Cryptographic Algorithms

Bart Preneel
COSIC-KU Leuven
bart.preneel(AT)esat.kuleuven.be @bpreneel1 preneel@infosec.exchange
June 2023

COSIC

KU LEUVEN

1

Definitions

1970s

Confidentiality
Integrity
Availability

	data	entities
confidentiality	encryption	anonymity
authentication	data authentication	"identification"

Don't use the word authentication without defining it

Authorisation

Non-repudiation of origin, receipt

Contract signing

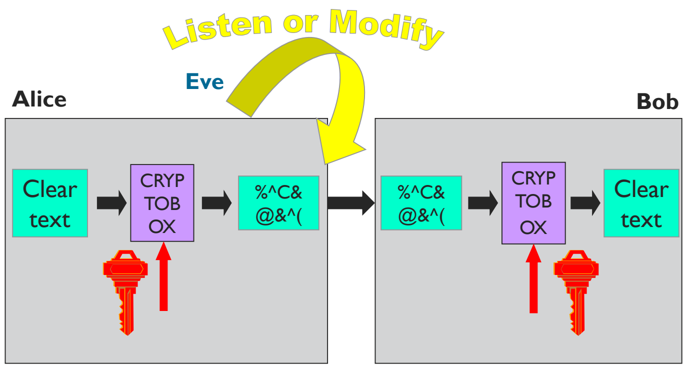
Notarisation and Timestamping

2

KU LEUVEN

2

Cryptology: principle



3

KU LEUVEN

3

Outline

- Symmetric cryptology
  - confidentiality
  - data authentication
  - authenticated encryption
- Public key cryptology (asymmetric cryptology)
- Hybrid cryptology

4

KU LEUVEN

4

Symmetric cryptology: confidentiality

- Old cipher systems:
  - transposition, substitution
- Opponent and her power
- One time pad
- Stream ciphers
- Block ciphers
- Authenticated encryption

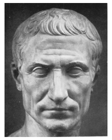
5

5

Old cipher systems (pre 1900)

Caesar cipher: shift letters over k positions in the alphabet (k is the secret key)

THIS IS THE CAESAR CIPHER
WKLV LV WKH FDHVDU FLSKHU



Julius Caesar never changed his key (k=3)

6

6

Cryptanalysis example:

```
TIPGK RERCP JZJZJ WLE     GVCTX EREPC WMWMW JYR
UJQHL SFSDQ KAKAK XMF     HWDUY FSFQD XNXNX KZS
VKRIM TGTER LBLBL YNG     IXEVZ GTGRE YOYOY LAT
WLSJN UHUFS MCMCM ZOH     JYFWA HUHSF ZPZPZ MBU
XDTKO VOVGT NDNDN API     KZGXB IVITG AQAQA NCV
YNULP WKWHU OEOEO BQJ     LAHYC JWJUH BRBRB ODW
ZOVMQ XKXIV PFPFP CRK     MBIZD KXKVI CSCSC PEX
APWNR YLYJW QGQGQ DSL     NCJAE LYLWJ DTDTD QFY
BQXOS ZMXKX RHRHR ETM     ODKBF MZMXK EUEUE RGZ
CRYPT ANALY SISIS FUN     PELCG NANYL FVFVF SHA
DSZQU BOBMZ TJTJT GVO     QFMDH OBOZM GWGWG TIB
ETARV CPCNA UKUKU HWP     RGNEI PCPAN HXHXH UJC
FUBSW DQDOB VLVLV IXQ     SHOFJ QDQBO IYIYI VKD
```

Plaintext? 7 k = 17

7

Old cipher systems (pre 1900) (2)

- Substitutions

ABCDEFGHIJKLMNOPQRSTUVWXYZ

MZNJSOAXFQGYKHLUCTDVWBIRPE

- Transpositions

TRANS OIPSR
POSIT NOTNT
IONS OSAI

! Easy to break using statistical techniques

8

8

Security

- there are n! different substitutions on an alphabet with n letters
- there are n! different transpositions of n letters
- n=26: **n!=403291461126605635584000000 = 4 . 10^{26} keys**
- trying all possibilities at 1 nanosecond per key requires....

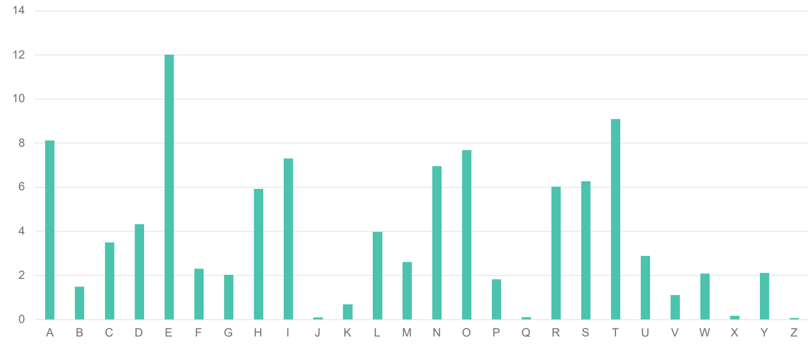
$$4.10^{26} \;/(\underbrace{10^9}_{\text{keys per second}} . \underbrace{10^5}_{\text{seconds per day}} . \underbrace{4\ 10^2}_{\text{days per year}}) = 10^{10} \text{ years}$$

9

KU LEUVEN

9

Letter distributions



Substitutions ABCDEFGHIJKLMNOPQRSTUVWXYZ
MZNJSOAXFQGYKHLUCTDVWBIRPE

10

KU LEUVEN

10

Assumptions on Eve (the opponent)

- A scheme is broken if Eve can deduce the key or obtain additional plaintext
- Eve can always try all keys till "meaningful" plaintext appears: a brute force attack
  - solution: large key space
- Eve will try to find shortcut attacks (faster than brute force)
  - history shows that designers are too optimistic about the security of their cryptosystems

11

KU LEUVEN

11

Assumptions on Eve (the opponent)

- Cryptology = cryptography + cryptanalysis
- Eve knows the algorithm, except for the key (Kerckhoffs's principle)

- increasing capability of Eve:
  - knows some information about the plaintext (e.g., in English)
  - knows part of the plaintext
  - can choose (part of) the plaintext and look at the ciphertext
  - can choose (part of) the ciphertext and look at the plaintext

