



Инновационный Евразийский университет

Кафедра

«Энергетика, металлургия и информационные технологии»

СЛАЙД-ЛЕКЦИЯ

по дисциплине

«Основы информационной безопасности»

Тема: Обмен ключами по схеме Диффи-Хеллмана

Образовательные программы:

6В06101 «Информатика»

6В06102 «Информационные системы»

6В06103 «Вычислительная техника и программное обеспечение»

Разработчик:

старший преподаватель, м.и. И.И. Ляшенко

Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

План лекции:

1. Введение

2. Алгоритм обмена ключами

3. Возможности использования алгоритм Диффи-Хэллмана



1. Введение

Алгоритм Диффи — Хэллмана (англ. Diffie-Hellman, DH) — алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Алгоритм был впервые опубликован Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом в 1976 году.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

В 2002 году Хеллман предложил называть данный алгоритм «Диффи — Хеллмана — Меркля», признавая вклад Меркля в изобретение криптографии с открытым ключом.

Цель схемы — обеспечить двум пользователям защищенную возможность сообщить друг другу ключ, чтобы они могли прибегнуть к ней для шифрования последующих сообщений. Сам по себе алгоритм ограничивается процедурой обмена ключами.



2. Алгоритм обмена ключами

Эффективность алгоритма Диффи-Хеллмана опирается на трудность вычисления дискретных логарифмов.

Формально дискретный логарифм можно определить следующим образом. Сначала определяется первообразный корень простого числа p как число, степени которого порождают все целые числа от 1 до $p - 1$.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Это значит, что если a является первообразным корнем простого числа p , то все числа

$$a \bmod p, a^2 \bmod p, \dots, a^{p-1} \bmod p$$

должны быть разными и представлять все целые числа от 1 до $p - 1$ в некоторой перестановке.

Для любого целого числа b и любого первообразного корня a простого числа p однозначно определяется показатель степени i , при котором

$$b = a^i \bmod p, \quad \text{где } 0 < i < (p - 1).$$



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Этот показатель степени обычно называется дискретным логарифмом, или индексом b по основанию a , рассматриваемому по модулю p . Это значение записывается в форме $ind_{a,p}(b)$.



сотовый телефон Sagem vectroTEL X8 обеспечивает абсолютную конфиденциальность переговоров посредством специальной встроенной системы шифрования, базирующейся на использовании алгоритма Диффи-Хеллмана с 1024-битным ключом



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Глобальные открытые элементы	
q	Простое число
α	$\alpha < q$ и α - первообразный корень q
Вычисление ключа пользователем <u>A</u>	
Выбор секретного <u>X_a</u>	$X_a < q$
Вычисление открытого <u>Y_a</u>	$Y_a = \alpha^{X_a} \bmod q$
Вычисление ключа пользователем <u>B</u>	
Выбор секретного <u>X_b</u>	$X_b < q$
Вычисление открытого <u>Y_b</u>	$Y_b = \alpha^{X_b} \bmod q$
Вычисление секретного ключа пользователем <u>A</u>	
$K = (Y_b)^{X_a} \bmod q$	
Вычисление секретного ключа пользователем <u>B</u>	
$K = (Y_a)^{X_b} \bmod q$	

Алгоритм обмена ключами по схеме Диффи-Хеллмана



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

В этой схеме имеется два открытых для всех числа: простое число q и целое число α , являющееся первообразным корнем q . Предположим, пользователи А и В намерены обменяться ключами.

Пользователь А выбирает случайное целое число $X_a < q$ и вычисляет

$$Y_a = \alpha^{X_a} \bmod q .$$



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Точно так же пользователь В независимо выбирает случайное целое число $X_b < q$ и вычисляет

$$Y_b = \alpha^{X_b} \bmod q.$$

Каждая сторона сохраняет значение X в тайне и делает значение Y свободно доступным другой стороне.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Пользователь А вычисляет ключ по формуле

$$K = (Y_b)^{X_a} \bmod q,$$

а пользователь В — по формуле

$$K = (Y_a)^{X_b} \bmod q.$$

Эти две формулы вычисления дают одинаковые результаты.

$$\begin{aligned} K &= (Y_b)^{X_a} \bmod q = (\alpha^{X_b} \bmod q)^{X_a} \bmod q = \\ &= (\alpha^{X_b})^{X_a} \bmod q = \alpha^{X_a X_b} \bmod q = (\alpha^{X_a})^{X_b} \bmod q = \\ &= (\alpha^{X_a} \bmod q)^{X_b} \bmod q = (Y_a)^{X_b} \bmod q. \end{aligned}$$



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Итак, обе стороны обменивались секретным ключом. А поскольку при этом X_A и X_B были только в личном использовании и поэтому сохранились в тайне, противнику придется работать только с q , α , Y_a и Y_b . Таким образом, ему придется вычислять дискретный логарифм, чтобы определить ключ.

