Лекция

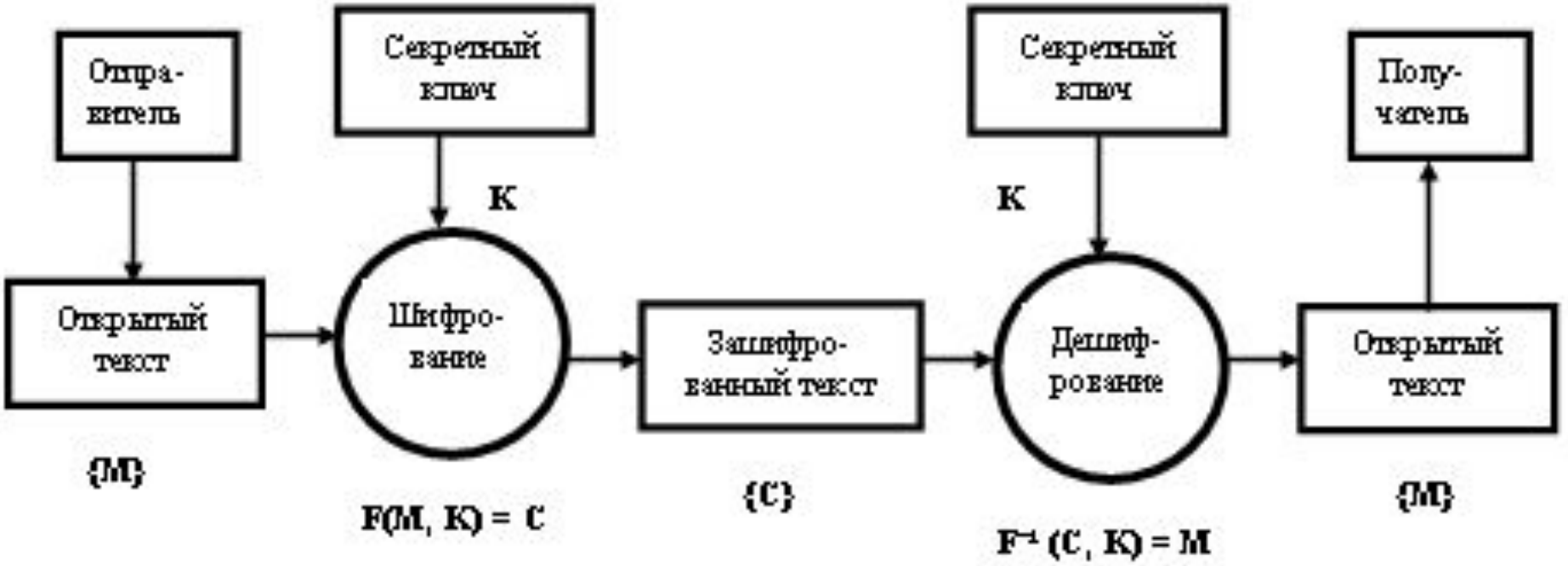
Вопросы информационной безопасности в Интернет

Информационная безопасность включает следующие понятия:

- Конфиденциальность;
- Аутентификация;
- Целостность сообщения;
- Управление доступом.