12

KU LEUVEN

12

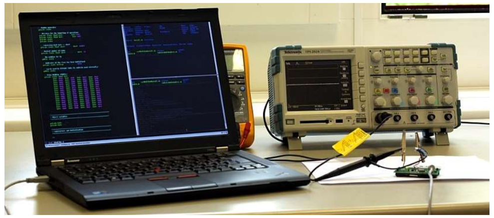
New assumptions on Eve

- Eve may have access to side channels
  - timing attacks
  - simple power analysis
  - differential power analysis
  - acoustic attacks
  - electromagnetic interference
  - micro-architecture attacks
- Eve may launch (semi-)invasive attacks
  - differential fault analysis
  - probing of memory or bus

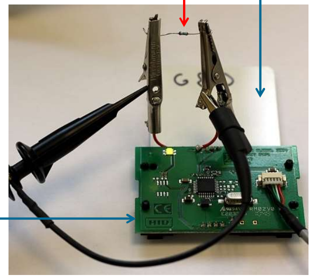
KU LEUVEN

13

Side channel analysis: power setup



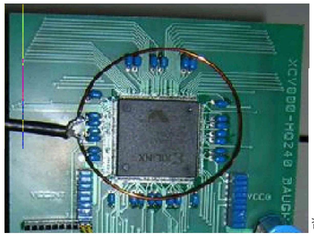
Measure voltage over a resistor to measure the current (and thus the power consumption) of a smart card



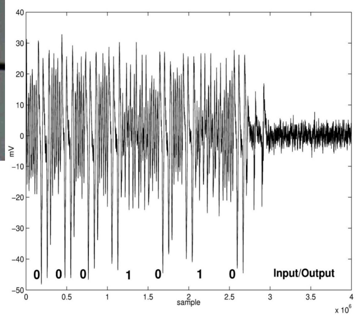
KU LEUVEN

14

Side channel analysis: electromagnetic setup



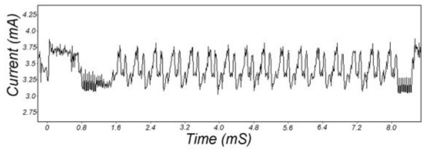
Use simple antenna to measure radiation of an FPGA computing a public key operation



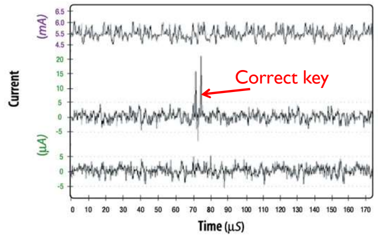
KU LEUVEN

15

Simple and differential power analysis: DES block cipher



DES on a smart card: power consumption



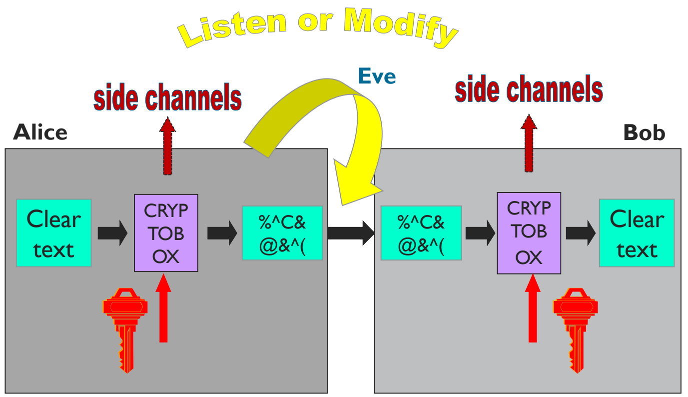
average power

2 correlation methods (example of success and failure)

KU LEUVEN

16

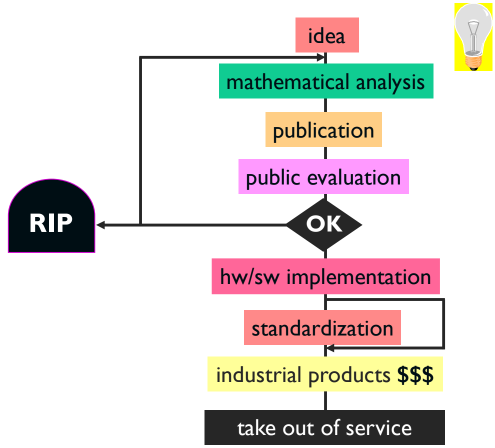
Cryptology + side channels



17

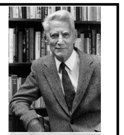
17

Life cycle of a cryptographic algorithm



18

One time pad



Vernam scheme (1917)

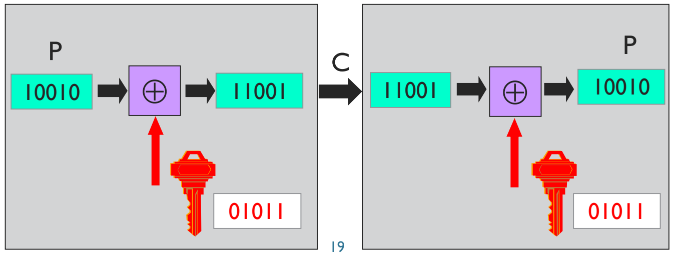
Shannon (1948)

Mauborgne: one time pad (1917+x)

F. Miller (1882)

key is random string, as long as the plaintext

information theoretic proof of security



19

19

One time pad: properties

- perfect secrecy: ciphertext gives opponent no additional information on the plaintext or H(P|C)=H(P)
- impractical: key is as long as the plaintext
- but this is optimal: for perfect secrecy one has always H(K) $\geq$ H(P)

20

20

One time pad: Venona Project (1942-1948)

$c_1 = p_1 + k$
$c_2 = p_2 + k$
then $c_1 - c_2 = p_1 - p_2$

Example:
c1 V c2
(not +)

a skilled cryptanalyst can recover p_1 and p_2 from $p_1 - p_2$ using the redundancy in the language

reuse of key material is also known as "transmission in depth"

