Bell-Northern Research разработала прототип безопасного телефонного терминала **ISDN** (Integrated Services Digital Network, Цифровая сеть с интегрированием услуг). Как телефонный аппарат, терминал остался на уровне прототипа. В результате появился Уровень безопасности пакетов данных (Packet Data Security Overlay). Терминал использует схему обмена ключами Diffie-Hellman, цифровые подписи RSA и DES для шифрования данных. Он может передавать и принимать речь и данные со скоростью 64 Кбит/с.

Ключи В телефон встроена пара "открытый ключ/закрытый ключ" для длительного использования . Закрытый ключ хранится в устойчивом от вскрытия модуле телефона. Открытый ключ служит для идентификации телефона . Эти ключи являются частью самого телефонного аппарата и не могут быть изменены . Кроме того, в телефоне хранятся еще два открытых ключа. Одним из них является открытый ключ владельца аппарата. Этот ключ используется для проверки подлинности команд владельца, он может быть изменен по команде, подписанной владельцем.

Так пользователь может передать кому-то другому право владения аппаратом. В телефоне также хранится открытый ключ сети. Он используется для проверки подлинности команд аппаратуры управления сетью и проверки подлинности вызовов от других пользователей сети .

Этот ключ также можно изменить командой, подписанной владельцем. Это позволяет владельцу менять сеть, к которой подключен его аппарат. Эти ключи рассматриваются как ключи длительного пользования - они меняются редко, если вообще меняются. В телефоне также хранится пара "открытый ключ/закрытый ключ" для краткосрочного использования . Они встроены в сертификат, подписанный центром управления ключами . Два телефона обмениваются сертификатами при установлении соединения. Подлинность этих сертификатов удостоверяется открытым ключом сети . Обмен сертификатами и их проверка выполняются только при установлении безопасного соединения между аппаратами. Для установления безопасного соединения между людьми протокол содержит дополнительный компонент.

В аппаратном ключе зажигания, который вставляется в телефон владельцем, хранится закрытый ключ владельца, зашифрованный секретным паролем, известным только владельцу (его не знает ни телефонный аппарат, ни центр управления сетью, ни еще кто-нибудь). Ключ зажигания также содержит сертификат, подписанный центром управления сетью, в который включены открытый ключ владельца и некоторая идентификационная информация (имя, компания, специальность, степень допуска, любимые сорта пиццы, и прочее). Все это также зашифровано.

Для дешифрирования этой информации и ввода ее в телефон пользователь вводит свой секретный пароль с клавиатуры аппарата . Телефонный аппарат использует эту информацию для соединения, но она удаляется после того, как пользователь извлечет свой ключ зажигания . В телефоне также хранится набор сертификатов, выданных центром управления сетью . Эти сертификаты удостоверяют право конкретных пользователей пользоваться конкретными телефонными аппаратами .

Вызов **Б** А происходит следующим образом.

1) А вставляет в телефон свой ключ зажигания и вводит свой пароль.
2) Телефон опрашивает ключ зажигания, чтобы определить личность А и выдать сигнал "линия свободна".
3) Телефон проверяет свой набор сертификатов, проверяя, что А имеет право использовать этот аппарат .
4) А набирает номер, телефон определяет адресата звонка.
5) Два телефона используют протокол обмена ключами на базе криптографии с открытыми ключами, чтобы генерировать уникальный и случайный сеансовый ключ. Все последующие этапы протокола шифруются с помощью этого ключа.
6) Телефон А передает свой сертификат и идентификатор пользователя .
7) Телефон **Б** проверяет подписи сертификата и идентификатора пользователя, используя открытый ключ сети.
8) Телефон **Б** инициирует последовательность запросов/ответов

. Для этого необходимо в реальном времени отправлять подписанные ответы на запросы . (Это помешает злоумышленнику использовать сертификаты, скопированные из предыдущего обмена .) Один ответ должен быть подписан закрытым ключом телефона А, а другой - закрытым ключом А .

9) Если Б нет у телефона, то его телефон звонит.

0) Если Б дома, он вставляет в телефон свой ключ зажигания. Его телефон опрашивает ключ зажигания и проверяет сертификат Б, как на этапах (2) и (3).

1) Б передает свой сертификат и идентификатор пользователя

2) Телефон А проверяет подписи Б, как на этапе (7) и инициирует последовательность запросов/ответов, как на этапе (8).

3) Оба телефона выводят на свои экраны личность и номер телефона другого пользователя .

4) Начинается безопасный разговор.

5) Когда одна из сторон вешает трубку, удаляются сеансовый ключ, а также сертификаты, которые телефон Б получил от телефона А, и сертификаты, которые телефон А получил от телефона Б .

