



http://www.ecrypt.eu.org




The Cryptographic Year in Review

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




November 2011




Cryptography \neq 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)

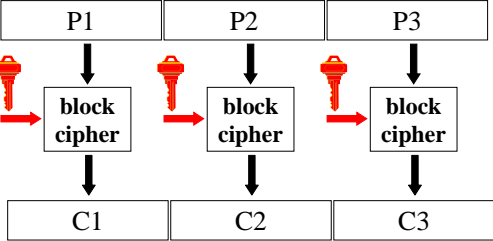


Outline


- Cryptography
 - block ciphers
 - stream ciphers
 - hash functions
 - modes
 - digital signatures
- PKI
- Hacks



Block ciphers

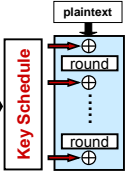


- larger data units: 64...128 bits
- memoryless
- repeat simple operation (round) many times

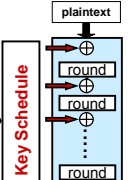


AES variants (2001)

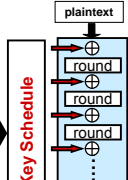
AES-128
10 rounds
sensitive




AES-192
12 rounds
classified



AES-256
14 rounds
secret and top secret



Light weight key schedule, in particular for the 256-bit version



AES: security

- mathematical cryptanalysis:
 - best attack: related key attack on AES-256 with complexity 2^{119} plaintexts and time
 - no attack has been found that can exploit this structure (in spite of the claimed algebraic attack [Courtois'02])
- implementation level attack
 - cache attack precluded by bitsliced implementations or by hardware support (Intel)
 - fault attack requires special countermeasures

New announcement: August 2011 ISSE 2011
 [Bogdanov-Khovratovich-Rechberger]

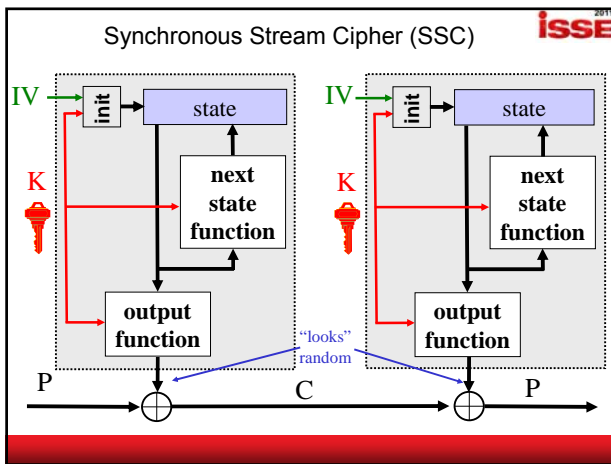
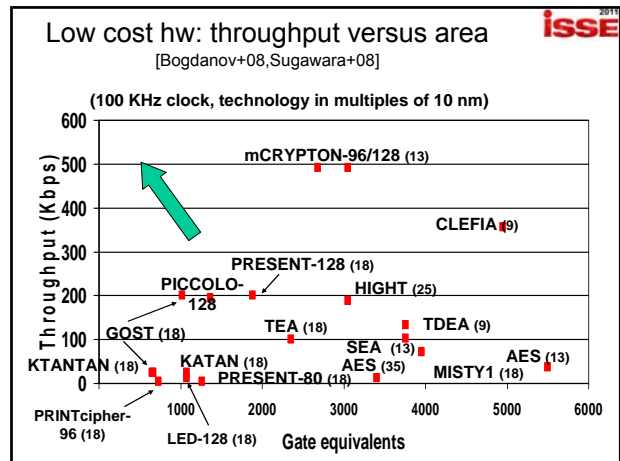
No related keys (attack in 2005)

For AES-128: with 2^{88} plaintext/ciphertext pairs, the effective key size can be reduced by 2 bits (AES-126)

