Лекция 1. Определение криптографического протокола. Цели протоколов. Некоторые примеры.

Косолапов Ю.В.

ЮФУ

7 сентября 2020 г.

Содержание

- Прикладная криптография. Протоколы, алгоритмы и исходный код на C, Шнайер Б.
- Криптографические протоколы. Основные свойства и уязвимости. Черемушкин А.В.
- Лекции по криптографии. Музыкантский А. И., Фурин В. В.

Что такое протокол?

Определение

Протокол – описание распределенного алгоритма, в процессе выполнения которого два **участника** (или более) последовательно выполняют **определенные действия** и обмениваются сообщениями для достижения **определенной цели**.

Что такое протокол?

Определение

Протокол – описание распределенного алгоритма, в процессе выполнения которого два **участника** (или более) последовательно выполняют **определенные действия** и обмениваются сообщениями для достижения **определенной цели**.

Ключевые понятие в этом определении:

- Участники (participants).
- Действия (operations).
- Цели (goals).

Участники

Участники (субъекты, стороны):

Участники

Участники (субъекты, стороны):

- Примеры: пользователи (абоненты), клиентские и серверные приложения.

Участники

Участники (субъекты, стороны):

- Примеры: пользователи (абоненты), клиентские и серверные приложения.
- Важно: участники принимают **активное** участие.

Участники

Участники (субъекты, стороны):

- Примеры: пользователи (абоненты), клиентские и серверные приложения.
- Важно: участники принимают **активное** участие.
- Пассивные наблюдатели не являются участниками.

Действия

Действия участников:

Действия

Действия участников:

- *Цикл* (проход) протокола (round, pass) – период времени между двумя точками синхронизации (!).

Действия

Действия участников:

- *Цикл* (проход) протокола (round, pass) – период времени между двумя точками синхронизации (!).
- *Шаг* (протокола) (step, action) – конкретное законченное действие, выполняемое участником (протокола) во время одного цикла (прохода) протокола.

Действия

Действия участников:

- *Цикл* (проход) протокола (round, pass) – период времени между двумя точками синхронизации (!).
- *Шаг* (протокола) (step, action) – конкретное законченное действие, выполняемое участником (протокола) во время одного цикла (прохода) протокола.
- *Сеанс* (session) – это конкретная реализация протокола с конкретными участниками.

Действия

Действия участников:

- *Цикл* (проход) протокола (round, pass) – период времени между двумя точками синхронизации (!).
- *Шаг* (протокола) (step, action) – конкретное законченное действие, выполняемое участником (протокола) во время одного цикла (прохода) протокола.
- *Сеанс* (session) – это конкретная реализация протокола с конкретными участниками.

Замечание

Отправку данных D от участника A участнику B будем обозначать обычно так:

$$A \to B : D$$

Цели

Цели протоколов:

Цели

Цели протоколов:

- *Цель* – это назначение прокола.

Цели

Цели протоколов:

- *Цель* – это назначение прокола.
- Примеры целей: установление соединения (TCP), маршрутизация (RIP, OSPF), аутентификация участника (по паролю).

Цели

Цели протоколов:

- *Цель* – это назначение прокола.
- Примеры целей: установление соединения (TCP), маршрутизация (RIP, OSPF), аутентификация участника (по паролю).
- Цели еще называют функциями или сервисами (поэтому иногда говорят о функциях-сервисах).

Протоколы безопасности

Определение

Протокол безопасности– это протокол, целью которого является обеспечение некоторой функции безопасности (обеспечение цели безопасности).

[1] Meadows, C.: An outline of a taxonomy of computer security research and development. In: Michael, J.B., Ashby, V., Meadows, D., (ed.) Proceedings on the 1992–1993 Workshop on New Security Paradigms, pp. 33–35. ACM (1993)

Протоколы безопасности

Определение

Протокол безопасности– это протокол, целью которого является обеспечение некоторой функции безопасности (обеспечение цели безопасности).

