Krzysztof Gaj, Anna Górska, Karol Górski
© ENIGMA Systemy Ochrony Informacji Sp. z o.o.

ul. Cietrzewia 8, 02-492 Warszawa
http://www.enigma.com.pl

Francuskie tłumaczenia przygotował p. Nicolas Courtois.

Słowniczek terminów związanych z kryptologią i ochroną informacji angielsko - francusko - polski

10 listopada 2003 roku

Legenda:
N - określenie występuje w Polskich Normach dotyczących ochrony informacji
A - określenie powszechnie używane i akceptowane
R - określenie rzadkie (nieakceptowane)
O - określenie obce (używane w języku polskim)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Akronimy

English	Français	Polski	Uwagi
-- A --			
abuse		nadużycie (N)	
access control	contrôle d'accès	kontrola dostępu (N)	PN-ISO 7498-2
accountability		rozliczalność (N)	PN-I-02000
acquirer	acheteur, acquéreur	nabywca (N)	
adaptive attack	attaque dynamique, attaque adaptative	atak adaptacyjny	
adversary	adversaire	oponent, przeciwnik	
affine function		funkcja afiniczna	
application programming interface (API)	"API"	API (O), interfejs oprogramowania (R)	
assurance		uzasadnienie zaufania (N)	PN-ISO/IEC 15408
asymmetric cryptography	cryptographie asymétrique	kryptografia asymetryczna (N)	PN-I-02000 patrz również „public key cryptography”
attack	attaque	atak (N)	PN-I-02000
attribute certificate		certyfikat uprawniający	
audit	audit	audyt (N)	PN-I-02000
authentication	authentification	uwierzytelnienie (N), autentyzacja (R), autentykacja (R)	PN-ISO/IEC 9798
authentication initiator		inicjator uwierzytelnienia (N)	PN-I-02000
authentication responder			
authorization	autorisation	uprawnianie (N), autoryzowanie (A), autoryzacja (N)	PN-I-02000
availability	disponibilité	dostępność	PN-I-02000
avalanche criterion	critère d'avalanche	kryterium lawinowości (A)	
-- B --			
balanced Boolean function, binary balanced function		zrównoważona funkcja boolowska	
balancedness		zrównoważenie	

BAN (Burroughs, Abadi, Needham) logic		logika BAN	
bent function		bent-funkcja	
binding	liant	wiążący	
biometric device	dispositif biométrique	urządzenie biometryczne (A)	
biometric	biométrique	biometryczny (N)	PN-I-02000
birthday attack	attaque d'anniversaires	atak z wykorzystaniem paradoksu dnia urodzin (A)	
birthday paradox	paradoxe d'anniversaires	paradoks dnia urodzin (A)	
bit commitment	mise en gage	zobowiązanie bitowe (A)	
blind signature		ślepy podpis cyfrowy	
blinding	masquage, transformation “en aveugle”	maskowanie (A)	
block cipher	chiffrement par blocks	szyfr blokowy (N)	
brute-force attack	attaque exhaustive, recherche exhaustive	atak na zasadzie pełnego przeglądu (N), atak wyczerpujący (A)	patrz również „exhaustive attack”
bug	un micro caché	pluskwa (A)	

-- C --

CA certificate		zaświadczenie certyfikacyjne, certyfikat urzędu ds. certyfikatów, certyfikat CA	
cipher block chaining (CBC)	mode CBC, chiffrement avec chaînage des blocs	wiązanie bloków szyfrogramu (A), wiązanie bloków zaszyfrowanych (A)	
capability			
cardholder		posiadacz karty	
card issuer	émetteur des cartes	wydawca kart (N)	
certificate	certificat	certyfikat (N)	
certificate of primality		certyfikat pierwszości	
certification authority	l'organisme (agrée) de certification	organ certyfikacji (N), urząd ds. certyfikacji (A), urząd ds. certyfikatów (A)	PN-I-02000
certification path		ścieżka certyfikacji	
certificate policy		polityka certyfikacji	
certification practice statement		regulamin pracy Urzędu ds. Cetryfikatów	
certificate repository	annuaire de certificats	składnica certyfikatów	
certificate revocation list (CRL)	la liste de révocation des certificats	lista unieważnionych certyfikatów (A), CRL (O)	
cipher feedback (CFB)	mode CFB, chiffrement par rétroaction	sprzężenie zwrotne z szyfrogramu (A), szyfrowe sprzężenie zwrotne (N, R)	
challenge	défi, un "challenge"	wyzwanie (N)	PN-ISO/IEC 9798
challenge-response protocol	protocole de type prouveur-vérifieur	protokół wyzwanie-odpowiedź (A)	
chaotic cryptosystem		kryptosystem chaotyczny	
characteristic		charakterystyka	
checksum	somme de contrôle	suma kontrolna (A)	
Chinese Remainder Theorem (CRT)	le théorème chinois	Chińskie Twierdzenie o Resztach (A)	
chosen plaintext attack	attaque à texte clair choisi	atak za pomocą wybranego tekstu jawnego (N), atak z wybranym tekstem jawnym (A)	

