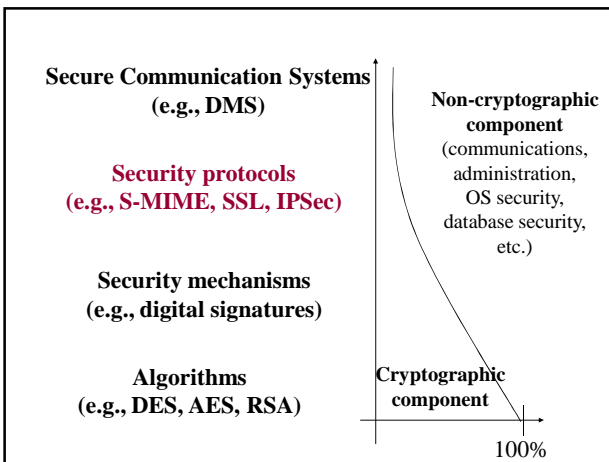


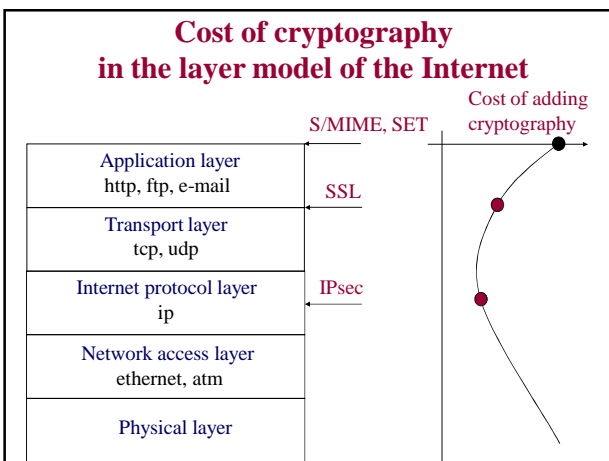
Lecture 12

Security Protocols

Cryptographic Standards

Companies Developing Cryptographic Hardware





S/MIME: Secure Electronic E-mail

- protocol developed by RSA Data Security, Inc. in cooperation with consortium of several big companies in 1995
- work on the corresponding Internet standard started by IETF, 1997
- enables secure communication between e-mail programs from various companies
- multiple products using S/MIME (e.g., Netscape Communicator, Microsoft Outlook, Entrust, and many others)

Cryptographic algorithms:

Triple DES, RC2-40, AES / D-H, RSA / DSS / SHA-1, MD5

Competition: PGP

SSL: Secure WWW

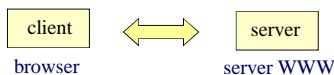
Secure Sockets Layer

- protocol developed by Netscape in 1994
- SSL v. 3.0 in use since 1996, SSL v.2.0 withdrawn
- since 1996 work on the equivalent Internet standard IETF TLS - *Transport Layer Security*, **TLS 1.0 = SSL 3.1**
- the most widely deployed security protocol
 - Secure browsers, e.g., MS Explorer, Mozilla Firefox
 - Secure servers, e.g., Microsoft Server, Apache HTTP Server

Multiple libraries: e.g., OpenSSL (open source)

Competition: almost none, in the past S-HTTP, PCT

SSL: Secure WWW



1. Parameter negotiation
2. Server authentication
3. Client authentication (only on request)
4. Key Exchange
5. Confidential and authenticated message exchange

Cryptographic algorithms:

Confidentiality: none, RC4-40, RC2-40, DES-40
RC4-128, RC2-128, DES, IDEA, Triple DES, AES

Digital signatures: RSA, DSS

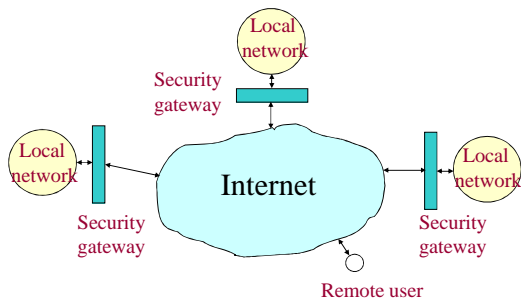
Hash functions: SHA-1, MD5

Key agreement: RSA, D-H, Fortezza

SSL: Encryption Algorithms

Block cipher		Stream cipher	
Algorithm	Key size	Algorithm	Key size
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		
AES	128, 192, 356		

IPsec: Virtual Private Networks (VPN)



- local networks may belong to the same or different organizations
- security gateways may come from different vendors

IPsec: Virtual Private Networks (VPN)

VPN = Economic alternative to networks based on leased lines
 Cost reduction up to 70% !

