

Lecture 13

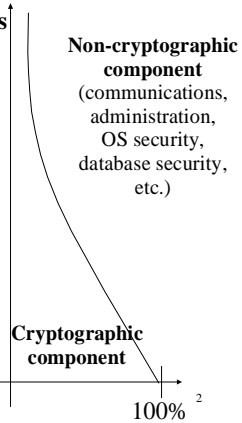
Security Protocols Cryptographic Standards

Secure Communication Systems
(e.g., Defense Message System)

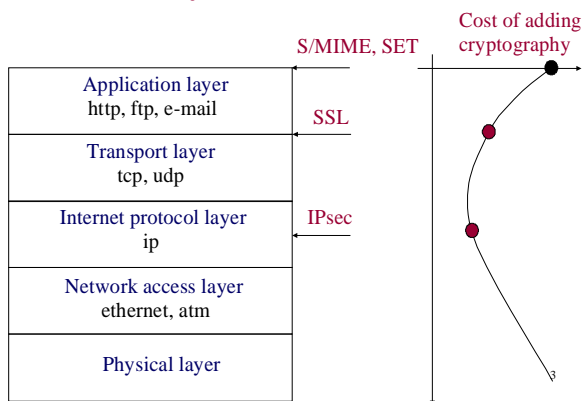
Security protocols
(e.g., S-MIME, SSL, IPSec)

Security mechanisms
(e.g., digital signatures)

Algorithms
(e.g., DES, AES, RSA)



Cost of cryptography in the layer model of the Internet



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

4

SSL: Secure WWW

Secure Sockets Layer

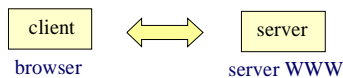
- protocol developed by Netscape in 1994
- SSL v. 3.0 in use since 1996, SSL v.2.0 withdrawn
- since 1996 work on the equivalent Internet standard IETF TLS - Transport Layer Security, **TLS 1.0 = SSL 3.1**
- the most widely deployed security protocol

Secure browsers, e.g., Mozilla, MS Explorer
Secure servers, e.g., Apache, MicrosoftIIS

Multiple libraries: SSL Ref (Netscape), OpenSSL (open source), SSL Plus (Consensus Development), SSLeay, SSLJava, etc.

Competition: almost none, in the past S-HTTP, PCT ⁵

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

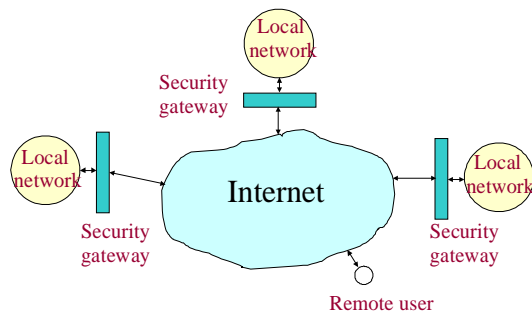
6

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, 256		

7

IPsec: Virtual Private Networks (VPN)



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

8

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
- second version, RFC 2401 from 1998
- third version, RFC 4301 from 2005
- 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 (RFCs from 2005)
 authentication: HMAC-MD5, HMAC-SHA-1
 key agreement: IKE

Competition: SSL, PPTP (Microsoft)

9

Follow-up Course:

ISA 666 Internet Security Protocols

10

Cryptographic standards

11

Secret-key cryptography standards

Federal standards

Banking standards

International standards

NIST



ANSI



ISO

FIPS 46-1 DES
FIPS 46-2 DES

X3.92 DES

ISO 8732 Modes of operation of a 64-bit cipher

FIPS 81 Modes of operation

X3.106 DES modes of operation

FIPS 46-3 Triple DES

X9.52 Modes of operation of Triple DES

ISO 10116 Modes of operation of an n-bit cipher

FIPS 197 AES

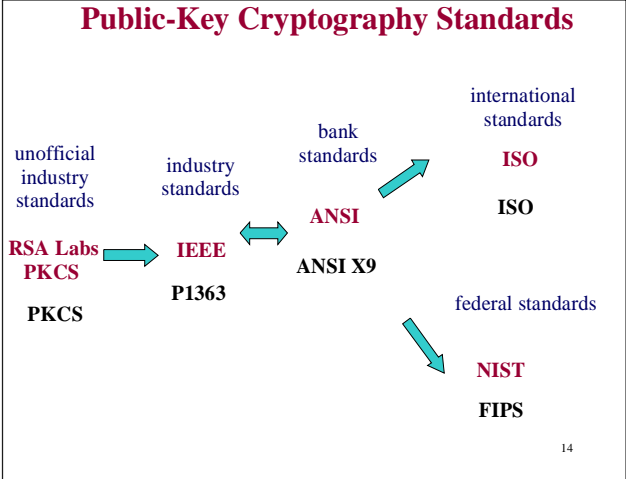
NIST FIPS
National Institute of Standards and Technology
Federal Information Processing Standards

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.

13



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.