English	Français	Polski	Uwagi
ciphering	chiffrement	szyfrowanie (A)	
cipher strength	la solidité du chiffre	moc szyfru	
ciphertext	le texte chiffré, le chiffre	szyfrogram (N), tekst zaszyfrowany (A)	
ciphertext only attack	attaque à texte chiffré connu	atak tekstem zaszyfrowanym (N), atak z tekstem zaszyfrowanym (A)	
claimant		podmiot uwierzytelniany (N)	PN-ISO/IEC 9798
classified	classifié	klasyfikowane (A)	
claw-free permutation pair		odporna na kolizje para permutacji	
cleartext		tekst jawny (N)	PN-I-02000
collision resistance	résistance aux collisions	odporność na kolizje (A)	
commercial security			
commitment		dane powierzone (N), zobowiązanie	PN-I-02000
completeness	complétude	zupełność (A)	
compromise	compromettre	naruszenie ochrony danych (N), kompromitacja (R)	PN-I-02000
computational security	sécurité calculatoire	bezpieczeństwo obliczeniowe (A)	
computationally infeasible, intractable	calculatoirement infaisable, intraitable	obliczeniowo niewykonalne	
computer network security	la sécurité des réseaux	zabezpieczenia sieci komputerowych	
concrete security			
confidentiality	confidentialité	poufność (N)	PN-I-02000
confirmer-designated signature		podpis ze wskazaniem potwierdzającego	
confusion	confusion	nieregularność (A), konfuzja (R)	
convertible undeniable signature			
correlation immunity		odporność na korelacje, nieskorelowanie	
covert channel	canal caché	ukryty kanał (A)	
cracker	intrus	włamywacz, cracker (O)	
credentials		dane uwierzytelniające (N)	PN-I-02000
cross-certificate pair		para certyfikatów wzajemnych	
cross-certification	certification mutuelle	certyfikacja wzajemna (A), kroscertyfikacja (A)	
cryptanalysis	cryptanalyse	kryptoanaliza (N)	PN-I-02000
cryptoalgorithm	algorithme de cryptographie	algorytm kryptograficzny	
cryptographic area		obszar kryptograficzny	
cryptographic check value		kryptograficzna wartość kontrolna (N)	PN-ISO/IEC 9798-4
cryptographic device	dispositif de cryptographie	urządzenie kryptograficzne (A)	
cryptographic equipment	des équipements cryptographiques	sprzęt kryptograficzny (N)	
cryptographic module	module cryptographique	moduł kryptograficzny (A)	
cryptography	cryptographie	kryptografia (N)	PN-I-02000
cryptology	cryptologie	kryptologia (N)	PN-I-02000
cryptoperiod		okres ważności klucza kryptograficznego (N)	PN-I-02000

cryptosystem	cryptosystème	kryptosystem (A), system kryptograficzny (A)	
cut and choose (protocol)		(protokół) podziel i wybierz	

-- D --

DEK (Data Encryption Key)	la clef de chiffrement	klucz szyfrujący dane (A)	
data integrity	intégrité des données	integralność danych (A)	
data origin authentication	authentification de la source des données	uwierzytelnienie źródła danych (A)	
data protection	protection des données	ochrona danych (N)	PN-I-02000
decipherment, decryption	déchiffrement, décryptage	deszyfrowanie (N), odszyfrowanie (A) rozszyfrowanie (A)	
dedicated hash function (DHF)		dedykowana funkcja skrótu	PN-ISO/IEC 10118-3
dictionary attack	attaque du dictionnaire	atak słownikowy (A)	
differential		uogólniona charakterystyka, wyrażenie różnicowe	
differential cryptanalysis	cryptanalyse différentielle	kryptoanaliza różnicowa (A)	
differential fault analysis		różnicowa analiza błędów	
differential power analysis (DPA)		różnicowa analiza mocy	
diffusion	diffusion	rozproszenie (A), dyfuzja (A)	
digital notary	notaire électronique		
digital signature	signature électronique	podpis cyfrowy (A), podpis elektroniczny (R)	
digital signature law	loi régulant la signature électronique	prawo o podpisach cyfrowych (A)	
disclosure		ujawnienie (N)	PN-I-02000
discrete logarithm	logarithme discret	logarytm dyskretny (A)	
discretionary access control (DAC)		uznaniowa kontrola dostępu (DAC)	PN-I-02000
distinguishing identifier		identyfikator wyróżniający (A)	
distinguished name (DN)		nazwa wyróżniająca	
domain Data Recovery Centre (DRC)	domaine centre de récupération des données	domena (A) centrum odtwarzania danych	
dual signature		podwójny podpis	

