ОБЗОР АЛГОРИТМОВ И СИСТЕМ ШИФРОВАНИЯ

Администрирование ИС 2014

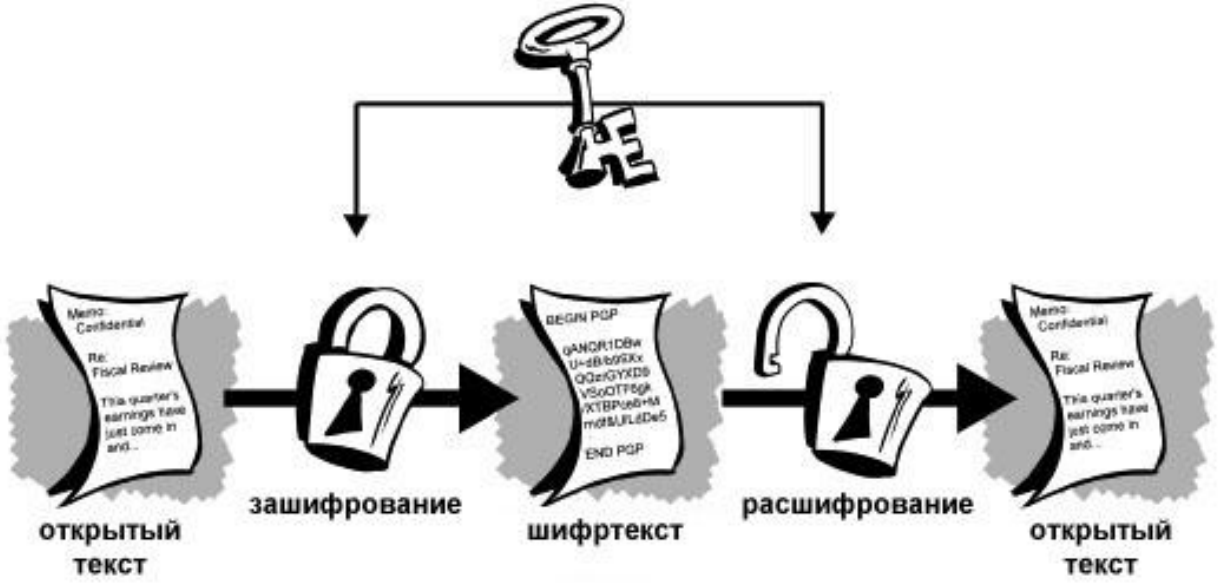
План

- Классификация алгоритмов шифрования
- Симметричные алгоритмы
- Ассиметричные алгоритмы
- Гибридные криптосистемы
- Хэширование
- ЭЦП
- Серитификаты

Классификация алгоритмов шифрования

- Симметричные (с секретным, единым ключом, одноключевые, single-key).
  - Потоковые (шифрование потока данных):
    - с одноразовым или бесконечным ключом (infinite-key cipher);
    - с конечным ключом (система Вернама - Vernam);
    - на основе генератора псевдослучайных чисел (ПСЧ).
  - Блочные (шифрование данных поблочно):
    - Шифры перестановки (permutation, P-блоки);
    - Шифры замены (подстановки, substitution, S-блоки):
      - моноалфавитные (код Цезаря);
      - полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);
    - Составные (таблица 1):
      - Lucipher (фирма IBM, США);
      - DES (Data Encryption Standard, США);
      - FEAL-1 (Fast Enciphering Algoritm, Япония);
      - IDEA/IPES (International Data Encryption Algorithm/
      - Improved Proposed Encryption Standard, фирма Ascom-Tech AG, Швейцария);
      - B-Crypt (фирма British Telecom, Великобритания);
      - ГОСТ 28147-89 (СССР); * Skipjack (США).
- Асимметричные (с открытым ключом, public-key):
  - Диффи-Хеллман DH (Diffie, Hellman);
  - Райвест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman);
  - Эль-Гамаль ElGamal.