- development by IETF (*Internet Engineering Task Force*) started in 1994, first IPsec version, RFC 1825-29, published in 1995
- IPsec required in IPv6, optional w IPv4
- S/WAN (*Secure Wide Area Network*) interoperability test for products developed by various vendors, 1995

Algorithms:

confidentiality: DES, Triple DES, AES, RC5, IDEA, CAST, Blowfish, Triple IDEA
 authentication: HMAC-MD5-96, HMAC-SHA-1-96
 key agreement: IKE

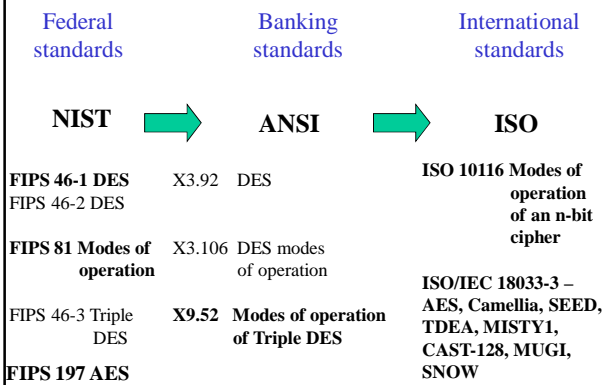
Competition: SSL, PPTP (Microsoft)

Follow-up Course:

ISA 656 Network Security

Cryptographic standards

Secret-key cryptography standards

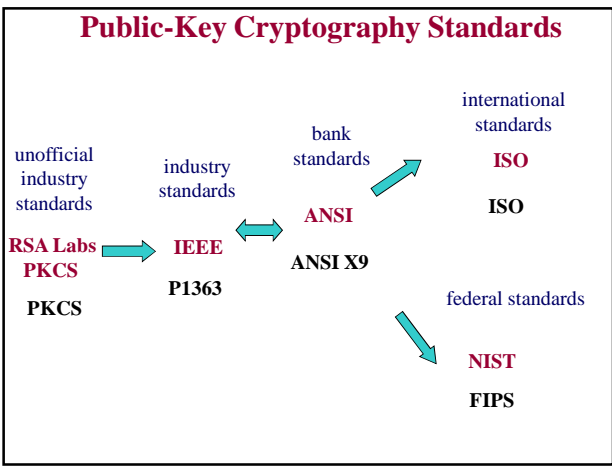


NIST FIPS
National Institute of Standards and Technology
Federal Information Processing Standards

American Federal Standards

Required in the government institutions

Original algorithms developed in cooperation with the National Security Agency (NSA), and algorithms developed in the open research adapted and approved by NIST.



PKCS
Public-Key Cryptography Standards

Informal Industry Standards
developed by RSA Laboratories

in cooperation with
 Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell, Sun

First, except PGP, formal specification of RSA and formats of messages.

IEEE P1363

Working group of IEEE including representatives of major cryptographic companies and university centers from USA, Canada and other countries

Part of the Microprocessors Standards Committee

Modern, open style

Quarterly meetings + multiple teleconferences +
+ discussion list + very informative web page
with the draft versions of standards

IEEE P1363

Combined standard including the majority of modern public key cryptography

Several algorithms for implementation of the same function

Tool for constructing other, more specific standards

Specific applications or implementations may determine a profile (subset) of the standard

ANSI X9

American National Standards Institute

Work in the subcommittee X9F
developing standards for **financial institutions**

Standards for the wholesale
(e.g., interbank)
and retail transactions
(np. bank machines, smart card readers)

ANSI represents U.S.A. in **ISO**

ISO
International Organization for Standardization

International standards

Common standards with IEC -
International Electrotechnical Commission

ISO/IEC JTC1 SC 27
Joint Technical Committee 1, Subcommittee 27

Full members (21):

Australia, Belgium, Brazil, Canada, China, Denmark, Finland,
France, Germany, Italy, Japan , Korea, Holland , Norway ,
Poland, Russia , Spain, Sweden, Switzerland , UK,
USA