-- E --

eavesdropping	espionnage, écoutes, oreille indiscrète	podsłuch	
electronic code book (ECB)	carnet de codage électronique	elektroniczna książka kodowa (A)	
electronic data interchange (EDI)		elektroniczna wymiana danych (A)	
electronic cash	la monnaie électronique	elektroniczna gotówka (A)	
electronic commerce	le commerce électronique	elektroniczny handel (A)	
electronic payments	payements électroniques	elektroniczne płatności (A)	
elliptic curve	courbe elliptique	krzywa eliptyczna (A)	
elliptic curve cryptosystem (ECC)	cryptosystème utilisant des courbes elliptiques, basé sur les courbes elliptiques, cryptosystème des courbes elliptiques	kryptosystem oparty na krzywej eliptycznej (A)	
elliptic curve discrete logarithm	le logarithme discret sur une courbe elliptique	logarytm dyskretny na krzywej eliptycznej	

English	Français	Polski	Uwagi
encipherment	chiffrement, cryptage	szyfrowanie (N), enkrypcja (R)	
encryption		szyfrowanie (N)	
entity		podmiot	
entity authentication		uwierzytelnienie podmiotu (N)	PN-ISO/IEC 9798
entropy		entropia	
exhaustive (key space) attack	attaque exhaustive	atak wyczerpujący (A)	
existential forgery		egzystencjalne fałszerstwo	
exponent	exposant	wykładnik (A)	

-- F --

factorization / factoring	factorisation (des entiers)	faktoryzacja (A), rozkład na czynniki pierwsze (A)	
fail-stop signature		podpis typu fail-stop	
fault injection		wstrzykiwanie błędów	
feedback shift register	registre à décalage	rejestr przesuwający ze sprzężeniem zwrotnym (A)	
fingerprint	empreinte	skrót danych (N)	
firewall	un "firewall"	firewall (O), ściana przeciwogniowa (R), zapora przeciwogniowa (R)	
forward certificate		certyfikat wychodzący	
frequency analysis	analyse des fréquences	analiza częstości (A)	

-- G --

group signature		podpis grupowy	

-- H --

hacker	un "hacker"	haker (A), hacker (O)	
hardware	matériel (informatique)	sprzęt (A)	
hash function	fonction de hachage	funkcja skrótu (N), funkcja haszująca (R)	PN-ISO/IEC 10118
hash value, hash code	un haché	skrót (N)	PN-ISO/IEC 10118
home banking	banque à domicile	home banking (O)	

-- I --

identification	identification	identyfikacja (N)	
identity certificate		certyfikat identyfikujący	
impersonation, masquerade	usurpation, mascarade	naśladowanie (N), maskarada (N)	
impossible differential			
initial value	valeur initiale	wartość początkowa (A)	
initialisation vector (IV)	valeur initiale	wektor początkowy (A), wektor inicjujący (A) wektor inicjalizacyjny (A)	
instance hiding computation, blind computation	calcul sur des données confidentielles, calcul en aveugle		
integrity	intégrité	integralność (N)	PN-I-02000
interception	interception	przechwycenie	
interleaving attack		atak przeplotowy (N)	
intruder		intruz	
iterated block cipher		iteracyjny szyfr blokowy (A)	
Information Technology Security Evaluation Criteria (ITSEC)		Kryteria oceny zabezpieczeń teleinformatyki (A) ITSEC (O)	

-- K --

Key Encryption Key (KEK)	clé mère	klucz szyfrujący klucze (A)	
key	clef, clé	klucz (N)	
key agreement	génération de clef	uzgadnianie klucza (N)	
key archival	archivage de clef	archiwizacja klucza	
key backup	sauvegarde de clé	wykonywanie kopii zapasowej klucza	
key distribution	distribution des clés	dystrybucja kluczy (A)	
key diversification		dywersyfikacja kluczy	
Key Distribution Center (KDC)	centre de distribution de clés	centrum dystrybucji kluczy (A)	
key escrow	séquestre de clefs	deponowanie klucza (A)	
key escrow cryptography		kryptografia kontrolowana	
key establishment	établissement d'une clé	ustalanie klucza (N)	
key exchange	échange de clef	wymiana klucza	
key generation		generowanie klucza	
key management	gestion de clés	zarządzanie kluczami (N)	
key recovery	récupération de clef	odtwarzanie klucza (A)	
key scheduling	génération de clefs	generowanie kluczy wewnętrznych	
key stream	flot de clés	strumień klucza (A)	
key transport	transmission de clef	przekazanie klucza (N), transport klucza (A)	
key validation			
knapsack problem	le problème du sac à dos, le problème de sous-ensemble	problem plecakowy (A), zagadnienie plecakowe	
known plaintext attack	attaque à texte clair connu	atak znanym tekstem jawnym (N), atak ze znanym tekstem jawnym (A)	

-- L --

law enforcement	autorités judiciaires	wymiar sprawiedliwości	
law enforcement access field (LEAF)		pole dostępu dla służb wymiaru sprawiedliwości	
linear approximation		aproksymacja liniowa	