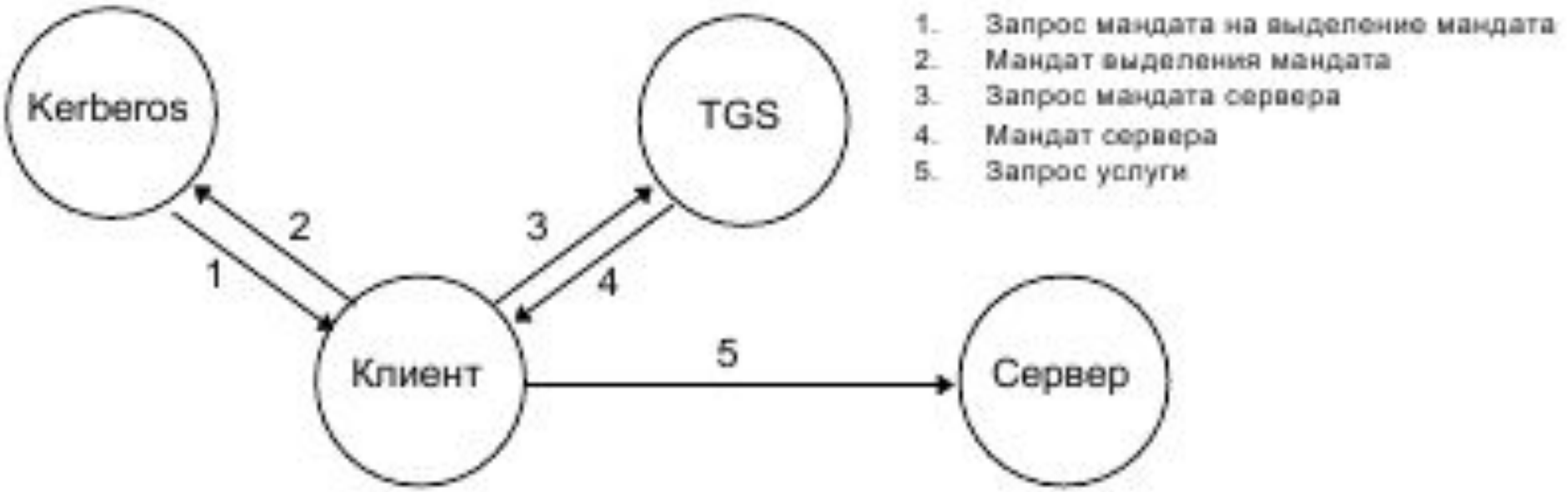
Каждый ключ DES уникален для каждого звонка. Он существует только внутри двух телефонных аппаратов и только в течение разговора, а после его окончания немедленно уничтожается. Если злоумышленник добудет один или оба участвовавших в разговоре аппарата, он не сможет расшифровать ни один предшествующий разговор, в котором участвовали эти два аппарата.

STU обозначает "Secure Telephone Unit" (Безопасный телефонный модуль), разработанный в NSA безопасный телефон. По размерам и форме этот модуль почти такой же, как и обычный телефон, и может быть использован также, как и обычный телефон. Аппараты устойчивы к взлому, без ключа они работают как несекретные. Они также включают порт передачи данных и помимо передачи речи могут быть использованы для безопасной передачи данных по модемному каналу. Уитфилд Диффи описал STU-III. STU-III производятся AT&T и GE. За 1994 год было выпущено 300000-400000 штук. Новая версия, Secure Terminal Equipment (STE, Безопасный терминал), работает по линиям ISDN.

Kerberos представляет собой разработанный для сетей TCP/IP протокол проверки подлинности с доверенной третьей стороной. Служба Kerberos, работающая в сети, действует как доверенный посредник, обеспечивая безопасную сетевую проверку подлинности, дающую пользователю возможность работать на нескольких машинах сети. Kerberos основан на симметричной криптографии (реализован DES, но вместо него можно использовать и другие алгоритмы). При общении с каждым объектом сети Kerberos использует отличный общий секретный ключ, и знание этого секретного ключа равносильно идентификации объекта . Kerberos был первоначально разработан в МТИ для проекта Афина. Модель Kerberos основана на протоколе Needham-Schroeder с доверенной третьей стороной. В модели Kerberos существуют расположенные в сети объекты - клиенты и серверы. Клиентами могут быть пользователи, но могут и независимые пр о- граммы, выполняющие следующие действия: загрузку файлов, передачу сообщений, доступ к базам данных, доступ к принерам, получение административных привилегий, и т.п.

Kerberos хранит базу данных клиентов и их секретных ключей. Для пользователей-людей секретный ключ является зашифрованным паролем. Сетевые службы, требующие проверки подлинности, и клиенты, которые хотят использовать эти службы, регистрируют в Kerberos свои секретные ключи. Так как Kerberos знает все секретные ключи, он может создавать сообщения, убеждающие один объект в подлинности другого. Kerberos также создает сеансовые ключи, которые выдаются клиенту и серверу (или двум клиентам) и никому больше. Сеансовый ключ используется для шифрования сообщений, которыми обмениваются две стороны, и уничтожается после окончания сеанса .

Для шифрования Kerberos использует DES. Kerberos версии 5 использует режим CBC.



Этапы проверки подлинности Kerberos

Протокол Kerberos . Клиент запрашивает у Kerberos мандат на обращение к Службе выделения мандатов (Ticket-Granting Service, TGS). Этот мандат, зашифрованный секретным ключом клиента, посылается клиенту. Для использования конкретного сервера клиент запрашивает у TGS мандат на обращение к серверу.