For AES-192: only 2^{80} plaintext/ciphertext pairs

For AES-256: only 2^{40} plaintext/ciphertext pairs

Very minor impact on security and very hard to extend



- GSM** ISSE 2011
- A5/1 weak
 - [Barkan+03] requires seconds (software not available so requires math)
 - [Nohl10]: Kraken = 2 Terabyte of Rainbow tables <http://reflexor.com/trac/a51>
 - A5/2 trivially weak (milliseconds) – withdrawn in 2007 (took 8 years)
 - A5/3 (= Kasumi) seems ok but slow adoption (even if in 1.2 billion out of 3 billion handsets)
 - Simpler attacks on GSM
 - eavesdrop after base station (always cleartext)
 - switch off encryption (can be detected)
 - SMS of death

ISSE 2010 ISSE 2011

GSM

- growing number of open source tools to intercept: GnuRadio, Airprobe, OpenBTS
- but needs more work (1-2 years?)

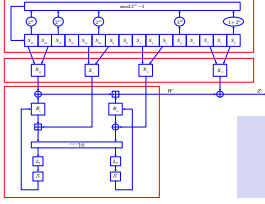
ComputerWeekly.com

Jan 2011

- GSM** ISSE 2011
- be careful when rolling out 2-factor authentication via SMS
 - war texting hacks on car systems and SCADA systems [Black Hat, Aug'11]
- intercepting mobile phone traffic is illegal

International

- China:
 - ZUC as 3rd algorithm in LTE (also SMII, SMIII)
 - National Cryptography Industry Standards Technical Committee established on 19/10/2011



Every algorithm used in China needs to be designed in China


- US: NIST is very active in standardization

Hash functions

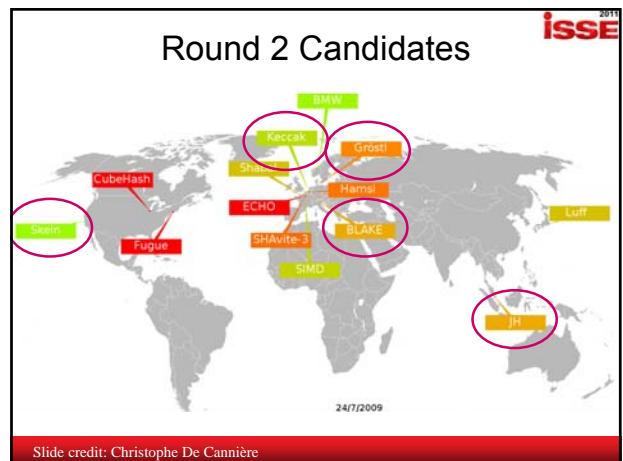
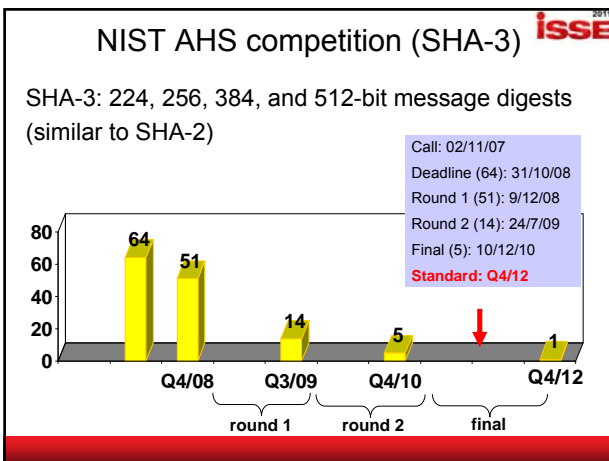
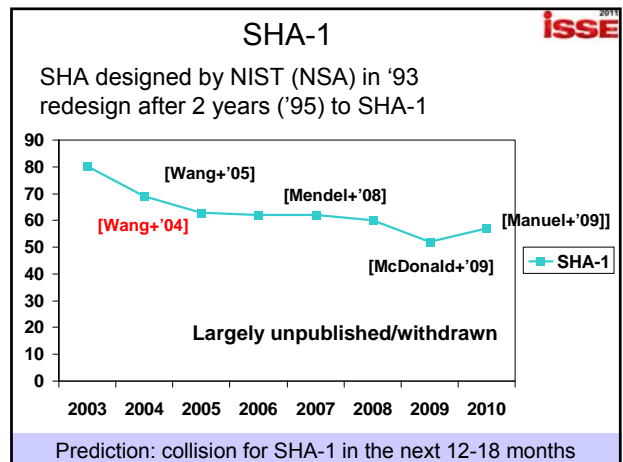
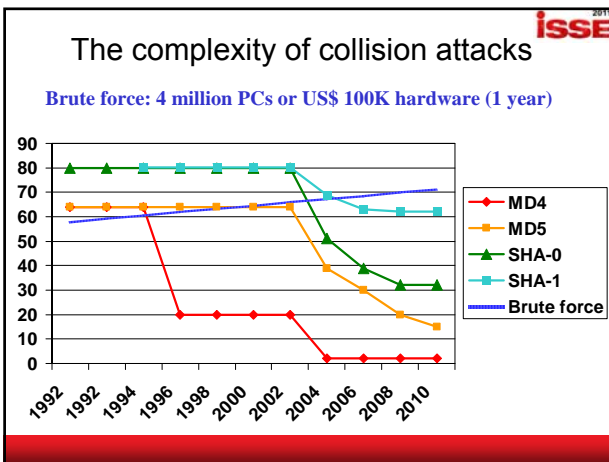
Protect short hash value rather than long text

