A. függelék
Kapcsolódó szabványok

USA ANSI szabványok	
ANSI #	Tárgy
X9.17	kulcsgondozás és véletlenszám-generálás
X9.30-1	digitális aláírás algoritmus (DSA)
X9.30-2	SHA hash függvény a DSA számára
X9.31-1	RSA aláíró algoritmus
X9.31-2	hash függvények az RSA számára
X9.42	Diffi e-Hellman kulcscsere
X9.45	attribútum-tanúsítványok
X9.52	3DES
X9.55	tanúsítványok és visszavonási listák
X9.57	tanúsítvány menedzsment
USA FIPS szabványok	
FIPS #	Tárgy
FIPS 46-2	a DES leírása
FIPS 74	irányelvek a DES használatához
FIPS 81	a DES működési módjai
FIPS 112	jelszavak használata
FIPS 113	adat hitelesítés (CBC-MAC)
FIPS 140-1	kriptomodulokkal kapcsolatos biztonsági követelmények
FIPS 171	kulcsgenerálás
FIPS 180-1	a SHA-1 hash függvény
FIPS 185	kulcs-escrow (Clipper & SKIPJACK)
FIPS 186	digitális aláírás szabvány (DSA és ECDSA)
FIPS 196	partner hitelesítés

Nemzetközi ISO szabványok	
ISO #	Tárgy
7498-2	OSI biztonsági architektúra
8372	64 bites blokkrejtjelezők működési módjai
9594-8	hitelesítési keretrendszer (X.509)
9796	digitális aláírás üzenet visszaállítással (pl. RSA)
9797	integritásvédelmi mechanizmusok (MAC)
9798-1	partnerhitelesítés – bevezető
9798-2	– szimmetrikus rejtjelezéssel
9798-3	– nyilvános kulcsú technikákkal
9798-4	– kulcsolt egyirányú függvényekkel
9798-5	– zero-knowledge technikák felhasználásával
9979	kriptográfi ai algoritmus nyilvántartás
10116	*n* bites blokkrejtjelezők működési módjai
10118-1	hash függvények – bevezető
10118-2	– blokkrejtjelezőkből konstruált
10118-3	– dedikált algoritmusok
10118-4	– moduláris aritmetikára épülő
11770-1	kulcsgondozás – bevezető
11770-2	– szimmetrikus kulcsú technikák
11770-3	– aszimmetrikus kulcsú technikák
13888-1	letagadhatatlanság – bevezető
13888-2	– szimmetrikus kulcsú technikák
13888-3	– aszimmetrikus kulcsú technikák
14888-1	digitális aláírás (hash-and-sign technikák) – bevezető
14888-2	– identitás alapú mechanizmusok
14888-3	– tanúsítvány alapú mechanizmusok
15946	elliptikus görbékre épülő kriptográfi ai technikák

PKCS (Public-Key Cryptography Standards) szabványok	
PKCS #	Cím
PKCS 1	RSA encryption standard
PKCS 3	Diffi e-Hellman key-agreement standard
PKCS 5	Password-based encryption standard
PKCS 6	Extended-certifi cate syntax standard
PKCS 7	Cryptographic message syntax standard
PKCS 8	Private-key information syntax standard
PKCS 9	Selected attribute types
PKCS 10	Certifi cation request syntax standard
PKCS 11	Cryptographic token interface standard
Néhány kapcsolódó Internet RFC	
RFC #	Tárgy
RFC 2104	a HMAC algoritmus leírása
RFC 2246	TLS (Transport Layer Security) protokoll (SSL 3.1)
RFC 2401	az IPSec biztonági architektúra áttekintése
RFC 2402	– az AH protokoll leírása
RFC 2406	– az ESP protokoll leírása
RFC 2408	– az ISAKMP protokoll leírása (kulcscsere)
RFC 2409	– az IKE protokoll leírása (kulcscsere)
Néhány kapcsolódó GSM specifi káció	
3GPP TS #	Tárgy
55.205	példák az A3 és az A5 algoritmusokra (GSM MILENAGE)
55.216	az A5/3 és a GEA3 (GPRS) rejtjelező algorimtusok leírása