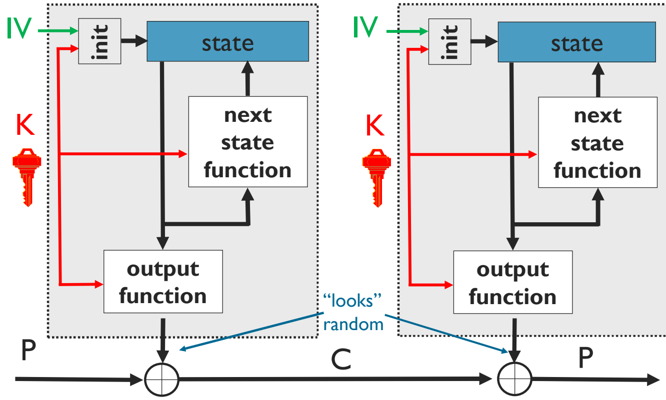
https://en.wikipedia.org/wiki/Venona_project

21

KU LEUVEN

21

Synchronous Stream Cipher (SSC)



22

KU LEUVEN

22

Exhaustive key search

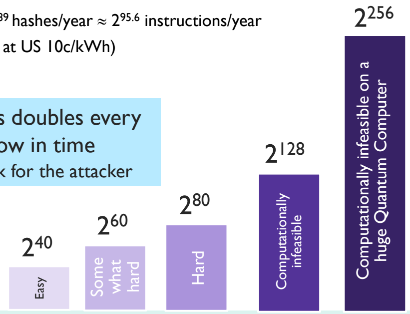
2023: 1 million machines with 16 cores @ 4 GHz can do 2^{56} instructions/sec or 2^{80} instructions/year

» trying 1 key ≈ 100 instructions

Bitcoin: 200 Exahashes/sec = $2^{67.4}$ hashes/sec or 2^{89} hashes/year ≈ $2^{95.6}$ instructions/year

» Electricity: 100 TWh/year (or \$10B/year at US 10c/kWh)

Moore's "law": speed of computers doubles every 18 months: key lengths need to grow in time
but adding 1 key bit doubles the work for the attacker



Key length recommendations 2023 | 1 year | 20 years | 50 years
not for NSA

23

KU LEUVEN

23

Widely used stream ciphers

- A5/1 (GSM) (64 or 54)
- E0 (Bluetooth) (128)
- RC4 (browser) (40-128)

} insecure!

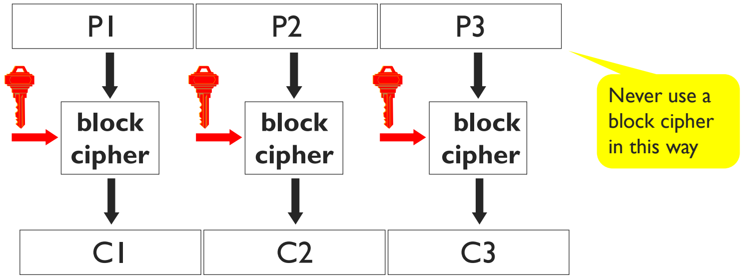
- SNOW-3G (3GSM) (128)
- HC-128 (128)
- Trivium (80)
- ChaCha20 (128)

24

KU LEUVEN

24

Block cipher



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

25

KU LEUVEN

25

Block cipher

- large table: list n-bit ciphertext for each n-bit plaintext
  - if n is large: very secure (codebook)
  - but for an n-bit block: 2^n values
  - impractical if $n \geq 32$
- alternative n = 64 or 128
  - simplify the implementation
  - repeat many simple operations

26

KU LEUVEN

26

Widely used block ciphers

- DES: outdated
- 3-DES: financial sector
- AES
- KASUMI (3G/4G)
- Keeloq (remote control for cars, garage doors)

27

KU LEUVEN

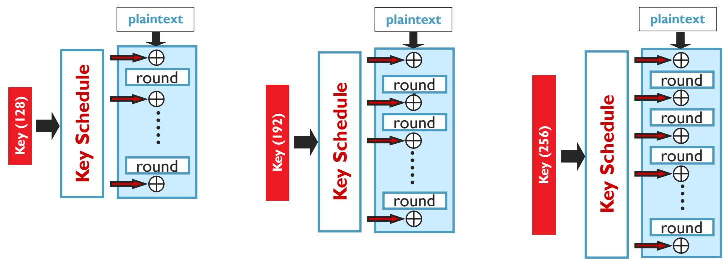
27

AES variants (2001)

AES-128
10 rounds
Sensitive/classified (SECRET)

AES-192
12 rounds
Classified (TOP SECRET)

AES-256
14 rounds
Classified (TOP SECRET)



28

KU LEUVEN

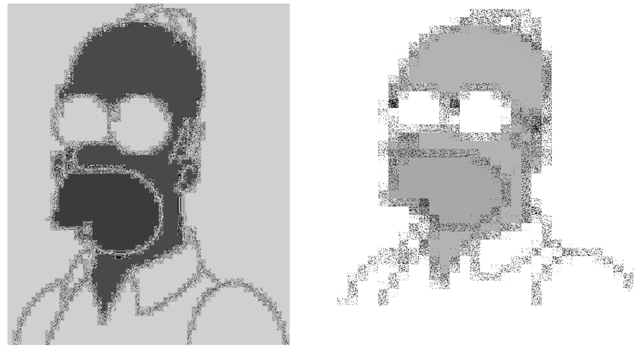
28

An example plaintext

29

29

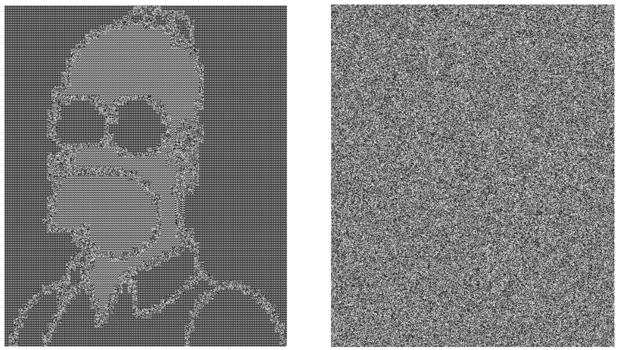
Encrypted with substitution and transposition cipher



30

30

Encrypted with AES in ECB and CTR mode

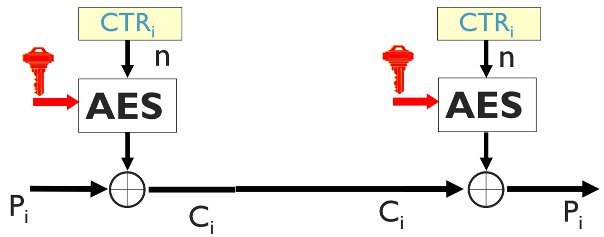


31

31

CounTer Mode (CTR)

$C_i = P_i \oplus E_K(CTR_i)$, CTR_i ++



state initialized CTR_0 = IV

all 0? or random? or nonce? or ….?

