ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ, ИНФОРМАТИКИ И МЕХАНИКИ

Реализация криптопротокола распределения ключей Менезиса-Кью-Ванстоуна

Воронков Борис Николаевич, к. т. н., доцент
Школин Александр Андреевич,
студент 5-го курса факультета ПММ

Воронеж - 2021

Постановка задачи

Рассмотреть этапы перехода от первого, классического протокола Диффи-Хеллмана распределения закрытых ключей по незащищённым каналам связи к стандартизированному протоколу Менезиса-Кью-Ванстоуна.

- Реализовать моделирование и анализ работы данного криптографического протокола.

Протокол Диффи-Хеллмана

Предложенный в 1976 году двумя американскими математиками У. Диффи и М. Хеллманом, первый в истории криптографии протокол распределения ключей по незащищённым каналам связи, подтвердил, за более чем сорок лет применения, свою эффективность и надёжность. Безопасность данного криптографического протокола обусловлена вычислительной трудностью нахождения дискретных логарифмов в конечном поле большого объёма. Протокол Диффи-Хеллмана положил начало двухключевой (асимметричной) криптографии и, фактически, решил многовековую проблему функционирования симметричных (одноключевых) криптосистем, в которых две стороны обмена сообщениями должны доверять друг другу и пользоваться единым, секретным ключом при шифровании.

Протокол Диффи-Хеллмана

- Суть протокола состоит в следующем. Два абонента A и B хотят получить общий секретный ключ для использования, в дальнейшем, симметричной криптосистемы. Для этого A и B согласованно выбирают два больших целых числа (порядка двухсот или более десятичных разрядов): p и α . При этом¶
- 1. Пусть p – большое простое число ($p \sim 10^{300}$), α – примитивный корень (элемент) простого поля Галуа; $\alpha \in Z_p^*, \quad 1 < \alpha \le p-1$;

$$\left\{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p-1} \equiv 1 (\mathrm{mod}\ p)\right\} = Z_p^*$$

. α и p – общедоступны.¶

Протокол Диффи-Хеллмана

- 2. → K_A и K_B – закрытые ключи пользователей A и B. K_A и K_B – большие, случайные целые числа.
- 3. → A: $y_A = \alpha^{K_A} \bmod p$; B: $y_B = \alpha^{K_B} \bmod p$; y_A и y_B – открытые ключи пользователей.
- 4. → A и B обмениваются открытыми ключами по незащищённому каналу.
- 5. → A и B вычисляют общий секретный ключ:
- ……A: $K_S = (y_B)^{K_A} \bmod p = (\alpha^{K_B})^{K_A} \bmod p$;
- ……B: $\hat{K}_S = (y_A)^{K_B} \bmod p = (\alpha^{K_A})^{K_B} \bmod p$;
- …… $K_S = \hat{K}_S$, так как $(\alpha^{K_B})^{K_A} = (\alpha^{K_A})^{K_B}$. Теперь общий секретный ключ K_S можно использовать для обмена шифрованными данными на основе симметричной криптосистемы. Например, воспользовавшись межгосударственным стандартом ГОСТ Р 34.12-2018

Простой протокол обмена ключами Диффи-Хеллмана отлично справляется с пассивной атакой, но, к сожалению, не обеспечивает ни одного из основных свойств протоколов распределения ключей: ни аутентификацию параметров, ни подтверждение ключа, ни аутентификацию участников протокола. Активный противник может построить атаку на протокол методом включения в канал (атака "Человек посередине"). В итоге он сможет контролировать весь обмен данными между участниками. При этом они не смогут обнаружить подмену данных и будут уверены, что связываются непосредственно друг с другом.

В последующем было предложено ещё несколько протоколов. Так, в 1978 году был опубликован транспортный протокол Нидхема-Шрёдера, который требует предварительной аутентификации открытых ключей абонентов A и B. В 1980 году – бесключевой трёхэтапный протокол Ади Шамира, тоже подверженный атаке «Человек посередине». В 1988 году появился первый вариант стандарта X.509 для инфраструктуры открытых ключей и инфраструктуры управления привилегиями. Данный протокол включал в себя не только передачу подключей абонентов, из которых и формировался общий секретный ключ, но и аутентификацию сторон с использованием цифровой подписи.

