

CRYPTOGRAPHY

quick guide from <http://www.bilbaodigital.es>

Authentication	PKI	framework with the following components
Integrity	CA/CRL	issues digital certificates to authorized users
Confidentiality	RA	reduces the load of CA
Non-repudiation	X.509	standard for digital certificates

type of encryption	advantages	disadvantages	security
symmetric private key	faster	key distribution	key > 256 bits (uncrac
asymmetric public key	confid. ^ authentication	slower (math functions)	more secure
(asymmetric protocol is used to exchange private key whichone the communication is encrypted)			
The security of an algorithm cannot exceed its key length (any algorithm can be cracked by BF), but it can be smaller			

Cryptographic Algorithms CONFIDENTIALITY	year	developer	key (bits)	type of encryption	attacks	applications
Diffie-Hellman	1976	Whitfield Diffie, Martin Hellman	512 < k < 1024	asymmetric (discrete logarithm)	non-authenticated (MiM)	SSL, IPSec
DES (ECB CBC salt CFM/OFB stream)	1977	NIST and IBM	56	symmetric (block 64 bits)	brute force	RSA message encryption, IPSec
RSA *very secure algorithm	1977	MIT - Rivest, Shamir, Adleman	< 4096	asymmetric (prime numbers)	not significant	OS (IE, FF), NICS, SmartCards, SSL
RC4	1987	Ron Rivest	40-256	symmetric (stream)	weak keys ^ 40 bits BF	SSL, WEP, WPA, Kerberos, SSH, RDP
IDEA	1991	James lassey	128	symmetric (block 64 bits)	none	PGP v1 (pubring.pkr ^ secing.skr), OpenPGP
3DES	1998	Walter Tuchman (IBM)	56, 112, 168	symmetric (block 64 bits)	chosen/know plaintext (112)	VPN (Linux), electronic payment, IPSec, MS One
Blowfish	1993	Bruce Schneier	32-448	symmetric (block 64 bits)	none	CS-Cart, GnuPG, Putty, Truecrypt, X-Cart
Twofish	1998	Bruce Schneier, ...	128-256	symmetric (block 128 bits)	none	cryptcat, GnuPG, PGP, TrueCrypt,
AES Rijndael	2002	Vincet Rijmen and Joan Daemen	128 192 256	symmetric (block 126 192 256 bits)	not significant	RAR, WinZIP, BitLocker, TrueCrypt, IPSec, GPG
XOR, Base64, Uuencode (very weak)						

HASH (one-way function) INTEGRITY	year	developer	output size (bits)	attacks	applications
MD5	1991	Ronald Rives	128	not collision resistant	check integrity of files, store passwords, digital s
SHA1	1995	NIST, NSA	160	rainbow tables	SSL, TLS, PGP, SSH, S/MIME, IPSec
SHA2	2001	NIST, NSA	256-512	none	U. S. Government applications

Digital Signature | AUTHENTICATION

Cryptographic Protocols	OSI layer	developer	cracking tools	action	cryptographic attacks	cryptographic applications
Secure MIME	7	FBI	Magic Lantern	keystroke logger	Known plaintext	EFS EncryptOnClick
SSH	5	FBI	Carnivore	online sniffing	Ciphertext only	ABC Chaos Encrypt HTML source
PPTP	5	Mark Miller	PGPCrack	PGP brute-forcer	MiM	Advanced File Encryptor
SSL	4	Microsoft	Diskprobe	recovers last EFS encrypted file	Replay	Advanced HTML Encrypt and Password Protect
TLS	4	Passware, Inc.	Passware	app pass recovery	Chosen plaintext	Alive File Encryption
IPSec	3	Atstake - Symantec	L0ftcrack	dictionay and brute force vs SAM	Chosen ciphertext	Crypt edit
EAP		Openwall	John the Ripper	hybrid attack	Rubber hose	Encrypt my Folder
		CryptoHeaven, Inc.	CryptoHeaven	2024-4048 asymmetric 256 bits key		SafeCryptor
Resources:		http://www.cryptool.com	AMI Decode	bios cracker		Polar Crypto Light