32

32

CTR: properties

- different IV necessary; otherwise insecure (Venona)
- uses only encryption
- key stream independent of plaintext: can be pre-computed
- no error propagation: errors are only copied
- random access on decryption
- optimal for hardware:
  - parellellism: one can process multiple counter values at the same time
  - pipelining: no need to know the ciphertext block corresponding to the current plaintext block to start processing the next plaintext block
- risk: what if counters are (accidentally) reset to same value?

33 KU LEUVEN

33

Encryption limitations

- Typically does not hide the **leng**th of the plaintext (unless randomized padding but even then…)
- Ciphertext becomes random string: "normal" crypto does not encrypt a credit card number into a (valid) credit card number
- Does **not** hide existence of plaintext (requires steganography)
- Does **not** hide that Alice is talking to Bob (e.g. Tor)
- Does **not** hide traffic volume (requires dummy traffic)

34 KU LEUVEN

34

Symmetric cryptology: data authentication

- the problem
- hash functions without a key
  - MDC: Manipulation Detection Codes
- hash functions with a secret key
  - MAC: Message Authentication Codes

35 KU LEUVEN

35

Data authentication: the problem

- encryption provides confidentiality:
  - prevents Eve from learning information on the cleartext/plaintext
  - but does not protect against modifications (active eavesdropping)
- Bob wants to know:
  - the **source** of the information (data origin)
  - that the information has not been **modified**
  - (optionally) the **destination** of the information
  - (optionally) **timeliness** and **sequence**

There are no applications that require encryption without data authentication
(but this can still be found in legacy applications with as excuse performance)

KU LEUVEN

36

Data authentication: the problem

- problem of replay of messages needs to be addressed at higher layer (e.g. transaction counter in financial systems)
- specific challenges:
  - very long streams
  - versioning systems
  - noisy data
  - ,....

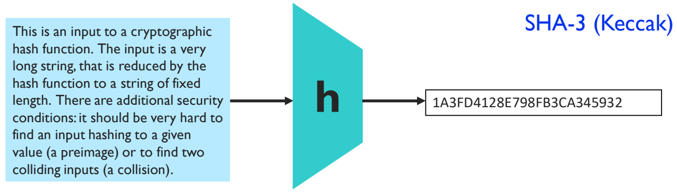
37

37

Data authentication: hash function

- MDC (manipulation detection code)
- Protect short hash value rather than long text

(MD5)
(SHA-1), SHA-256, SHA-512
RIPEMD-160
SHA-3 (Keccak)

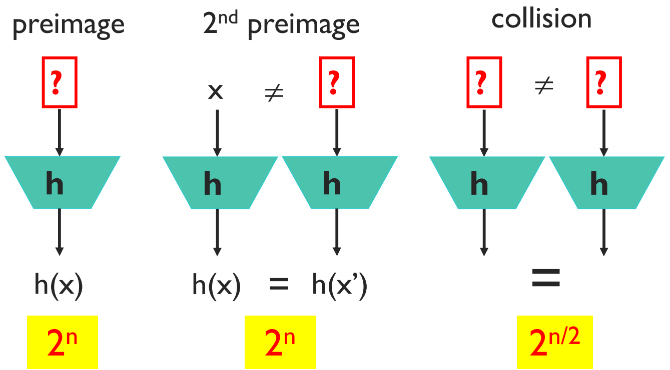


Shift authenticity of file to authenticity of short hash value

38

38

Hash function: security requirements (n-bit result)



39

39

Data authentication: hash function

- preimage resistance: for given y, hard to find input x such that h(x) = y (2^n operations)
- 2^{nd} preimage resistance: hard to find x'≠ x such that h(x') = h(x) (2^n operations)
- collision resistance: hard to find (x,x') with x' ≠ x such that h(x') = h(x) ($2^{n/2}$ operations)

40

40

Widely used hash functions

- MD5
  - (2^{nd}) preimage 2^{128} steps (improved to 2^{123} steps)
  - collisions 2^{64} steps

shortcut: Aug. '04: 2^{39} steps; '09: 2^{20} steps

- SHA-1:
  - (2^{nd}) preimage 2^{160} steps
  - collisions 2^{80} steps

0.15 M$ for 1 year in 2023

shortcut: Aug. '05: 2^{69} steps

Feb. 2017: 2^{61} steps

- SHA-2 family (2002)
- SHA-3 family (2013) – Keccak (Belgian design)
  - (2^{nd}) preimage 2^{256} .. 2^{512} steps
  - collisions 2^{128} .. 2^{256} steps

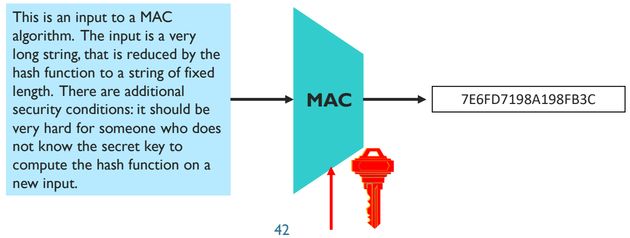
41 KU LEUVEN

41

Data authentication: MAC algorithms

- Replace protection of authenticity of (long) message by protection of secrecy of (short) key
- Append MAC to the plaintext