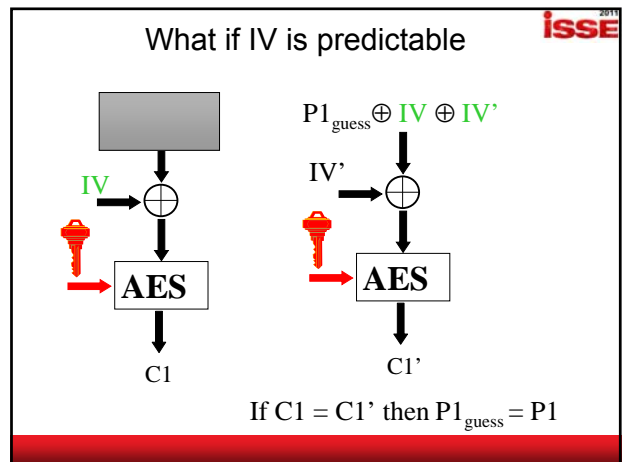
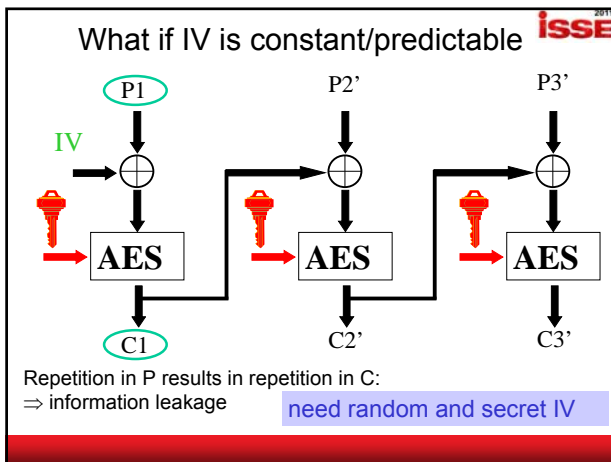
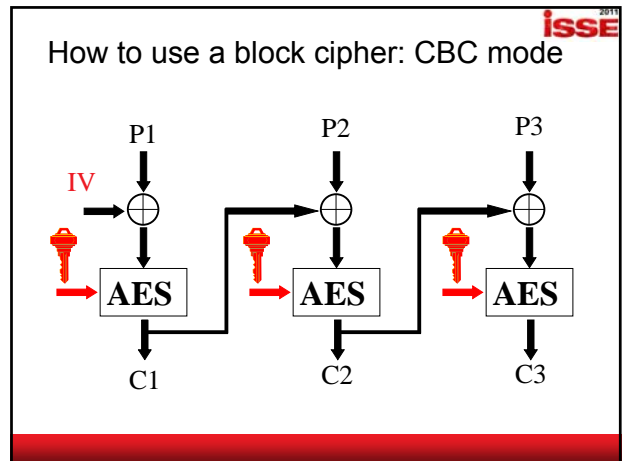
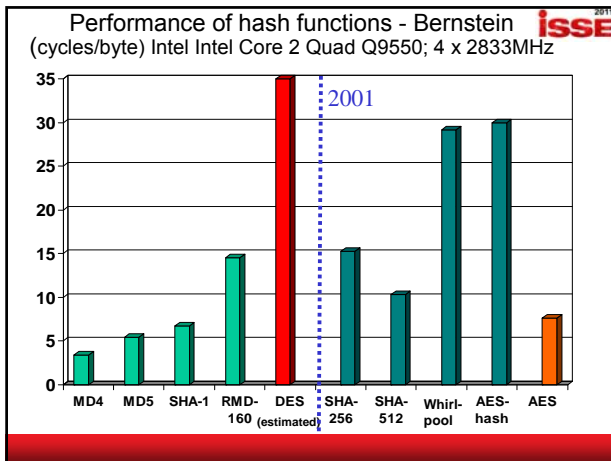
- collision resistance
- preimage resistance
- 2nd preimage resistance