Целью кибербезопасности является защита прав и ожиданий, связанных с данными, а также защита процессов, связанных с данными [1].

[1] Meadows, C.: An outline of a taxonomy of computer security research and development. In: Michael, J.B., Ashby, V., Meadows, D., (ed.) Proceedings on the 1992–1993 Workshop on New Security Paradigms, pp. 33–35. ACM (1993)

Протоколы безопасности

Определение

Протокол безопасности– это протокол, целью которого является обеспечение некоторой функции безопасности (обеспечение цели безопасности).

Целью кибербезопасности является защита прав и ожиданий, связанных с данными, а также защита процессов, связанных с данными [1]. Таким образом:

- права и обязанности индуцируют цели безопасности;

[1] Meadows, C.: An outline of a taxonomy of computer security research and development. In: Michael, J.B., Ashby, V., Meadows, D., (ed.) Proceedings on the 1992–1993 Workshop on New Security Paradigms, pp. 33–35. ACM (1993)

Протоколы безопасности

Определение

Протокол безопасности– это протокол, целью которого является обеспечение некоторой функции безопасности (обеспечение цели безопасности).

Целью кибербезопасности является защита прав и ожиданий, связанных с данными, а также защита процессов, связанных с данными [1]. Таким образом:

- права и обязанности индуцируют цели безопасности;
- права зависят от страны, и различаются для корпораций, частных лиц, и правительства.

[1] Meadows, C.: An outline of a taxonomy of computer security research and development. In: Michael, J.B., Ashby, V., Meadows, D., (ed.) Proceedings on the 1992–1993 Workshop on New Security Paradigms, pp. 33–35. ACM (1993)

Некоторые цели безопасности

Цели:

- анонимность;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;
- защита авторских прав;
- делегирование/отзыв полномочий;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;
- защита авторских прав;
- делегирование/отзыв полномочий;
- свобода слова;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;
- защита авторских прав;
- делегирование/отзыв полномочий;
- свобода слова;
- идентификация;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;
- защита авторских прав;
- делегирование/отзыв полномочий;
- свобода слова;
- идентификация;
- целостность;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;
- защита авторских прав;
- делегирование/отзыв полномочий;
- свобода слова;
- идентификация;
- целостность;
- приватность;

Некоторые цели безопасности

Цели:

- анонимность;
- аутентификация;
- авторизованный перехват сообщений;
- доступность ресурсов/информации;
- цензура;
- конфиденциальность;
- защита авторских прав;
- делегирование/отзыв полномочий;
- свобода слова;
- идентификация;
- целостность;
- приватность;
- отслеживаемость;
- ...

Стойкость протокола

Стойкость протокола

Нарушитель

Участник (*внутренний*) протокола, нарушающий предписанные протоколом действия.

Стойкость протокола

Нарушитель

Участник (*внутренний*) протокола, нарушающий предписанные протоколом действия.

Противник

Внешний субъект (или коалиция субъектов), наблюдающий за передаваемыми сообщениями и, возможно, вмешивающийся в работу участников путем *перехвата*, *искажения* (модификации), *вставки* (создания новых), *повтора* и *перенаправления* сообщений, *блокирования* передачи и т. п.

Стойкость протокола

Нарушитель

Участник (*внутренний*) протокола, нарушающий предписанные протоколом действия.

Противник

Внешний субъект (или коалиция субъектов), наблюдающий за передаваемыми сообщениями и, возможно, вмешивающийся в работу участников путем *перехвата*, *искажения* (модификации), *вставки* (создания новых), *повтора* и *перенаправления* сообщений, *блокирования* передачи и т. п.

Стойкость

Способность противостоять атакам противника и/или нарушителя, как правило, имеющим целью нейтрализацию одной или нескольких функций безопасности и, прежде всего, получение секретного ключа.

Криптографические протоколы

Определение

Криптографический протокол — это протокол безопасности, в котором используются криптографические методы/алгоритмы.