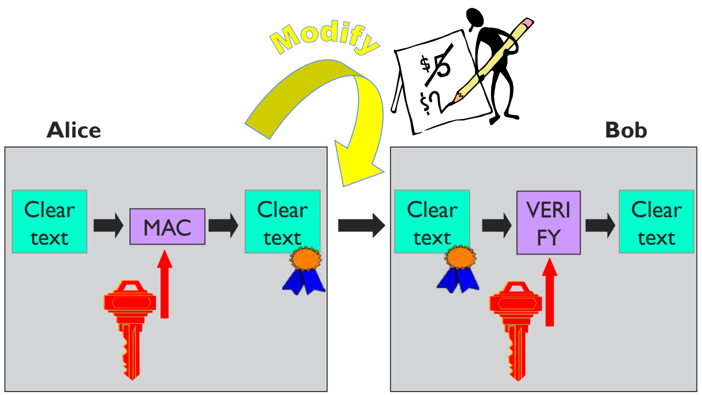
CBC-MAC
(CMAC/LMAC)
HMAC
GMAC



42 KU LEUVEN

42

Data authentication: MAC algorithms



43 KU LEUVEN

43

Data authentication: MAC algorithms

- typical MAC lengths: (32)..64..96 bits
  - forgery attacks: 2^m steps with m the MAC length in bits
- typical key lengths: (56)..112..160 bits
  - exhaustive key search: 2^k steps with k the key length in bits
- birthday attacks: security level smaller than expected

44 KU LEUVEN

44

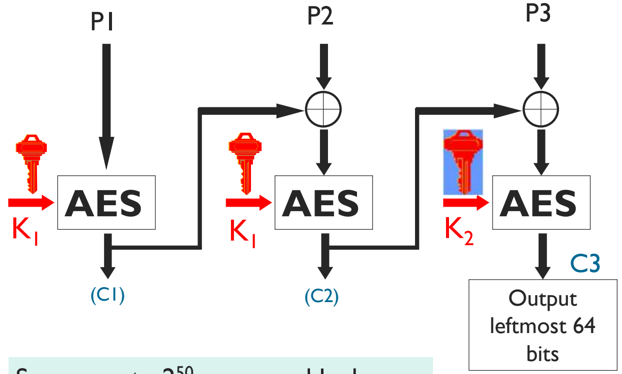
MAC algorithms

- Banking: CBC-MAC based on triple-DES
- Internet: HMAC and CBC-MAC based on AES
- information theoretic secure MAC algorithms (authentication codes): GMAC/Poly1305
  - rather efficient
  - part of the key refreshed per message

45

45

CBC-MAC based on AES (LMAC)



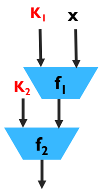
Secure up to 2^{50} message blocks

46

46

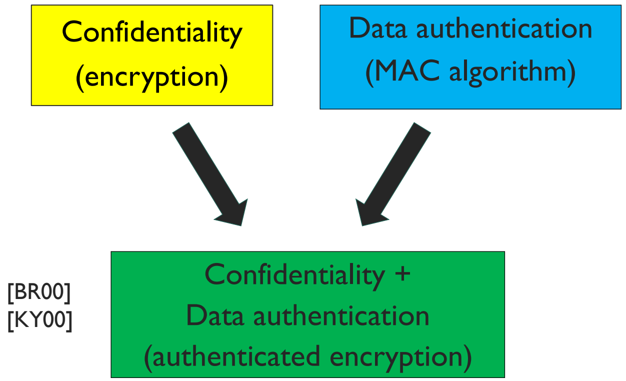
MAC based on a hash function

- Insufficient: hash secret key with data
- **HMAC**:
  - $h_K(X) = h(h(K_1||x)||K_2)$
  - not secure with MD4/MD5
  - Ok with SHA-1/SHA-2/SHA-3



47

Authenticated Encryption



48

48

Authenticated Encryption

Generic composition [BN'00][NRS'14]

- Encrypt-then-MAC with 2 independent keys
  - IPsec, TLS 1.2, 1.3
- MAC-then-Encrypt with 2 independent keys
  - TLS 1.1 and older, 802.11i WiFi
- MAC-and-Encrypt with 2 independent keys

Design "from scratch"

- Integrated authenticated encryption schemes: combined operation with 1 key: see next slide

49 KU LEUVEN

49

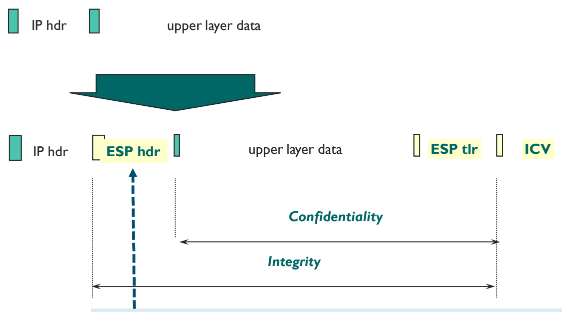
Authenticated Encryption: properties wish list

- Associated data
- Parallelizable
- Online for encryption
- Security reduction
- Resistance to nonce reuse
- Incremental tags
- Fragmentation
- No release of unverified plaintext
- Committing encryption
- Flexible implementation sizes
- Performance: speed/size
- Secure implementations: constant time/power analysis/EM analysis/fault attacks…

50 KU LEUVEN

50

IPsec - ESP Transport mode



Need to authenticate this field but can't encrypt it

51 KU LEUVEN

51

Long history to achieve AE based on block ciphers

- Ad hoc schemes
  - Jueneman ('80s)
  - PCBC (Kerberos)
  - iaPCBC
  - WEP for WiFi 802.11
- 2nd generation
  - CCM
  - GCM
  - EAX
  - CWC
- 1st schemes with proofs
  - RPC [Katz-Yung'00]
  - IAPM [Jutla'01]
  - XECB and XCBC [GD'01]
  - OCB1, OCB2, OCB3 [RBBK'01]
- 3rd generation
  - Chacha20-Poly1305
  - GCM-SIV
  - BTM
  - McOE-G
  - Aegis

52 KU LEUVEN

52

AE: block cipher based

	# passes	//	Online (encr)	Nonce Misue	Patents (but all expired)
IAPM	1	√	√		√
XECB	1	√	√		√
OCB	1	√	√		√
CCM	2				
GCM	1*	√	√		
EAX	2		√		
CWC	2	√	√		
AEGIS	1	√	√		
GCM-SIV	2			√	
BTM	1	√		√	
McOE-G	1*		√	√	

53 KU LEUVEN

53

Caesar competition for Authenticated Encryption

2013-2019 https://competitions.cr.yp.to/caesar.html

	Name	Designers
Lightweight	Ascon	C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer
	ACORN	H. Wu
High speed	Aegis	H. Wu, B. Preneel
	OCB	T. Krovetz, P. Rogaway
Robust	COLM	J. Jean, I. Nikolić, T. Peyrin, Y. Seurin
	AES-COPA	E. Andreeva, A. Bogdanov, N. Datta, A. Luykx, B. Mennink, M. Nandi, E. Tischhauser, K. Yasuda