Методы шифрования

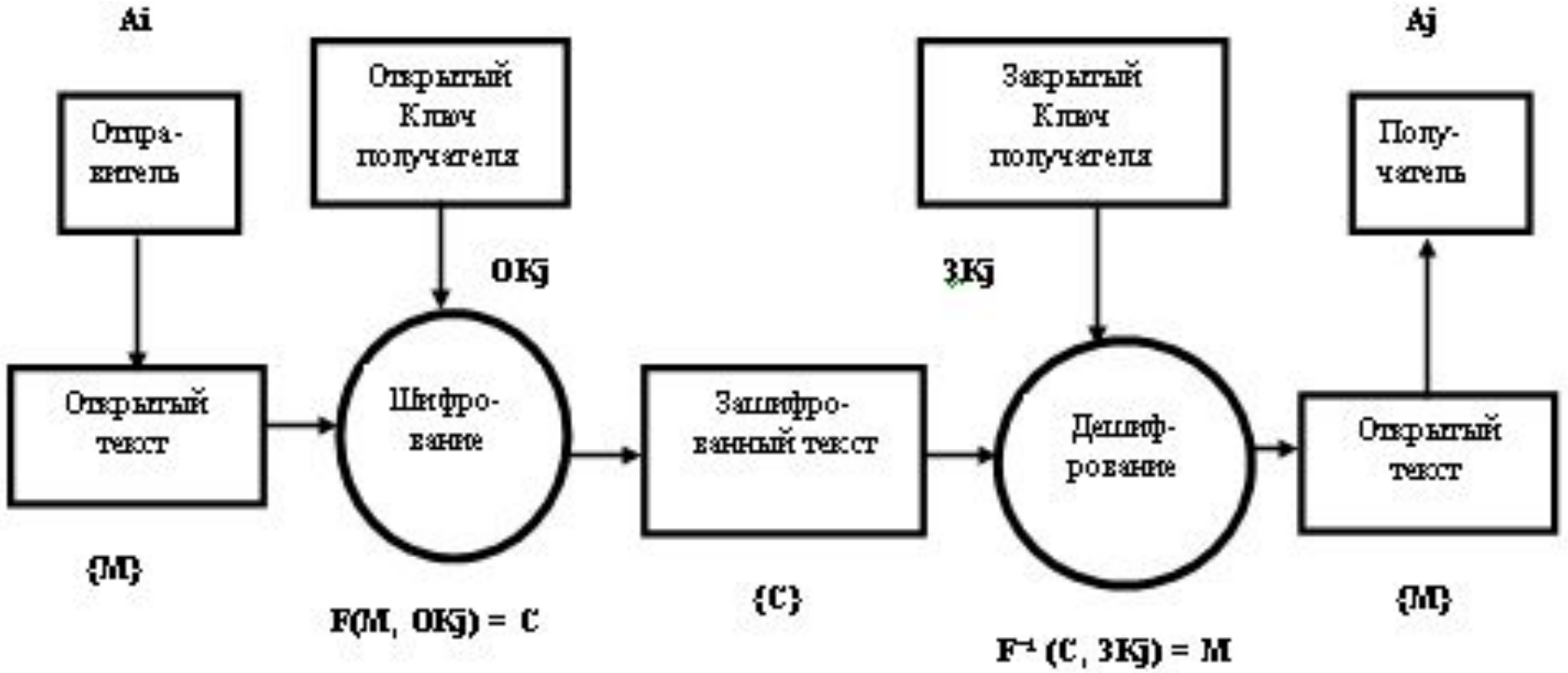
- 1. **Симметричные ключи** (системы с общим секретным ключом).



