**ГЛОССАРИЙ**

**AES (***Advanced* *Encryption* *Standard***) –** *Алгоритм* шифрования, действующий в качестве государственного стандарта в области шифрования данных в США с 2001 года. В основу стандарта положен *шифр* *Rijndael*. *Шифр* *Rijndael*/*AES* (то есть рекомендуемый стандартом) характеризуется размером блока 128 *бит*, длиной ключа 128, 192 или 256 *бит* и количеством раундов 10, 12 или 14 в зависимости от длины ключа. Основу *Rijndael* составляют так называемые линейно-подстановочные преобразования. В алгоритме широко используются табличные вычисления, причем все необходимые таблицы задаются константно, т.е. не зависят ни от ключа, ни от данных.

**Ciphertext** – зашифрованное сообщение (закрытый текст, криптограмма).

**CTR** – режим работы блочного шифра, который позволяет генерировать ключи при поточном шифрования информации.

**Deciphering** – *расшифрование*.

**DES (Data Encryption Standard) –** *Алгоритм* шифрования, действовавший в качестве государственного стандарта в области шифрования данных в США с 1977 по 2001 годы. Основные параметры *DES*: размер блока 64 бита, *длина ключа* 56 *бит*, количество раундов – 16. *DES* является классической сетью Фейштеля с двумя ветвями. *Алгоритм* преобразует за несколько раундов 64-битный *входной* *блок данных* в 64-битный выходной блок. Стандарт *DES* построен на комбинированном использовании перестановки, замены и гаммирования.

**DSS** (*Digital Signature Standard*) – стандарт США на цифровую подпись. В основе стандарта лежит *алгоритм*, называемый *DSA* (*Digital Signature Algorithm*) и являющийся вариацией подписи Эль-Гамаля.

**Enciphering –** преобразование открытого текста в криптограмму (зашифрование).

**Нash function** – хеш-*функция*.

**LFSR**(*linear* *feedback* *shift register* ) – линейный *сдвиговый регистр* с обратной связью.

**OFB** – режим работы блочного шифра, который позволяет генерировать ключи при поточном шифрования информации.

**Рlaintext** – исходное сообщение или *открытый текст*.

**Stream cipher** – *поточный шифр*.

**Абсолютная норма языка** – максимальное количество *бит* информации, которое может быть передано одним символом некоторого языка, при условии, что все последовательности символов в языке равновероятны.

**Активная криптографическая атака** – при такой атаке противник имеет возможность модифицировать передаваемые сообщения и даже добавлять свои сообщения.

**Алгоритм BBS** – один из методов генерации псевдослучайных чисел. Название алгоритма происходит от фамилий авторов - L. Blum, M. Blum, M. Shub. *Алгоритм* может использоваться в криптографии. Для вычислений очередного числа xn+1 по алгоритму *BBS* используется формула Описание: х_{n+1} = х_n^2 mod\ M, где Описание: M = pq является произведением двух больших простых p и q.

**Алгоритм RC4** – *алгоритм*, разработанный для генерации псевдослучайных чисел. Может использоваться для генерации ключей при поточном шифровании.

**Алгоритм RSA** – *алгоритм* шифрования с открытым ключом. Название алгоритма составлено из первых букв фамилий авторов: Р.Ривеста (R.Rivest), А.Шамира (A.Shamir) и Л.Адлемана (L.Adleman). *Алгоритм* *RSA* основан на сложности задачи факторизации больших чисел. Данный *алгоритм* является, возможно, наиболее популярным и широко применяемым *асимметричным алгоритмом* в *криптографических системах*.

**Алгоритм Диффи-Хеллмана** – *алгоритм* шифрования с открытым ключом. Этот *алгоритм* основан на трудности вычислений *дискретных логарифмов*. *Алгоритм Диффи-Хеллмана* может использоваться для *распределения ключей*, которые могут быть использованы для симметричного шифрования.

**Алгоритм Евклида** – математический *алгоритм*, который может использоваться для нахождения наибольшего общего делителя двух чисел.

**Алгоритм шифрования с открытым ключом (**или**асимметричный криптоалгоритм)** – криптографический *алгоритм*, в котором для шифрования и расшифрования используются разные ключи.

**Алгоритм Эль-Гамаля** – *алгоритм* шифрования с открытым ключом, основанный на трудности вычислений *дискретных логарифмов*. *Алгоритм* Эль-Гамаля может быть использован для шифрования данных, для формирования цифровой подписи и для согласования общего ключа. Этот *алгоритм* фактически использует схему Диффи-Хеллмана, чтобы сформировать общий *секретный ключ* для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот *ключ*.

