Глоссарий криптографических терминов

Англо-русский словарь по криптографии

(из книги "Прикладная криптография" Б. Шнайера)

Английский термин	Рекомендуемый русский перевод	Может быть, более правильный по смыслу / написанию, но не общепринятый / слишком длинный	Неправильный перевод/калька
A			
adjudicator	арбитр		
algorithm	алгоритм		
asymmetric	асимметричный		
block	блочный		
continued fraction	непрерывных дробей		
extended Euclidian	расширенный алгоритм Евклида		
factoring	разложения на множители, факторизации		
general number field sieve	[общего] решета числового поля		решето поля чисел
knapsack	1. ранцевый 2. укладки ранца (рюкзака)	1. на основе задачи об укладке ранца	
linear syndrome	линейного синдрома		
polynomial	полиномиальный		
Pollard's	Полларда		
public-key	с открытым ключом		с открытыми ключами
quadratic sieve	квадратичного решета		
secret-sharing	разделения секрета		
secure multiparty computation	тайных многосторонних вычислений		
stream cipher	потокового (поточного) шифрования		
superpolynimial	сверхполиномиальный		
symmetric	симметричный		

arbitrator	посредник		
attack	атака		вскрытие
adaptive-chosen ...	на основе адаптивно подобранных ...		
best affine approximation	на основе лучшего афинного приближения		
block replay	повтора блока		
birthday	"дней рождений"	на основе парадокса "дней рождений"	
brute-force	лобовая, "в лоб"		грубой силой
chosen- ...	на основе подобранных ...		
ciphertext-only	на основе шифртекста		
common-modulus	при использовании общих модулей		
correlation	корреляционная		
dictionary	по словарю		
derived sequence	на основе выводимой последовательности		
exhaustive search	полным перебором		
insertion	вставкой		
low decryption exponent	раскрытие малого открытого показателя		
low encryption exponent	раскрытие малого закрытого (секретного) показателя		
known-plaintext	на основе открытого текста		по известному открытому тексту
man-in-the-middle	"человек посередине"		
meet-in-the-middle	"встреча посередине"		
replay	с повторной передачей		
resend	с повторной отсылкой		
authentication	аутентификация, проверка подлинности		
avalanche effect	лавинный эффект		
B			
bias	смещение		
blinding factor	маскирующий множитель		
blob	блоб		капля
block replay	повтор блока		

Blum integers	числа Блюма		
C			
certification authority	орган сертификации		
cipher	шифр		код
block	блочный		
homophonic	омофонический		
monoalphabetic	моноалфавитный, одноалфавитный		
polyalphabetic	полиалфавитный, многоалфавтный		
poligram	полиграммный		
product	составной		
stream	потоковый		
substitution	подстановочный, подстановки		
transposition	перестановочный, перестановки		
Vigenere	Виженера		
ciphertext	шифртекст, зашифрованный текст, шифрограмма	шифротекст	шифрованный текст
stealing	похищение шифртекста		
cleartext	открытый текст		
clock	такт (в регистрах сдвига)		
clocking	тактирование		
characteristic	характеристика (в ДКА)		
code	код		шифр
collision	коллизия		конфликт, столкновение
complementation	комлементарность, дополнение		
compromise	компрометировать		
compromised	скомпрометированный		
confusion	перемешивание		путаница
congruent	сравнимый с		конгруэнтный
congruence	сравнимость		
connection integer	число обратной связи		
correlation immunity	корреляционная стойкость		
cryptanalysis	криптоанализ		
differential	дифференциальный		

linear	линейный		
related-key	на основе связанных ключей		
cryptanalyst	криптоаналитик, дешифровальщик		
cryptographer	криптограф		
cryptography	криптография		
asymmetric	ассиметричная		
multiple-key public-key	с несколькими открытыми ключами		
public key	с открытым ключом		с открытими ключами
cryptology	криптология		
cryptosystem	криптосистема		
fair	"законная"		
hybrid	гибридная, смешанная		
identity-based	личностная		
"cut-and-choose"	"разделяй и выбирай"		
D			
decrypt	расшифровать		дешифровать, раскриптовать, раскодировать
decryption	расшифрование, расшифровка		дешифрование
digital cash	электронные деньги		электронная наличность
diffusion	рассеивание		диффузия
disavow	дезавуировать; отказаться		
discrete logarithm	дискретный логарифм		
divide-and-conquer	"разделяй и властвуй"		
E			
elliptic curve	эллиптическая кривая		
cryptosystem	криптосистема на эллиптических кривых		
encoding	закодировать, кодировать		
encrypt	зашифровать, шифровать (только если понятно из контекста)		закриптовать, закодировать
encryption	зашифрование, шифрование		шифровка
link-by-link	канальное		
end-to-end	оконечное, абонентское		

