10.05.03 Информационная безопасность автоматизированных систем

Защита информации в сетях. Протоколы аутентификации

Информационная безопасность

- **Информационная безопасность –** состояние защищенности информационной системы, включая саму информацию и поддерживающую её инфраструктуру.
- Информационная система находится в **состоянии защищённости,** если обеспечены её конфиденциальность, доступность и целостность
- **Конфиденциальность –** гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешён (авторизованным пользователям)
- **Доступность –** гарантия того, что авторизованные пользователи всегда получат доступ к данным
- **Целостность –** гарантия сохранности данными правильности значений

Информационная безопасность

? Политика информационной безопасности

1. Минимальный уровень привилегий на доступ к данным, который необходим
2. Единая точка обмена с зоной public
3. Баланс надёжности защиты всех уровней
4. Используемые средства при отказе должны переходить в режим максимальной защиты
5. Баланс возможного ущерба от реализации угрозы и затрат на её предотвращение

Информационная безопасность

- Сетевой, или межсетевой экран (брэндмауэр, файрволл) – это комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части сети от другой путём анализа проходящего между ними трафика

Информационная безопасность

? Функции фаервола:

1. Анализ, контроль и регулирование трафика (функция фильтрации)
2. Роль посредника между внутренними и внешними серверами (функция прокси-сервера)
3. Фиксирование всех событий (функция аудита)

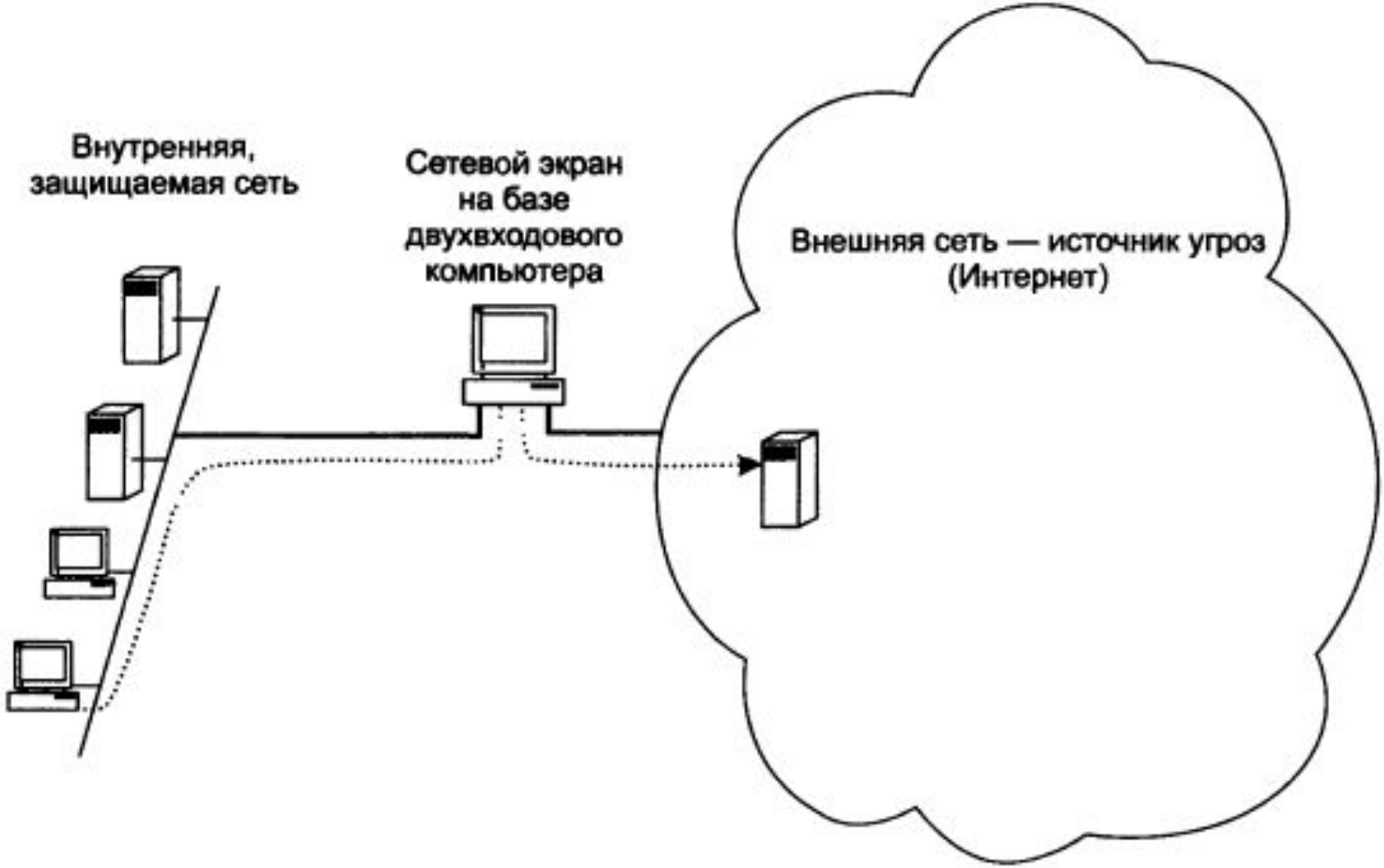
? Дополнительные функции:

1. Антивирусная защита
2. Шифрование трафика
3. Фильтрация сообщений по содержимому
4. Предупреждение и обнаружение вторжений и атак
5. Функции VPN
6. Трансляция сетевых адресов