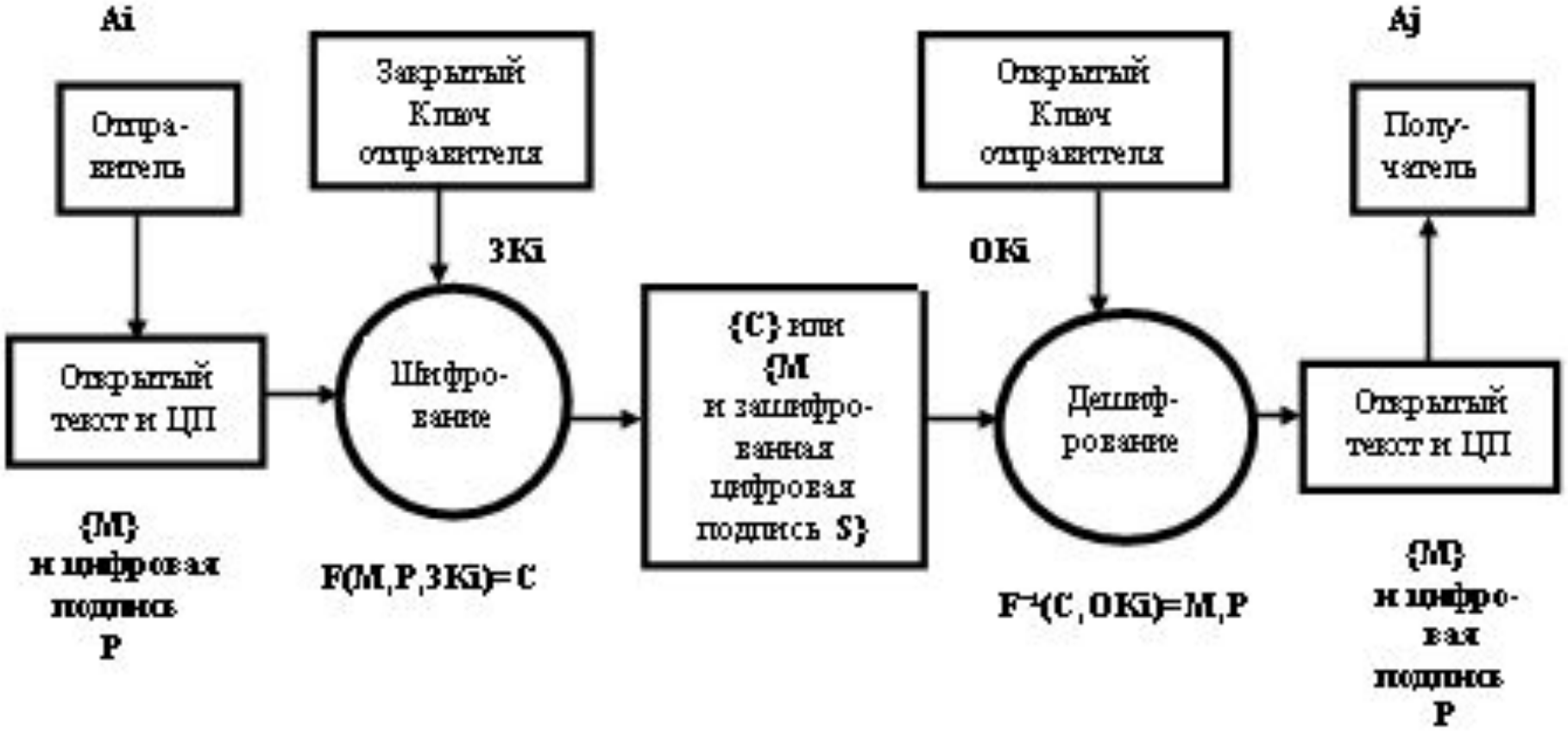
Методы шифрования

- 1. **Симметричные ключи** (системы с общим секретным ключом).