- Кроме того, на одном из шагов протокола абонент А должен был подтверждать получение сообщения от В при помощи отправления подписанного сообщения. Использование меток времени противодействовало атакам с повторным использованием сообщений или с блокированием канала и отправлением искажённых (подделанных) сообщений. Принятию искажённых сообщений противодействовало также наличие цифровой подписи.
- Наконец, сочетание нескольких недостатков предыдущих протоколов было устранено в 1995 году применением протокола Менезиса-Кью-Ванстоуна (MQV-протокола), стандартизированного в 2000-м году.

Протокол Менезиса-Кью-Ванстоуна

Протокол MQV состоит в следующем. Пользователи A и B имеют каждый свой открытый и закрытый ключи.

Открытый ключи пользователей

A: $(y_A = \alpha^{K_A} \bmod p ; K_A)$

B: $(y_B = \alpha^{K_B} \bmod p ; K_B)$.

Пользователь A знает открытый ключ y_B, а абонент B знает открытый ключ y_A.

Протокол MQV

Теперь необходимо сгенерировать сеансовую пару ключей

A: $(C = \alpha^{\gamma} \bmod p; \gamma)$

B: $(D = \alpha^{\delta} \bmod p; \delta)$.

После этого пользователи обмениваются открытыми сеансовыми ключами, что напоминает протокол Диффи-Хеллмана: A отправляет B открытый ключ C, а B отправляет A открытый ключ D.

Теперь A знает: $y_A; y_B; C; D; K_A; \gamma$.

Абоненту B известны: $y_A; y_B; C; D; K_B; \delta$.

Протокол MQV

Чтобы получить общий секретный ключ пользователь A задаёт число λ, равное размеру сообщения в битах, делённому на 2 (для протокола MQV на эллиптических кривых $\lambda = 80$).

Далее пользователь A:

1. Задаёт $i = C$.
2. Находит $S_A = (i \pmod{2^\lambda}) + 2^\lambda$.
3. Задаёт $j = D$.
4. Вычисляет $T_A = (j \pmod{2^\lambda}) + 2^\lambda$.
5. Находит $h_A = \gamma + S_A \cdot K_A$.
6. Вычисляет $P_A = (D \cdot y_B^{T_A})^{h_A} \bmod p$.

Протокол MQV

Пользователь B производит те же вычисления, взяв свои закрытые ключи:

1. Задаёт $i = D$.
2. Находит $S_B = (i \,(\mathrm{mod}\, 2^{\lambda})) + 2^{\lambda}$.
3. Задаёт $j = C$.
4. Вычисляет $T_B = (j \,(\mathrm{mod}\, 2^{\lambda})) + 2^{\lambda}$.
5. Находит $h_B = \delta + S_B \cdot K_B$.
6. Вычисляет $P_B = (C \cdot y_A^{\,T_B})^{h_B} \bmod p$.

Как видно, $P_A = P_B$ – это и будет общим секретным ключом.

Плюсы и минусы протокола MQV

Преимущества протокола MQV:

1. Устойчивость к атаке «Человек посередине».
2. Небольшой размер сообщения.
3. Удобная реализация протокола, не требующая от пользователя электронной подписи под каждым сообщением.
4. По сравнению с RSA, формирование общего закрытого ключа происходит в разы быстрее, потому что в криптосистеме RSA много времени занимает генерация новых простых чисел, на которых основана генерация новых открытых и закрытых ключей.

Недостатком MQV-протокола является необходимость привлечения центра сертификации открытых ключей пользователей, чтобы подтвердить их аутентичность.

Программная реализация протокола MQV

Реализуем алгоритм получения общего секретного ключа для пользователей A и B в программной среде Visual Studio 2010.

На рисунке 1 приведен пример.