**Алфавит** - конечное множество используемых для кодирования информации символов.

**Атака "человек-в-середине"** (англ. "man-in-the-middle") – термин в криптографии, обозначающий ситуацию, когда атакующий способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале связи.

**Взаимно простые числа** – числа, не имеющие общих делителей (кроме единицы).

**Гаммирование** – метод шифрования, основанный на "наложении" гамма-последовательности на *открытый текст*. Обычно это суммирование в каком-либо конечном *поле* (суммирование по модулю).

**Генератор псевдослучайных чисел** **(ГПСЧ)** – некоторый *алгоритм* или устройство, которые создают последовательность *бит*, внешне похожую на случайную.

**ГОСТ 28147-89** – российский стандарт на блочный *алгоритм симметричного шифрования*.

**ГОСТ Р34.10-2001** – новый российский стандарт на *алгоритм* формирования и *проверки ЭЦП*. Основан на сложности взятия дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции по ГОСТ Р34.11-94. Размер формируемой цифровой подписи – 512 *бит*.

**ГОСТ Р34.10-94** – российский стандарт на *алгоритм* формирования и *проверки ЭЦП*, действующий с 1995 года. В стандарте используется модификация схемы шифрования с открытым ключом Эль-Гамаля и *алгоритм* выработки хэш-функции по ГОСТ Р34.11-94.

**ГОСТ Р 34.11-94** – российский стандарт на функцию хеширования.

**Задача факторизации** – нахождение двух или более натуральных чисел, дающих при перемножении заданное число.

**Закрытый ключ** – *ключ*, используемый в асимметричных криптографических алгоритмах, который должен храниться в секрете.

**Избыточность** – в теории информации характеристика *помехоустойчивого кода*, показывающая, насколько увеличена *длина* кодового слова по сравнению с обычным непомехоустойчивым кодом. Для многих помехоустойчивых кодов *избыточность* можно определить как *отношение* числа контрольных разрядов к общему числу разрядов кодового слова.

**Избыточность языка** – статистическая величина, обозначающая *избыточность* информации, содержащейся в тексте на определённом языке.

**Инверсия по модулю** – такое *натуральное число*, которое при умножении по модулю на данное число дает в результате единицу.

**Инфраструктура открытых ключей** – комплекс программно-аппаратных средств, организационно-технических и административных мероприятий, обеспечивающих абонентам системы связи необходимый сервис для управления их открытыми ключами.

**Каноническое разложение на множители** – такое разложение на множители, при котором все множители являются простыми и записаны в порядке возрастания.

**Ключ** – *информация*, необходимая для шифрования и расшифрования сообщений.

**Код** – в теории информации совокупность знаков, а также система правил, позволяющая представлять информацию в виде набора таких знаков.

**Кодовое слово** – в теории информации любой ряд допустимых знаков в соответствии с используемой системой правил.

**Комбинированный (композиционный) шифр** – криптографическое *преобразование данных*, получаемое в результате комбинации нескольких подряд примененных простых шифров.

**Криптоанализ** – наука о преодолении криптографической защиты информации.

**Криптографическая система защиты информации** – система защиты информации, в которой используются криптографические методы для шифрования данных.

**Криптографический протокол** – *алгоритм* взаимодействия двух или более абонентов с использованием криптографических средств, в результате которой абоненты достигают своей цели, а их противники - не достигают.

**Криптография** – наука, изучающая построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия.

**Криптосистемы на эллиптических кривых** – *группа* алгоритмов с открытым ключом, использующих в качестве математического аппарата свойства *эллиптических кривых* на плоскости.

**Криптостойкость** – характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

**Линейный конгруэнтный генератор** псевдослучайных чисел – один из простейших ГПСЧ, который для вычисления очередного числа Описание: k_i использует формулу Описание: k_i=(a \times k_{i-1}+b) mod\ c, где Описание: а, b, с — некоторые *константы*, a Описание: k_{i-1} — предыдущее *псевдослучайное число*.

**Линейный сдвиговый регистр с обратной связью** – вариант *сдвигового регистра* с обратной связью. *Обратная связь* в таком регистре реализуется просто как сумма по модулю 2 всех (или некоторых) битов регистра.

**Малая теорема Ферма** – известная теорема, сформулированная П. Ферма, лежащая в основе алгоритма шифрования по системе *RSA*

**Метод Фибоначчи с запаздываниями** – один из методов генерации псевдослучайных чисел. Может использоваться в криптографии.

**Минимальное кодовое расстояние** – наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код.

**Наибольший общий делитель** чисел Описание: а и Описание: b – наибольшее число Описание: с, которое делит и Описание: а и Описание: b: с = **НОД**(a, b).