Если все в порядке, TGS посылает мандат клиенту. Затем клиент предъявляет серверу этот мандат вместе с удостоверением. И снова, если атрибуты клиента правильны, сервер предоставляет клиенту доступ к услуге.

c	= клиент
s	= сервер
a	= сетевой адрес клиента
v	= начало и окончание времени действия мандата
t	= метка времени
K_x	= секретный ключ x
$K_{x,y}$	= сеансовый ключ для x и y
$(m)K_x$	= m, шифрованное секретным ключом x
$T_{x,y}$	= мандат x на использование y
$A_{x,y}$	= удостоверение x для y

Таблица сокращений Kerberos

Kerberos использует два типа атрибутов: мандаты и удостоверения. Мандат используется для безопасной передачи серверу личности клиента, которому выдан этот мандат В нем также содержится информация, которую сервер может использовать для проверки того, что клиент, использующий мандат, - это именно тот клиент, которому этот мандат был выдан

.. Удостоверение - это дополнительный атрибут, предъявляемый вместе с мандатом. Мандат Kerberos имеет следующую форму:

$$Tc,s = s, \{c, a, v, K_{c,s}\}K_s.$$

Мандат хорош для одного сервера и одного клиента. Он содержит имя клиента, его сетевой адрес, имя сервера, метку времени и сеансовый ключ. Эта информация шифруется секретным ключом сервера.

Если клиент получил мандат, он может использовать его для доступа к серверу много раз - пока не истечет срок действия мандата. Не может расшифровать мандат (он не знает секретного ключа сервера), но он может предъявить его серверу в зашифрованной форме. Прочитать или изменить мандат при передаче его по сети невозможно . Удостоверение Kerberos имеет следующую форму:

$$A_{c,s} = \{c, t, \text{ключ}\}K_{c,s}$$

Клиент создает его каждый раз, когда ему нужно воспользоваться услугами сервера .

Удостоверение содержит имя клиента, метку времени и необязательный дополнительный сеансовый ключ, генерировать удостоверения по мере надобности (ему известен общий секретные ключ).

Все эти данные шифруются сеансовым ключом, общим для клиента и сервера. В отличие от мандата удостоверение используется только один раз. Однако это не проблема, так как клиент может генерировать удостоверения по мере надобности.

Использование удостоверения преследует две цели. Во первых, оно содержит некоторый открытый текст, зашифрованный сеансовым ключом. Это доказывает, что клиенту известен ключ. Что не менее важно, зашифрованный открытый текст включает метку времени. Злоумышленник, которому удалось записать и мандат, и удостоверение, не сможет использовать их спустя два дня.

1. Клиент-Kerberos: c,tgs
2. Kerberos-клиент: {K c,tgs}K c, {T c,tgs}K tgs
3. Клиент-TGS: {A c,s}K c,tgs{T c,tgs} K tgs,s
4. TGS-клиент: {K c,s}K c,tgs{T c,s}K s
5. Клиент-сервер: {A c,s}K c,s {T c,s}K s

Получение первоначального мандата У клиента есть часть информации, доказывающей его личность - его пароль . Понятно, что не хочется за- ставлять клиента передавать пароль по сети. Протокол Kerberos минимизирует вероятность компрометации па- роля, но при этом не позволяет пользователю правильно идентифицировать себя, если он не знает пароля . Клиент посылает сообщение, содержащее его имя и имя его сервера TGS на сервер проверки подлинности Kerberos. (может быть несколько серверов TGS.)

На практике пользователь просто вводит свое имя и программа входа в систему посылает запрос. Сервер проверки подлинности Kerberos ищет данные о клиенте в своей базе данных ..

Если информация о клиенте есть в базе данных, Kerberos генерирует сеансовый ключ, который будет использоваться для обмена данными между клиентом и TGS. Он называется Мандатом на выделение мандата (Ticket Granting Ticket, TGT). Kerberos шифрует этот сеансовый ключ секретным ключом клиента .
Затем он создает для клиента TGT, доказывающий подлинность клиента TGS, и шифрует его секретным ключом TGS.
Сервер проверки подлинности посылает эти два зашифрованных сообщения клиенту
Теперь клиент расшифровывает первое сообщение и получает сеансовый ключ . Секретный ключ является однонаправленной хэш-функцией клиентского пароля, поэтому у законного пользователя не будет никаких проблем. Самозванец не знает правильного пароля и, следовательно, не может расшифровать ответ сервера проверки подлинности. Доступ запрещается, и самозванный клиент не может получить мандат или сеансовый ключ.

Клиент сохраняет TGT и сеансовый ключ, стирая пароль и хэш-значение. Эта информация уничтожается для уменьшения вероятности компрометации.
Если враг попытается скопировать память клиента, он получит только TGT и сеансовый ключ. Эти данные важны, но только на время жизни TGT. Когда срок действия TGT истечет, эти сведения станут бессмысленными. Теперь в течение времени жизни TGT клиент может доказывать TGS свою подлинность.
Клиенту требуется **получить отдельный серверный мандат** для каждой нужной ему услуги . TGS выделяет мандаты для отдельных серверов. Когда клиенту нужен мандатон посылает запрос к TGS. TGS, получив запрос, расшифровывает TGT своим секретным ключом. Затем TGS использует включенный в TGT сеансовый ключ, чтобы расшифровать удостоверение . Наконец TGS сравнивает информацию удостоверения с информацией мандата, сетевой адрес клиента с адресом отправителя запроса и метку времени с текущим временем. Если все совпадает, TGS разрешает выполнение запроса. Проверка меток времени предполагает, что часы всех компьютеров синхронизированы с точностью до минут.

