Acrónimos

	A
AEA	Advanced Encryption Algorithm
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASN.1	Abstract Sintax Notation 1
AWT	Abstract Window Toolkit
	B
	C
C	CountryCode
CA	Certification Authority
CBC	Cipher Block Chaining
CCE	Criptografia de Curva Elíptica
CD	Compact Disc
CDROM	Compact Disc Read Only Memory
CFB	Cipher FeedBack
CGI	Common Gateway Interface
CN	CommonName
CPS	Certificate Practice Statement
CPU	Central Proccesing Unit
CRL	Certificates Revokated List
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
	D
DEA	Data Encryption Algorithm

DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman
DHE	Diffie-Hellman Elíptico
DN	DistinguishedName
DPA	Differential Power Analysis
DSS	Digital Signature Standard
	E
ECB	Electronic Code Book
	F
FEAL	Fast data Enciphment ALgorithm
FNMT	Fábrica Nacional de Moneda y Timbre
	G
GNU	GNU's Not UNIX
GPL	General Public Licence
GUI	Graphic User Interface
	H
HMAC	Hash Message Authenticaction Codes
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
	I
IAIK	Applied Information Procesing and Communications (en alemán)
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITU	International Telecommunication Union
	J
J2SDK	Java 2 Standard Development Kit
JCA	Java Cryptographic Architecture
JCE	Java Cryptographic Extension
JCSI	Java Crypto and Security Implementation
JFC	Java Foundation Classes

JKS	Java KeyStore
JRE	Java Runtime Enviroment
JSP	Java Server Pages
JVM	JAva Virtual Machine
	K
KDC	Key Distribution Center
KDE	Kool Desktop Environment
	L
L	Localityname
	M
MAC	Message Authentication Codes
MD	Message Digest
MDC	Modification Detection Codes
MIME	Multipurpose Internet Mail Extensions
	N
NSA	National Security Agency
NBS	National Bureau of Standards
NIST	National Institute of Standards Technology
	Ñ
	O
O	OrganizationName
OCSP	Online Certificate Status Protocol
OAEP	Optimal Asymmetric Encryption Padding
OFB	Output FeedBack
OS	Operating System
OU	OrganizationUnitName
	P
PBE	Password-Based Encryption
PC	Personal Computer
PEM	Privacy-Enhanced Mail
PFE	Problema de la Factorización Entera

PGP	Pretty Good Privacy
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infraestructure
PLD	Problema del Logaritmo Discreto
PLDE	Problema del Logaritmo Discreto Elíptico
PSS	Padding Signature Standard
	Q
	R
RA	Registration Authority
RC	Ron's Code o Rivest's Ciphers
RFC	Request for Comments Document
RSA	Rivest-Shamir-Adleman
	S
S	StateName
SAFER	Secure And Fast Encryption Routine
SDK	Standard Development Kit
SET	Secure Electronic Transactions
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
S/MIME	Secure Multipurpose Internet Mail Extensions
SO	Sistema Operativo
SPA	Simple Power Analysis
SSL	Security Socket Layer
	T
TLS	Transport Layer Security
TTP	Trusted Third Parts
TUG	Universidad de Tecnologia de Graz
	U
UIT	Unión Internacional de Telecomunicaciones
	V
VPN	Virtual Private Network

W	
X	
Y	
Z	

Tabla 31: Lista de acrónimos