**Норма языка** – величина, характеризующая *количество информации*, приходящееся на один символ сообщения.

**Одноразовая лента** (или **одноразовый блокнот**, или **шифр Вернама)** – один из возможных вариантов реализации совершенно секретной системы. Может быть реализован как гаммирование с бесконечной гаммой.

**Односторонняя функция** – математическая *функция*, которую относительно легко вычислить, но трудно найти по значению функции соответствующее *значение* аргумента. То есть, зная х легко вычислить Описание: f(x), но по известному Описание: f(x) трудно найти подходящее *значение* Описание: x.

**Односторонняя функция с люком** (или **с секретом**) – это особый вид *односторонних функций*, имеющих некоторый секрет (*люк*), позволяющий относительно быстро вычислить обратное *значение* функции.

**Основная теорема арифметики** – теорема утверждающая, что любое *натуральное число* большее единицы либо само является простым, либо может быть разложено на *произведение* простых делителей, причем единственным способом (если не обращать внимания на порядок следования сомножителей).

**Открытый ключ** – *ключ*, используемый в асимметричных криптографических алгоритмах, который может не храниться в секрете.

**Пассивная криптографическая атака** – *атака*, при которой противник не имеет возможности изменять передаваемые сообщения. При *пассивной атаке* возможно лишь прослушивание передаваемых сообщений, их *дешифрование* и *анализ трафика*.

**Помехоустойчивый код** – код, позволяющий обнаруживать и корректировать ошибки при хранении и передаче сообщений.

**Поточный шифр** – *шифр*, который выполняет *шифрование* входного сообщения по одному биту (или байту) за операцию. Поточный *алгоритм* шифрования устраняет необходимость разбивать сообщение на *целое число* блоков. Поточные шифры используются для шифрования данных в реальном времени.

**Принцип Керкхоффса** – правило разработки криптографических систем, согласно которому в засекреченном виде держится *ключ шифрования*, а остальные параметры системы шифрования могут быть открыты без снижения *стойкости алгоритма*. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей. Впервые данный принцип сформулировал в XIX веке голландский криптограф Огюст Керкхоффс.

**Присоединяемые цифровые подписи** – подписи, вычисленные по хеш-коду документа. Такие цифровые подписи представляют собой некоторый числовой код, который необходимо пристыковывать к подписываемому документу. Само сообщение при этом не шифруется и передается в открытом виде вместе с цифровой подписью отправителя.

**Пропорциональные** или **монофонические** **шифры** – методы замены, в которых уравнивается частота появления зашифрованных знаков.

**Простое число** – *натуральное число*, которое не имеет делителей, кроме самого себя и единицы.

**Расстояние единственности** шифра (или **расстояния уникальности**) – величина, показывающая, сколько букв зашифрованного сообщения необходимо перехватить для однозначного восстановления ключа.

**Расстояние по Хэммингу** – в теории информации число разрядов кодовых слов, в которых они различны.

**Режим** **ECB (Electronic CodeВook) –** Один из режимов использования блочного алгоритма шифрования. Режим *ECB* (переводится как "электронная кодовая книга"**) –** это режим простой поблочной замены. В этом режиме каждый блок исходных данных шифруется независимо от остальных блоков, с применением одного и того же ключа шифрования.

**Режим CBC (Chipher Block Chaining)** – режим сцепления блоков шифра. Один из режимов использования блочного алгоритма шифрования. Преобразование в режиме *CBC* выполняется следующим образом: каждый блок открытого текста складывается по модулю 2 с результатом шифрования предыдущего блока. Таким образом, результаты шифрования предыдущих блоков влияют на *шифрование* следующих блоков.

**Сдвиговый регистр с обратной связью** состоит n-битного *сдвигового регистра* и устройства обратной связи. Когда нужно извлечь *бит*, все биты *регистра сдвигаются* вправо на одну позицию. Новый крайний слева *бит* определяется функцией обратной связи от остальных битов. Сдвиговые регистры с обратной связью могут применяться для получения потока псевдослучайных *бит*.

**Сертификат открытого ключа** – *информация*, заверенная цифровой подписью центра, и включающая *открытый ключ* и другие данные об абоненте (*идентификатор* алгоритма электронной подписи, имя удостоверяющего центра, срок годности сертификата, *имя пользователя*, которому принадлежит сертификат и др).

**Сжатие информации** – процесс преобразования исходного сообщения из одной кодовой системы в другую, в результате которого уменьшается *размер сообщения*.

**Символ** - это любой знак, в том числе буква, цифра или знак препинания.

**Симметричное шифрование (шифрование с закрытым ключом)** – методы обратимого преобразования данных, в которых используется один и тот же *ключ*, который обе стороны информационного обмена должны хранить в секрете от противника.