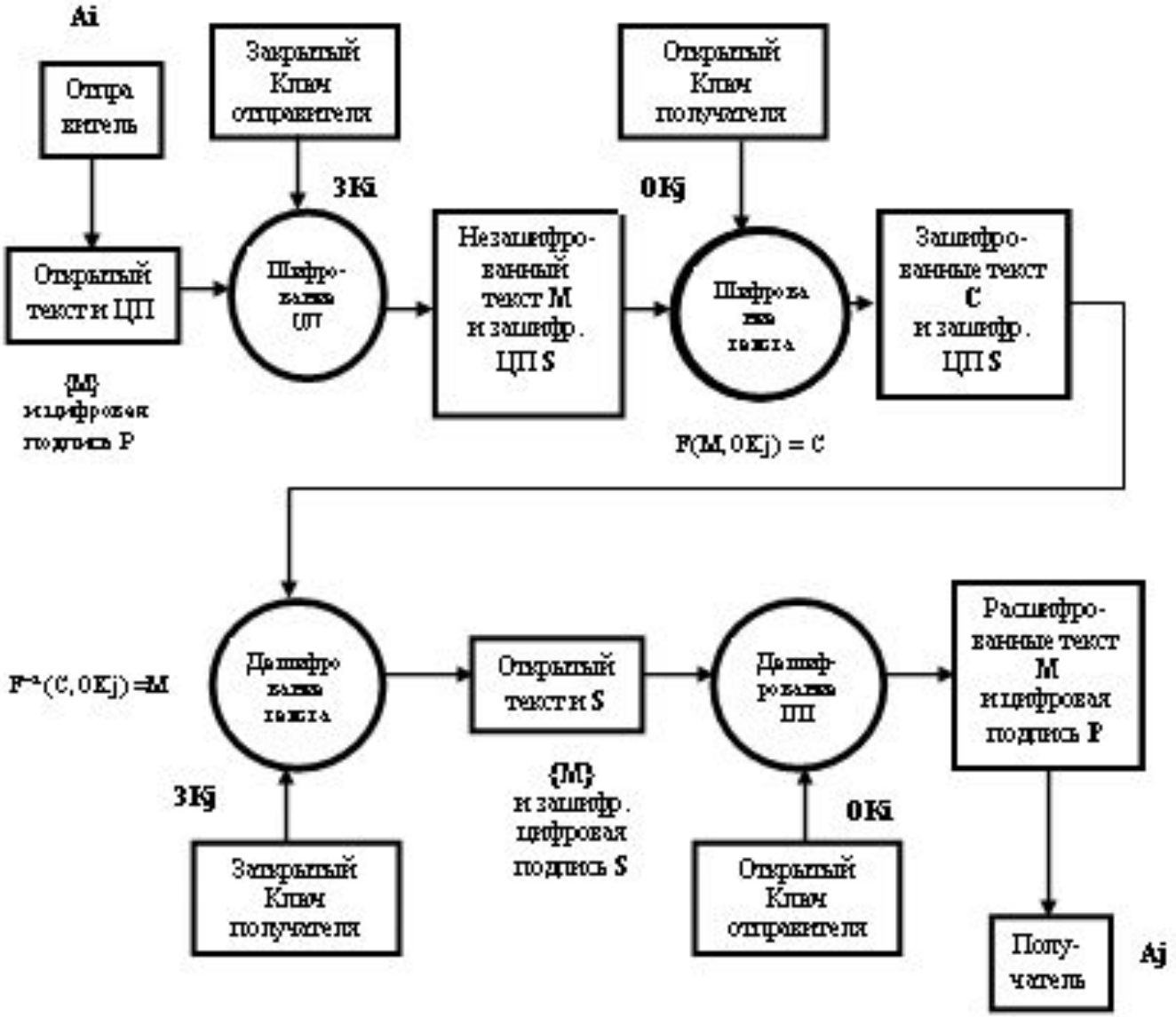
Шифрование текста



Цифровая подпись

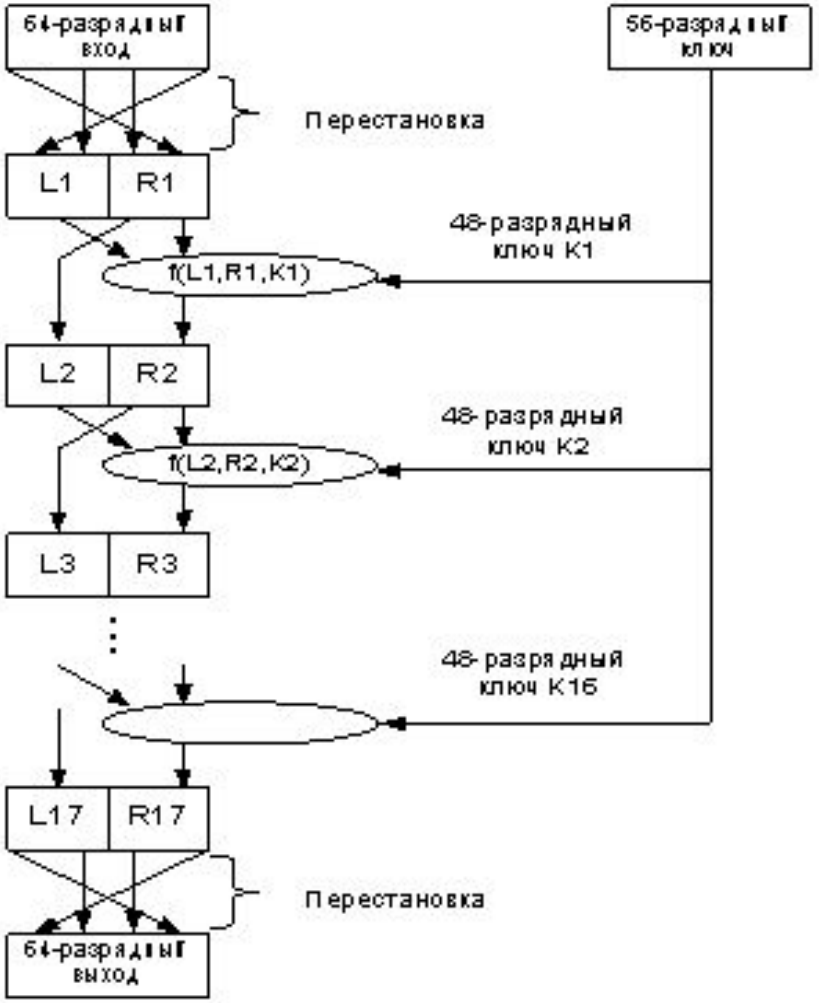


Цифровая подпись и шифрование текста



Алгоритмы шифрования

- Стандарт DES.



Основные операции алгоритма DES

- Стандарты FEAL-N и FEAL-NX, 1989 г.
  N – число внутренних циклов (итераций), длина ключей – 64 и 128 бит.
- ГОСТ 28147-89, СССР, принят в 1989г., впервые опубликован в 1992г., длина ключа – 256 бит.

Основные достоинства аппаратных шифраторов:

- гарантия неизменности алгоритма шифрования
- наличие аппаратного датчика случайных чисел, используемого при создании криптографических ключей
- возможность прямой загрузки ключей шифрования в специализированный процессор аппаратного шифратора с персональных идентификаторов - носителей типа смарт-карт
- хранение ключей шифрования в памяти шифропроцессора
- выполнение опций, именуемых функциями "электронного замка «
- возможность разгрузки центрального процессора

Алгоритмы электронной цифровой подписи

Впервые идею ЭЦП предложили в 1976г. У. Диффи и М. Хеллман, Стенфордский университет, США. В основе алгоритма – общий секретный ключ.

Стандарт RSA, 1977г., Массачусетский Технологический институт США. В основе алгоритма – открытый и закрытый (секретный) ключи.

Метод Эль Гамаля, 1985г., США. В основе алгоритма – идея дискретного логарифмирования.

ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного алгоритма».