Симметричные алгоритмы шифрования



Основная проблема – передача ключа

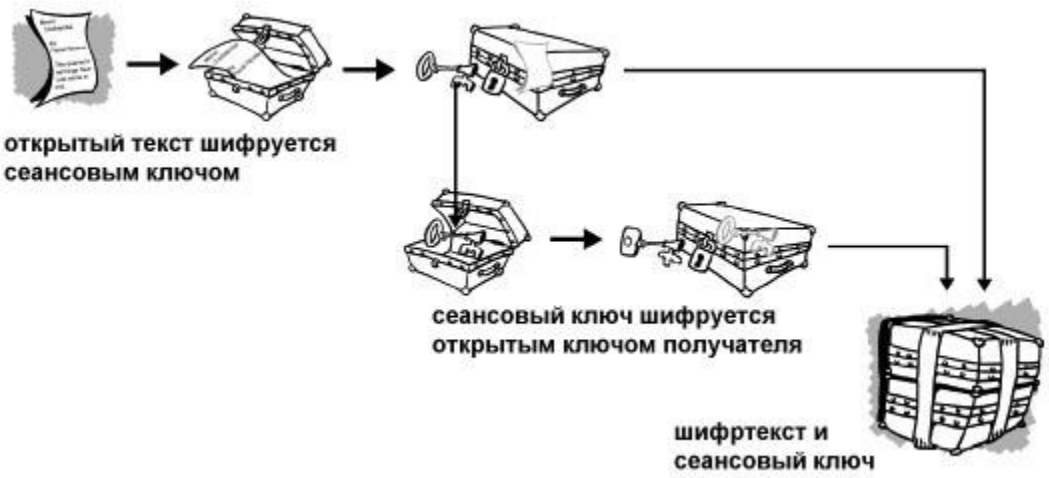
Асимметричные алгоритмы шифрования

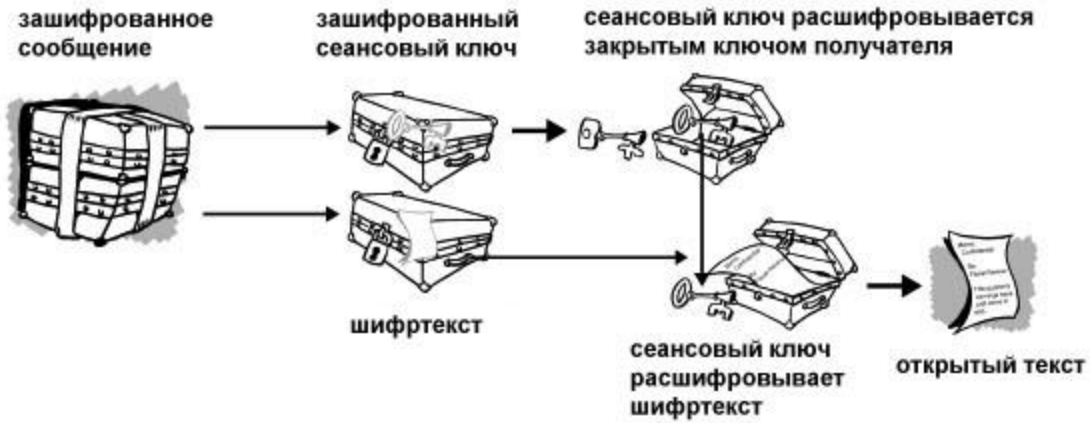
Сравнение симметричных и асимметричных алгоритмов шифрования

Симметричный алгоритм	Ассиметричный алгоритм
Криптостойкость при равной длине ключа	✓
Скорость	✓
Рост объема шифротекста	✓
Вычислительные затраты	✓
Проблема передачи ключа	✓

Внимание! Рассматривается сферический конь в вакууме

Алгоритмы действий PGP





Проблема человека посередине

Атака «человек посередине - 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.

