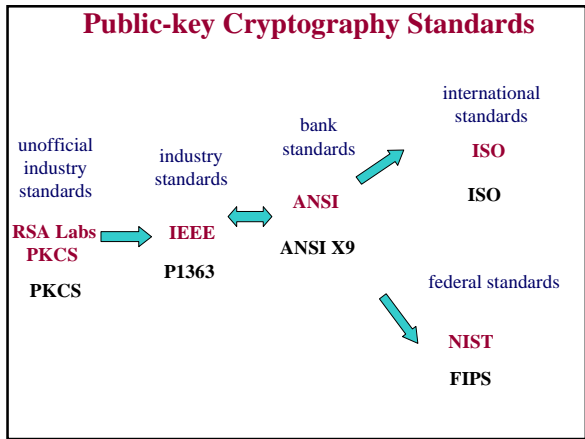


Lecture 16

Cryptographic standards



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

Quaterly 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

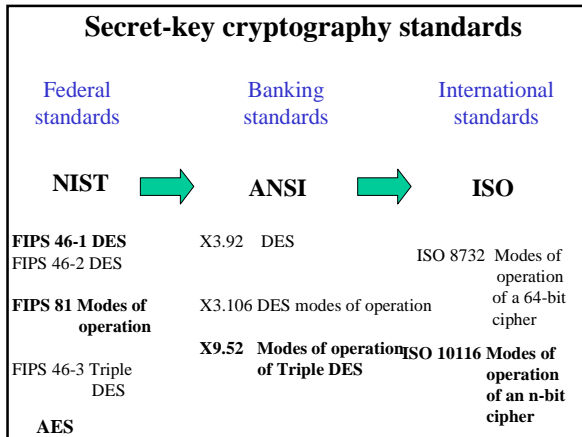
Review of the standard after 5 years
= ratification, corrections or revocation

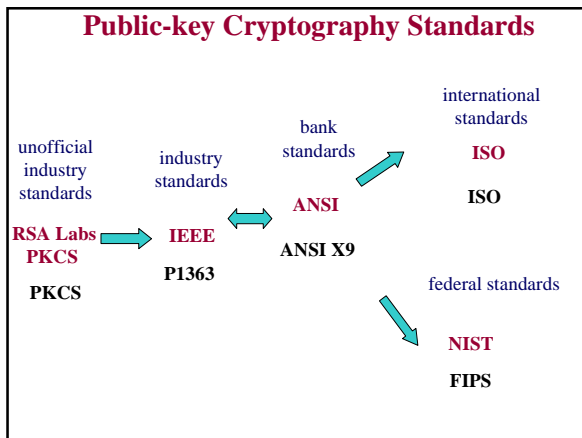
NIST FIPS
National Institute of Standards and Technology
Federal Information Processing Standards

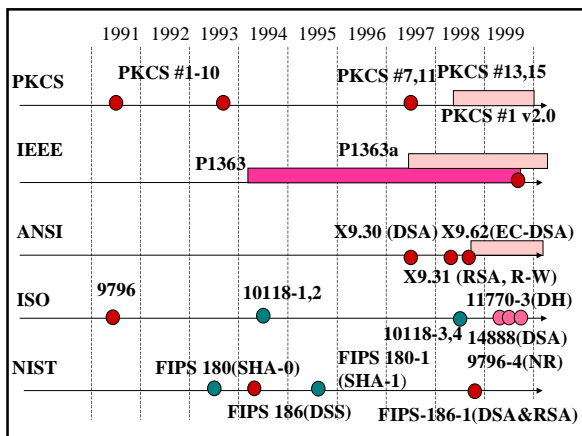
American Federal Standards

Required in the government institutions

Original algorithms developed in cooperation with the National Security Agency (NSA)







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 186-1 RSA	FIPS 186 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			

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		
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