Безопасность глобальной сети Internet

Аутентификация в протоколах IP

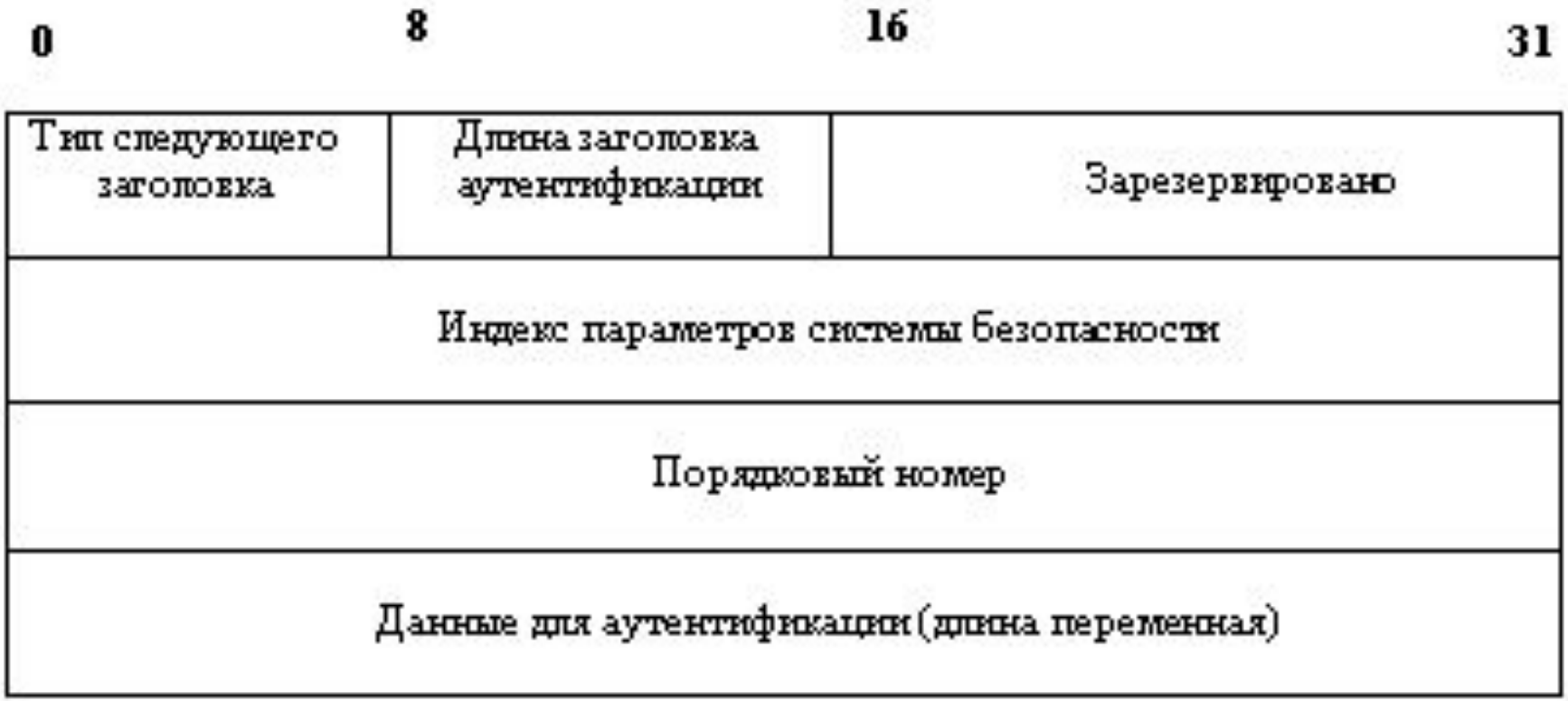
Заголовок IPv4	Заголовок TCP	Данные протокола IP

(а)

Заголовок IPv4	Заголовок аутентификации	Заголовок TCP	Данные протокола IP

(б)

Формат заголовка аутентификации



Использование программы PGP для шифрования сообщений электронной почты

PGP (Pretty Good Privacy) – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности.

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи, т.к. эта программа построена на принципе публичной криптографии или обмене открытыми (публичными) ключами.

Пользователи могут в открытом виде посылать друг другу свои публичные ключи с помощью сети Интернет и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

PGP шифрует сообщение таким образом, что никто кроме получателя сообщения, не может ее расшифровать. Создатель PGP Филипп Циммерман открыто опубликовал код программы, который неоднократно был исследован специалистами-криптоаналитиками высочайшего класса и ни один из них не нашел в программе каких-либо слабых мест

Как работает PGP

Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку сообщения (например, через модем) и увеличивает надежность шифрования. Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании "рисунков", присущих текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти "рисунки" и таким образом повышает надежность зашифрованного сообщения.

Затем PGP генерирует сессионный ключ, который представляет собой случайное число, созданное за счет движений вашей мышки и нажатий на клавиши клавиатуры.

Как только данные будут зашифрованы, сессионный ключ зашифровывается с помощью публичного ключа получателя сообщения и отправляется к получателю вместе с зашифрованным текстом.

Расшифровка происходит в обратной последовательности. Программа PGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует зашифрованный текст.

Ключи

Ключ - это число, которое используется криптографическим алгоритмом для шифрования текста. Как правило, ключи - это очень большие числа. Размер ключа измеряется в битах. Число, представленное 1024 битами - очень большое. В публичной криптографии, чем больше ключ, тем его сложнее взломать.

В то время как открытый и закрытый ключи взаимосвязаны, чрезвычайно сложно получить закрытый ключ исходя из наличия только открытого ключа, однако это возможно при наличии большой компьютерной мощности. Поэтому крайне важно выбирать ключи подходящего размера: достаточно большого для обеспечения безопасности и достаточно малого для обеспечения быстрого режима работы. Более большие ключи будут более надежными в течение более длительного срока времени. Поэтому если вам необходимо зашифровать информацию с тем, чтобы она хранилась в течение нескольких лет, то необходимо использовать более длинный ключ.