Принцип атаки:

Предположим, объект 'A' планирует передать объекту 'B' некую информацию. Объект 'C' обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи собственно информации, которую 'C' планирует перехватить.

Для совершения атаки 'C' «представляется» объекту 'A' как 'B', а объекту 'B' — как 'A'. Объект 'A', ошибочно полагая, что он направляет информацию 'B', посылает её объекту 'C'.

Объект 'C', получив информацию, и совершив с ней некоторые действия (например, скопировав или модифицировав в своих

Хэши

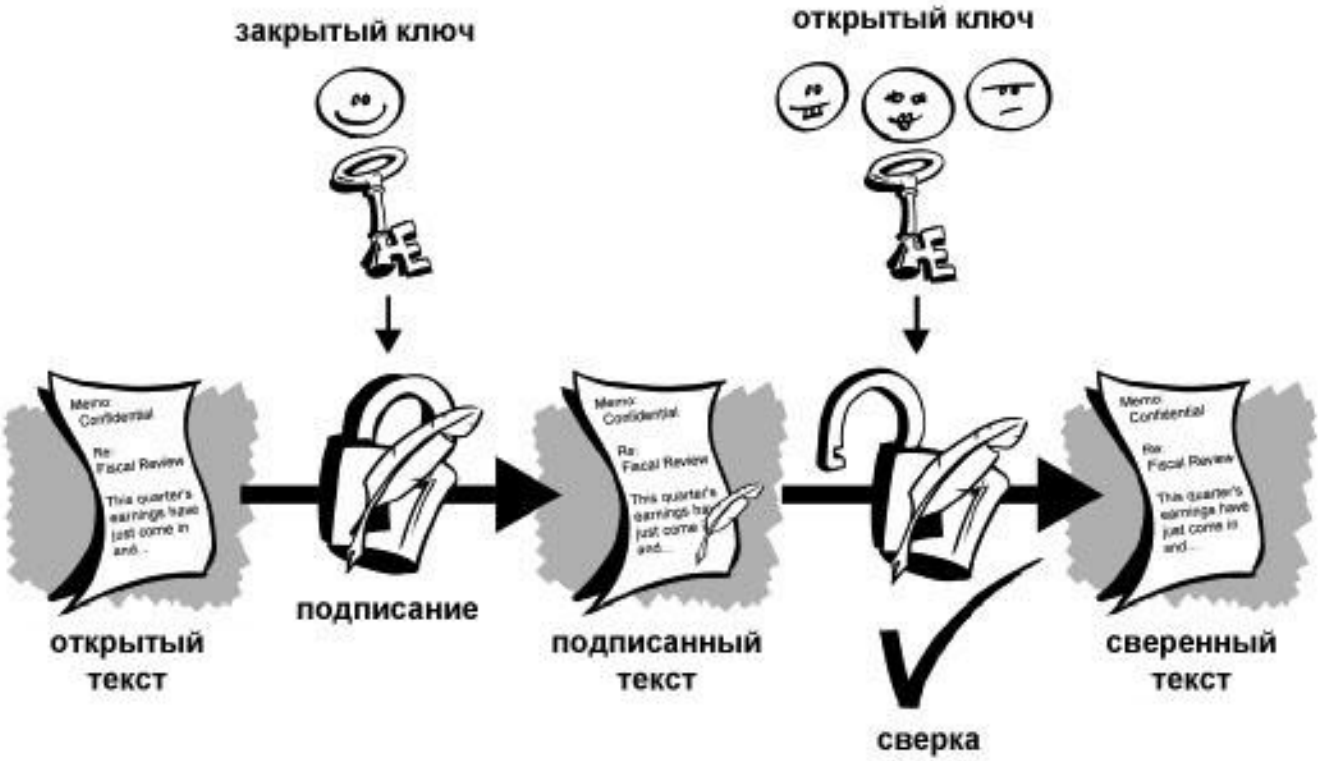

хэш-функция
открытый текст
дайдж
ный за
дайджест сообщения

Криптографические хеш-функции

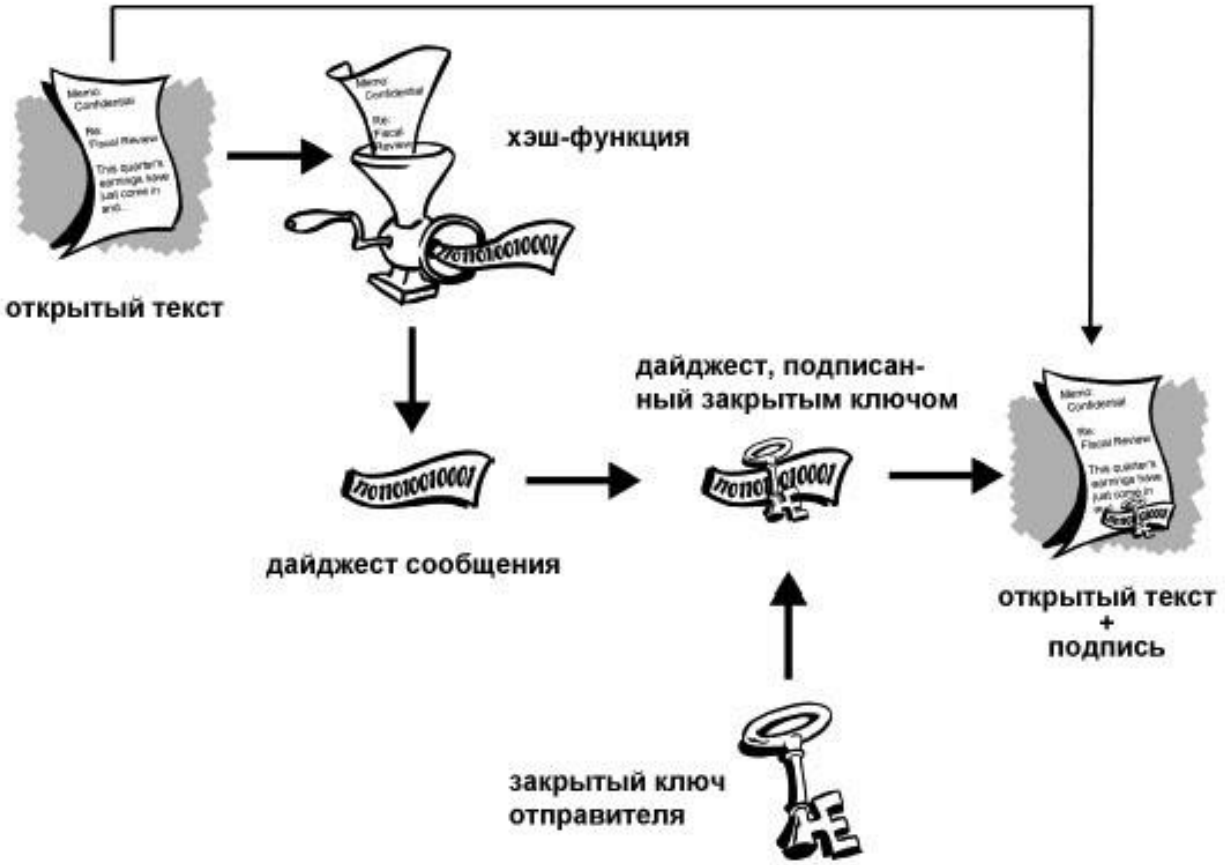
Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии. Для того чтобы хеш-функция *H* считалась криптографически стойкой, она должна удовлетворять трем основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

- *Необратимость*: для заданного значения хеш-функции *m* должно быть вычислительно неосуществимо найти блок данных X, для которого H(X)=m .
- Стойкость к *коллизиям первого рода*: для заданного сообщения *M* должно быть вычислительно неосуществимо подобрать другое сообщение *N*, для которого H(N)=H(M).
- Стойкость к *коллизиям второго рода*: должно быть вычислительно неосуществимо подобрать пару сообщений , имеющих одинаковый хеш.