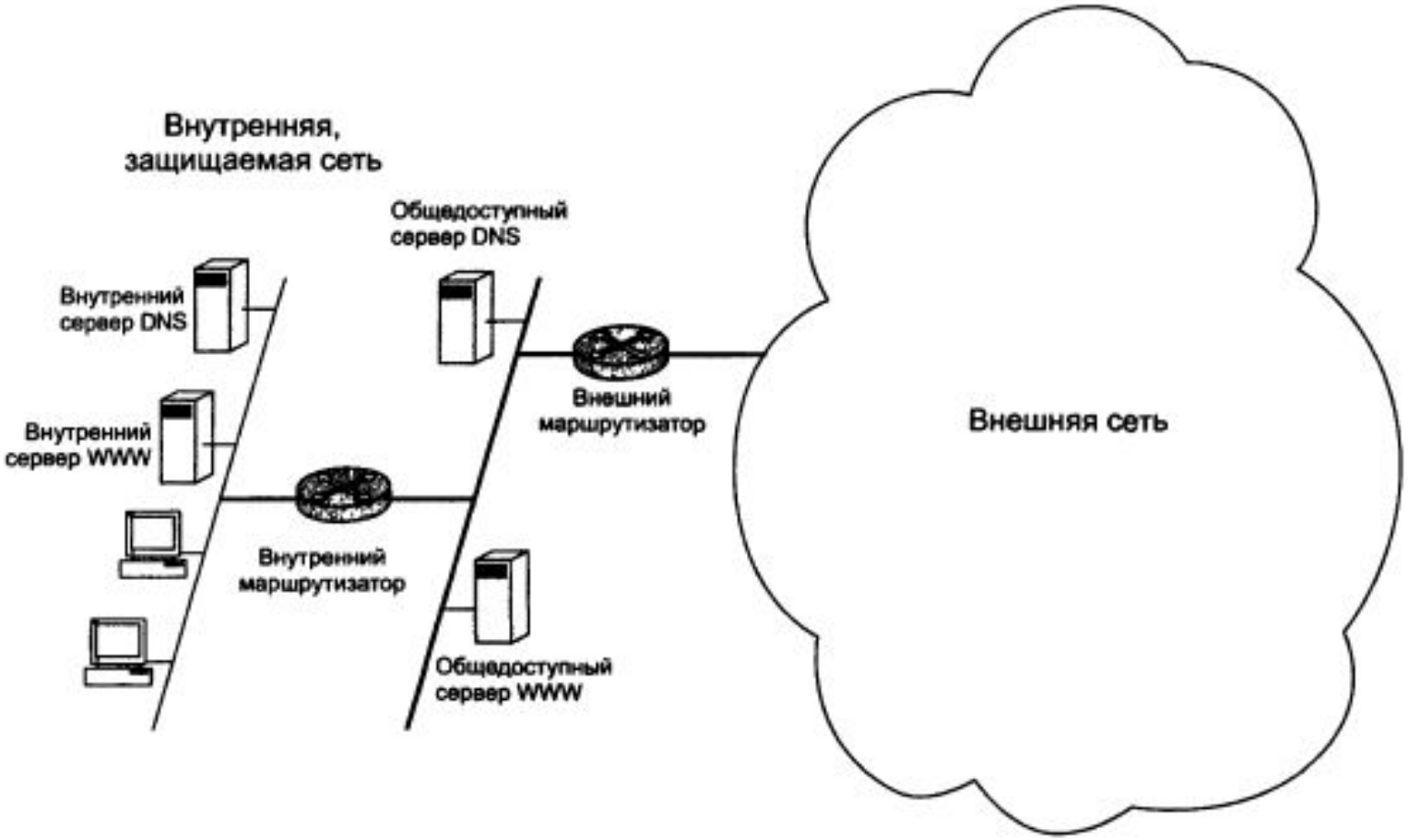
Информационная безопасность

- Сетевые экраны сетевого уровня (экраны с фильтрацией пакетов)
- Сетевые экраны сеансового уровня (с отслеживанием состояния соединений, фильтрация с учетом контекста)
- Сетевые экраны прикладного уровня

Информационная безопасность



Информационная безопасность

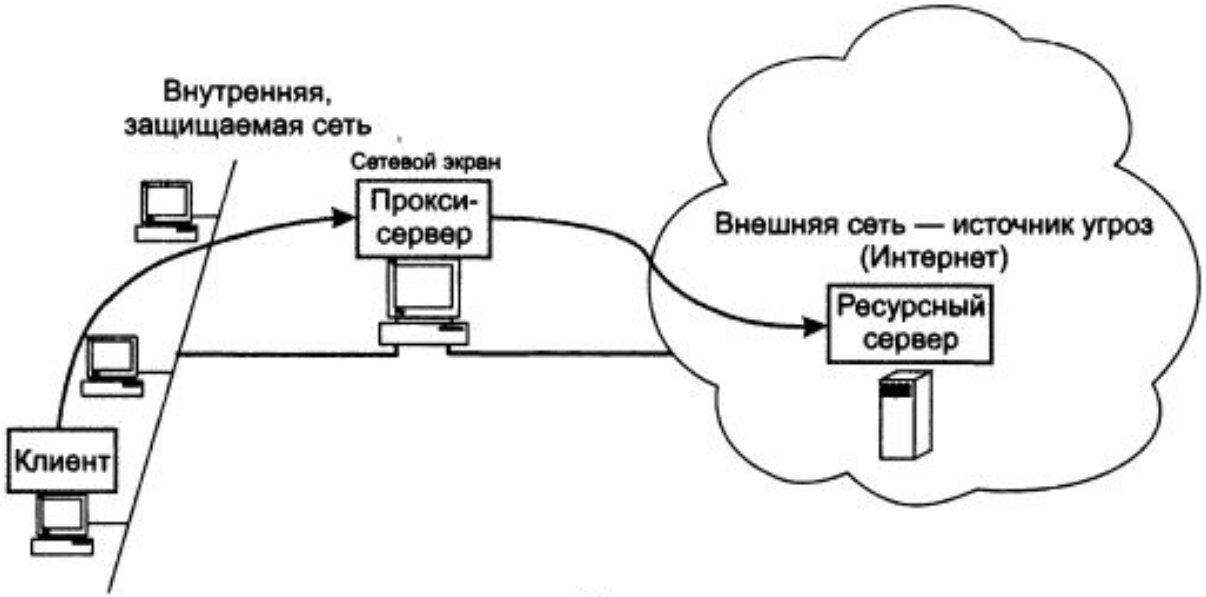


Информационная безопасность

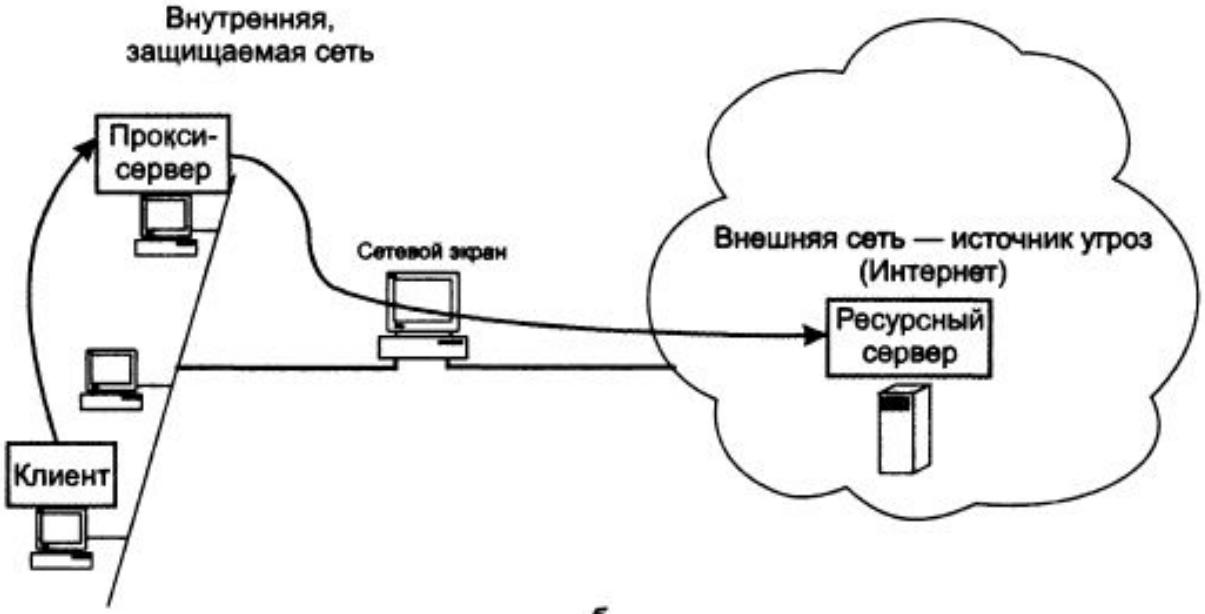
- Сеть периметра, или демилитаризованная зона (DMZ) –сеть между внешней и внутренней сетями
- Внешний маршрутизатор имеет свою политику безопасности, менее строгую и рассчитанную на активное взаимодействие с внешней сетью
- Внутренний маршрутизатор может иметь более строгую политику безопасности