Selected from 52 submissions – a 5-year effort

OCB2 has been broken at Crypto 2019 (bug in security proof) – but OCB3 is still ok

AEGIS: nonce-based Authenticated Encryption

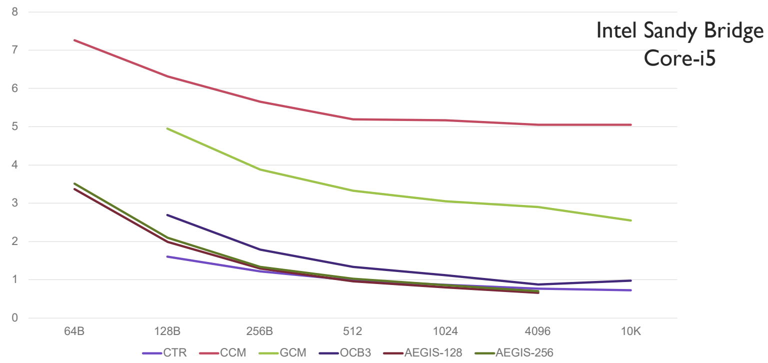
- stream cipher using AES instruction
- 2x faster than AES-GCM: 0.287 cycles/byte
- multiple implementations available (including in Linux kernel)

54 KU LEUVEN

54

AEGIS Performance:

0.287 cycles/byte on Skylake, 0.66 cycles/byte on Sandy Bridge



55 KU LEUVEN

55

Lightweight cryptography competition (2015-2023)

https://csrc.nist.gov/projects/lightweight-cryptography

Authenticated Encryption with Associated Data (AEAD)

- AEAD and hashing for constraint environments
- AEAD for hardware environments

Status

Start: 2015

Feb. 2019: Round 1: regular submissions 56

Aug. 2019: Round 2: candidates left 32

Mar. 2021: 10 finalists

ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, Xoodyak

Feb. 2023: 1 winner: ASCON

56 KU LEUVEN

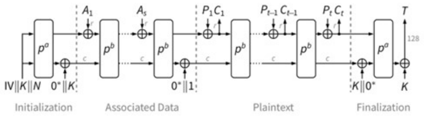
56

NIST competition for Lightweight Cryptography

ASCON: permutation-based AEAD + hash function

https://ascon.iaik.tugraz.at/

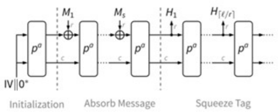
- Ascon-128
- Ascon-128a



4-12 cycles/byte on high-end processors

20-56 cycles/byte on low-end processors

- Ascon-Hash
- Ascon-Xof



- same structure
- same permutation
- 320-bit state size
- r={64,128} bit rate
- a=12, b={6,8} rounds

57 KU LEUVEN

57

Outline

- Symmetric cryptology
  - confidentiality
  - data authentication
  - authenticated encryption
- Public key cryptology (asymmetric cryptology)
- Hybrid cryptology

58 KU LEUVEN

58

Public-key cryptology

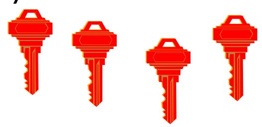
- the problem
- public-key encryption
- digital signatures
- Diffie-Hellman
- RSA

59 KU LEUVEN

59

Limitation of symmetric cryptology

- Reduce security of information to security of keys

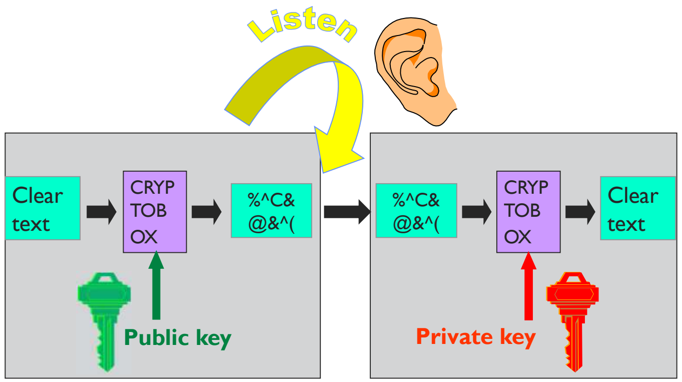


- But: how to establish these secret keys?
  - cumbersome and expensive
  - or risky: all keys in 1 place
- Do we really need to establish secret keys?

60 KU LEUVEN

60

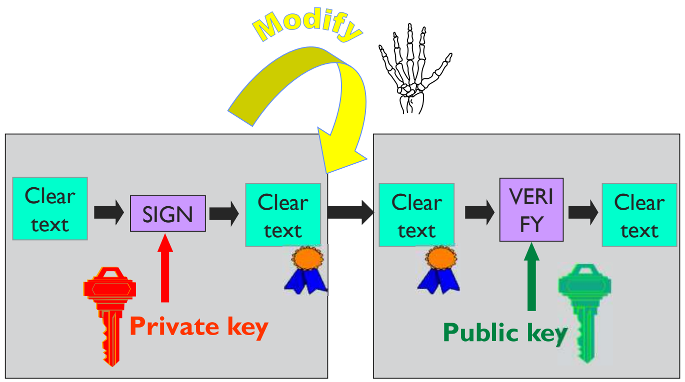
Public key cryptology: encryption



61 KU LEUVEN

61

Public key cryptology: digital signature



62 KU LEUVEN

62

A public-key agreement protocol: Diffie-Hellman

Before: Alice and Bob have never met and share no secrets; they know a public system parameter α

generate x *compute* α^x	$\xrightarrow{\alpha^x}$ $\xleftarrow{\alpha^y}$	*generate* y *compute* α^y
compute $k=(\alpha^y)^x$		*compute* $k=(\alpha^x)^y$

After: Alice and Bob share a short term key k

Eve cannot compute $\boldsymbol{k}$: in several mathematical structures it is hard to derive x from α^x (the discrete logarithm problem)

63 KU LEUVEN

63

RSA ('78)