Цифровая подпись



Использование хеш-функций



Перечень алгоритмов ЭП

Асимметричные схемы:

- FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA
- Схема Эль-Гамаля
- Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых)
- Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001
- Схема Диффи-Лампорта

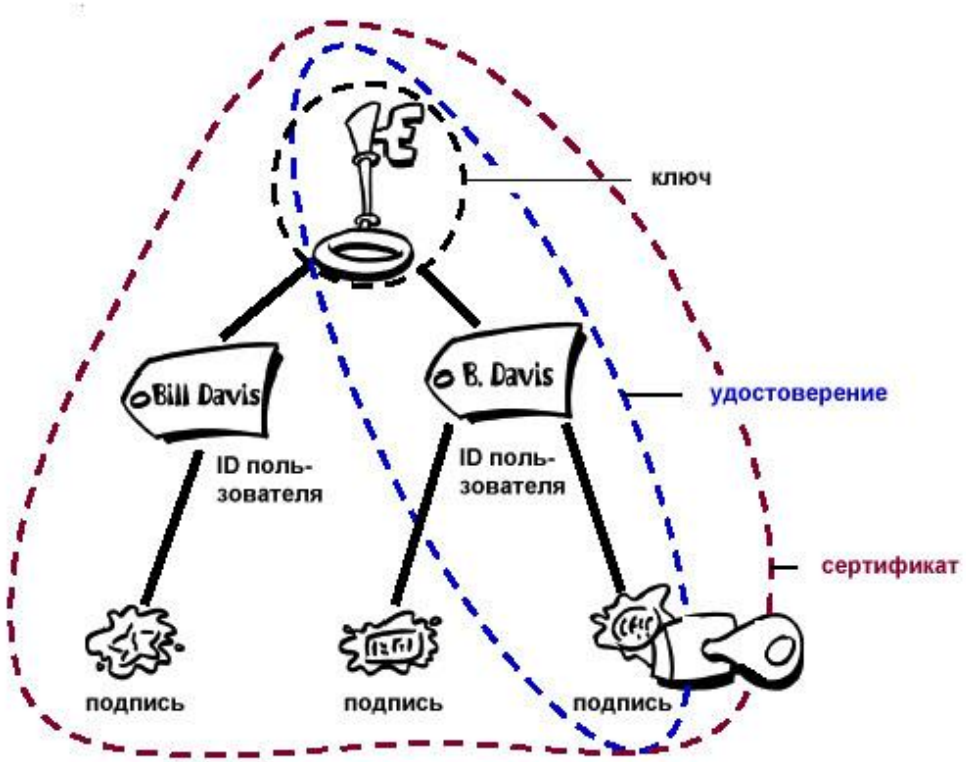
Структура и цель сертификата

Цифровой сертификат состоит из трёх компонентов:

- открытого ключа;
- сведений сертификата (информация о личности пользователя, как то: имя, ID, и т.п.);
- одной или более цифровых подписей.

Цель ЭЦП на сертификате — указать, что сведения сертификата были заверены третьим лицом или организацией. В то же время цифровая подпись не подтверждает достоверность сертификата как целого; она является поручительством только того, что подписанный ID связан с данным открытым ключом.

Модель сертификата



Таким образом, сертификат, обычно, — это открытый ключ с прикреплёнными к нему одной или несколькими формами ID плюс отметка подтверждения от доверенного лица.

Распространение сертификатов

Сертификаты применяются, когда нужно обменяться с кем-нибудь ключами.

Способы распространения:

- Ручной
- В виде хранилища-депозитария (сервера сертификатов)

Ручной способ характерен для небольших групп людей, устанавливающих криптографированную связь (не составит труда просто передать друг другу дискеты или отправить электронные письма, содержащие копии их ключей).