В ответ на правильный запрос TGS возвращает правильный мандат, который клиент может предъявить серверу. TGS также создает новый сеансовый ключ для клиента и сервера, зашифрованный сеансовым ключом, общим для клиента и TGS. Оба этих сообщения отправляются клиенту . Клиент расшифровывает сообщение и извлекает сеансовый ключ.

Запрос услуги Теперь клиент может доказать свою подлинность серверу. Клиент создает удостоверение, состоящее из его имени, сетевого адреса и метки времени, зашифрованное сеансовым ключом, который был генерирован TGS для сеанса клиента и сервера. Запрос состоит из мандата, полученного от Kerberos (уже зашифрованного секретным ключом сервера) и зашифрованного идентификатора**.** Сервер расшифровывает и проверяет мандат и удостоверение, как уже обсуждалось, а также проверяет адрес клиента и метку времени. Если приложение требует взаимной проверки подлинности, сервер посылает клиенту сообщение, состоящее из метки времени, зашифрованной сеансовым ключом . При необходимости клиент и сервер могут шифровать дальнейшие сообщения общим ключом.

Стив Белловин (Steve Bellovin) и Майкл Мерритт (Michael Merritt) проанализировали некоторые потенциальные уязвимые места Kerberos. Возможно кэширование и повторное использование старых удостоверений. время жизни бывает достаточно большим, часто до восьми часов. Использование удостоверений основаны на том, что все часы сети более или менее синхронизированы. Большинство сетевых протоколов поддержки единого времени небезопасны. Kerberos также чувствителен к вскрытиям с угадыванием пароля. Самым опасным является вскрытие, использующее специальное программное обеспечение. Kerberos не является общедоступным, но код МТИ доступен свободно. KryptoKnight (**КриптоРыцарь)** является системой проверки подлинности и распределения ключей, разработанной в IBM. Это протокол с секретным ключом, использующий либо DES в режиме CBC или MD5. KryptoKnight поддерживает четыре сервиса безопасности: - Проверка подлинности пользователя (называемая единственной подписью - single sign-on) - Двусторонняя проверка подлинности - Распределение ключей - Проверка подлинности содержания и происхождения данных

С точки зрения пользователя, KryptoKnight похож на Kerberos. Вот некоторые отличия: — Для проверки подлинности и шифрования мандатов KryptoKnight использует хэш-функцию.
— KryptoKnight не использует синхронизированных часов, используются только текущие запросы.
— Если А нужно связаться с Б, одна из опций KryptoKnight позволяет А послать сообщение Б, а затем позволяет Б начать протокол обмена ключами.
KryptoKnight, как и Kerberos, использует мандаты и удостоверения. Он содержит и TGS, но в KryptoKnight называются серверами проверки подлинности. Разработчики KryptoKnight потратили немало усилий, минимизируя количество сообщений, их размер и объем шифрования.
SESAME означает Secure European System for Applications in a Multivendor Environment - Безопасная европейская система для приложений в неоднородных средах . Это проект Европейского сообщества: ICL в Великобритании, Siemens в Германии и Bull во Франции.

SESAME представляет собой систему проверки подлинности и обмена ключами. Она использует протокол Needham-Schroeder, применяя криптографию с открытыми ключами для связи между различными безопасными доменами.

Общая криптографическая архитектура (Common Cryptographic Architecture, CCA) была разработана компанией **IBM**, чтобы обеспечить криптографические примитивы для конфиденциальности, целостности, управления ключами и обработки персонального идентификационного кода (PIN). Управление ключами происходит с помощью векторов управления (control vector, CV). Каждому ключу соответствует CV, с которым ключ объединен операцией XOR. Ключ и CV разделяются только в безопасном аппаратном модуле. CV представляет собой структуру данных, обеспечивающую интуитивное понимание привилегий, связанных с конкретным ключом. Отдельные биты CV обладают конкретным смыслом при использовании каждого ключа, применяемого в CGA. CV передаются вместе с зашифрованным ключом в структурах данных, называемых ключевыми маркерами (key token).

Внутренние ключевые маркеры используются локально и содержат ключи, шифрованные локальным главным ключом (master key, MK). Внешние ключевые маркеры используются для обмена шифрованными ключами между системами. Ключи во внешних ключевых маркерах зашифрованы ключами шифрования ключей (key-encrypting key, KEK). Управление KEK осуществляется с помощью внутренних ключевых маркеров. Ключи разделяются на группы в соответствии с их использованием . Длина ключа также задается в CV. Ключи одинарной длины - 56-битовые – используются для таких функций, как обеспечение конфиденциальности и сообщений. Ключи двойной длины - 112-битовые - применяются для управления ключами, функций PIN и других специальных целей. Ключи могут быть DOUBLE-ONLY (только двойные), правые и левые половины которых должны быть различны, DOUBLE (двойные) половины которых могут случайно совпасть, SINGLE-REPLICATED (одинарные-повторенные), в которых правые и левые половины равны, или SINGLE (одинарные), содержащие только 56 битов. CGA определяет аппаратную реализацию ряда типов ключей, используемых для некоторых операций

CV проверяется в безопасном аппаратном модуле: для каждой функции. CGA вектор должен соответствовать определенным правилам. При помощи XOR KEK или MK с CV получается вариант KEK или MK, и извлеченный ключ для дешифрирования открытого текста сообщения используется только при выполнении функции CGA.

При генерации новых ключей CV задает способ использования созданного ключа.