Ключи хранятся на жестком диске вашего компьютера в зашифрованном состоянии в виде двух файлов: одного для открытых ключей, а другого – для закрытых. Эти файлы называются "кольцами" (keyrings). В течение работы с программой PGP вы, как правило, будете вносить открытые ключи ваших корреспондентов в открытые "кольца". Ваши закрытые ключи хранятся в вашем закрытом "кольце".

Цифровая подпись

Огромным преимуществом публичной криптографии также является возможность использования цифровой подписи, которая позволяет получателю сообщения удостовериться в личности отправителя сообщения, а также в целостности (верности) полученного сообщения.

Цифровая подпись исполняет ту же самую функцию, что и ручная подпись. Однако ручную подпись легко подделать. Цифровую же подпись почти невозможно подделать.

Для определения целостности полученного сообщения используется хеш-функция. В чем-то она похожа на "контрольную сумму", или код проверки ошибок CRC, который компактно представляет сообщение и используется для проверки сообщения на наличие изменений.

Хеш-функция

"Хэш-функция" действует таким образом, что в случае какого-либо изменения информации, пусть даже на один бит, результат "хэш-функции" будет совершенно иным. С помощью "хэш-функции" и закрытого ключа создается "подпись", передаваемая программой вместе с текстом.

При получении сообщения получатель использует PGP для восстановления исходных данных и проверки подписи.

При условии использования надежной формулы "хэш-функции" невозможно вытащить подпись из одного документа и вложить в другой, либо каким-то образом изменить содержание сообщения. Любое изменение подписанного документа сразу же будет обнаружено при проверке подлинности подписи.

Парольная фраза

Еще одним средством защиты в PGP является парольная фраза.

Парольная фраза - это сочетание нескольких слов, которое теоретически более надежно, чем парольное слово. Парольная фраза должна быть такой, чтобы ее потом не забыть и чтобы третьи лица не могли ее разгадать.

Если вы забудете свою парольную фразу, то уже никогда не сможете восстановить свою зашифрованную информацию. Ваш закрытый ключ абсолютно бесполезен без знания парольной фразы.

Генерация ключей

1. Нажмите кнопку "ПУСК" и выберете команду "Выполнить". Выберете программу PGPKEYS.

2. Зайдите в меню KEYS и выполните команду NEW KEY.

- Нажмите на «Далее»
- Введите свое имя и электронный адрес
- Нажмите на «Далее»
- Выберите размер ключа 2048 или 1024 и нажмите на «Далее»
- Выделите фразу key pair never expires (срок действия ключевой пары никогда не истекает) и нажмите на «Далее»
- Два раза введите секретный пароль и нажмите на «Далее»

Программа начнет генерировать пару ключей. Если программе не хватает информации, то она может попросить нажать на несколько клавиш наугад и подвигать мышку. Это необходимо выполнить.

Затем программа сообщит, что процесс генерации ключей закончен.

- Нажмите на «Далее»
- Потом еще раз нажмите на «Далее»
- Затем нужно нажать на команду Done

На этом процесс создания пары ключей закончился и можно начинать пользоваться программой.

3. Обменяйтесь со своими корреспондентами открытыми ключами. Для этого необходимо исполнить команду LAUNCH PGP KEYS, выделить свой ключ (файл со своим именем) в окошке, нажать на правую кнопку мышки и выбрать команду EXPORT.

Появится окошко, с помощью которого можно указать путь, где сохранить файл с названием <ваше_имя.asc>.

Этот файл необходимо выслать своему корреспонденту, в обмен на его открытый ключ.

Как только вы получите открытый ключ своего корреспондента, надо его запустить, нажав на него двойным щелчком мышки, выделить его в окошке и выполнить команду IMPORT.

4. Теперь можно пересылать друг другу зашифрованные сообщения, которые шифруются открытым ключом получателя сообщения.

Свой открытый ключ можно поместить на специальном сервере, тогда он будет доступен всем желающим вести с вами переписку. Программа PGP сама предлагает вам выбрать, как сообщить корреспондентам свой общедоступный ключ - храня его на сервере или послав письмом.