Информационная безопасность

- Прокси-сервер – тип приложения, выполняющего роль посредника между клиентскими и серверными частями распределённых приложений.
- Прокси-сервера бывают прикладного уровня и уровня соединений


Внутренняя,
защищаемая сеть
Сетевой экран
Прокси-
сервер
Внешняя сеть — источник угроз
(Интернет)
Ресурсный
сервер
Клиент

а


Внутренняя,
защищаемая сеть
Прокси-
сервер
Сетевой экран
Внешняя сеть — источник угроз
(Интернет)
Ресурсный
сервер
Клиент

б

AAA

- Аутентификация
- Авторизация
- Аудит

- Аутентификация пользователя – это процедура доказательства пользователем того, что он подлинный

- Аутентификация, в процессе которой используются методы шифрования, а аутентификационная информация не передаётся по сети, называется строгой

AAA

- Аутентификация на уровне приложений
- Аутентификация устройств
- Аутентификация данных

AAA

- **Авторизация** – это процедура контроля доступа легальных пользователей к ресурсам системы и предоставление каждому из них именно тех прав, которые были ему определены администратором

- **Избирательный доступ** – с явным указанием идентификатора
- **Мандатный подход** – в соответствии с уровнем допуска

AAA

- **Централизованная схема на базе сервера -** принцип «единого входа». Kerberos, TACACS, RADIUS

- **Децентрализованная схема**

AAA

- **Аудит –** это набор процедур мониторинга и учета всех событий, представляющих потенциальную угрозу для безопасности системы

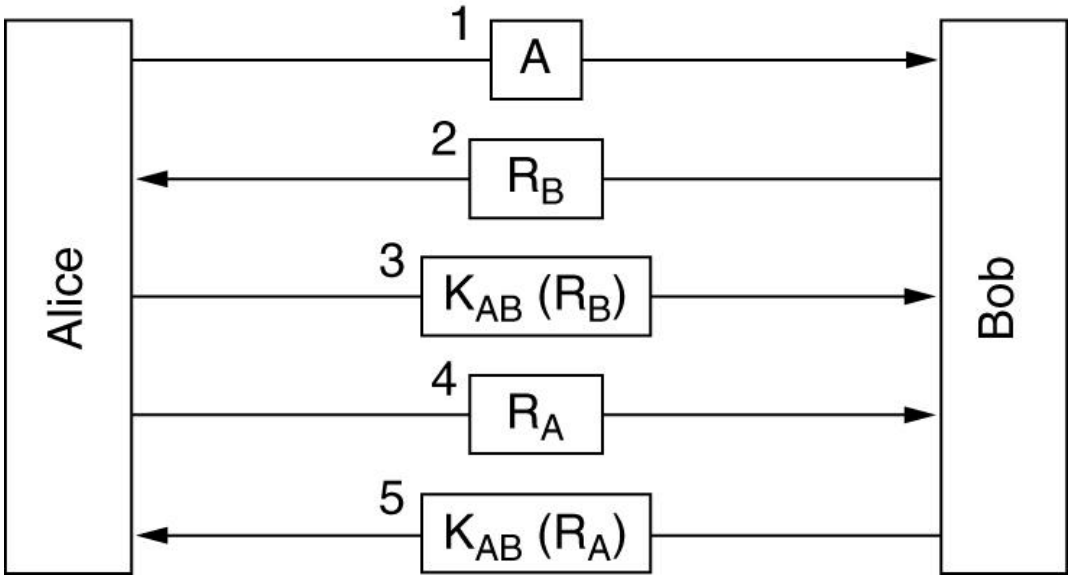
AAA

- Общая схема протоколов аутентификации:
- Алиса хочет установить защищенное соединение с Бобом или считающимся надёжным Центром распространения ключей
- Посылается определённая последовательность различных сообщений в разных направлениях, осле завершения работы протокола Алиса должна быть уверена что говорит с Бобом и обратно.
- Так же должен быть установлен ключ сеанса

Аутентификация на базе общего секретного ключа

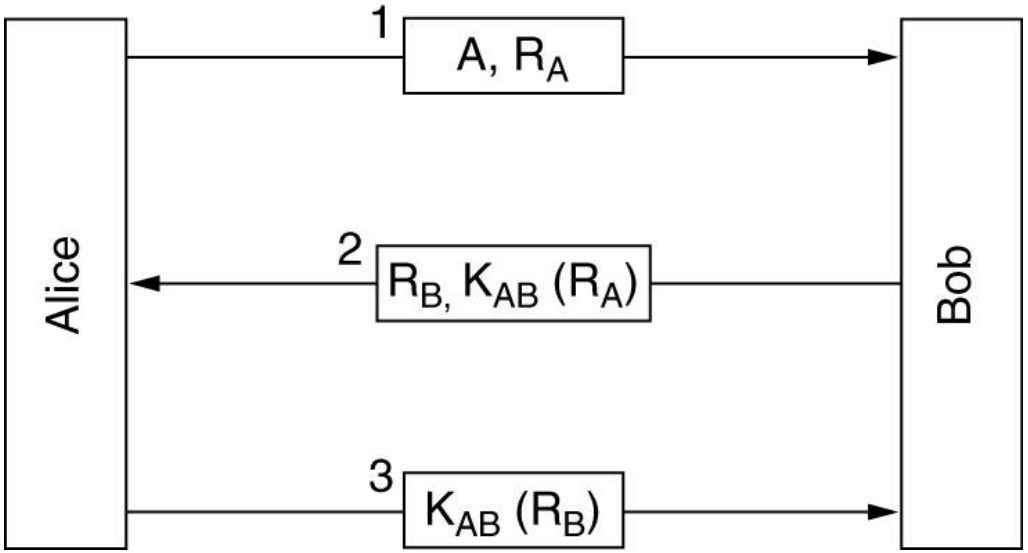
- Пусть есть общий секретный ключа Kab
- Принцип: одна сторона генерирует случайное число, вторая сторона его преобразует и отправляет обратно
- Протоколы типа отклик-отзыв