English	Français	Polski	Uwagi
linear complexity, linear span	complexité linéaire	złożoność liniowa (A)	
linear cryptanalysis	cryptanalyse linéaire	kryptoanaliza liniowa (A)	
linear expression		wyrażenie liniowe	
linear feedback shift register		rejestr przesuwny z liniowym sprzężeniem zwrotnym	
linear function		funkcja liniowa	
log		rejestr, dziennik	
login		rejestracja, rejestrować się	
logout		wyrejestrować się	

-- M --

man in the middle attack		atak metodą przechwytywania przez podmiot pośredniczący	
mandatory access control (MAC)		obowiązkowa kontrola dostępu (N)	PN-I-02000
masquerade, impersonation	usurpation, mascarade	maskarada (N), naśladowanie (N)	
Modification Detection Code (MDC)			
meet in the middle attack	attaque dans le milieu	atak ze spotkaniem w środku	
merchant	fournisseur de service, marchand	sprzedawca, merchant (O)	
message	message	wiadomość (A)	
message authentication	authentification d'un message	uwierzytelnianie wiadomości (N)	PN-I-02000
message authentication code (MAC)	un MAC, un code d'authentification	kod uwierzytelnienia wiadomości (N), kod uwierzytelniający wiadomość (N), MAC (O)	PN-I-02000
message digest	un "digest"	skrót wiadomości	
message recovery		odtwarzanie wiadomości	
mode of operation	mode d'opération	tryb działania (N), tryb pracy (A)	PN-I-02000
modular arithmetic	arithmétique modulaire	arytmetyka modularna (A), arytmetyka modulo (A)	
modulus	un modulus	moduł (N)	
monoalphabetic cipher	chiffre monoalphabétique	szyfr monoalfabetyczny (A)	
multilevel security			
multiparty computation	calcul réparti (sur des données confidentielles)		
multiple encipherment	surchiffrement	wielokrotne szyfrowanie	
mutual authentication	authentification mutuelle	uwierzytelnienie wzajemne (A)	

-- N --

nonce	violeur		
nonlinearity		nieliniowość	
non-malleability		niedeformowalność	
non-repudiation	non-répudiation	niezaprzeczalność (N)	PN-I-02000
notary	notaire	notariusz (A)	
National Security Agency (NSA)	la NSA	Narodowa Agencja Bezpieczeństwa (A)	No Such Agency, Never Say Anything, Notre Sale Agence (Fr.) :-)
Number Field Sieve (NFS)	le crible algébrique	sito ciał liczbowych (A)	
number theory	la théorie des nombres	teoria liczb (A)	

-- O --

object identifier		identyfikator obiektu	
oblivious transfer	transfert équivoque		
output feedback (OFB)	rétroaction de la sortie, mode OFB	sprzężenie zwrotne z wyjścia (A), wyjściowe sprzężenie zwrotne (N, R)	
one-time pad	le masque jetable, le "one-time-pad"	szyfr z kluczem jednorazowym (A)	
one-way function	fonction à sens unique	funkcja jednokierunkowa (N)	PN-I-02000
on-line password guessing attack		odgadywanie haseł na bieżąco (A)	

-- P --

packet filter			
pad		dopełniać (A)	
padding	ajout de bits	dopełnienie (A)	
password	mot de passe	hasło (N)	PN-I-02000
PCMCIA card, PC card		karta PCMCIA (A)	
Privacy Enhanced Mail (PEM)		bezpieczna poczta elektroniczna (A)	
perfect nonlinear function		funkcja doskonale nieliniowa	
perfect secrecy	la sécurité parfaite	poufność doskonała (A)	
permutation	permutation, bijection	permutacja (A)	
Personal Identification Number (PIN)	le PIN	osobisty numer identyfikacyjny (N), personalny identyfikacyjny numer (R)	PN-I-02000
Public Key Infrastructure (PKI)		infrastruktura kryptografii klucza publicznego	
plaintext	texte clair	tekst jawny (N), tekst otwarty	PN-I-02000
plaintext aware encryption		szyfrowanie wymagające znajomości tekstu jawnego	
policy	politique	polityka (N)	
polyalphabetic cipher	chiffrement polyalphabétique	szyfr polialfabetyczny (A)	
polynomial security		bezpieczeństwo wielomianowe	
preimage resistance		odporność na wyznaczenie przeciwobrazu	
2nd preimage resistance		odporność na wyznaczenie drugiego przeciwobrazu	
primality test	test de primalité	test pierwszości (A)	
prime (number)	un (nombre) premier	liczba pierwsza (A)	
privacy	confidentialité	prywatność (N)	PN-I-02000
private key	clef privée	klucz prywatny (N)	
proactive cryptography		kryptografia proaktywna	
probabilistic encryption	chiffrement probabiliste	szyfrowanie probabilistyczne	
product cipher		szyfr kaskadowy szyfr złożeniowy	
propagation criterion		kryterium propagacji	
proprietary cipher	chiffre propriétaire	szyfr firmowy	
protection profile		profil zabezpieczeń (N)	PN-ISO/IEC 15408
provably secure	prouvablement sûr	udowadnialnie bezpieczny (A)	
prover	prouveur	udowadniający (A)	
pseudoprime (number)		liczba pseudopierwsza	
pseudorandom	pseudo-aléatoire	pseudolosowy (A)	
pseudorandom bit generator		pseudolosowy generator ciągów binarnych	