probabilistic	вероятностное		
error	ошибка		
propagation	распространение ошибки		
entity	сущность; объект		
escrow	депонирование		
F			
factorization	разложение на множители, факторизация		
failsafe	отказоустойчивый		
feedback with carry shift register (FCSR)	регистр сдвига с обратной связью по переносу (РСОСП)		
fingerprint	цифровой отечаток		отпечаток пальца
finite field	конечное поле		
function	функция		
compression	сжимающая		
Euler totient function	Эйлера		
bent	бент-		
G			
Galois field	поле Галуа		
generator	1. генератор 2. образующая		
additive	аддитивный		
alternating	чередующийся		
bilateral stop-and-go	двусторонный "старт-стоп"		
clock-controlled	с управлением тактированием, с неравномерным движением		
combination	комбинирующий		
filter	фильтрующий		
keystream	гаммы		
linear congruental	линейный конгруэнтный		
multispeed inner-product	многоскоростной скалярного произведения		
self-decimated	самопрореживающий		
shrinking	сжимающий		
stop-and-go	"старт-стоп"		
threshold	пороговый		
graph isomorphism	изоморфизм графов		

greatest common divisor (gcd)	наибольший общий делитель (НОД)		
H			
Hamiltonian cycle	Гамильтонов цикл		
hash	хэш		
function	-функция		
value	-значение, свертка		
one-way	однонаправленная	вычислимая в одну сторону	
trapdoor	с потайным входом, с лазейкой; ключевая		с люком
I			
increment	инкремент, приращение		
identification	идентификация		
identity	личность		
initialization vector	вектор инициализации, синхропосылка		
index calculus			
index of coincidence	индекс совпадений		
integrity	целостность		
interleave	чередование		
irreducible	неприводимый (многочлен)		
K			
key	ключ		пароль
backup	резервная копия		
complement	комплементарный	обладающий свойством дополнительности	
distribution	распределение		
dereferencing	разыменование		
escrow	депонирование		условное вручениие
exchange	обмен		
expansion	расширение		
generating	генерация		
lifetime	время жизни		
management	управление		распределение
master key	главный ключ		
	переговоры о согласовании		

negotiation	ключа		
revocation	отзыв		
scheduling	развертка, расширение		
semiweak	полуслабый		
session	сеансовый		сессионный
verification	проверка		
weak	слабый		
key certification authority	орган сертификации ключей		
key distribution center	центр распределения ключей		
key-encryption key	ключ шифрования ключей		
keyspace	пространство ключей		
flat	плоское		
nonlinear	нелинейное		
reduced	сокращенное		
keystream	гамма [шифра]		поток ключей
L			
leakage	утечка		
least common multiple, lcm	наименьшее общее кратное, НОК		
linear complexity profile	профиль линейной сложности		
linear consistency	линейная согласованность		
linear feedback shift register	регистр сдвига с линейной обратной связью (РСЛОС)		
M			
message authentication code (MAC)	код аутентификации сообщения; имитовставка		
mode	режим [шифра]		
block chaining (BC)	сцепления блоков		
cipher block chaining (CBC)	сцепления блоков шифртекста		
cipher block chaining with checksum (CBCC)	сцепления блоков шифртекста с контрольной суммой		
cipher-feedback (CFB)	с обратной связью по шифртексту; гаммирования с обратной связью		
counter	счетчика		

electronic codebook (ECB)	электронной кодовой книги; простой замены		
output-feedback (OFB)	с обратной связью по выходу		
output feedback with a nonlinear function (OFBNLF)	с нелинейной обратной связью по выходу		
plaintext block chaining (PBC)	сцепления блоков открытого текста		
plaintext feedback (PFB)	с обратной связью по открытому тексту		
propagating cipher block chaining (PCBC)	сцепления блоков шифртекста с распространением ошибки		
modular	модулярная, по модулю		модульная
arithmetic	арифметика		
exponentiation	возведение в степень		
reduction	приведение по модулю		
modulo	модуль		
multiple-key public-key cryptography	криптография с несколькими открытыми ключами		
N			
nonce	случайное число (в протоколах)		
nonrepudiation	неотрицаемость		
nonresidue	невычет		
number	число		
2-adic	2-адическое		
composite	составное		
Fibonacci	Фибоначчи		
Lucas	Лукаса		
magic	магическое		
prime	простое		
relatively prime	взаимно простое		
strong prime	сильное простое		
theory	теория чисел		
O			
one-time pad	одноразовый блокнот		
one-way accumulator	однонаправленный сумматор		
P			

