
**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**

**План лекции:**

**1. Введение**

**2. Алгоритм обмена ключами**

**3. Возможности использования алгоритм Диффи-Хэллмана**

# 1. Введение

**Алгори́тм Ди́ффи — Хе́ллмана (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.**

**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*.**

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

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

**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**

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

**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***

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

# Алгоритм обмена ключами по схеме Диффи-Хеллмана

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

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

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

**Точно так же пользователь B независимо выбирает случайное целое число $X_в < q$ и вычисляет**

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

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

**Пользователь А вычисляет ключ по формуле**

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

**а пользователь В — по формуле**

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

**Эти две формулы вычисления дают одинаковые результаты.**

$$K = (Y_b)^{Xa} \bmod q = (\alpha^{Xb} \bmod q)^{Xa} \bmod q =$$
$$= (\alpha^{Xb})^{Xa} \bmod q = \alpha^{XaXb} \bmod q = (\alpha^{Xa})^{Xb} \bmod q =$$
$$= (\alpha^{Xa} \bmod q)^{Xb} \bmod q = (Y_a)^{Xb} \bmod q.$$

**Итак, обе стороны обменялись 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 $q$, $\alpha$, $Y_a$ и $Y_b$. Таким образом, ему придется вычислять дискретный логарифм, чтобы определить ключ.**

**Например, чтобы определить ключ пользователя B, противнику нужно вычислить**

$$X_b = ind_{\alpha,q}(Y_b).$$

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

**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.**

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

**Каждый вычисляет свой открытый ключ:**

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

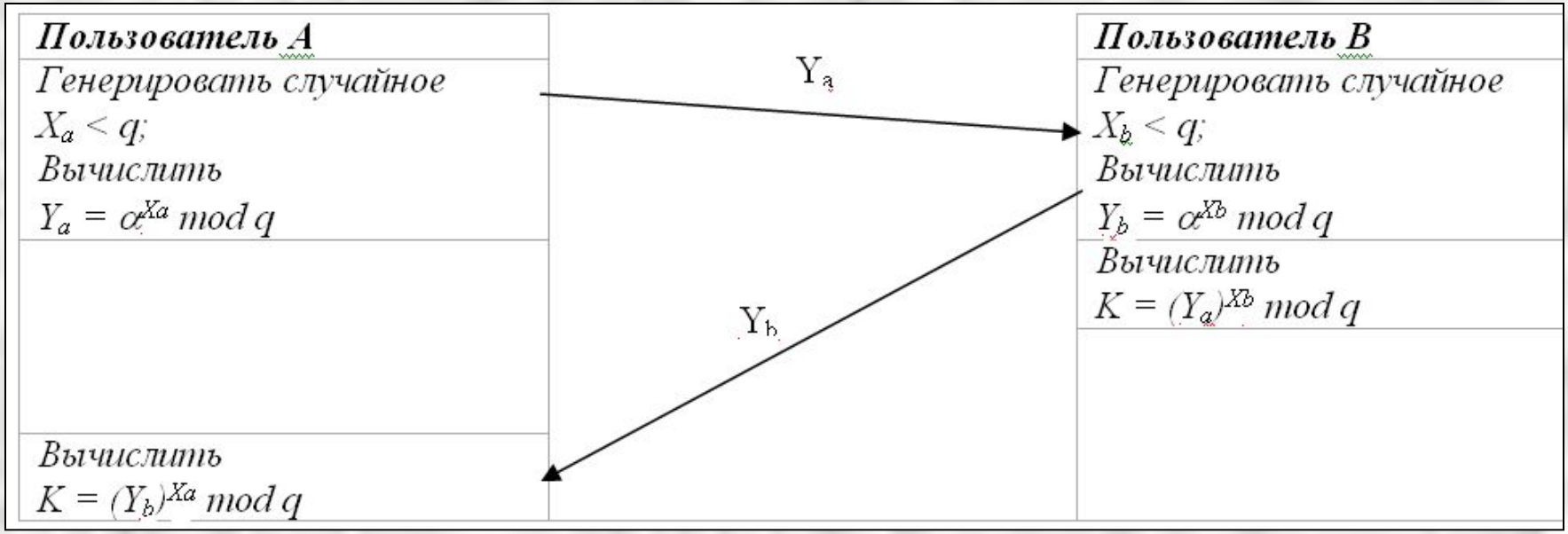
$$Y_b = 5^{58} = 44 \bmod 97.$$

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

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

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

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

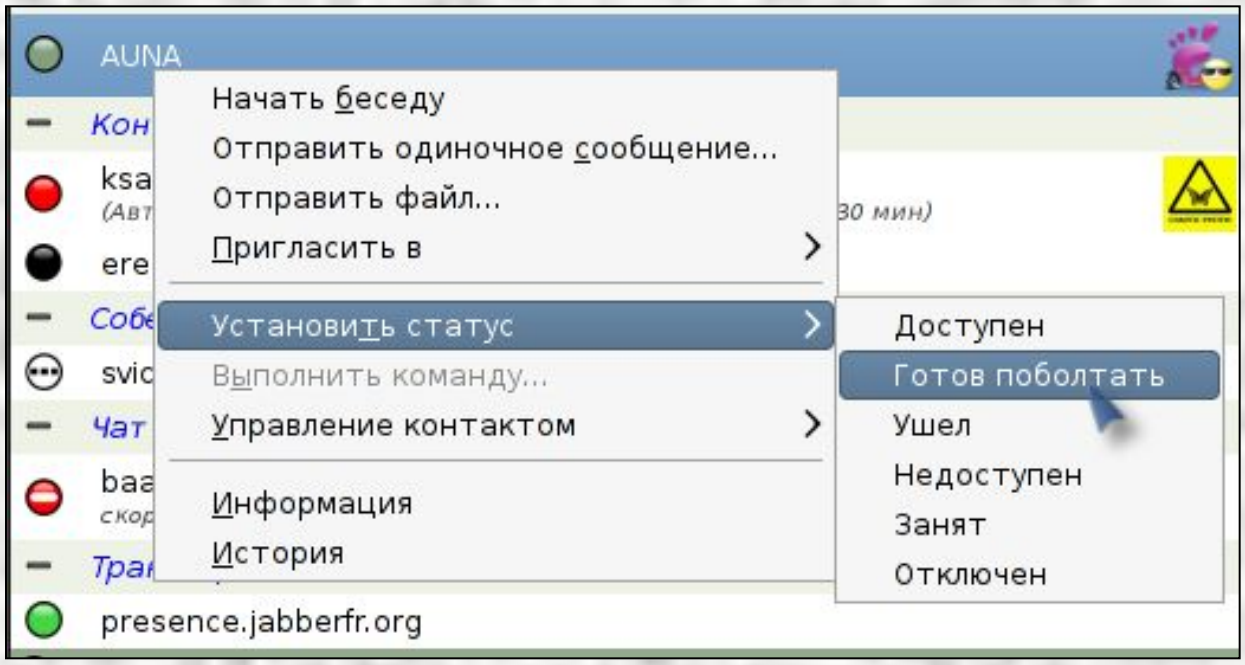



# Обмен ключами по схеме Диффи-Хеллмана

## 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 $Y_a$.**

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




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

**Если централизованно хранящийся каталог надежен, то этот 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.**