English	Français	Polski	Uwagi
pseudorandom function generator		pseudolosowy generator funkcji	
pseudorandom invertible permutation generator		pseudolosowy, odwracalny generator permutacji	
public key	clef publique	klucz publiczny (N)	
public key cryptography	cryptographie à clef publique	kryptografia z kluczem publicznym (N), kryptografia publicznego klucza (A)	PN-I-02000
public key cryptosystem	cryptosystème à clef publique	kryptosystem klucza publicznego (A)	
pure cipher			

-- Q --

quadratic sieve	crible quadratique	sito kwadratowe (A)	
quantum computer	ordinateur quantique	komputer kwantowy (A)	
quantum cryptography	cryptographie quantique	kryptografia kwantowa (A)	

-- R --

random	aléatoire	losowy (A)	
random number		liczba losowa	
randomizer			
redundancy	redondance	nadmiarowość (A), redundancja (R)	
reference monitor			
reflection attack		atak metodą odbicia lustrzanego (N), atak lustrzany	
registration authority	registre d'utilisateurs	organ ds. rejestracji użytkowników, urząd ds. rejestracji użytkowników	
related key attack	attaque avec des clefs (re)liés	atak kluczami pokrewnymi (A)	
remotely keyed encryption		szyfrowanie z kluczem zdalnym	
replay		powtórzenie	
replay attack	attaque à répétition	atak metodą powtórzenia (N), atak powtórzeniowy (A)	
resiliency		zrównoważenie wyższego rzędu	
reverse certificate		certyfikat przychodzący, certyfikat zwrotny	
reverse engineering	désassemblage		
revocation	révocation	unieważnienie (A)	
risk analysis	analyse des risques	analiza ryzyka (N)	PN-I-02000
root certification authority	autorité centrale de certification	główny organ certyfikujący, główny urząd ds. certyfikacji główny urząd ds. certyfikatów, główny urząd certyfikujący	
round function	fonction d'une tour / d'un "round"	funkcja rundy	

-- S --

*-property		własność gwiazdy (N), *-własność (N),	PN-I-02000 (model Bella – LaPaduli)

salt	sel		
secure application module (SAM)		moduł bezpieczeństwa aplikacji	
substitution box (S-box)	boîte S	S-box (O), skrzynka podstawieniowa (A)	
secrecy	confidentialité	tajność	
secret key	le clef secrète	klucz tajny (N)	
secret sharing	le partage de secret	dzielenie sekretu (A)	
secure envelope		koperta zabezpieczająca	
secure messaging		bezpieczna wymiana wiadomości	
security	sécurité, sûreté	bezpieczeństwo (A), zabezpieczenie (A)	
security domain			
security enforcing function		funkcja realizująca zabezpieczenia, funkcja zabezpieczająca	
security layer	une couche de sécurité	warstwa zabezpieczeń (A)	
security mechanism	un mécanisme de sécurité	mechanizm zabezpieczenia (N)	
security module (SM)		moduł bezpieczeństwa (N)	PN-I-02000
security policy	politique de sécurité	polityka bezpieczeństwa (N), polityka zabezpieczenia (A), polityka zabezpieczeń (A)	PN-I-02000
security relevant function		funkcja istotna dla zabezpieczenia	
security service	service de protection des données	usługa zabezpieczenia (N), usługa ochrony informacji (A)	
security target		dokument wymagań zabezpieczenia, zadanie zabezpieczeń (N)	PN-ISO/IEC 15408
seed	germe	ziarno	
selective forgery		selektywne fałszerstwo	
self certificate		autocertyfikat	
semantic security	sécurité sémantique	bezpieczeństwo semantyczne	
semi-bent function			
sender	l'expéditeur	nadawca (A)	
session key	le clef de session	klucz sesyjny (A)	
sequence number		numer kolejny (N)	PN-ISO/IEC 9798-2
shadow			
shortcut attack		atak na skróty	
signature	signature	podpis (A)	
signature scheme	un schéma de signature	schemat podpisu (N)	
signature verification	vérification de la signature	weryfikacja podpisu (A)	
signed data		podpisane dane	
signing	signature	podpisywanie (A)	
simple security property		podstawowa własność bezpieczeństwa	Bell – LaPadula
single sign on			
small subgroup attack		atak przez wprowadzenie do małej podgrupy	
smart card	la carte à puce, la carte à microprocesseur	karta inteligentna (A), karta elektroniczna (N)	programowalna, patrz "wired logic card"
sniffing			
snooping			
software	logiciel	oprogramowanie (A)	
substitution permutation network (SPN)		sieć podstawieniowo-przestawieniowa (A)	
spice			
spoof		zwieść (A)	
spread spectrum		rozszerzone widmo	