padding	заполнение, дополнение (блока байтами)		
pass phrase	парольная фраза		
permutation	перестановка		пермутация
plaintext	открытый текст		
polynomial	1. многочлен, полином 2. полиномиальный		
dence	плотный		
irreducible	неприводимый		
primitive	примитивный		
sparse	разреженный		
pre-image	прообраз		
primitive	1. примитив 2. примитивный корень [по модулю]		
privacy	[право на] личную жизнь; конфиденциальность		
problem	задача		
graph isomorphism	об изоморфизме графов		
hard	трудная, труднорешаемая		
intractable	труднорешаемая		
knapsack	об укладке ранца (рюкзака)		о рюкзаке
NP-complete	NP-полная		
three-satisfiability	3-выполнимости		
tractable	разрешимая		
[Boolean formula] satisfiability	о выполнимости [булевой формулы]		
undecidable	неразрешимая		
protocol	протокол		
adjudicated	с арбитром		
all-or-nothing disclosure of secrets	раскрытия секретов "все или ничего"		
anonymous message broadcast	анонимной [широковещательной] передачи сообщения		
arbitrated	с посредником		с арбитром
bit commitment	вручения бита на хранение	залог секретного бита	предъявление бита
digital cash	цифровых денег		

digital certified mail	заказной электронной почты		
[fair] coin flipping	подбрасывания монеты ["по телефону"]		
disavowal	отрицания, дезавуирования		
interactive	интерактивный, диалоговый		
interlock	взаимоблокировки		
mental poker	мысленного покера		
minimum-disclosure proofs	доказательства с минимальным разглашением		
oblivious transfer	передача с забыванием		
secret sharing	разделения секрета		
secret splitting	разбиения секрета		
secure circuit evaluation	тайного вычислени схемы		
secure elections	тайного голосования		
secure multiparty computation	тайных коллективных вычислений		
self-enforcing	самодостаточные		
simultaneous contract signing	одновременного подписани контракта		
simultaneous exchange of secrets	одновременного обмена секретами		
wide-mouth frog	не переводится, дословно "лягушка с широко открытым ртом"		
zero-knowledge proof	доказательства с нулевым разглашением		
pseudo-hadamard transform (PHT)	псевдоадамарово преобразование		
pseudo-random	псевдослучайная		
-sequence	последовательность		
-sequence genetaror	генератор псевдослучайной последовательности (гаммы)		
R			
rate (of the language)	энтропия языка		
rate (of the cipher)	скорость (шифра)		
residue	вычет		остаток
complete set of	полная система вычетов		
quadratic	квадратичный		

reduced set of	приведенная система вычетов		
round	раунд; основной шаг		
S			
salt	привязка; синхропосылка		соль
S-box	S-блок; узел замены		
secrecy	секретность, стойкость		
ideal	идеальная секретность		
perfect	совершенная секретность		
secure	стойкий, надежный (о шифре); безопасный, защищенный; тайный (о голосовании); секретный		
seed	начальное значение; синхропосылка	число для инициализации ГПСП	зерно, затравка
shadow, share	доля (в пороговых схемах)		
signature	подпись		
blind	"вслепую"		слепая
completely blind	совершенно слепая		
convertible undeniable	преобразумая неоспоримая		
designated confirmer	подтверждаемая доверенным лицом		
entrusted undeniable	доверительная неоспоримая		
digital	[электронная] цифровая (ЭЦП)		
fail-stop	с обнаружением подделки		
group	групповая		
multiple	многократная		
oblivious	с забыванием		рассеяная
proxy	по доверенности		
subliminal-free	свободная от скрытого канала		
undeniable	неоспоримая		неотрицаемая
strong	стойкий		
subliminal [channel]	скрытый [канал]		подсознательный
symbol			
Legendre	символ Лежандра		

Jacobi	символ Якоби		
T			
tap	отвод, точка съема		
theorem	теорема		
Fermat's little	малая теорема Ферма		
Chinese remainder	китайская теорема об остатках		
ticket	мандат (в Kerberos)		
U			
uncertainty	неопределенность		
unicity distance	расстояние единственности		расстояние уникальности
unpredictable	непредсказуемый		
W			
whitening	отбеливание	забеливание (?)	
witness	свидетельство (в алгоритмах проверки на простоту)		
Z			
zero-knowledge	нулевое разглашение		нулевое знание