Аутентификация на базе общего секретного ключа



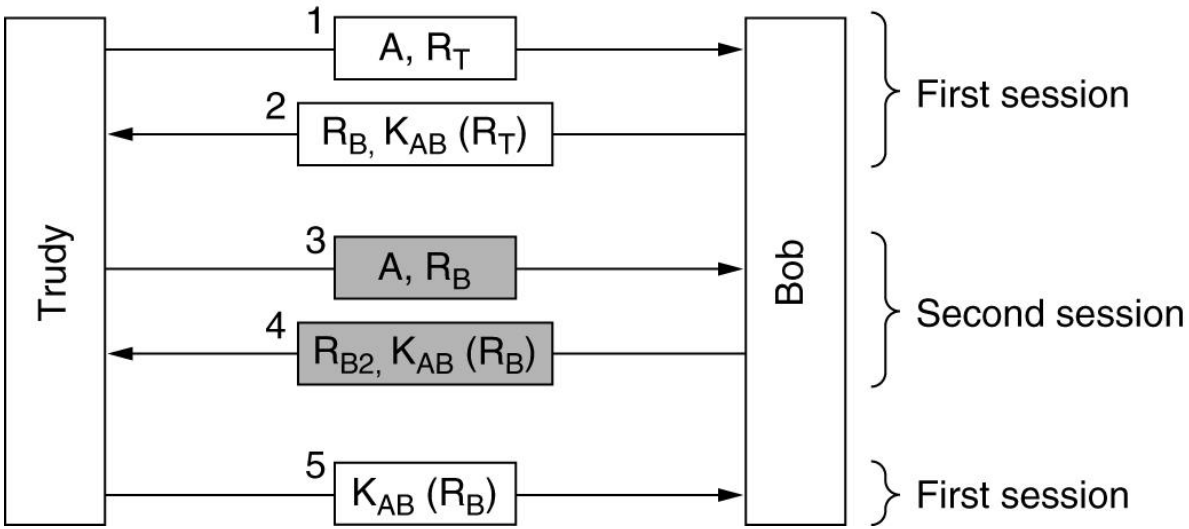
- Two-way authentication using a challenge-response protocol.

Аутентификация на базе общего секретного ключа



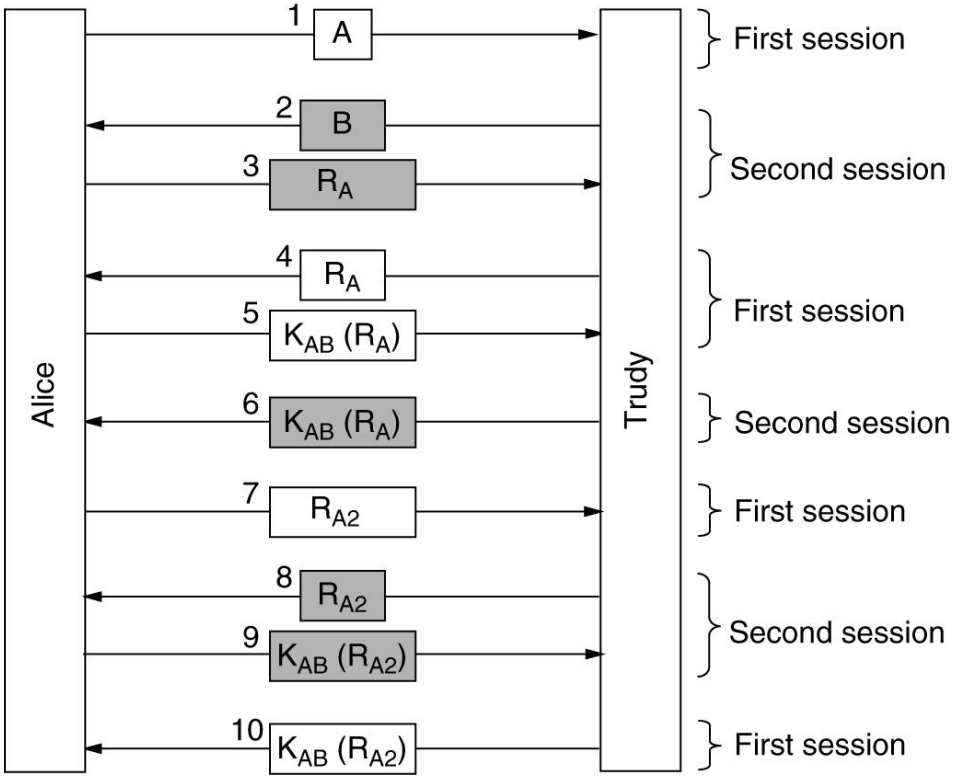
A shortened two-way authentication protocol.

Аутентификация на базе общего секретного ключа



The reflection attack. Зеркальная атака

Аутентификация на базе общего секретного ключа



Аутентификация на базе общего секретного ключа

? Правила, применимые при разработке протокола аутентификации:

1. Инициатор сеанса должен подтверждать своб сущность первым
2. Следует использовать 2 раздельных общих секретных ключа Kab и K’ab
3. Инициатор и отвечающий должны выбирать оклики из различных непересекающихся наборов
4. Протокол должен противостоять атакам с повторным сеансом

Аутентификация на базе общего секретного ключа

- **HMAC** (сокращение от англ. hash-based message authentication code, хеш-код идентификации сообщений). Наличие способа проверить целостность информации, передаваемой или хранящийся в ненадежной среде является неотъемлемой и необходимой частью мира открытых вычислений и коммуникаций. Механизмы, которые предоставляют такие проверки целостности на основе секретного ключа, обычно называют кодом аутентичности сообщения (MAC). Как правило, MAC используется между двумя сторонами, которые разделяют секретный ключ для проверки подлинности информации, передаваемой между этими сторонами. Этот стандарт определяет MAC. Механизм, который использует криптографические хеш-функции в сочетании с секретным ключом называется HMAC.