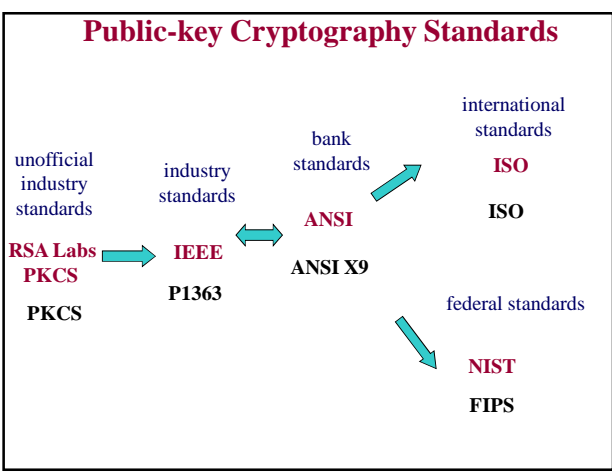
ISO: International Organization for Standardization

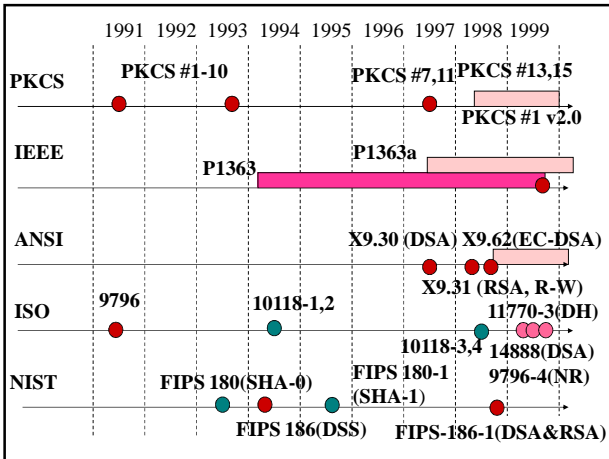
Long and laborious process of the standard development

Minimum 3 years

Study period
NP - New Proposal
WD - Working Draft
CD - Committee Draft
DIS - Draft International Standard
IS - International Standard

Review of the standard after 5 years
= ratification, corrections or revocation





IEEE P1363			
	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption	RSA with OAEP		
signature	RSA & R-W with ISO-14888 or ISO 9796	DSA, NR with ISO 9796	EC-DSA, EC-NR with ISO 9796
key agreement		DH1, DH2 and MQV	EC-DH1, EC-DH2 and EC-MQV

IEEE P1363a			
	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption	RSA with OAEP	new scheme	new scheme
signature	RSA & R-W with ISO-14888 or ISO 9796	DSA, NR with ISO-9796	EC-DSA, EC-NR with ISO 9796
key agreement	new scheme	DH1, DH2 & MQV	EC-DH1, EC-DH2 & EC-MQV

ANSI X9 Standards

	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption	X9.44 RSA		
signature	X9.31 (RSA & R-W)	X9.30 DSA	X9.62 EC-DSA
key agreement		X9.42 DH1, DH2, MQV	X9.63 EC-DH1, 2 EC-MQV

Industry standards - PKCS

	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption	PKCS #1 RSA		PKCS #13 new scheme
signature	PKCS #1 (RSA & R-W)		PKCS #13 EC-DSA
key agreement		PKCS #2 DH	PKCS #13 EC-DH1, 2 EC-MQV

NIST - FIPS

	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption			
signature	FIPS 186-2 RSA	FIPS 186-2 DSA	FIPS 186-2 EC-DSA
key agreement			

International standards ISO			
	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption			
signature	ISO 14888-2 ISO 9796-2	ISO-14888-3 ISO 9796-3	ISO-14888-3 ISO 9796-3
key agreement		ISO-11770-3	ISO-11770-3

Notes for users of cryptographic products (1)

Agreement with a standard does not guarantee the security of a cryptographic product!