English	Français	Polski	Uwagi
standard	norme	norma (N)	
stand-alone		wolnostojący (A)	
steganography, disappearing cryptography, information hiding, obfuscation techniques	steganographie	steganografia	
stream cipher	chiffrement par flots	szyfr strumieniowy (A)	
strict avalanche criterion (SAC)	le SAC (critère d'avalanche strict)	kryterium silnej lawinowości	
strong authentication		silne uwierzytelnienie (A)	
strong primes		silne liczby pierwsze (A)	
subliminal channel	canal subliminal	kanał podprogowy (A)	
substitution	substitution	podstawienie (A)	
symmetric cryptography, classical cryptography	cryptographie symétrique, cryptographie classique	kryptografia symetryczna (A)	
system security officer		inspektor zabezpieczenia systemu (N)	PN-I-02000

-- T --

tamper evident	facile à pénétrer	ujawniający penetrację	
tamper proof	difficile à pénétrer	odporny na penetrację	
tamper resistant	protégé contre la pénétration	zabezpieczony przed penetracją	
target of evaluation		przedmiot oceny (N)	PN-I-02000, PN-ISO/IEC 15408
threat		zagrożenie (N)	PN-I-02000, PN-ISO/IEC 15408
threshold encryption			
threshold scheme	un schéma à seuil	schemat progowy (A)	
ticket	billet, ticket	bilet (N)	
ticket-granting ticket (TGT)			
timestamp	l'empreinte d'horodatage	znacznik czasu (N)	PN-ISO/IEC 9798-2
timestamping (digital)	horodatage	znakowanie czasem, elektroniczne oznaczanie czasu, elektroniczne datowanie	
time variant parameter		parametr zmienny w czasie (N)	PN-ISO/IEC 9798-2
timing attack	attaque sur le temps	analiza czasowa (N)	
token	jeton, "token"	token (N), przekaz, żeton, komunikat	PN-I-02000
traffic analysis	analyse du trafic	analiza strumienia ruchu (N)	
trapdoor function	fonction trappe, fonction à brèche secrète	funkcja z zapadką (A), funkcja pułapkowa (N, R)	
trapdoor one-way function	fonction trappe à sens unique	funkcja jednokierunkowa z zapadką (A), funkcja jednokierunkowa pułapkowa (N)	
Trojan horse	cheval de Troie	koń trojański (N)	
truncated differential			
Trusted Computing Base (TCB)		wiarygodna baza obliczeniowa (N), wiarygodna platforma obliczeniowa	PN-I-02000
trusted channel		kanał wiarygodny (N), bezpieczny kanał	PN-I-02000, PN-ISO/IEC 15408

trusted path		wiarygodna ścieżka (N), bezpieczna ścieżka	PN-I-02000, PN-ISO/IEC 15408
trusted third party (TTP)	le tiers de confiance	zaufana trzecia strona (N)	PN-I-02000, PN-ISO/IEC 9798

-- U --

unapproximable predicate		nieaproksymowalny predykat	
undeniable signature	signature incontestable	niezaprzeczalny podpis cyfrowy	
unicity distance		odległość do jednoznacznego rozwiązania	
uniqueness/timeliness		niepowtarzalność/aktualność	PN-ISO/IEC 9798
unilateral authentication		jednostronne uwierzytelnienie (N)	PN-ISO/IEC 9798
universal forgery		fałszerstwo uniwersalne	
universal one-way hash function (UOWHF)		uniwersalna, jednokierunkowa funkcja skrótu	
unpredictable	imprévisible	nieprzewidywalny (A)	
unconditional security	sécurité inconditionnelle	bezwarunkowe bezpieczeństwo (A)	

-- V --

verifier	vérifieur	weryfikator (N), podmiot weryfikujący (N)	PN-ISO/IEC 9798
virus	virus (informatique)	wirus (N)	
visual cryptography			
Virtual Private Network (VPN)		wirtualna sieć prywatna	
vulnerability		podatność (N)	PN-I-02000

-- W --

weak key	une clef faible	słaby klucz (A)	
web browser		przeglądarka (A)	
white noise	bruit blanc	biały szum	
wired logic card	carte à mémoire, carte à logique câblée	karta pamięciowa	nieprogramowalna (patrz smart card)
wiretap		urządzenie do podsłuchu łączy	
wiretapping	les écoutes	podsłuchiwanie łączy (A)	
witness		poświadczenie (N)	PN-I-02000, PN-ISO/IEC 9798-5
work factor	le facteur de travail		
workstation	la station de travail	stacja robocza (A)	
worm	un ver	robak (N)	
World Wide Web (WWW)		WWW (O), Wielka Wszechświatowa Wioska	

-- Z --

zero-knowledge proof/protocol (ZKP)	un protocole/preuve à divulgation nulle, sans divulgation, "Zero Knowledge"	protokoły / dowody wiedzy zerowej (A)	

English	Français	Polski	Uwagi

Dziękujemy dr inż. Włodzimierzowi Chocianowiczowi z firmy FILSYS i z Politechniki Szczecińskiej za zgłoszone propozycje, uwagi i sugestie.