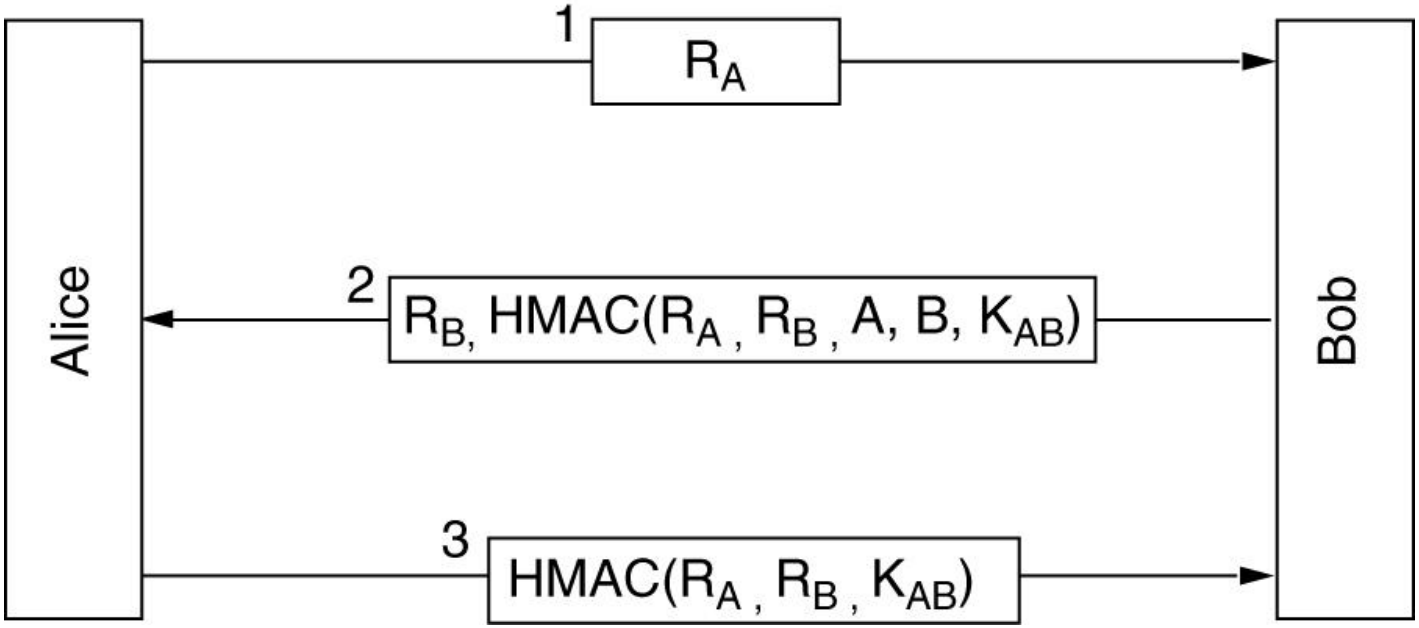
Аутентификация на базе общего секретного ключа

- Основная цель:
- Для того чтобы можно было использовать имеющиеся хэш-функции без изменений, в частности, хэш-функций, которые уже есть в программном продукте, и их код уже доступен.
- Чтобы сохранить первоначальное исполнение хэш-функции без каких нибудь значительных ухудшений
- Использовать и обрабатывать ключи более простым способом.
- Для легкой заменяемости базовой хэш-функции в том случае, если более быстрая и более безопасная хэш-функция будет доступна позже.
- Разработчики: Хьюго Кравчик, Михир Беллар и Ран Каннетти.

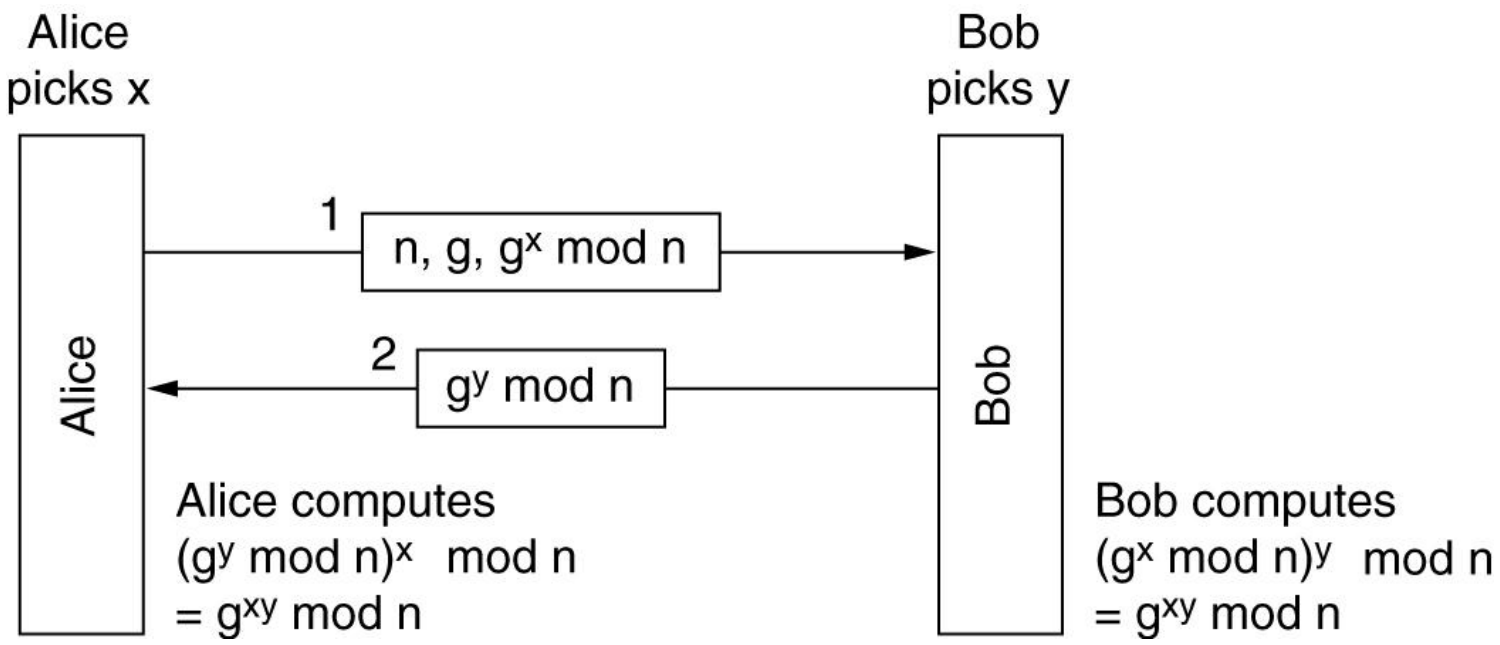
Аутентификация на базе общего секретного ключа

- В последние годы наблюдается повышенный интерес к разработке MAC на основе криптографических хэш-функций, например, MD5, SHA-1 или RIPEMD-160. А мотивы этого интереса просты:
- Криптографические хэш-функции обычно в программах работают быстрее, чем при использовании симметричных блочных шифров, такие как DES.
- Библиотечные коды для криптографической хэш-функции широко доступны.
- Хэш-функции, такие как MD5, не предназначены для использования в качестве MAC и не могут быть использованы непосредственно для этой цели, поскольку они не опираются на секретный ключ. Было сделано несколько предложений для включения секретного ключа в существующие хэш-алгоритмы. HMAC получил наибольшую поддержку.