Security =
secure algorithms (guaranteed by standards)

- proper choice of parameters
- secure implementation
- proper use

Notes for users of cryptographic products (2)

Agreement with the same standard does not guarantee the compatibility of two cryptographic products !

compatibility =

- the same algorithm (guaranteed by standards)
 - the same protocol
- the same subset of algorithms
- the same range of parameters

Major Companies Developing Cryptographic Hardware

RSA Expo Floorplan



Security Processors



<http://www.broadcom.com/>
Irvine, CA



<http://www.hifn.com/>
Los Gatos, CA



<http://www.caviumnetworks.com/>
Mountain View, CA

Security Processors

- Applications: SSL, IPSec, WLAN
- 50 Mbps-10 Gbps encryption speed
- 1 K to 40 K sessions/sec
- I/O Options: PCIe, PCI/PCI-X, HT
- Programmable multi-protocol support in a single design
- Complete single-chip security solution for both symmetric and asymmetric security processing with dynamic adaptability

Selected Processors (1)



Chip name	Encryption algorithms	HMAC algorithms	Data rate [Mbps]	Public key algorithms	Other
Broadcom BCM5823	DES-CBC 3DES-CBC AES-CBC AES-CTR	SHA-1 MD5	500	DH RSA	On-chip RNG
Broadcom BCM5841	3DES-CBC AES-CBC AES-CTR	SHA-1 MD5	4,800	none	In-line IPsec processing. On-chip SA database. RNG.

Selected Processors (2)



Chip name	Encryption algorithms	HMAC algorithms	Data rate [Mbps]	Public key algorithms	Other
HIFn 7956	DES-CBC 3DES-CBC AES-CBC AES-CTR ARC4	SHA-1 MD5	632	DH RSA	IPsec header and trailer processing. IKE support. On-chip SA database. LZS and MPPC compression. RNG
HIFn 8350 HIPP III	DES-CBC 3DES-CBC AES-CBC AES-CTR ARC4	SHA-1 MD5 AES-XCBC	4,000	DH RSA	In-line IPsec processing. On-chip SA database. IKE processing. RNG

Selected Processors (3)



Chip name	Encryption algorithms	HMAC algorithms	Data rate [Mbps]	Public key algorithms	Other
CN1010	3DES AES RC4	SHA-1 MD5	1,000	DH RSA	IPsec header and trailer processing, IKE support. On-chip SA database. RNG
CN1340	3DES AES RC4	SHA-1 MD5	3,200	DH RSA	In-line IPsec processing. On-chip SA database. IKE processing. RNG

RSA – results reported in the industry using ASICs

Number of the RSA 1024-bit signatures per second:

SafeNet, SafeXcel 1842:

2,100

Cavium, CN1340, Nitrox

42,000

Network Processors with Cryptographic Accelerators

Netronome <http://www.netronome.com>
Pittsburgh, PA

Network Processors with Cryptographic Accelerators



Chip name	Encryption algorithms	HMAC algorithms	Data rate [Mbps]	Public key algorithms	Other
Intel IXP2850	DES-CBC 3DES-CBC AES-CBC	SHA-1	10,000	none	Network processor with cryptographic accelerator. Can do flow-through processing.

Smart Card Chips

- [Atmel](#) San Jose, CA
- [Renesas](#) Tokyo, Japan
- [Infineon](#) Neubiberg, Bavaria, Germany
- [Samsung](#) South Korea
- [ST Microelectronics](#) GENEVA, Switzerland
- [NXP Semiconductors](#) Eindhoven, The Netherlands

Smart Cards

- [Gemalto](#) = Gemplus + Axalto (formerly Schlumberger)
- [Oberthur Card Systems](#)
- [SAGEM Morpho Inc.](#) Tacoma, WA
- [G&D](#) (Giesecke & Devrient) Munich, Germany
- [athena Smartcard Solutions Ltd.](#) Israel
- [CardLogix](#) Irvine, CA

Hardware Accelerators for Password Recovery

[Tableau](#)

Waukesha, WI

[Accelerator](#)

Crypto Device Makers

[Thales](#)

UK

[nCipher](#)

Cambridge, UK

Crypto Cores

[Helion Technology](#)

Cambridge, England

[Conexant / Amphion](#)

Newport Beach, CA

[Certicom](#)

Mississauga, Ontario, Canada

Cryptography and Computer Network Security	Advanced Applied Cryptography
Modular integer arithmetic	Operations in the Galois Fields $GF(2^n)$
<ul style="list-style-type: none"> • Historical ciphers • Classical encryption (DES, Triple DES) • Public key encryption (RSA) • Hash functions and MACs • Digital signatures • Public key certificates • PGP • Secure Internet Protocols • Cryptographic standards 	<ul style="list-style-type: none"> • AES • Stream ciphers • Elliptic curve cryptosystems • Random number generators • Smart cards • Attacks against implementations (timing, power, fault analysis) • Efficient and secure implementations of cryptography • Security in various kinds of networks (IPSec, wireless) • Zero-knowledge identification schemes