Криптографические протоколы

Определение

Криптографический протокол — это протокол безопасности, в котором используются криптографические методы/алгоритмы.

Полнота (completeness)

Свойство криптографического протокола, означающее, что при выполнении честными участниками протокол решает ту задачу, для которой он создан.

Криптографические протоколы

Определение

Криптографический протокол — это протокол безопасности, в котором используются криптографические методы/алгоритмы.

Полнота (completeness)

Свойство криптографического протокола, означающее, что при выполнении честными участниками протокол решает ту задачу, для которой он создан.

Корректность (soundness) = Стойкость

Способность криптографического протокола противостоять угрозам со стороны противника и/или нарушителя, не располагающего необходимой секретной информацией, но пытающегося выполнить протокол за участника A, который по определению должен такой информацией владеть.

Цели для криптографических протоколов

Цели для криптографических протоколов

- *Аутентификация источника данных* — обеспечивает возможность проверки того, что полученные данные действительно созданы конкретным источником.

Цели для криптографических протоколов

- *Аутентификация источника данных* — обеспечивает возможность проверки того, что полученные данные действительно созданы конкретным источником.
- *Аутентификация сторон* — обеспечивает возможность проверки того, что одна из сторон информационного взаимодействия действительно является той, за которую она себя выдает.

Цели для криптографических протоколов

- *Аутентификация источника данных* — обеспечивает возможность проверки того, что полученные данные действительно созданы конкретным источником.
- *Аутентификация сторон* — обеспечивает возможность проверки того, что одна из сторон информационного взаимодействия действительно является той, за которую она себя выдает.
- *Конфиденциальность данных* — Обеспечивает невозможность несанкционированного получения доступа к данным или раскрытия данных.

Цели для криптографических протоколов (продолжение)

- *Невозможность отказа* — обеспечивает невозможность отказа одной из сторон от факта участия в информационном обмене (полностью или в какой-либо его части).

Цели для криптографических протоколов (продолжение)

- *Невозможность отказа* — обеспечивает невозможность отказа одной из сторон от факта участия в информационном обмене (полностью или в какой-либо его части).
- *Целостность данных* — обеспечивает возможность проверки того, что защищаемая информация не подверглась несанкционированной модификации или разрушению.

Цели для криптографических протоколов (продолжение)

- *Невозможность отказа* — обеспечивает невозможность отказа одной из сторон от факта участия в информационном обмене (полностью или в какой-либо его части).
- *Целостность данных* — обеспечивает возможность проверки того, что защищаемая информация не подверглась несанкционированной модификации или разрушению.
- *Разграничение доступа* — обеспечивает невозможность несанкционированного использования ресурсов системы.

Предположения, используемые при анализе протоколов

Предположения, используемые при анализе протоколов

- *Perfect cryptography assumption* – все стандартные криптографические примитивы удовлетворяют условию совершенной стойкости; слабости могут быть вызваны только непродуманным порядком действий, предписанных самим протоколом.

Предположения, используемые при анализе протоколов

- *Perfect cryptography assumption* – все стандартные криптографические примитивы удовлетворяют условию совершенной стойкости; слабости могут быть вызваны только непродуманным порядком действий, предписанных самим протоколом.
- Strong typing assumption (строгое соблюдение типов) – все участники правильно понимают форматы получаемых сообщений и корректно распознают типы полей в записи передаваемых сообщений.

Предположения, используемые при анализе протоколов

- *Perfect cryptography assumption* – все стандартные криптографические примитивы удовлетворяют условию совершенной стойкости; слабости могут быть вызваны только непродуманным порядком действий, предписанных самим протоколом.
- Strong typing assumption (строгое соблюдение типов) – все участники правильно понимают форматы получаемых сообщений и корректно распознают типы полей в записи передаваемых сообщений.
- Honest participants (честность участников) – все участники точно выполняют предписанный согласно протоколу порядок действий.