При необходимости обеспечить достаточную надёжность и безопасность, предоставления возможности хранения и обмена ключами, используют системный подход.

Такая система может реализоваться в форму простого хранилища-депозитария или иметь более сложную и комплексную структуру, предполагающую дополнительные возможности администрирования ключей, и называемую *инфраструктурой открытых ключей* (*Public Key Infrastructure, PKI*).

Серверы-депозитарии

Сервер-депозитарий, также называемый сервером сертификатов, или сервером ключей, — это база данных, позволяющая пользователям оставлять и извлекать из неё цифровые сертификаты.

Сервер ключей также может предоставлять некоторые административные функции, помогающие компании поддерживать свою политику безопасности. Например, на хранение могут оставляться только ключи, удовлетворяющие определённым критериям.

Инфраструктуры открытых ключей (PKI)

PKI, как и сервер-депозитарий, имеет базу хранения сертификатов, но, в то же время, предоставляет сервисы и протоколы по управлению открытыми ключами. В них входят возможности выпуска, отзыва и системы доверия сертификатов. Главной же возможностью PKI является введение компонентов, известных как *Центр сертификации* (*Certification Authority, CA*) и *Центр регистрации* (*Registration Authority, RA*).

Центр сертификации (ЦС) создаёт цифровые сертификаты и подписывает их своим закрытым ключом. Из-за важности своей роли, ЦС является центральным компонентом инфраструктуры PKI. Используя открытый ключ ЦС, любой пользователь, желающий проверить достоверность (подлинность) конкретного сертификата, сверяет подпись Центра сертификации и, следовательно, удостоверяется в целостности содержащейся в сертификате информации.

Как правило, Центром регистрации (ЦР) называется система лиц, процессов и устройств, служащая целям регистрации новых пользователей в структуре PKI (зачислению) и дальнейшему администрированию постоянных пользователей системы. Также, ЦР может производить «веттинг» — процедуру проверки того, принадлежит ли конкретный открытый ключ предполагаемому владельцу.

ЦР — это человеческое сообщество: лицо, группа, департамент, компания или иная ассоциация. С другой стороны, ЦС — обычно, программа, выдающая сертификаты своим зарегистрированным пользователям.

Роль ЦР-ЦС аналогична той, что выполняет государственный паспортный отдел.

Формат сертификатов

Как правило, цифровой сертификат — это набор идентифицирующих сведений, связанных с открытым ключом и подписанных доверенным третьим лицом (посредником), дабы доказать их подлинность и взаимосвязность. Сертификат может быть представлен в виде ряда форматов.

PGP поддерживает два формата сертификатов:

- Сертификаты стандарта PGP (чаще называемые просто ключами PGP)
- Сертификаты стандарта X.509

Алгоритм DES

DES (*Data Encryption Standard*) — симметричный алгоритм шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт (FIPS 46-3). DES имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для DES рекомендовано несколько режимов:

- режим электронной кодовой книги (ECB — Electronic Code Book),
- режим сцепления блоков (CBC — Cipher Block Chaining),
- режим обратной связи по шифротексту (CFB — Cipher Feed Back),
- режим обратной связи по выходу (OFB — Output Feed Back).

Прямым развитием DES в настоящее время является Triple DES.

Алгоритм AES

Advanced Encryption Standard (**AES**), также известный как **Rijndael** (произносится [rɛinda:l] (Рейндол)) —симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES. Национальный институт стандартов и технологий США (*National Institute of Standards and Technology*, NIST) опубликовал спецификацию AES 26 ноября 2001 года после пятилетнего периода, в ходе которого были созданы и оценены 15 кандидатур. 26 мая 2002 года AES был объявлен стандартом шифрования. AES является одним из самых распространённых алгоритмов симметричного шифрования.

Поддержка AES (и только его) введена фирмой Intel в семейство процессоров x86 начиная с Intel Core i7-980X Extreme Edition, а затем на процессорах Sandy Bridge.