Например, чтобы определить ключ пользователя В, противнику нужно вычислить

$$X_b = \text{ind}_{\alpha, q}(Y_b).$$

После этого он сможет вычислить ключ K точно так же, как это делает пользователь В.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Защищенность обмена ключами по схеме Диффи-Хеллмана опирается фактически на то, что в то время, как степени по модулю некоторого простого числа вычисляются относительно легко, вычислять дискретные логарифмы оказывается очень трудно.

Для больших простых чисел последнее считается задачей практически неразрешимой.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Пример. Обмен ключами строится на использовании простого числа $q = 97$ и его первообразном корне $\alpha = 5$. Пользователи А и В выбирают секретные ключи $X_a = 36$ и $X_b = 58$ соответственно.

Каждый вычисляет свой открытый ключ:

$$Y_a = 5^{36} = 50 \text{ mod } 97,$$

$$Y_b = 5^{58} = 44 \text{ mod } 97.$$



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

После того как пользователи обмениваются открытыми ключами, каждый из них может вычислить общий секретный ключ:

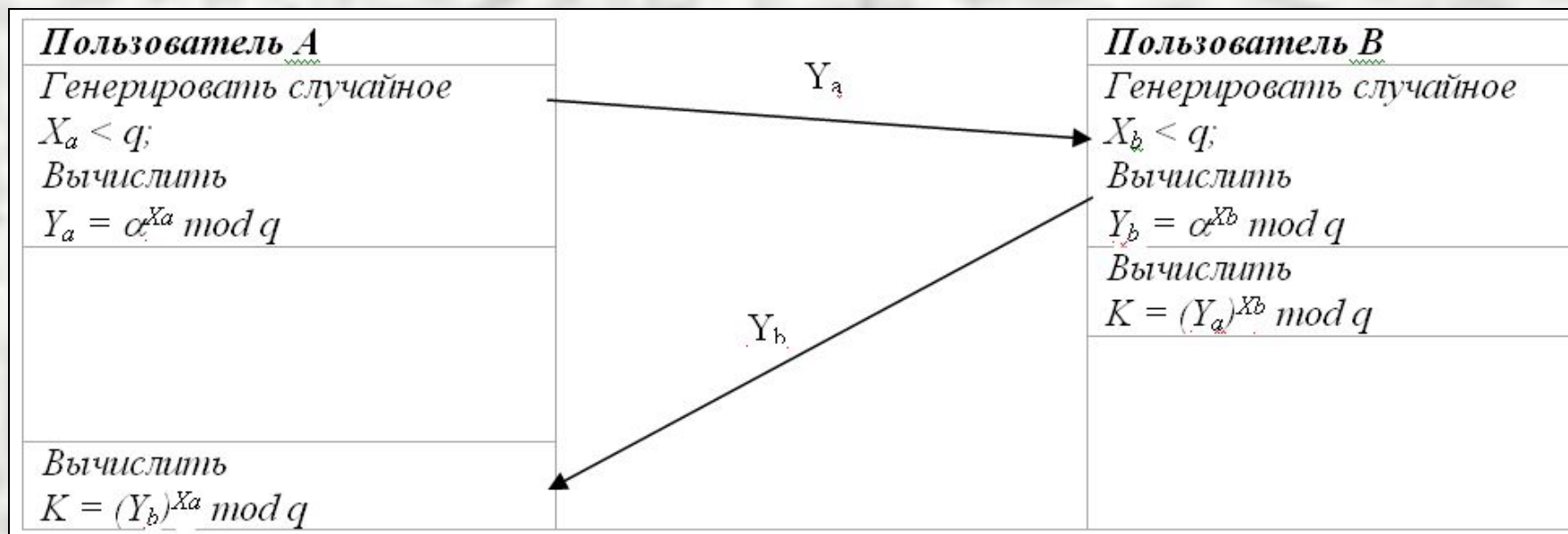
$$K = (Y_b)^{X_a} \bmod 97 = 44^{36} = 75 \bmod 97,$$

$$K = (Y_a)^{X_b} \bmod 97 = 50^{58} = 75 \bmod 97.$$

Имея $\{50, 44\}$, противнику не удастся с легкостью вычислить 75.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана



Обмен ключами по схеме Диффи-Хеллмана



3. Возможности использования алгоритм Диффи-Хэллмана

Для примера другой возможности использования алгоритма Диффи-Хеллмана рассмотрим некоторую группу пользователей (например, всех пользователей локальной сети) и предположим, что каждый из этих пользователей должен сгенерировать секретное значение X_a для долгосрочного применения и вычислить открытое значение Y_a .