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



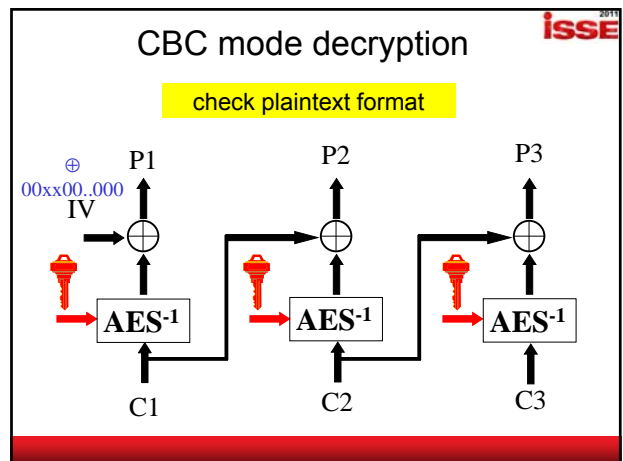


SSL BEAST attack

- SSL/TLS: IV = previous ciphertext block = predictable
 - leads to **chosen plaintext** attack
- [Duong-Rizzo'11] prepend using HTML5 WebSockets variable length plaintext so that secret part of plaintext can be guessed byte by byte
 - rather slow
- Fixed in TLS 1.1 (2006!) but no adoption
- SSL 3.0 accepted anyway for backward compatibility

Choosing a good name helps for PR

SSL/TLS stripping is a much easier attack



XML Encryption attack isSE 2011

- **Reaction attack:** chosen plaintext (decryption queries) and observe error message
- XML decryption checks validity of plaintext (specific character encoding)
- [Jager-Somorovsky11] decrypt 160 bytes using 2000 decryption queries (100 seconds)
- Countermeasure:
 - unified error message
 - changing mode
 - authenticated encryption: non-trivial

Authenticated encryption isSE 2011

needed for network security, but only fully understood by crypto community around 2000 (too late)
dump CBC mode

standards:

- **CCM:** CTR + CBC-MAC [NIST SP 800-38C]
- **GCM:** CTR + GMAC [NIST SP 800-38D]

both are suboptimal but patent free

properties

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

- IAPM
- XECB
- OCB

The risks of ElGamal (1/3) isSE 2011

ElGamal-type signatures (including DSA, ECDSA)
public parameters: prime number p , generator g
(modulo p operation omitted below)

private key x , public key $y = g^x$

signature (r, s)

- generate temporary private key k and public key $r = g^k$
- solve s from $h(m) \equiv x r + k s \pmod{p-1}$

verification:

- Signature verification: $1 < r < p$ and $h(m) \equiv y^r r^s \pmod{p}$

The risks of ElGamal (2/3) isSE 2011

long term keys: $y = g^x$
short term keys: $r = g^k$

the value k has to be protected as strongly as the value x

- Ex. 1: NIST had to redesign the DSA FIPS standard because of a subtle flaw in the way k was generated [Bleichenbacher'01]
- Ex 2: attack on ElGamal as implemented in GPG [Nguyen'03]

The risks of ElGamal (3/3) isSE 2011

$y = g^x$

signature:

- $r = g^k$
- $h(m) \equiv x r + k s \pmod{p-1}$

what if k would be the same every time?