Для распределения ключей CGA применяет комбинацию криптографии с открытыми ключами и криптографии с секретными ключами. KDC шифрует сеансовый ключ для пользователя секретным главным ключом, разделяемым с этим пользователем. Распределение главных ключей происходит с помощью криптографии с открытыми ключами.

Разработчики системы выбрали такой гибридный подход по двум причинам . 1.эффективность. Криптография с открытыми ключами требует больших вычислительных ресурсов, если сеансовые ключи распределяются с помощью криптографии с открытыми ключами, система может повиснуть

2. обратная совместимость, система может быть с минимальными последствиями установлена поверх существующих схем с секретными ключами.

CGA-системы проектировались так, чтобы они могли взаимодействовать с различными другими системами . При контакте с несовместимыми системами функция трансляции вектора управления (Control Vector Translate, CVXLT) позволяет системам обмениваться ключами.

Аппаратура закрытия коммерческих данных (Commercial Data Masking Facility, CDMF) представляет собой экспортируемую версию CGA

Для использования в схеме проверки подлинности ISO, также известной как протоколы X.509, рекомендуется криптография с открытыми ключами. Эта схема обеспечивает проверку подлинности по сети. Хотя конкретный алгоритм не определен ни для обеспечения безопасности, ни для проверки подлинности, спецификация рекомендует использовать RSA.

Сертификат X.509.
Наиболее важной частью X.509 используемая им структура сертификатов открытых ключей. Доверенный Орган сертификации (Certification Authority, CA) присваивает каждому пользователю уникальное имя и выдает подписанный сертификат, содержащий имя и открытый ключ пользователя.

Поле версии определяет формат сертификата. Последовательный номер уникален для конкретного CA. Следующее поле определяет алгоритм, использованный для подписи сертификата , вместе со всеми необходимыми параметрами. Выдавшей организацией является CA. Срок действия представляет собой пару дат, сертификат действителен в промежутке между этими двумя датами . Субъект - это имя пользователя. Информация об открытом ключе включает название алгоритма, все необходимые параметры и открытый ключ . Последним полем является подпись CA. Сертификаты могут храниться в базах данных на различных узлах сети . Пользователи могут посылать их друг другу. Истечении срока действия сертификата он должен быть удален из всех общедоступных каталогов . Однако CA, выдавший сертификат, должен продолжать хранить его копию, которая может потребоваться при разрешении возможных споров. Сертификаты также могут быть отозваны, либо из-за компрометации ключа пользователя, либо из-за того, что CA больше не хочет подтверждать сертификат данного пользователя

Протоколы проверки подлинности. А для связи с Б: 1. извлекает из базы данных последовательность сертификации и открытый ключ Б. А может инициировать однопроходный, двухпроходный или трехпроходный протокол проверки подлинности.
Однопроходный протокол представляет собой простую передачу данных Б от А. Протокол устанавливает личности и А, и Б, а также целостность информации, передаваемой Б от А; обеспечивает защиту от вскрытия линии связи с помощью повтора.
В двухпроходном протоколе добавлен ответ Б. Протокол устанавливает, что именно Б посылает ответ и обеспечивает безопасность обеих передач и защищает от вскрытия повтором.
И в однопроходных, и в двухпроходных алгоритмах используются метки времени . В трехпроходном протоколе добавляется еще одно сообщение от А Б и позволяет избежать меток времени.

Почта с повышенной секретностью (Privacy-Enhanced Mail, PEM) представляет собой стандарт Internet для почты с повышенной секретностью, одобренный Советом по архитектуре Internet (Internet Architecture Board, IAB) для обеспечения безопасности электронной почты в Internet. Первоначальный вариант был разработан Группой секретности и безопасности (Privacy and Security Research Group, PSRG) Internet Resources Task Force (IRTF), а затем их разработка была передана в Рабочую группу PEM Internet Engineering Task Force (IETF) PEM Working Group. Протоколы PEM предназначены для шифрования, проверки подлинности, проверки целостности сообщения и управления ключами. PEM является расширяемым стандартом. Процедуры и протоколы PEM разработаны так, чтобы быть совместимыми со множеством подходов к управлению ключами, включая симметричную схему и использование открытых ключей для шифрования ключей шифрования данных. Сообщения шифруются алгоритмом DES в режиме CBC.

Проверки целостности сообщения (Message Integrity Check, MIC), использует MD2 или MD5. Симметричное управление ключами может применять либо DES в режиме , либо тройной DES с двумя ключами (режим EDE). Для управления ключами PEM также поддерживает сертификаты открытых ключей, используя RSA (длина ключа до 1024 битов) и стандарт X.509 для структуры сертификатов.

Инфраструктура управления ключами использует общий корень для всей сертификации Internet. Центр регистрационной политики (Internet Policy Registration Authority, IPRA) определяет глобальную стратегию, применимую ко всей иерархии. Ниже корня - IPRA - находятся Центры сертификационной политики (Policy Certification Authorities, PCA), каждый из которых определяет и опубликовывает свою стратегию регистрации пользователей и организаций. Каждый PCA сертифицирован IPRA. Следом за PCA идут CA, сертифицирующие пользователей и и управляющие организационными подразделениями. Первоначально предполагалось, что большинство пользователей будет регистрироваться в качестве членов организаций

Доверенные информационные системы (TIS, Trusted Information Systems), частично поддерживаемые Управлением по передовым научным проектам правительства Соединенных Штатов , включают реализацию PEM (TIS/PEM). Разработанные для платформ UNIX, они были также перенесены на VMS, DOS и Windows. Хотя спецификации PEM определяют для Internet один главный сертификационный центр , TIS/PEM поддерживает существование нескольких иерархий сертификации.