Предположения, используемые при анализе протоколов

- *Perfect cryptography assumption* – все стандартные криптографические примитивы удовлетворяют условию совершенной стойкости; слабости могут быть вызваны только непродуманным порядком действий, предписанных самим протоколом.
- Strong typing assumption (строгое соблюдение типов) – все участники правильно понимают форматы получаемых сообщений и корректно распознают типы полей в записи передаваемых сообщений.
- Honest participants (честность участников) – все участники точно выполняют предписанный согласно протоколу порядок действий.
- Bounded number of sessions (ограниченное число сеансов) – для сведения задачи к конечному числу состояний.

Модель угрозы Долева — Яо

Злоумышленник **может**

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;
- посылать любому пользователю сообщения от имени любого другого пользователя.

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;
- посылать любому пользователю сообщения от имени любого другого пользователя.

Злоумышленник **не может**

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;
- посылать любому пользователю сообщения от имени любого другого пользователя.

Злоумышленник **не может**

- угадывать случайные числа, выбранные из достаточно большого множества;

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;
- посылать любому пользователю сообщения от имени любого другого пользователя.

Злоумышленник **не может**

- угадывать случайные числа, выбранные из достаточно большого множества;
- расшифровать не имея ключа, либо корректно зашифровать сообщение при условии использования некоторого идеального алгоритма шифрования;

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;
- посылать любому пользователю сообщения от имени любого другого пользователя.

Злоумышленник **не может**

- угадывать случайные числа, выбранные из достаточно большого множества;
- расшифровать не имея ключа, либо корректно зашифровать сообщение при условии использования некоторого идеального алгоритма шифрования;
- найти секретный ключ по открытому ключу (при использовании криптосистем с открытым ключом);

Модель угрозы Долева — Яо

Злоумышленник **может**

- получить любое сообщение, передаваемое по сети;
- являться авторизованным пользователем сети, и поэтому, в частности, имеет право устанавливать соединение с любым другим пользователем;
- стать стороной, принимающей сообщения от любой передающей стороны;
- посылать любому пользователю сообщения от имени любого другого пользователя.

Злоумышленник **не может**

- угадывать случайные числа, выбранные из достаточно большого множества;
- расшифровать не имея ключа, либо корректно зашифровать сообщение при условии использования некоторого идеального алгоритма шифрования;
- найти секретный ключ по открытому ключу (при использовании криптосистем с открытым ключом);
- получить доступ к закрытым, внутренним ресурсам, например, к

Типичные атаки на протоколы

Типичные атаки на протоколы

- Подмена (impersonation);

Типичные атаки на протоколы

- Подмена (impersonation);
- Повторное навязывание сообщения (replay attack);

Типичные атаки на протоколы

- Подмена (impersonation);
- Повторное навязывание сообщения (replay attack);
- Атака отражением (reflection attack);

Типичные атаки на протоколы

- Подмена (impersonation);
- Повторное навязывание сообщения (replay attack);
- Атака отражением (reflection attack);
- Задержка передачи сообщения (forced delay);

Типичные атаки на протоколы

- Подмена (impersonation);
- Повторное навязывание сообщения (replay attack);
- Атака отражением (reflection attack);
- Задержка передачи сообщения (forced delay);
- Комбинированная атака (interleaving attack);

Типичные атаки на протоколы

- Подмена (impersonation);
- Повторное навязывание сообщения (replay attack);
- Атака отражением (reflection attack);
- Задержка передачи сообщения (forced delay);
- Комбинированная атака (interleaving attack);
- Атака с параллельными сеансами (parallel-session attack).

Пример 1. Снятие/постановка на охрану автомобиля (протокол)

Участники:

- брелок (**B**);
- блок управления (**M**) сигнализацией (находится в автомобиле).

Пример 1. Снятие/постановка на охрану автомобиля (протокол)

Участники:

- брелок (**B**);
- блок управления (**M**) сигнализацией (находится в автомобиле).