- $h(m_1) \equiv x r + k s \pmod{p-1}$
- $h(m_2) \equiv x r + k s \pmod{p-1}$

2 linear equations in 2 unknowns: easy to solve:
yields the signing key x

one solution: choose $k = h(m || x)$

Outline isSE 2011

- Context
- Cryptography
 - block ciphers
 - stream ciphers
 - hash functions
 - modes
 - digital signatures
- PKI
- Hacks

ISSE 2010 **Bad news: the CA mess** [Eckersley10] "An observatory for the SSLiverse"

- 10.8M servers start SSL handshake
- 4.3M use valid certificate chains
- **650 CA certs trustable by Windows or Mozilla in 50+ countries**
- 1.4M unique valid leaf certs
 - 300K signed by one GoDaddy cert
- 80 distinct keys used in multiple CA certs
- several CAs sign the IP address 192.168.1.2 (reserved by RFC 1918)
- 2 leaf certs have 508-bit keys
- Debian OpenSSL bug (2006-2008)
 - resulted in 28K vulnerable certs
 - fortunately only 530 validate
 - only 73 revoked

How can we fix this mess?

ISSE 2011 **CA incidents**

- March 2011 – Comodo: 9 fraudulent certs
 - via RA GlobalTrust.it/InstantSSL.it
- Summer 2011 – DigiNotar: 500+ fraudulent certs
 - meet-in-the-middle attack against Google users in Iran (300K unique IPs, 99% from Iran)
 - filed for bankruptcy 20 September 2011
- (Globalsign)

ISSE 2011 **CA incidents**

Malware signed by key of Government of Malaysia

ISSE 2011 **CA "incident"**

ISSE 2011 **RSA SecureID APT incident**

- Reported March 2011
 - probably started late 2010
- Spear phishing mail (marked as SPAM) installed malware via [2010_Recruitment_plan.xls](#)
- 760 companies may have been impacted by the same attack (20% of Fortune 100)
- RSA SecureID secret keys may have leaked, resulting in attacks on other parties: Lockheed Martin, L3
 - June 2010: SecureID tokens replaced
- apparently all the secrets in 1 place

ISSE 2011 **Secure Computation**

- PKI
- Banking
- Credit card
- Google
- ...

Multi-party computation

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

Multi-party computation becomes "truly practical"

Similar to first public key libraries 20 years ago

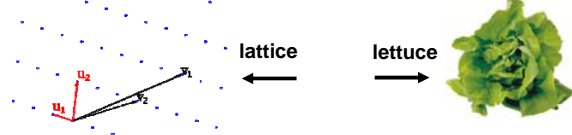
- EU: CACE project (Computer Aided Cryptography Engineering), www.cace-project.eu
- US: Brown Univ. + UCSD (Usenix 2010)

Examples

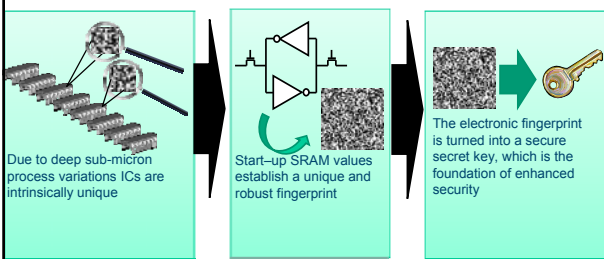
- efficient zero-knowledge proofs
- 2-party computation of AES (Bristol)
- secure auction of beetroots in Denmark (BRICS)
- oblivious transfer for road pricing (COSIC)

Fully homomorphic encryption

- From $E(x)$ and $E(y)$, you can compute $E(x+y)$, $E(c \cdot x)$ and $E(x \cdot y)$ **without decrypting**
- Many cool applications including cloud computing
- [Gentry'09] ideal lattices = breakthrough
- First implementations require only seconds [Vercauteren-Smart'10], [Gentry-Halevi'10], ...
 - but to ciphertext for 1 bit is 3 million bits and public key is several Mbyte
- Substantial improvements if restricted operations