Протокол безопасности сообщений (Message Security Protocol, MSP) - это военный эквивалент PEM. Он был разработан NSA в конце 80-х годов. Это совместимый с X.400 протокол уровня приложения для закрытия электронной почты. MSP в разрабатываемой сети оборонных сообщений (Defense Message System, DMS) Министерства обороны. Предварительный протокол безопасности сообщений (Preliminary Message Security Protocol, PMSP), который предполагается использовать для "несекретных, но важных" сообщений , представляет собой адаптированную для использования с X.400 и TCP/IP версию MSP. Этот протокол также называют Mosaic.

Pretty Good Privacy (PGP, весьма хорошая секретность) - это свободно распространяемая программа безопасной электронной почты, разработанная Филипом Циммерманном (Philip Zimmer-mann). Для шифрования данных она использует IDEA, для управления ключами и цифровой подписи - RSA (длина ключа до 2047 битов), а для однонаправленного хэширования - MD5.
Для получения случайных открытых ключей PGP использует вероятностную проверку чисел на простоту, используя для получения стартовых последовательностей интервалы между нажатиями пользователем клавиш на клавиатуре. PGP генерирует случайные ключи IDEA с помощью метода, в ANSI X9.17, Appendix C, используя вместо DES в качестве симметричного алгоритма IDEA. PGP также шифрует закрытый ключ пользователя с помощью хэшированной парольной фразы, а не пароля непосредственно.
Сообщения, зашифрованные PGP, имеют несколько уровней безопасности. Единственная вещь, известная криптоаналитику о зашифрованном сообщении, - это получатель сообщения при условии, что криптоаналитику известен ID ключа получателя.

Только расшифровав сообщение, получатель узнает, кем оно подписано, если оно подписано. Это резко отличается от сообщения PEM, в заголовке которого немало информации об отправителе, получателе и самом сообщении хранится в незашифрованном виде. Самой интересной особенностью PGP является распределенный подход к управлению ключами. Центров сертификации ключей нет, вместо этого в PGP поддерживается "сеть доверия". Каждый пользователь сам создает и распространяет свой открытый ключ . Пользователи подписывают ключи друг друга, создавая взаимосвязанное сообщество пользователей PGP.

PGP не определяет стратегию установки доверительных связей, пользователи сами решают, кому верить, а кому нет. PGP обеспечивает механизмы для поддержки ассоциативного доверия открытым ключам и для и с- пользования доверия. Каждый пользователь хранит набор подписанных открытых ключей в виде файла кольца открытых ключей (public-key ring). Каждый ключ кольца обладает полем законности ключа, определяющим уровень доверия к ключу конкретного пользователя .

Чем больше уровень доверия, тем больше пользователь уверен в законности ключа. Поле доверия к подписи измеряет, насколько пользователь верит тому, кто подписал открытые ключи других пользователей. И, наконец, поле доверия к владельцу ключа задает уровень, определяющий, насколько конкретный пользователь верит владельцу ключа, подписавшему другие открытые ключи. Это поле вручную устанавливается пользователем. PGP непрерывно обновляет эти поля по мере появления новой информации.
Самым слабым звеном этой системы является отзыв ключей: гарантировать, что кто-нибудь не воспользуется скомпрометированным ключом, невозможно . Если закрытый ключ А украден, А может послать некий сертификат отзыва ключа (key revocation certificate), но, так как некое распределение ключей уже произошло, нельзя гарантировать, что это сообщение будет получено всеми, использующими открытый ключ А в своем кольце ключей. И так как А должна будет подписать свой сертификат отзыва ключа своим закрытым ключом, то если она потеряет ключ, она не сможет и отозвать его

PGP доступна для MS-DOS, UNIX, Macintosh, Amiga и Atari.

Интеллектуальная карточка представляет собой пластиковую карточку, по размеру и форме как кредитная карточка, с встроенной компьютерной микросхемой (обычно 8-битовый микропроцессор), ОЗУ (четверть килобайта), ПЗУ (примерно 6-8 килобайт), и несколько килобайт либо EPROM (стираемое программируемое ПЗУ) или EEPROM (электронно стираемое программируемое ПЗУ).

В интеллектуальных карточках могут использоваться различные криптографические протоколы и алгоритмы. Они могут быть электронным кошельком, давая возможность тратить и получать электронные н а- личные. Карточки могут использоваться в протоколах проверки подлинности с нулевым знанием, они могут обладать собственными ключами шифрования.

Стандарты криптографии с открытыми ключами (Public-Key Cryptography Standards, PKCS) - это попытка компании RSA Data Security, Inc обеспечить промышленный стандарт для криптографии с открытыми ключами.

Универсальная система **электронных платежей** (Universal Electronic Payment System, UEPS) представляет собой банковское приложение, использующее интеллектуальные карточки, первоначально разработанное для сельской Южной Африки, но позднее принятое основными банковскими группами этой страны. **Микросхема Clipper** (известная также как MYK-78T) - это разработанная в NSA, устойчивая к взлому микросхема, предназначенная для шифрования переговоров голосом. Это одна из двух схем, реализующих правительственный Стандарт условного шифрования (Escrowed Encryption Standard, EES). VLSI Technologies, Inc. изготовила микросхему, а Mykotronx, Inc. запрограммировала ее. Сначала все микросхемы Clipper будут входить в Безопасное телефонное устройство Model 3600 AT&T. Микросхема реализует алгоритм шифрования Skipjack, разработанный NSA секретный алгоритм с шифрованием секретным ключом, только в режиме OFB.