**Система шифрования**, или **шифрсистема**, – это любая система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.

**Совершенно секретная** **система** – *криптографическая система*, для которой *анализ* зашифрованного текста не дает никакой информации об открытом тексте, кроме, возможно, его длины.

**Соседние кодовые слова** – кодовые слова, отличающиеся значением только одного разряда.

**Составное число** – *натуральное число*, которое делится, помимо самого себя и единицы, еще хотя бы на одно число.

**Функция Эйлера** позволяет подсчитать число натуральных чисел, не превосходящих n и, взаимно простых с n**.**

**Хеш-функция** – математическая или иная *функция*, которая для строки произвольной длины вычисляет некоторое целое *значение* или некоторую другую строку фиксированной длины.

**Хеш-код** – результат работы хеш-функции, некоторый характерный "признак" входного массива данных.

**Шифр** – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

**Шифр замены (подстановки)** основан на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

**Шифр многоалфавитной замены (или подстановки)** – *группа* методов шифрования подстановкой, в которых для замены символов исходного текста используется не один, а несколько алфавитов по определенному правилу.

**Шифр** **перестановки** основаны на том, что *входной* *поток* исходного текста делится на блоки, в каждом из которых выполняется *перестановка* символов. Ключом такого шифра является используемая при шифровании перестановочная *матрица* или *вектор*, указывающий правило перестановки.

**Шифр простой (**или**одноалфавитной) замены**, **простой подстановочный шифр**, **моноалфавитный шифр** — *группа* методов шифрования, которые сводится к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква *шифртекста*. Само *шифрование* заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать *алгоритм*, по которой она генерируется.

**Шифрование с закрытым ключом (симметричное шифрование)** – методы обратимого преобразования данных, в которых используется один и тот же *ключ*, который обе стороны информационного обмена должны хранить в секрете от противника.

**Шифрование с открытым ключом (асимметричное шифрование)** – методы шифрования, в которых для шифрования и расшифрования данных используются два разных ключа. При этом один из ключей (*открытый ключ*) может передаваться по открытому (незащищенному) каналу связи. *Шифрование* с открытым ключом используется на практике лишь со второй половины ХХ века.

**Центр сертификации** – организация или подразделение организации, которая выпускает сертификаты ключей электронной цифровой подписи и отвечает за управление ключами пользователей. Открытые ключи и другая *информация* о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

**Цифровые подписи с восстановлением документа** – подписи, которые как бы содержат в себе подписываемый документ: в процессе проверки подписи автоматически вычисляется и *тело документа*. Если при расшифровывании сообщение восстановилось правильно, значит, подпись была верной.

**Электронная (цифровая) подпись** – присоединяемый к сообщению *блок данных*, полученный с использованием криптографического преобразования. *Электронная подпись* позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

**Энтропия** сообщения – характеристика, введенная Шенноном. Определяет *количество информации*, приходящейся на одно элементарное сообщение источника, вырабатывающего статистически независимые сообщения. Является мерой неопределённости или непредсказуемости информации.

### Список сокращений

|  |  |  |
| --- | --- | --- |
| AES | Advanced Encryption Standard | Усовершенствованный стандарт шифрования |
| *BBS* | Blum – Blum – Shub | Алгоритм генерации псевдослучайных чисел |
| CA | Certification authority | Центр сертификации (удостоверяющий центр) |
| *CBC* | Chipher Block Chaining | Режим сцепления блоков шифра |
| *CTR* | CounTeR | Режим счетчика |
| DES | Data Encryption Standard | Стандарт шифрования данных |
| DSS | *Digital Signature Standard* | Стандарт цифровой подписи (США) |
| *ECB* | Electronic CodeВook | Режим простой поблочной замены |
| KDC | Key Distribution Center | Центр *распределения ключей* |
| *LFSR* | Linear feedback *shift register* | Линейный *сдвиговый регистр* с обратной связью |
| *OFB* | Output FeedBack | Режим обратной связи по выходу |
| PKI | Public Key Infrastructure | Инфраструктура открытых ключей |
| RLE | Run Length Encoding | Кодирование серий последовательностей |
| RSA | Rivest – Shamir – Adleman Algorithm | Алгоритм шифрования RSA |
| RNG | Random number generator | Генератор случайных чисел |
| ГПСЧ |  | *Генератор псевдослучайных чисел* |
| ГСЧ |  | Генератор случайных чисел |
| НОД |  | Наибольший общий делитель |
| ЭВМ |  | Электронная вычислительная машина |
| ЭЦП |  | Электронная цифровая подпись |