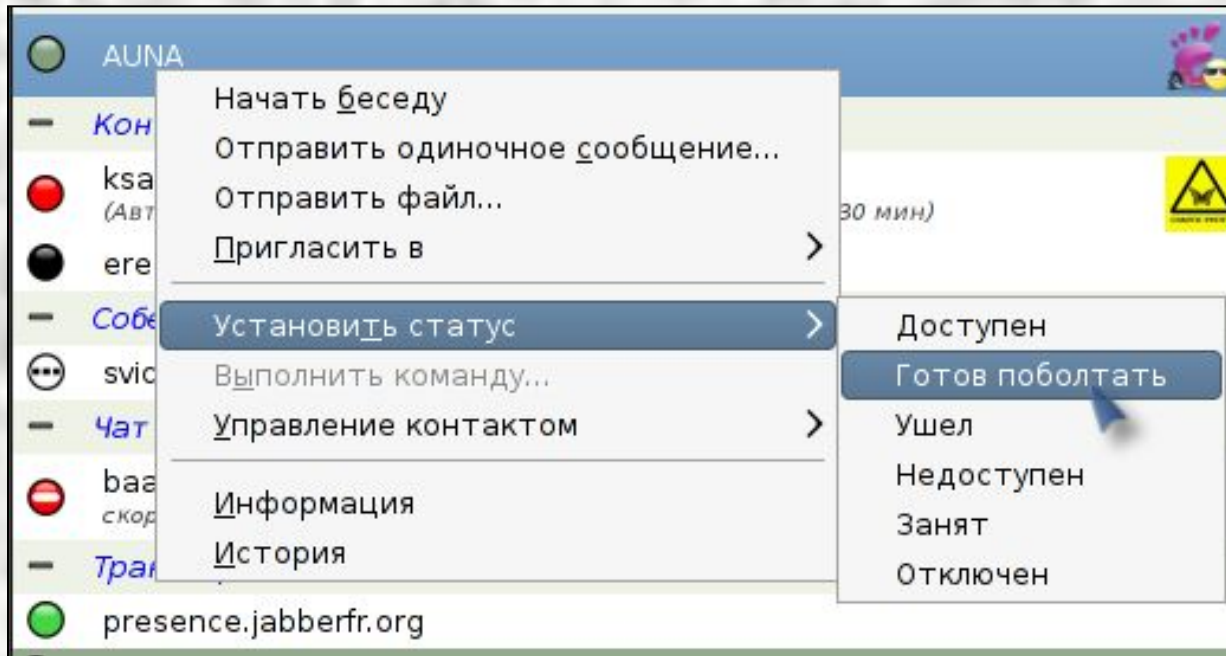


Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Все полученные таким образом открытые значения вместе с глобальными открытыми значениями q и a сохраняются централизованно в некотором каталоге. В любой момент пользователь В может получить доступ к открытому значению пользователя А, вычислить секретный ключ и использовать его для пересылки зашифрованного сообщения пользователю А.



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана



Gajim — полнофункциональный Python/GTK+ клиент обмена мгновенными сообщениями. Между двумя клиентами Gajim, по умолчанию, включается шифрование по алгоритму Диффи-Хеллмана



Лекция 9. Обмен ключами по схеме Диффи-Хэллмана

Если централизованно хранящийся каталог надежен, то эта форма коммуникации обеспечивает как конфиденциальность, так и определенную степень аутентификации. Поскольку только пользователи А и В могут определить ключ, другой пользователь не может прочитать сообщение (конфиденциальность). Получатель А знает, что только пользователь В мог создать сообщение, используя этот ключ (аутентификация). Однако такая схема не защищена от атак на основе воспроизведения сообщений.



Контрольные вопросы:

- 1. На чем основывается эффективность алгоритма Диффи-Хэллмана?**
- 2. Описать обмен ключами по схеме Диффи-Хеллмана.**
- 3. Описать возможности использования алгоритма обмена ключами Диффи-Хэллмана.**



Список используемых источников:

- 1. Бубнов А.А. Основы информационной безопасности. – М.: Академия, 2017. - 256 с.**
- 2. Ерохин В.В. Безопасность информационных систем. - М. : Флинта, 2016. - 184 с.**
- 3. Гашков С.Б. Криптографические методы защиты информации. - М.: Академия, 2010. - 300с.**
- 4. Мельников В.П. Информационная безопасность. – М.: Академия, 2013. - 336 с.**



Список используемых источников:

- 5. Мельников В.П. Защита информации. – М.: Академия, 2014. - 304 с.**
- 6. Бабаш А.В. Информационная безопасность. Лабораторный практикум. - М. : КНОРУС, 2013. - 136 с.**
- 7. Платонов В.В. Программно-аппаратные средства защиты информации. – М.: Академия, 2014. - 336 с.**