- choose 2 "large" prime numbers p and q
- modulus $n = p.q$
- compute $\lambda(n) = \mathrm{lcm}(p-1,q-1)$
- choose e relatively prime w.r.t. $\lambda(n)$
- compute $d = e^{-1} \bmod \lambda(n)$

- public key = (e,n)
- private key = d of (p,q)

encryption: $c = m^e \bmod n$
decryption: $m = c^d \bmod n$

The security of RSA is based on the "fact" that it is easy to generate two large primes, but that it is hard to factor their product

try to factor 2419

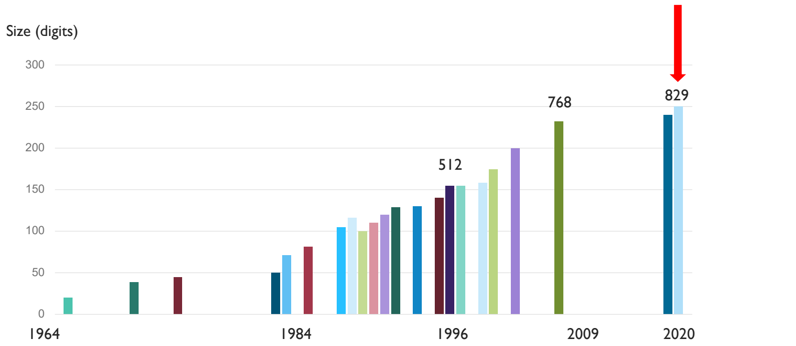
64 KU LEUVEN

64

Factorisation records

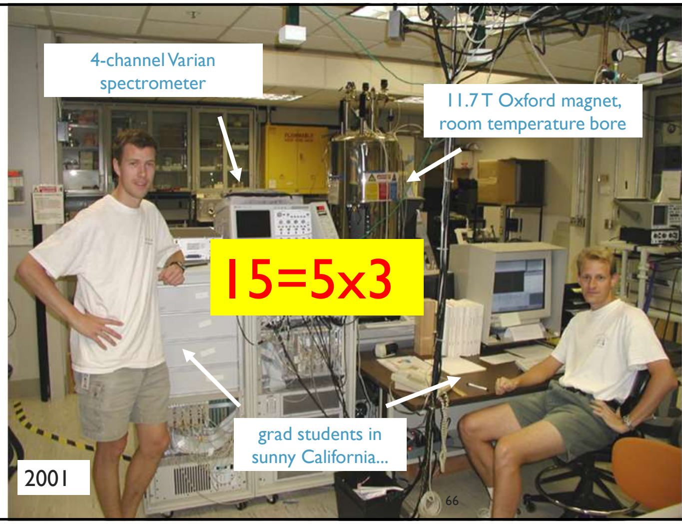
https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

total computation time: 2700 core-years
(Intel Xeon Gold 6130 2.1 GHz)
- sieving: 2450 physical core-years
- matrix: 250 physical core-years

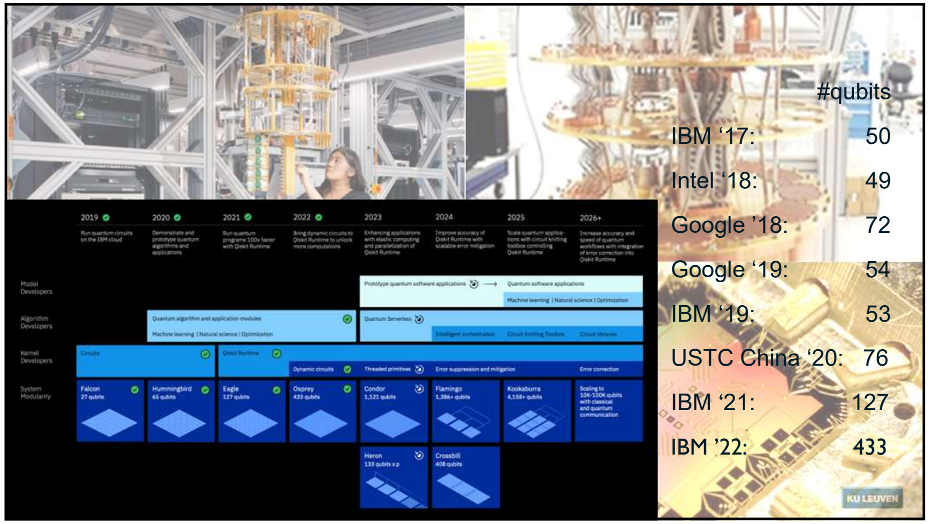


65

65

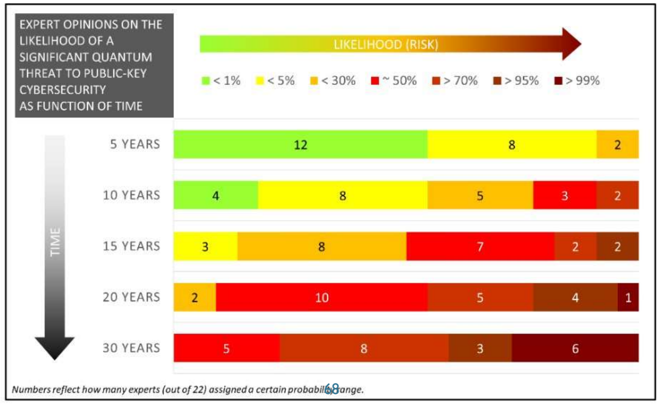


66



67

What do "the experts" say? (2022)



68

NIST: Winners and 4th round candidates

Family	Signatures	KEM / Encryption
Lattice-based	**Dilithium** **Falcon**	**Kyber** Saber NTRU FrodoKEM NTRUprime
Hash-based	**Sphincs+**	---
Code-based	---	Classic McEliece Bike HQC
Multivariate	~~GeMSS~~ ~~Rainbow~~	---
Other	~~SIKE~~ Picnic	---

BSI and ANSSI

69

69

2022: COSIC breaks two finalists

COSIC

A New Attack Easily Knocked Out a Potential Encryption Algorithm

SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.