Протокол постановки на сигнализацию

- **B** $\rightarrow$ **M**: SWITCHON – код постановки на сигнализацию (для каждого комплекта сигнализации код может быть уникальным);

Пример 1. Снятие/постановка на охрану автомобиля (протокол)

Участники:

- брелок (**B**);
- блок управления (**M**) сигнализацией (находится в автомобиле).

Протокол постановки на сигнализацию

- **B** $\rightarrow$ **M**: SWITCHON – код постановки на сигнализацию (для каждого комплекта сигнализации код может быть уникальным);

Протокол снятия с сигнализации

- **B** $\rightarrow$ **M**: SWITCHOFF – код снятия с сигнализации (для каждого комплекта сигнализации код может быть уникальным);

Пример 1. Снятие/постановка на охрану автомобиля (сессия)

Участники:

- **B**’ – брелок из комплекта с серийным номером N;
- **M**’ – блок управления сигнализацией из комплекта с серийным номером N (установлен в конкретном автомобиле A).

Пример 1. Снятие/постановка на охрану автомобиля (сессия)

Участники:

- **B**’ – брелок из комплекта с серийным номером N;
- **M**’ – блок управления сигнализацией из комплекта с серийным номером N (установлен в конкретном автомобиле A).

Момент времени t_1

Постановка

- $\mathbf{B}' \rightarrow \mathbf{M}'$: NJWDF158WFG

Снятие

- $\mathbf{B}' \rightarrow \mathbf{M}'$: N954FETF13

Пример 1. Снятие/постановка на охрану автомобиля (сессия)

Участники:

- **B**’ – брелок из комплекта с серийным номером N;
- **M**’ – блок управления сигнализацией из комплекта с серийным номером N (установлен в конкретном автомобиле A).

Момент времени t_1

Постановка

- $\mathbf{B}' \to \mathbf{M}'$: NJWDF158WFG

Снятие

- $\mathbf{B}' \to \mathbf{M}'$: N954FETF13

Момент времени t_2

Постановка

- $\mathbf{B}' \to \mathbf{M}'$: NJWDF158WFG

Снятие

- $\mathbf{B}' \to \mathbf{M}'$: N954FETF13

Пример 1. Снятие/постановка на охрану автомобиля (сессия)

Участники:

- **B**’ – брелок из комплекта с серийным номером N;
- **M**’ – блок управления сигнализацией из комплекта с серийным номером N (установлен в конкретном автомобиле A).

Момент времени t_1

Постановка

- $\mathbf{B}' \to \mathbf{M}'$: NJWDF158WFG

Снятие

- $\mathbf{B}' \to \mathbf{M}'$: N954FETF13

Момент времени t_2

Постановка

- $\mathbf{B}' \to \mathbf{M}'$: NJWDF158WFG

Снятие

- $\mathbf{B}' \to \mathbf{M}'$: N954FETF13

Какие проблемы у этого протокола?

Пример 2. Снятие/постановка на охрану автомобиля **одной кнопкой** (протокол)

Пример 2. Снятие/постановка на охрану автомобиля **одной кнопкой** (протокол)

Протокол постановки на сигнализацию

- $\mathbf{B}: C = E_{\mathbf{k}}(SN, CurrentCodeLock, N_{press}, < \cdots >)$
- $\mathbf{B} \rightarrow \mathbf{M}$: C
- $\mathbf{M}: D_{\mathbf{k}}(C) = (SN, CurrentCodeLock, N_{press}, < \cdots >)$
- $\mathbf{M}$: проверка ...

Пример 2. Снятие/постановка на охрану автомобиля **одной кнопкой** (протокол)

Протокол постановки на сигнализацию

- $\mathbf{B} : C = E_{\mathbf{k}}(SN, CurrentCodeLock, N_{press}, < \cdots >)$
- $\mathbf{B} \rightarrow \mathbf{M}$: C
- $\mathbf{M} : D_{\mathbf{k}}(C) = (SN, CurrentCodeLock, N_{press}, < \cdots >)$
- $\mathbf{M}$: проверка ...