Secure key storage with non-initialized SRAM



Due to deep sub-micron process variations ICs are intrinsically unique

Start-up SRAM values establish a unique and robust fingerprint

The electronic fingerprint is turned into a secure secret key, which is the foundation of enhanced security

Slide credit: Intrinsic-ID

Top 10 largest security incidents

- 130,000,000 2009-01-20 Heartland Payment Systems
- 94,000,000 2007-01-17 TJX Companies Inc.
- 90,000,000 1984-06-01 TRW, Sears Roebuck
- 77,000,000 2011-04-26 Sony Corporation (120 MEURO)
- 40,000,000 2005-06-19 CardSystems, Visa, MasterCard, Amex
- 35,000,000 2011-07-28 SK Communications, Nate, Cyworld
- 32,000,000 2009-12-14 RockYou Inc.
- 26,500,000 2006-05-22 U.S. Department of Veterans Affairs
- 25,000,000 2007-11-20 HM Revenue and Customs, TNT
- 24,600,000 2011-05-02 Sony Online Entertainment, Sony Corporation

Privacy violations

- Facebooks tracks users even if logged out
 - even non-Facebook users
- P2P traces TOR users [LeBond et al. Usenix LEET11]
- Speaker recognition from **encrypted** VoIP [Khan-Baig-Youssef]
- Facebook + face recognition = the end of privacy? [Acquisti]

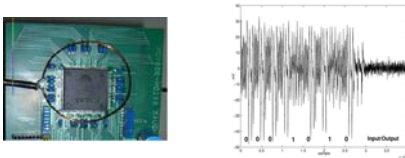
Wireless hacks around

- Police radio: APCP Project 25 [Clark+11]
- Car electronics: now wireless [Checkoway+11] or via MP3
- Electronic car lock denial of service attack
- iPhone encryption
- Keylogger in drone command & control center
- Flying drones for hacking
- Plug Bot




Side channel attacks power/electromagnetic

- Mifare MF4ICD40
 - Replaced by DESFire EV1
- Xilinx Virtex II Bitscream encryption
- ATMEL CryptoMemory EEPROM
- [examples: see Tim Kasper's talk of Tuesday]



And more problems...

- Amazon outage:
 - On April 21, 2011 Amazon Elastic Block Store (EBS) went offline, leaving the many Web and database servers depending on that storage broken. Not until Easter Sunday (April 24) was service restored to all users.
- Nikon camera authentication broken
- Hacking embedded devices through web interface (embedded web servers)
- Second water utility reportedly hit by hack attack. Water pump broken (18/11/2011)
- Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System

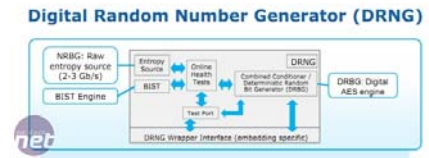


Not hacked in 2011



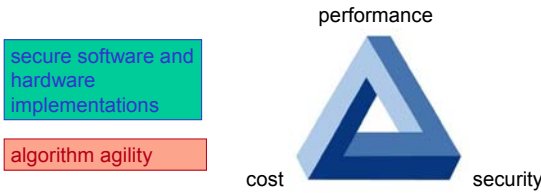
Good news

Intel adding security hardware



Challenges for crypto

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



Challenges for advanced crypto

- privacy enhancing technologies
- linking crypto with physical world
 - biometrics, physical uncloneable functions
- distributed secure execution
- whitebox cryptography
- crypto for nanotechnology

Conclusion

ISSE 2011

- AES is not broken but SHA-1 will be soon
- SHA-3 will be available late 2012
- lattice based crypto is resistant to quantum computers, but not a silver bullet for the cloud
- multiparty computation becomes practical

- upgrading remains problematic

- old attacks keep coming back and new attacks get better

2011 was an exciting year for hackers

The end

ISSE 2011



Thank you for
your attention