Wouter Castryck, Thomas Decru
Microsoft bounty of 50.000$

Paper 2022/214
Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

70

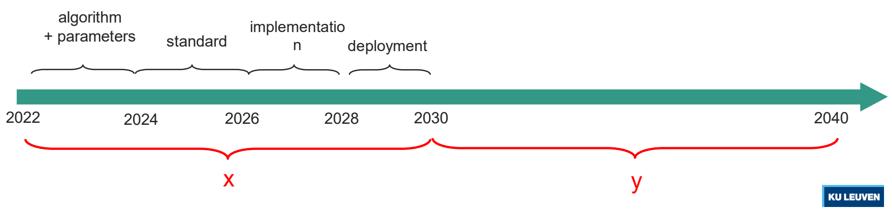
Slide credit: Jan-Pieter D'Anvers

70

When to switch to post-quantum cryptography? [Mosca]

Q = #years until first large quantum computer
x = #years it takes to switch (3-12 years)
y = #years data needs to be confidential (10 years)

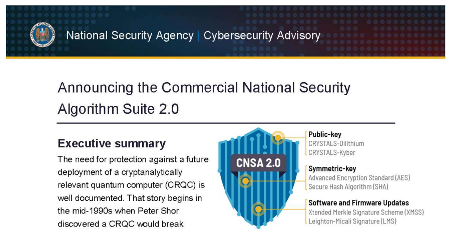
Need to start switching in the year 2023 + Q – x – y
e.g. Q = 18, x=8, y=10: today!



71

What did the NSA say in Sept.'22?

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF


National Security Agency | Cybersecurity Advisory

Announcing the Commercial National Security Algorithm Suite 2.0

Executive summary

The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break

AES-256, SHA-384, SHA-512
LMS/XMSS
CRYSTALS-Kyber, CRYSTALS-Dilithium level V

		2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Software/firmware signing	transition				Support							
Networking (VPN/routers)					and prefer						Exclusive	
Web browsers/servers												
Operating systems											Update/replace	
Niche (IoT, PKI)												

72

Hash-based signatures

- Sphincs+ (stateless)
  - Large (x100 vs pre-quantum)
  - Slow (x500 vs pre-quantum)
  - Alternative to lattice-based
  - Security very well understood
- Separate standardization (IETF) (stateful)
  - RFC 8554 Leighton-Micali signatures
  - RFC 8391 XMSS eXtended Merkle
  - Additional constraints on sender and receiver staying in sync
  - But x30 faster than stateless

Slide credit: Jan-Pieter D'Anvers

73 KU LEUVEN

73

How to continue?

- Pre-Quantum era
  - RSA / ECC
- Hybrid era
  - RSA / ECC + Post-Quantum
- Post-Quantum Era
  - Once confidence in post-quantum is high enough

New call for signature schemes: deadline 1 June 2023 – four more years

74 KU LEUVEN

74

Advantages of public key cryptology

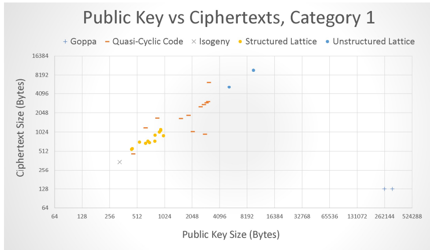
- Reduce protection of information to protection of authenticity of public keys
- Confidentiality without establishing secret keys
  - extremely useful in an open environment
- Data authentication without shared secret keys: digital signature
  - sender and receiver have different capability
  - third party can resolve dispute between sender and receiver

75 KU LEUVEN

75

Disadvantages of public key cryptology

- Calculations in software or hardware two to three orders of magnitude slower than symmetric algorithms
- Longer keys: 64-512 bytes rather than 10..32 bytes
- What if factoring is easy or if a large quantum computer can be built?
- Post-quantum cryptography



KU LEUVEN

76

Outline

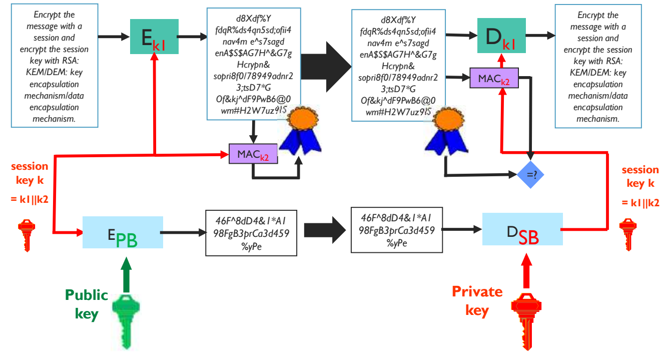
- Symmetric cryptology
  - confidentiality
  - data authentication
  - authenticated encryption
- Public key cryptology (asymmetric cryptology)
- Hybrid cryptology

77 KU LEUVEN

77

RSA encryption for long messages (KEM/DEM)

encryption: $c = m^e \bmod n$
decryption: $m = c^d \bmod n$

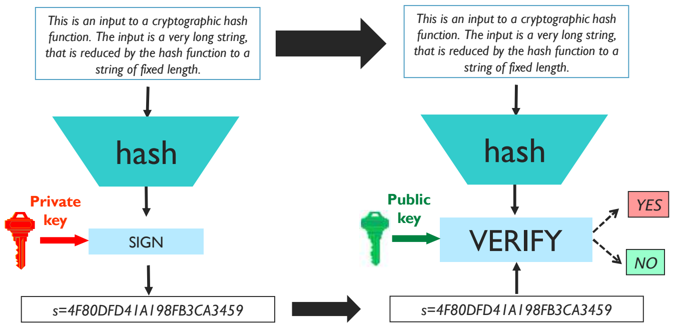


78 KU LEUVEN

78

RSA signatures for long messages (with appendix)

signature: $s = h(m)^d \bmod n$
verification: $h(m) = s^e \bmod n$?



79 KU LEUVEN

79

Selected books on cryptology

A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. The "bible" of applied cryptography. Thorough and complete reference work but slightly outdated– not suited as a first text book. http://www.cacr.math.uwaterloo.ca/hac

D. Boneh, V. Shoup, A Graduate Course in Applied Cryptography, https://toc.cryptobook.us/ Draft. Rather advanced course with interesting applications.

N. Smart, *Cryptography Made Simple*, Springer, 2015. Solid and up to date but on the mathematical side.

D. Stinson, M. Peterson, *Cryptography: Theory and Practice*, CRC Press, 4th Ed., 2018. Solid introduction, but only for the mathematically inclined.

J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall, 2014. Rigorous and theoretical approach.

80 KU LEUVEN

80