Протокол снятия с сигнализации

- $\mathbf{B} : C = E_{\mathbf{k}}(SN, CurrentCodeUnLock, N_{press}, < \cdots >)$
- $\mathbf{B} \rightarrow \mathbf{M}$: C
- $\mathbf{M} : D_{\mathbf{k}}(C) = (SN, CurrentCodeUnLock, N_{press}, < \cdots >)$
- $\mathbf{M}$: проверка ...

Пример 2. Снятие/постановка на охрану автомобиля **одной кнопкой** (сессия)

Пример 2. Снятие/постановка на охрану автомобиля **одной кнопкой** (сессия)

Протокол постановки на сигнализацию

- $\mathbf{B}'$: $bvrvftNJN54845bJBNpi3rbqec2334rc = E_{9834HJKBN78}(12345, DFG67GHJ22, 146, <\cdots>)$
- $\mathbf{B}' \rightarrow \mathbf{M}'$: $bvrvftNJN54845bJBNpi3rbqec2334rc$
- $\mathbf{M}'$: $D_{9834HJKBN78}(bvrvftNJN54845bJBNpi3rbqec2334rc) = (12345, DFG67GHJ22, 146, <\cdots>)$
- $\mathbf{M}'$: проверка ...

Пример 2. Снятие/постановка на охрану автомобиля **одной кнопкой** (сессия)

Протокол постановки на сигнализацию

- $\mathbf{B}'$: $bvrvftNJN54845bJBNpi3rbqec2334rc = E_{9834HJKBN78}(12345, DFG67GHJ22, 146, <\cdots>)$
- $\mathbf{B}' \to \mathbf{M}'$: $bvrvftNJN54845bJBNpi3rbqec2334rc$
- $\mathbf{M}'$: $D_{9834HJKBN78}(bvrvftNJN54845bJBNpi3rbqec2334rc) = (12345, DFG67GHJ22, 146, <\cdots>)$
- $\mathbf{M}'$: проверка ...

Протокол снятия с сигнализации

- $\mathbf{B}$: kjerwbvLJLBb428nlkjn*YN22 $= E_{9834HJKBN78}(12345, VKJJVL2@LK : B, 85, <\cdots>)$
- $\mathbf{B} \to \mathbf{M}$: kjerwbvLJLBb428nlkjn*YN22
- $\mathbf{M}$: $D_{9834HJKBN78}$(kjerwbvLJLBb428nlkjn*YN22) $= (12345, VKJJVL2@LK : B, 85, <\cdots>)$
- $\mathbf{M}$: проверка ...

Какие проблемы у этого протокола?

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Протокол постановки/снятия сигнализации

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Протокол постановки/снятия сигнализации

- **B** $\rightarrow$ **M**: запрос на выполнение действия

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Протокол постановки/снятия сигнализации

- **B** $\rightarrow$ **M**: запрос на выполнение действия
- **M** $\rightarrow$ **B**: случайное число R

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Протокол постановки/снятия сигнализации

- **B** $\rightarrow$ **M**: запрос на выполнение действия
- **M** $\rightarrow$ **B**: случайное число R
- **B** : $C = E_{\mathbf{k}}(R)$

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Протокол постановки/снятия сигнализации

- **B** $\rightarrow$ **M**: запрос на выполнение действия
- **M** $\rightarrow$ **B**: случайное число R
- **B** : $C = E_{\mathbf{k}}(R)$
- **B** $\rightarrow$ **M**: C, действие (lock/unlock)

Пример 3. Снятие/постановка на охрану автомобиля с аутентификацией

Протокол постановки/снятия сигнализации

- **B** $\rightarrow$ **M**: запрос на выполнение действия
- **M** $\rightarrow$ **B**: случайное число R
- **B** : $C = E_{\mathbf{k}}(R)$
- **B** $\rightarrow$ **M**: C, действие (lock/unlock)
- **M** : проверка ...