Dziękujemy panu Krzysztofowi Maćkowiakowi z Wydziału Informatyki i Zarządzania Politechniki Poznańskiej za duży wkład w rozszerzenie listy akronimów.

Autorzy zachęcają do zgłaszania uwag dotyczących obecnej wersji słowniczka oraz do nadsyłania propozycji nowych terminów i ich tłumaczeń. Uwagi prosimy kierować:

- listownie na adres: *ENIGMA Systemy Ochrony Informacji Sp. z o.o.*
  ul. Cietrzewia 8
  02-492 Warszawa

  z dopiskiem „SŁOWNICZEK”
- pocztą elektroniczną na adres: *slownik@enigma.com.pl*
- faksem na numer: *(22) 863 62 65 w. 25*

Nowe wersje słowniczka dostępne będą w sieci Internet pod adresem *http://www.enigma.com.pl*.

Autorzy zezwalają na nieograniczone rozpowszechnianie słowniczka (w formie elektronicznej lub papierowej) pod warunkiem zachowania jego integralności (w tym informacji o autorach i firmie).

Autorzy nie ponoszą odpowiedzialności za ew. błędy, nieścisłości i braki w treści słowniczka.

Lista akronimów

AAA	Authentication, Authorization, Accounting
AC	Access Condition
ACC	Access Control Center
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
ANSI	American National Standards Institute
API	Application Programming Interface
ARL	Authority Revocation List
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
AVA	Attribute Value Assertion
BAA	Best Affine Approximation
BAN	Burrows, Abadi, Needham
BBS	Blum Blum Shub
BCA	Brand Certificate Authority
BCI	Brand CRL Identifier
BER	Basic Encoding Rules
BGP	Border Gateway Protocol
CA	Certification Authority
CAPI	Cryptography API
CAW	Certification Authority Workstation
CBAC	Content Based Access Control
CBC	Cipher Block Chaining
CC	Common Criteria
CCA	Chosen Ciphertext Attack
CCA2	Chosen Ciphertext Adaptive Attack
CDH	Computational Diffie Hellman (Problem)
CDMF	Commercial Data Masking Facility
CDSA	Common Data Security Architecture
CER	Canonical Encoding Rules,
CERT	Computer Emergency Response Team
CESG	Communications and Electronics Security Group
CET	Cisco Encryption Technology
CFB	Cipher Feed Back
CFSR	Carry Feedback Shift Register
CHAP	Challenge Handshake Protocol
CIAC	Computer Incident Advisory Capability
CIK	Cryptographic Ignition Key
CIPSO	Common IP Security Option
CKL	Compromised Key List
CMS	Cryptographic Message Syntax
COMSEC	Communication Security
COPS	Common Open Policy Service
CPA	Chosen Plaintext Attack
CPS	Certification Practice Statement
CRAM	Challenge Response Authentication Mechanism
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CRT	Chinese Remainder Theorem
CSE	Communications Security Establishment
CSIRT	Computer Security Incident Response Team
CSOR	Computer Security Objects Register
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAC	Data Authentication Code

DAC	Discretionary Access Control
DASS	Distributed Authentication Security Service
DC	Differential Cryptanalysis
DCE	Distributed Computing Environment
DDH	Decisional Diffie Hellman (Problem)
DEA	Data Encryption Algorithm
DEK	Data Encrypting Key
DEM	Data Encapsulation Mechanism
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DII	Defense Information Infrastructure
DMS	Defence Messaging System
DN	Distinguished Name
DNS	Domain Name System
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptosystem
ECC	Error Correcting Code
ECDSA	Elliptic Curve DSA
EDI	Electronic Document Interchange
EE	End Entity
EES	Escrowed Encryption Standard
EMSEC	Emanations Security
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident ReSponse Teams
FPKI	Federal Public Key Infrastructure
FTP	File Transfer Protocol
GCA	Geopolitical Certificate Authority
GISA (BSI)	German Information Security Agency (Bundesamt fur Sicherheit Informationtechnik)
GMITS	Guidelines for the Management of Information Technology Security
GRE	Generic Routing Encapsulation
GSS	Generic Security Services
GULS	Generic Upper Layer Security
HEART	Hybrid Encryption, Authentication and nonRepudiation Transcoder
HMAC	Keyed Hashing Message Authentication Code
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
IACR	International Association for Cryptologic Research
ICMP	Internet Control Message Protocol
ICRL	Indirect Certificate Revocation List
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Integer Factorization
IGMP	Internet Gateway Message Protocol
IKE	Internet Key Exchange