Безопасный телефон AT&T (Telephone Security Device, TSD) - это телефон с микросхемой Clipper. На самом деле существует четыре модели TSD. Одна содержит микросхему Clipper, другая - экспортируемый фирменный алгоритм шифрования AT&T третья - фирменный алгоритм для использования внутри страны плюс экспортируемый алгоритм, а четвертая включает Clipper, внутренний и экспортируемый алгоритмы. Для каждого телефонного звонка TSD используют отличный сеансовый ключ. Пара TSD генерирует сеансовый ключ с помощью схемы обмена ключами Diffie-Hellman, независящей от микросхемы Clipper. Так как Diffie-Hellman не включает проверки подлинности, TSD использует два метода для предотвращения вскрытия "человек в середине".

TSD хэширует сеансовый ключ и выводит хэш-значение на маленьком экране в виде четырех шестнадцатеричных цифр. Собеседники проверяют, что на их экраны выведены одинаковые цифры . TSD генерирует случайные числа, используя источник шума и хаотичный усилитель с цифровой обратной связью.

Он генерирует битовый поток, который пропускается через постотбеливающий фильтр на базе цифрового процессора.
NSA - это Агентство национальной безопасности (National Security Agency, когда-то расшифровывалось шутниками как "No Such Agency" (никакое агентство) или "Never Say Anything" (никогда ничего не скажу), но теперь они более открыты), официальный орган правительства США по вопросам безопасности . Агентство было создано в 1952 году президентом Гарри Труменом в подчинении Министерства безопасности , и многие годы в секрете хранилось сам факт его существования. NSA воспринималось как электронная разведка, в его задачи входило подслушивать и расшифровывать все иностранные линии связи в интересах Соединенных Штатов. NSA ведет исследования в области криптологии, занимаясь как разработкой безопасных алгоритмов для з а- щиты коммуникаций Соединенных Штатов, так и криптоаналитические методы для прослушивания коммун и- каций за пределами США. NSA разработало ряд криптографических модулей различного назначения .

В этих модулях для различных приложений используются различные алгоритмы , и производители получают возможность извлечь один модуль и вставить другой в зависимости от желаний клиента . Существуют модули для военного использования (Тип I), модули для "несекретного, но важного" правительственного использования (Тип II), модули для корпоративного использования (Тип III) и модули для экспортирования (Тип IV). Национальный центр компьютерной безопасности (National Computer Security Center, NCSC), отделение NSA, отвечает за доверенную правительственную компьютерную программу, проводит оценку продуктов компьютерной безопасности (программных и аппаратных), финансирует исследования и публикует их результаты, разрабатывает технические руководства и обеспечивает общую поддержку и обучение. NCSC издает скандально известную "Оранжевую книгу". Ее настоящее название - Department of Defense Trusted Computer System Evaluation Criteria (Критерии оценки департамента оборонных доверенных компьютерных систем).

Классификация Оранжевой книги

D: Minimal Security (Минимальная безопасность)
C: Discretionary Protection (Защита по усмотрению)
C1: Discretionary Security Protection (Защита безопасности по усмотрению)
C2: Controlled Access Protection (Защита управляемого доступа)
B: Обязательная защита
B1: Labeled Security Protection
B2: Structured Protection (Структурная защита)
B3: Security Domains (Области безопасности)
A: Verified Protection (Достоверная защита)
A1: Verified Design (Достоверная разработка)

NIST - это Национальный институт стандартов и техники (National Institute of Standards and Technology), подразделение Министерства торговли США. Официальные стандарты опубликованы как издания FIPS (Федеральные стандарты обработки информации.

RSA Data Security, Inc. (RSADSI) была основана в 1982 году для разработки, лицензирования и коммерческого использования патента RSA. Имеет ряд коммерческих продуктов: пакет безопасности электронной почты, различные криптографические библиотеки. RSADSI также предлагает на рынке симметричные

Пять патентов принадлежат Public Key Partners (PKP) из Саннивэйла (Sunnyvale), Калифорния, партнерству RSADSI и Care-Kahn, Inc. - родительской компании Cylink.

Патенты Public Key Partners

№ патента	Дата	Изобретатели	Название патента
4200770	29.3.80	Hellman, Diffie, Merkle	Обмен ключами Diffie-Hellman
4218582	19.8.80	Hellman, Merkle	Рюкзаки Merkle-Hellman
4405829	20.9.83	Rivest, Shamir, Adleman	RSA
4424414	3.3.84	Hellman, Pohlig	Pohlig-Hellman
4995082	19.2.91	Schnorr	Подписи Schnorr

Международная ассоциация криптологических исследований (International Association for Cryptologic Research, IACR) - это всемирная криптографическая исследовательская организация . Ее целью является развитие теории и практики криптологии и связанных областей. Ее членом может стать любой. Ассоциация выступает спонсором двух ежегодных конференций, Crypto (проводится в августе в Санта-Барбаре) и Eurocrypt (проводится в в Европе), и ежеквартально издает The Journal of Cryptology и IACR Newsletter.