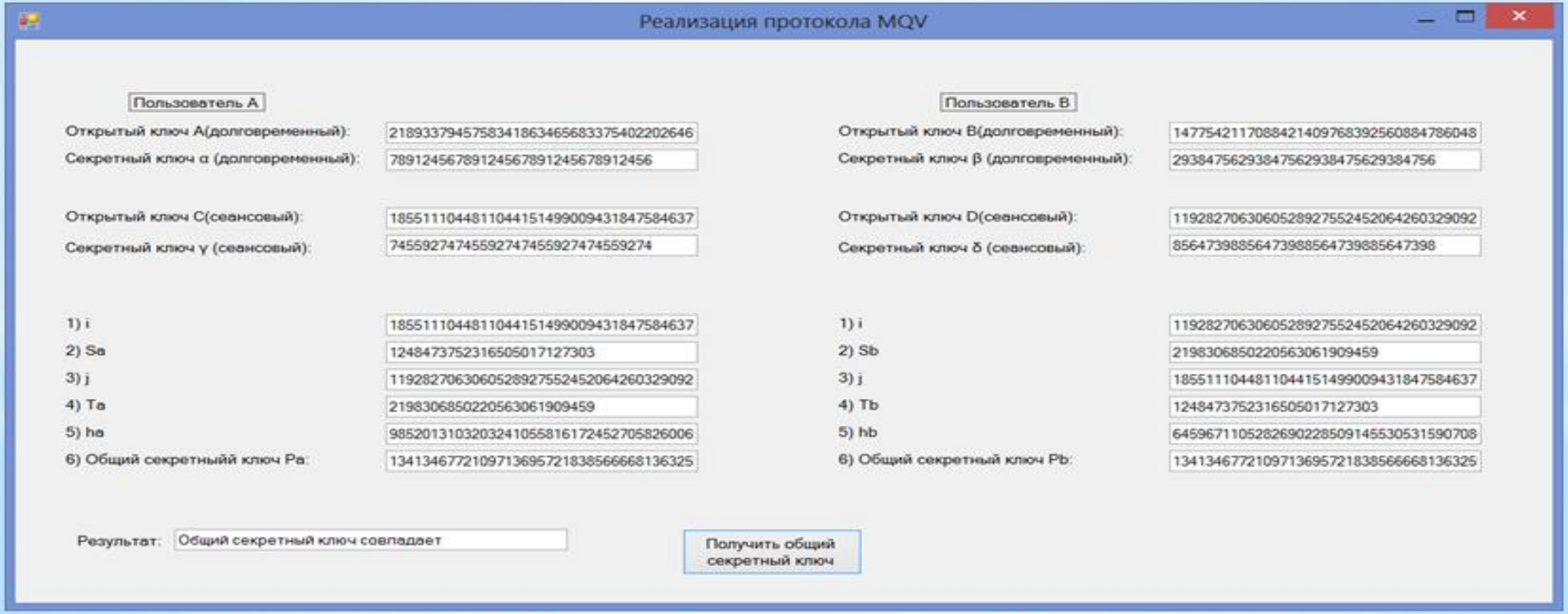
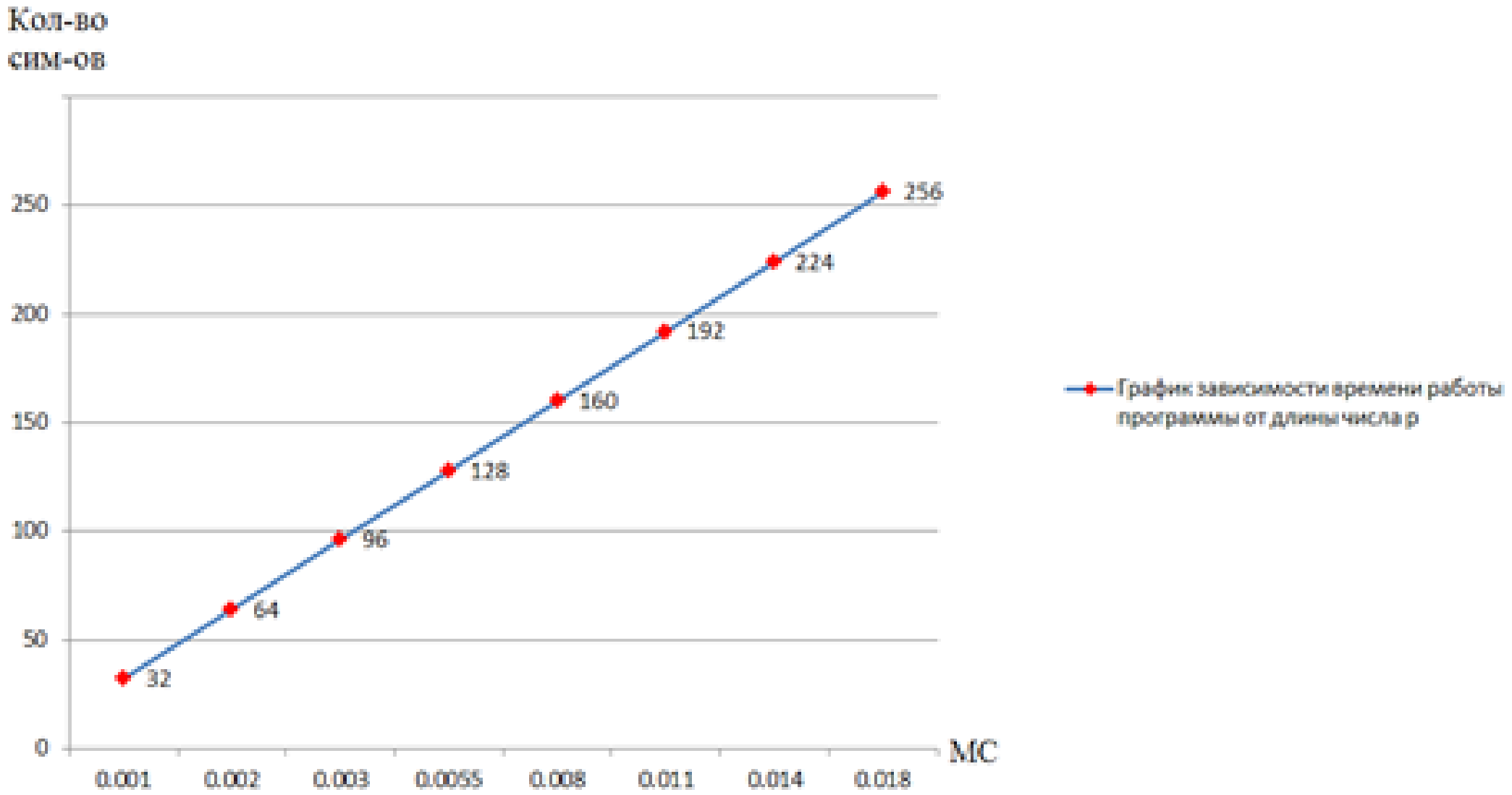