Аутентификация на базе HMAC

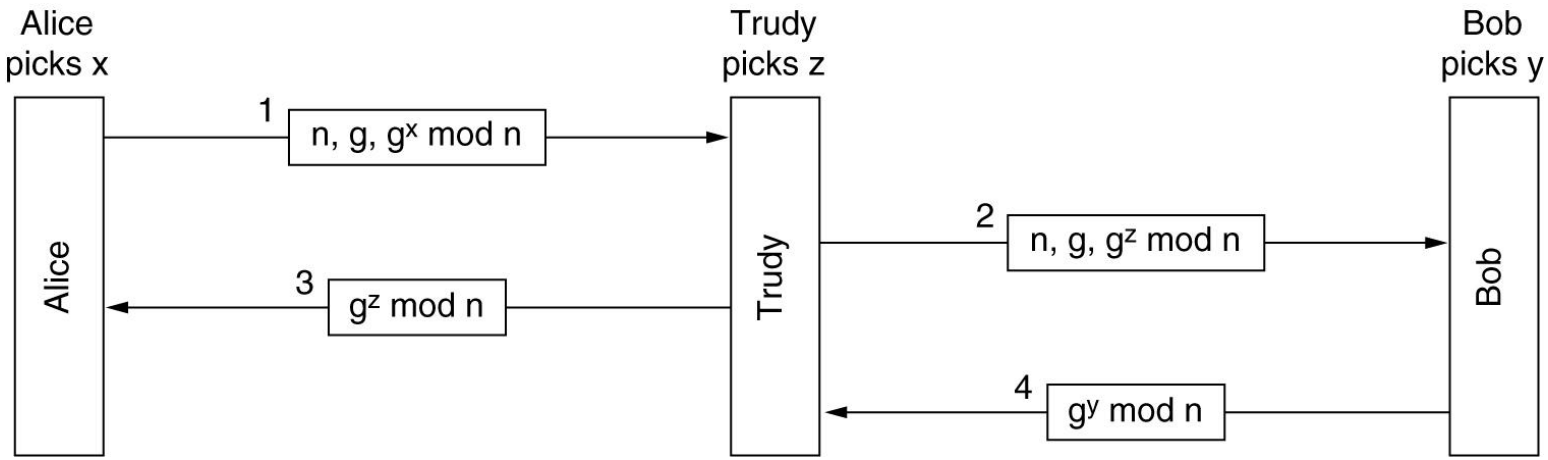


Установка общего ключа: протокол Диффи-Хелмана



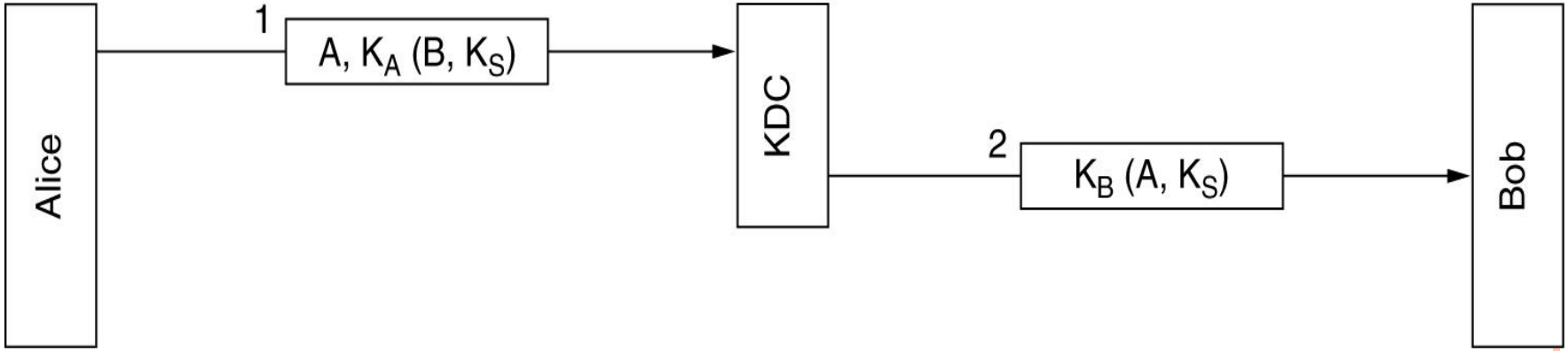
The Diffie-Hellman key exchange.

Установка общего ключа: протокол Диффи-Хелмана



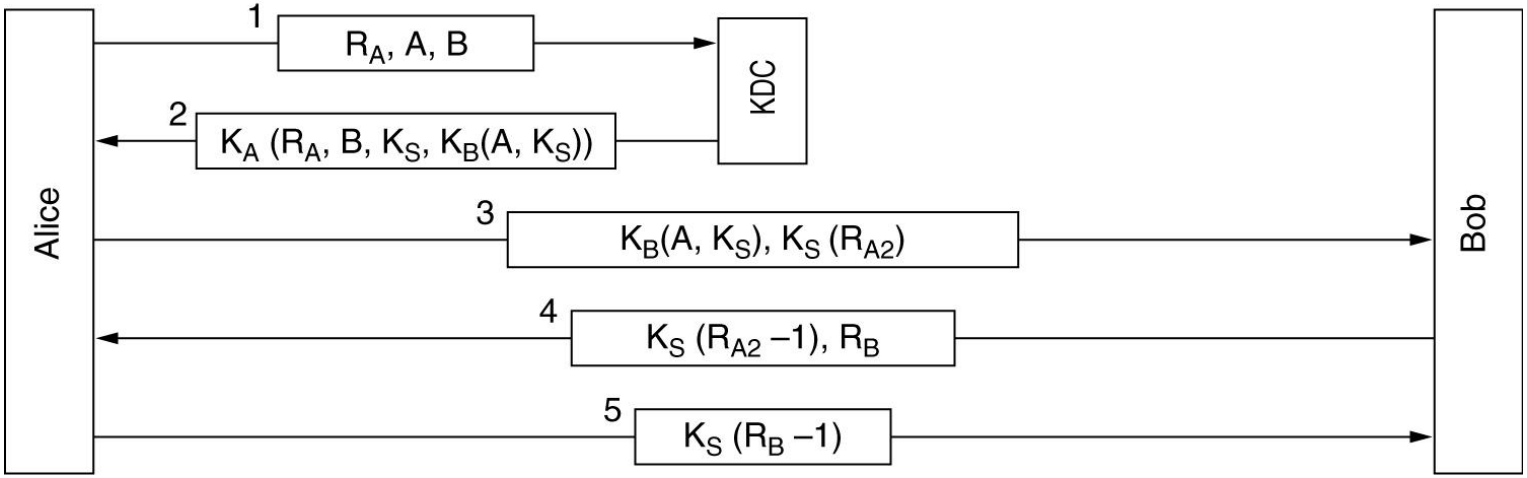
The bucket brigade or man-in-the-middle attack.