Программа исследования и развития передовых средств связи в Европе (Research and Development in Advanced Communication Technologies in Europe, RACE) была инициирована Европейским сообществом для поддержки предварительной проработки телекоммуникационных стандартов и технологий, поддерживающих Интегрированные высокоскоростные средства связи (Integrated Broadband Communication, IBC). В качестве части этой работы RACE учредило консорциум для Оценки примитивов целостности RACE (RACE Integrity Primitives Evaluation, RIPE), чтобы собрать в одно целое пакет технологий, соответствующих возможным требованиям к безопасности IBC. Консорциум RIPE образовали шесть ведущих европейских криптографических исследовательских групп

Условный доступ для Европы (Conditional Access for Europe, CAFE) - это проект в рамках программы ESPRIT Европейского сообщества 92-95 гг. Основным устройством CAFE служит **электронный бумажник**: маленький компьютер, очень похожий на карманный калькулятор

У него есть батарейка, клавиатура, экран и инфракрасный канал для связи с другими бумажниками. У каждого пользователя свой собственный бумажник , который обеспечивает его права и гарантирует его безопасность. Пользователь может непосредственно ввести свой пароль и сумму платежа. Отличие от кредитной карты пользователю не нужно отдавать свой бумажник кому-то, чтобы вы полнить транзакцию. Дополнительными возможностями являются: — Автономные транзакции. Система предназначена для замены обращения небольших сумм наличных, диалоговая система была бы слишком громоздка. — Устойчивость к потерям. Если пользователь потеряет свой бумажник, или бумажник сломается, или его украдут, пользователь не потеряет свои деньги. — Поддержка различных валют. — Открытая архитектура и открытая система. Пользователь должен иметь возможность заплатить за произвольные услуги., предоставляемые различными поставщиками. Система должна обеспечивать взаимодействие любого количества эмитентов электронных денег, а также взаимодействие бумажников различных типов и производителей . — Низкая стоимость

Профессиональные и промышленные группы, а также группы защитников гражданских свобод. Информационный центр по электронной тайне личности (Electronic Privacy Information Center, EPIC) был учрежден в 1994 году для привлечения общественного внимания к возникающим вопросам тайн личности, связанным с Национальной информационной инфраструктурой , таких как микросхемы Clipper, предложения по цифровой телефонии, национальные системы идентификационных номеров, тайны историй болезни и продажа сведений о потребителях.
Фонд электронного фронтира (Electronic Frontier Foundation, EFF) посвятил себя защите гражданских прав в киберпространстве. Рассматривая криптографическую политику США, EFF считает, что информация и доступ к криптографии являются фундаментальными правами, и поэтому с них должны быть сняты правительственные ограничения. Фонд организовал рабочую группу по цифровой безопасности и тайне личности (Digital Privacy and Security Working Croup), которая является коалицией 50 организаций и противодействует закону о цифровой телефонии. EFF также содействует ведению процессов против контроля за экспортом криптографии

Ассоциация по вычислительной технике (Association for Computing Machinery, ACM) - это международная компьютерная промышленная организация.

Институт инженеров по электричеству и радиоэлектронике (Institute of Electrical and Electronics Engineers , IEEE) - это другая профессиональная организация. Отделение в США изучает вопросы, связанные с тайной личности, включая криптографическую политику, идентификационные номера, и защита тайн в Internet, и разрабатывает соответствующие рекомендации.

Ассоциация производителей программного обеспечения (Software Publishers Association, SPA) - это торговая ассоциация, в которую входят свыше 1000 компаний, разрабатывающих программное обеспечение для персональных компаний. Они выступают за ослабление экспортного контроля в криптографии и поддерживают перечень коммерчески доступных зарубежных продуктов.

Sci.crypt - это телеконференция Usenet по криптологии. Ее читают примерно 100000 человек по всему миру .

Шифропанки (Cypherpunks) - это неформальная группа людей, заинтересованных в обучении и изучении криптографии. Они также экспериментируют с криптографией, пытаясь ввести ее в обиход. Согласно правительству США криптография относится к военному снаряжению . Это означает, что крипто- графия подчиняется тем же законам, что и ракета TOW или танк M1 Абрамс. Если вы продаете криптографический продукт без соответствующей экспортной лицензии, то вы - международный контрабандист оружием.
С началом в 1949 году холодной войны все страны НАТО (кроме Исландии), а затем Австралия, Япония и Испания, образовали КОКОМ - Координационный комитет для многостороннего контроля за экспортом (CoCom, Coordinating Committee for Multilateral Export Controls). Это неофициальная организация, призванная координировать национальные ограничения, касающиеся экспорта важных военных технологий в Советский Союз, страны Варшавского Договора и КНР .

Примерами контролируемых технологий являются компьютеры, станки для металлопроката и криптография .
Целью этой организации являлось замедление передачи технологий в указанные страны, и сдерживание, таким образом, их военного потенциала.
Правовые вопросы Являются ли цифровые подписи настоящими подписями? Будут ли они признаны судом? Некоторые предварительные правовые исследования привели к мнению, что цифровые подписи будут соответствовать требованиям законных подписей для большей части применений, включая коммерческое использование. В Соединенных Штатах законы о подписях, контрактах и торговых операциях находятся в юрисдикции штатов.