English	Français	Polski	Uwagi

IKMP	Internet Key Management Protocol
IMAP4	Internet Message Access Protocol, version 4
IP	Internet Protocol
IPRA	Internet Policy Registration Authority
IPSEC	Internet Protocol Security
IPSO	Internet Protocol Security Option
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
IV	Initialization Value
KDC	Key Distribution Centre
KEA	Key Exchange Algorithm
KEK	Key Encrypting Key
KEM	Key Encapsulation Mechanism
KMID	Key Material Identifier
KMP	Key Management Protocol
KRA	Key Recovery Alliance
KTC	Key Translation Centre
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LC	Linear Cryptoanalysis
LDAP	Lightweight Directory Access Protocol
LEAF	Law Enforcement Access Field
LFSR	Linear Feedback Shift Register
MAC	Mandatory Access Control
MAC	Message Authentication Code
MD	Message Digest
MDC	Modification Detection Check
MHS	Message Handling System
MIME	Multipurpose Internet Message Extensions
MISPC	Minimum Interoperability Specification for PKI Components
MISSI	Multilevel Information System Security Initiative
MLS	Multilevel Secure
MOSS	MIME Object Security Services
MSP	Message Security Protocol
NAT	Network Address Translation
NCSC	National Computer Security Center
NFS	Number Field Sieve
NIAP	National Information Assurance Partnership
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NNTP	Network News Transport Protocol
NSA	National Security Agency
NTP	Network Time Protocol
OAEP	Optimal Asymmetric Encryption Padding,
OCSP	Online Certificate Status Protocol
OFB	Output Feed Back
OID	Object Identifier
OPSEC	Operations Security
ORA	Organizational Registration Authority

OTP	One Time Password
PAA	Policy Approving Authority
PAP	Password Authentication Protocol
PER	Packed Encoding Rules
PC	Propagation Criterion
PCA	Policy Creation Authority
PCI	Protocol Control Information
PCMCIA	Personal Computer Memory Card International Association
PEM	Privacy Enhanced Mail
PFS	Public key Forward Secrecy
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PIX	Private Internet Exchange
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PMA	Policy Management Authority
POP	Proof Of Possession
POP3	Post Office Protocol, version 3
PP	Protection Profile
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role Based Access Control
RC2	Rivest Cipher #2
RDN	Relative Distinguished Name
RIP	Routing Information Protocol
RSA	Rivest, Shamir, Adleman
SA	Security Architecture
SAC	Strict Avalanche Criterion
SAID	Security Association Identifier
SAM	Secure Application Module
SAM	Security Access Module
SASL	Simple Authentication and Security Layer
SCA	Subordinate Certification Authority
SDE	Secure Data Exchange
SDNS	Secure Data Network System
SEPP	Secure Electronic Payment Protocol,
SET	Secure Electronic Transactions
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
S-HTTP	Secure Hypertext Transfer Protocol
SILS	Standards for Interoperable LAN/MAN Security
SKEMI	Secure Key Exchange Mechanism for Internet
SKIP	Simple Key-management for Internet Protocols
SLIP	Serial Line Internet Protocol
SMI	Security Management Infrastructure
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCKS	Socket Security
SP3	Security Protocol 3

SPI	Security Parameters Index
SPN	Substitution Permutation Network
SSCD	Secure Signature Creation Device
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On
SSO	System Security Officer
ST	Security Target
STANAG	Standardization Agreement
STT	Secure Transaction Technology,
TACACS	Terminal Access Controller Access Control System
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TELNET	Telecommunications Network Protocol
TEMPEST	Transient Electromagnetic Pulse Emanation Standard Transient Electromagnetic Pulse Emanation
	Surveillance Technology
TESS	The Exponential Encryption System
TGT	Ticket Granting Ticket
TLS	Transaction Layer Security
TLV	Tag-Length-Value
TSIG	Trusted Systems Interoperability Group
TTP	Trusted Third Party
UDP	User Datagram Protocol
UOWHF	Universal One Way Hash Function
URI	Uniform Resource Identifier
URL	Universal Resource Locator
URN	Uniform Resource Name
VPDN	Virtual Private Dial-Up Networks
VPN	Virtual Private Network
WWW	World Wide Web
XER	XML Encoding Rules,
ZKP	Zero Knowledge Proof / Protocol

English	Français	Polski	Uwagi

Historia wersji
10 listopada 2003

- dodano nowe akronimy nadesłane przez p. Krzysztofa Maćkowiaka
- wskazano (niektóre) polskie tłumaczenia występujące w Polskich Normach
- dodano hiperłącza do każdej litery