15

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

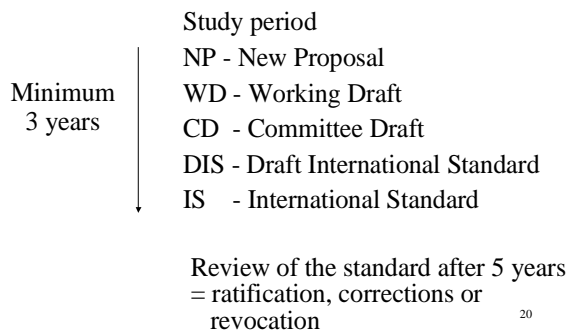
Joint Technical Committee 1, Subcommittee 27

Full members (21):

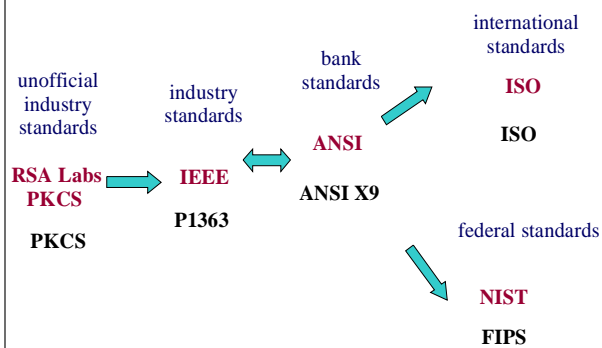
Australia, Belgium, Brazil, Canada, China, Denmark, Finland,
France, Germany, Italy, Japan , Korea, Holland , Norway ,
Poland, Russia , Spain, Sweden, Switzerland , UK,
USA

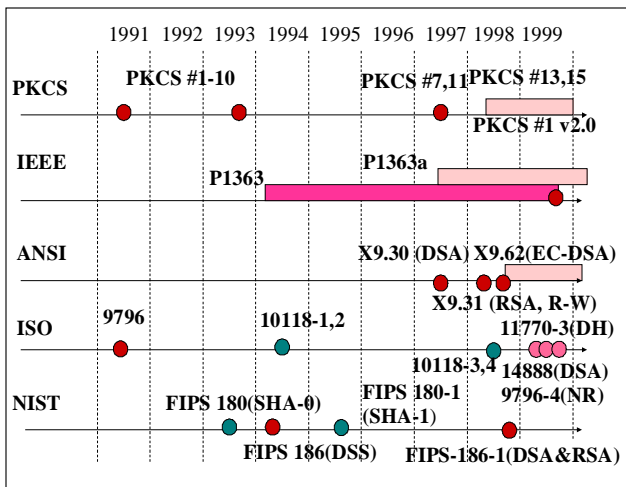
ISO: International Organization for Standardization

**Long and laborious process of
the standard development**



Public-key Cryptography Standards





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 i 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 186-1 RSA	FIPS 186 DSA	FIPS 186-2 EC-DSA
key agreement			

International standards ISO

	factorization	discrete logarithm	elliptic curve discrete logarithm
encryption			
signature	ISO 9796-1 ISO 9796-2	ISO-14888-3 ISO 9796-4	ISO-14888-3 ISO 9796-4
key agreement		ISO-11770-3	ISO-11770-3

Secure key sizes

	factorization	discrete logarithm	elliptic curve discrete logarithm
PKCS			
IEEE P1363			
ANSI X9	≥ 1024	≥ 1024	≥ 160
NIST FIPS		$512 \leq L \leq 1024$	
ISO			29

Padding schemes

	encryption	signatures with appendix	signatures with message recovery
PKCS	OAEP PKCS #1	PKCS #1	
IEEE P1363	OAEP	ISO 14888	ISO 9796
ANSI X9	OAEP	ISO 14888	ISO 9796
NIST FIPS			
ISO		ISO 14888	ISO 9796

Hash functions

	dedicated	based on block ciphers	based on modular arithmetic
PKCS	MD5 MD2		
IEEE P1363	SHA-1 RIPEMD-160		
ANSI X9	SHA-1 RIPEMD-160		
NIST FIPS	SHA-1, SHA-256 SHA-384, SHA-512		
ISO	SHA-1, RIPEMD-128, 160	MDC-2	MASH-1 MASH-2

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

Follow-up courses

Cryptography and Computer Network Security

ECE 646

Secure
Telecommunication
Systems
ECE 746
(Spring 2008)

Ubiquitous Computing
ECE699
(Fall 2008)

Computer Arithmetic
ECE 645
(Spring 2008)

34

Cryptography and Computer Network Security

Secure Telecommunication Systems

Modular integer arithmetic

Operations in the Galois Fields $GF(2^n)$

- Historical ciphers
- Classical encryption (DES, IDEA, RC5, AES)
- Public key encryption (RSA, DH, DSA)
- Hash functions and MACs
- Digital signatures
- Public key certificates
- PGP
- Secure Internet Protocols
- Cryptographic standards

- AES
- Stream ciphers
- Elliptic curve cryptosystems
- Random number generators
- Smart cards
- Attacks against implementations (timing, power analysis)
- Efficient and secure implementations of cryptography
- Security in various kinds of networks (IPSec, wireless)
- Zero-knowledge identification schemes

35