Аутентификация с помощью центра распространения ключей



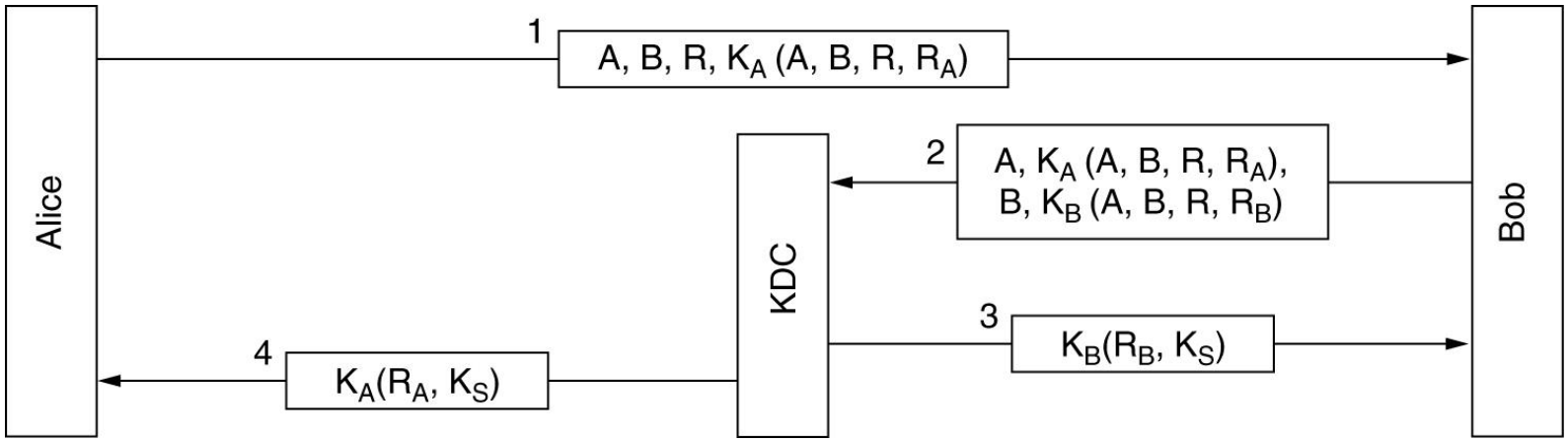
A first attempt at an authentication protocol using a KDC.

Аутентификация с помощью протокола Нидхэма-Шрёдера



The Needham-Schroeder authentication protocol.

Аутентификация с помощью протокола Отуэя-Риса

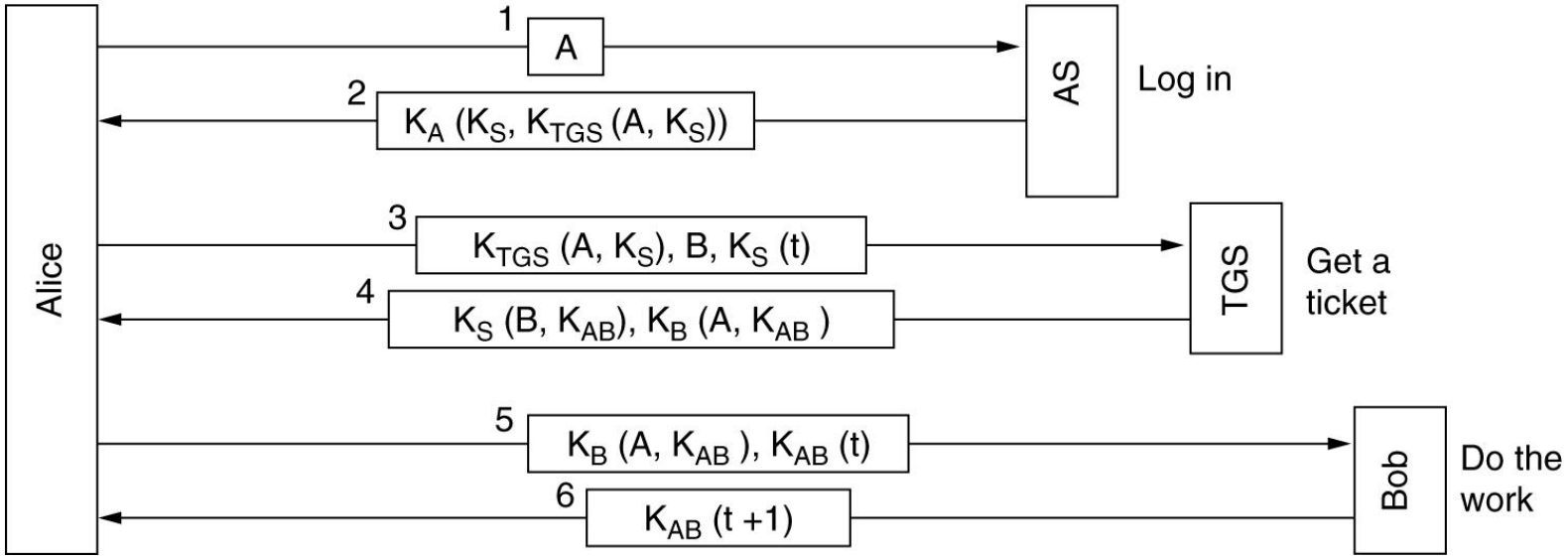


The Otway-Rees authentication protocol (slightly simplified).

Аутентификация с помощью протокола Kerberos

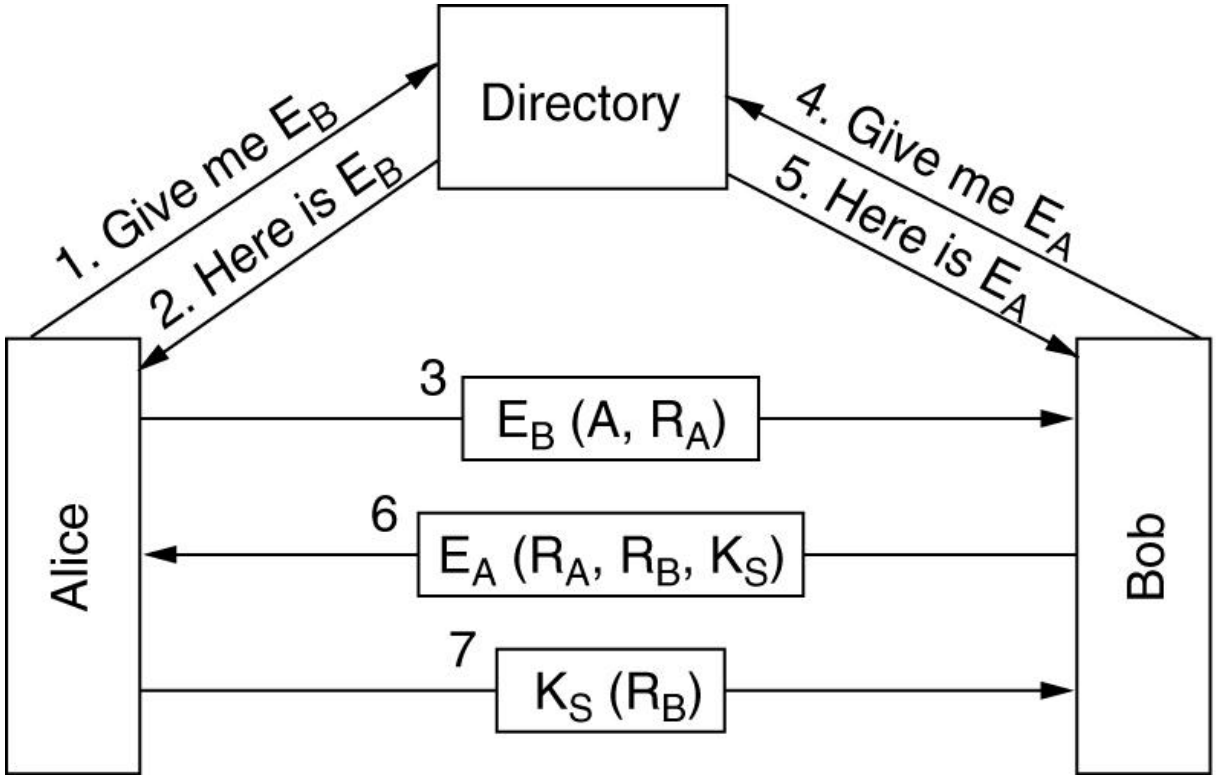
- Рабочая станция
- Сервер аутентификации (AS)
- Сервер выдачи билетов (TGS)
- Вторая рабочая станция

