



БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Криптографические протоколы

Лекция 1

Деркач Максим Юрьевич

September 2, 2019

- ▶ Основные понятия
- ▶ Атаки на протоколы
- ▶ Управление ключами, их классификация и жизненный цикл
- ▶ Протоколы аутентификации
- ▶ Протоколы распределения и обновления ключей
- ▶ Защищенные каналы передачи данных (IPSEC, SSL/TLS, ...)
- ▶ Протоколы электронного голосования



- ▶ А.В. Соколов "Защита информации в распределенных корпоративных сетях и системах"
- ▶ А.М. Миронов "Криптографические протоколы"

Список основных обозначений

- ▶ A, B - участники инфор. обмена
- ▶ S - центр распределения ключей (3-ья доверенная сторона)
- ▶ I - злоумышленник
- ▶ ID_X - идентификатор X
- ▶ K_{xy} - общий секретный ключ X, Y
- ▶ KS - секретный сеансовый ключ
- ▶ K_X^{pub} - открытый ключ X
- ▶ K_X^{sec} - секретный ключ X
- ▶ N_X - порядковый номер X
- ▶ $R_X, Nonce_X$ - (number used once) случайное число, выработанное X



БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Список основных обозначений



БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

- ▶ T_X - временная отметка, поставленная участником X
- ▶ TVP_X - одноразовый параметр X
- ▶ T_X/N_X - одноразовый параметр X , который является либо временной меткой, либо порядковым номером
- ▶ $E_k(M)$ -
- ▶ $D_k(M)$ -
- ▶ $MAC_k(M)$ -
- ▶ $h, h(M)$ -
- ▶ $Sign_{K_X^{sec}}(M)$ - ЭЦП сообщения M участника X
- ▶ $Cert_X$ - сертификат участника X
- ▶ $M_1 || M_2$ - конкатенация



Определение 1

Протокол - совокупность действий выполняемых в заданной последовательности двумя или более сторонами с целью достижения определенного результата.

Определение 2

Криптографический протокол - протокол, в котором используются криптографические средства (алгоритмы).

Определение 3

Сеанс - это однократное выполнение протокола.

1. Действия имеют строгую очередность от начала и до конца (ни одно действие не выполняется, пока не закончится другое).
2. Должно быть точно определено каждое действие.
3. Все стороны, участвующие в протоколе, должны заранее знать последовательность действий.

Классификация криптографических протоколов



1. на основе задач
2. по числу участников в протоколе
3. по числу передаваемых сообщений

Модель угрозы Долева-Яо

(Dolev-Yao)

Возможности злоумышленника:

- ✦ перехватывать \forall сообщение в сети
- ✦ вступать в контакт с другим пользователем
- ✦ получать сообщение от \forall пользователя
- ✦ посылать сообщение \forall пользователю, маскируясь под \forall другого пользователя

Злоумышленник не может:

- ✦ угадать случайное число, выбранное из достаточно большого множества
- ✦ восстановить открытый ключ по шифротексту, не имея правильного секретного ключа
- ✦ зашифровать исходное сообщение
- ✦ найти личный ключ, имея соответствующий открытый ключ
- ✦ иметь доступ к закрытым зонам вычислительной среды



БЕЛОРУССКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