Алгоритм Camellia

Camellia — алгоритм симметричного блочного шифрования (размер блока 128 бит, ключ 128, 192, 256 бит), один из финалистов европейского конкурса NESSIE (наряду с AES и Shacal-2), разработка японских компаний Nippon Telegraph and Telephone Corporation и Mitsubishi Electric Corporation (представлен 10 марта 2000 г.). Сертифицирован японской организацией CRYPTREC как рекомендованный для промышленного и государственного использования алгоритм.

Camellia является дальнейшим развитием алгоритма шифрования E2, одного из алгоритмов, представленных на конкурсе AES и с использованием элементов алгоритма MISTY1.

Структура алгоритма основана на классической цепи Фейстеля с предварительным и финальным забеливанием. Цикловая функция использует нелинейное преобразование (S-блоки), блок линейного рассеивания каждые 16 циклов (побайтовая операция XOR) и байтовую перестановку.

В зависимости от длины ключа имеет 18 циклов (128 разрядный ключ), либо 24 цикла (192 и 256 разрядный ключ).

Поддержка алгоритма Camellia введена в 2008 году в браузере Mozilla Firefox 3. Алгоритм патентован, однако распространяется под рядом свободных лицензий, в частности, является частью проекта OpenSSL.

Алгоритм IDEA

IDEA (***I****nternational* ***D****ata* ***E****ncryption* ***A****lgorithm*, международный алгоритм шифрования данных) симметричный блочный алгоритм шифрования данных, запатентованный швейцарской фирмой Ascom. Известен тем, что применялся в пакете программ шифрования PGP. В ноябре 2000 года IDEA был представлен в качестве кандидата в проекте NESSIE в рамках программы Европейской комиссии IST (*Information Societes Technology*, информационные общественные технологии).

Так как IDEA использует 128-битный ключ и 64-битный размер блока, открытый текст разбивается на блоки по 64 бит. Если такое разбиение невозможно, последний блок дополняется различными способами определённой последовательностью бит. Для избежания утечки информации о каждом отдельном блоке используются различные режимы шифрования. Каждый исходный незашифрованный 64-битный блок делится на четыре подблока по 16 бит каждый, так как все алгебраические операции, использующиеся в процессе шифрования, совершаются над 16-битными числами. Для шифрования и расшифрования IDEA использует один и тот же алгоритм.

Алгоритм RC4

RC4 (***Rivest Cipher 4*** или ***Ron's Code***, также известен как **ARCFOUR** или **ARC4** (***Alleged RC4***)) — потоковый шифр, широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритме безопасности беспроводных сетей WEP, для шифрования паролей в Windows NT).

Шифр разработан компанией RSA Security и для его использования требуется лицензия.

Алгоритм RC4, как и любой потоковый шифр, строится на основе параметризованного ключом генератора псевдослучайных битов с равномерным распределением. Длина ключа может составлять от 40 до 256 бит.

Основные преимущества шифра — высокая скорость работы и переменный размер ключа. RC4 довольно уязвим, если используются не случайные или связанные ключи, один ключевой поток используется дважды. Эти факторы, а также способ использования могут сделать криптосистему небезопасной (например WEP).

ГОСТ 28147-89

ГОСТ 28147-89 — советский и российский стандарт симметричного шифрования, введённый в 1990 году, также является стандартом СНГ.

Полное название — «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Блочный шифроалгоритм. При использовании метода шифрования с гаммированием, может выполнять функции поточного шифроалгоритма.

Использует блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками. Основа алгоритма шифра

Алгоритм RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования за разумное время (обратной операции) необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложения числа на простые множители.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

В криптографической системе с открытым ключом каждый участник располагает как открытым ключом (*public key*), так и закрытым ключом (*private key*). В криптографической системе RSA каждый ключ состоит из пары целых чисел. Каждый участник создаёт свой открытый и закрытый ключ самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому угодно или даже публиковать их.