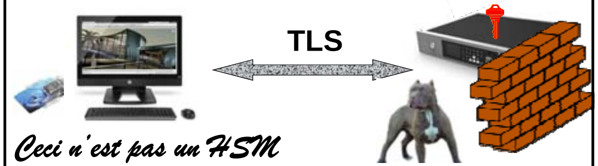
- discovered in May 2012 by Cert in Iran
- targeted cyber espionage in Middle Eastern countries
- vectors: LAN, USB, Bluetooth
- record audio, screenshots, keyboard activity and network traffic (including Skype)
- kill command to wipe out its traces (used on June 8 2012)
- advanced MD5 collision attack built-in to create fake certificate for Microsoft Enforced Licensing Intermediate PCA (Windows Update)
  - similar to but independent from rogue CA attack

37

Malicious certificates

- Aug' 11 Diginotar: target Iranian opposition
- May '12 Flame
  - June '12: Microsoft no longer supports RSA keys shorter than 1024 bits (except if signed before 1/1/2010)
  - NIST's deadline is 31/12/2013
- Sept. '12: Adobe problem





38

Hacks

- Privacy
  - Aug '12: US Federal Trade Commission orders web giant to pay $22.5m for violating privacy of rival Apple's Safari browser users
  - Politicians and laws talks about cookies, but web companies have found many other cool ways to keep tracking users
- Java
  - Aug'12: Super-critical 0-day exploits **2** bugs
- Browsers
  - Sept '12: new 0-day on Internet Explorer

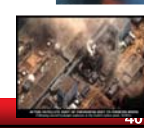
39

Does Big Data Means Big Hacks?

psychology: humans are very bad at managing and evaluating risks in complex systems

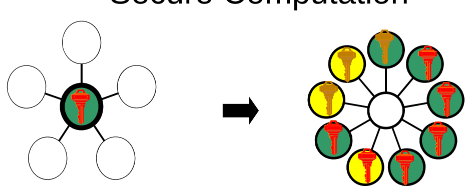
economics: information security risks are typically systemic with large market failures in part due to negative externalities (e.g. software, e-commerce)

not so different from other areas: the larger the scale, the larger the risk (too big to fail)



40

Secure Computation



- PKI
- banking
- credit card
- Google
- eBay
- …

multi-party computation

"you can trust it because you don't have to"

41

Summary

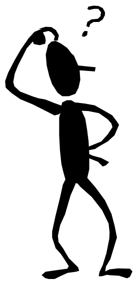
- AES is not broken but SHA-1 will be soon
- SHA-3 has been selected
- key generation remains problematic
- need to develop post quantum crypto
- multiparty computation becomes practical
- upgrading and fixing remains problematic
- old attacks keep coming back and new attacks get better

2012 was an exciting year for cryptanalysts

42

The end

Thank you for
your attention



8 nov '12 ICC Ghent

29-30 nov '12
www.foryoureyesonly.be

4-8 March'13 www.secappdev.org

4-7 June'13 COSIC course
www.cosic.be

43