Аутентификация с помощью протокола Kerberos



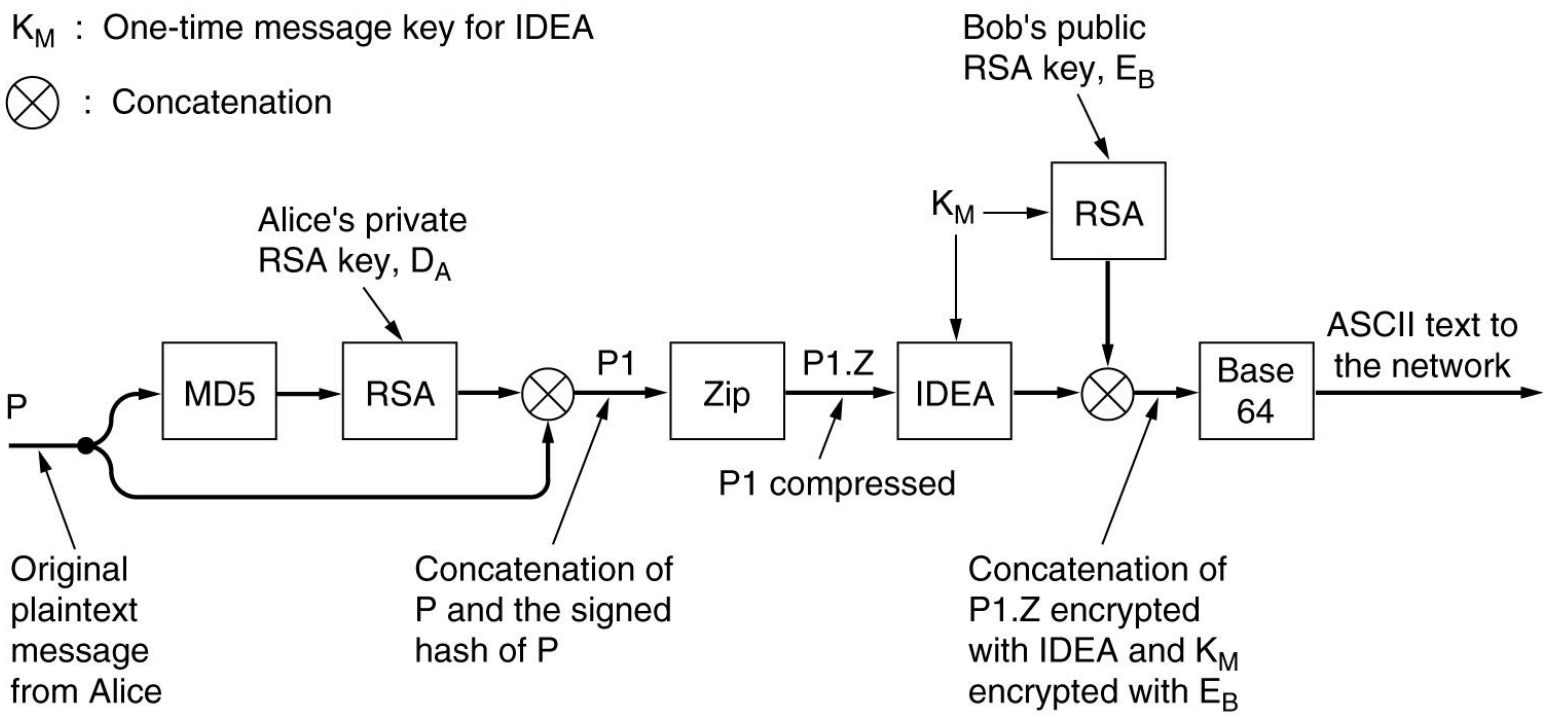
- The operation of Kerberos V4.

Аутентификация с помощью открытых ключей



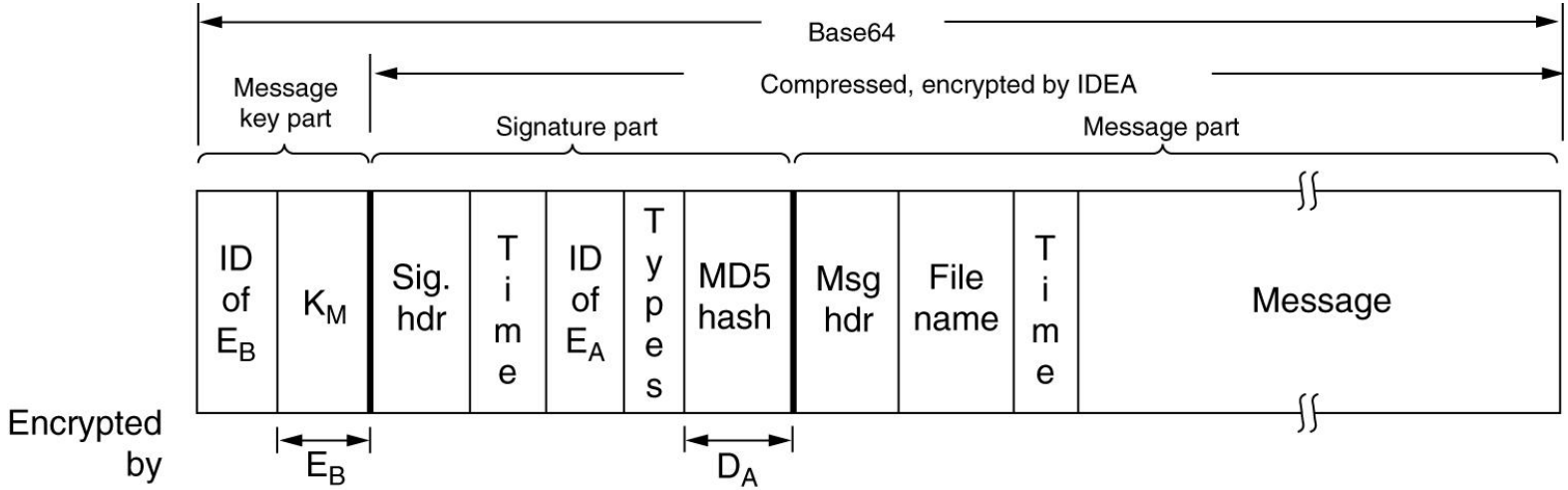
- Mutual authentication using public-key cryptography.

PGP



- PGP in operation for sending a message.

PGP



- A PGP message.