Рисунок 1. Пример получения общего секретного ключа

График зависимости времени работы программы от длины числа p



Выводы

Таким образом, в работе рассмотрены этапы двадцатилетнего перехода от первого, классического протокола Диффи-Хеллмана распределения секретных ключей по незащищённым каналам связи к стандартизированному протоколу Менезиса-Кью-Ванстоуна. Кратко описаны достоинства и недостатки, разработанных в этот период протоколов. Реализовано компьютерное моделирование протокола MQV. Проведённый вычислительный эксперимент и выявленный линейный характер зависимости времени работы компьютерной программы от длины ключа подтверждают теоретические предположения и позволяют обоснованно выбирать значения параметров протокола MQV, а также возможность, на основе данной программы, создавать новые приложения для защищённой связи с использованием современных стандартов блочного и поточного шифрования.

Библиография

1. Diffie B. W. New Directions in Cryptography / B. W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976. – Pp. 644 – 654.

2. Ниссенбаум О. В. Криптографические протоколы: Учебное пособие / О. В. Ниссенбаум. – Тюмень: Изд-во Тюменского гос. ун-та, 2007. – 112 с.

3. Menezes A. Some New Key Agreement Protocols Providing Implicit Authentication / A. Menezes, M. Qu, S. Vanstone // workshop record, 2nd Workshop Selected Areas in Cryptography (SAC-95), Ottawa, Canada, May 1995. – Pp. 22 – 32.

4. Standard IEEE P1363-2000. – URL: https://perso.telecom-paristech.fr/guilley/recherche/cryptoprocesseurs/ieee/00891000.pdf (дата обращения 5.01.2021)

5. ГОСТ Р 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2018. – 17 с.

Б Л А Г О Д А Р Ю
З А В Н И М А Н И Е !