**Часть 2 – Протоколы идентификации и аутентификации**

*Задание 1. Протокол Фейга-Фиата-Шамира*

Описание:

Стороны А и В выбирают простые секретные числа *p* и *q* и вычисляют открытое число *N* по формуле:

(2.1.1)

Сторона А выбирает секретный ключ с условием:

НОД (2.1.2)

Затем сторона А вычисляет открытый ключ по формуле:

(2.1.3)

Сторона А выбирает случайное число *r*, исходя из условия:

(2.1.4)

Сторона А отправляет стороне В значения *r, N, .* Сторона В вычисляет значение по формуле:

(2.1.5)

И отправляет стороне А значение x, которое должно удовлетворять условию . После этого сторона А вычисляет значение y по формуле:

(2.1.6)

Сторона А отправляет стороне В вычисленное значение *y.* После чего сторона В вычисляет по формуле:

(2.1.7)

Если стороны А совпадает с стороны В, то идентификация прошла успешно.

Выполним процедуру идентификации для трех циклов аккредитации в соответствии с протоколом Фейга-Фиата-Шамира:

1. Согласно исходным данным
2. Рассчитаем N по формуле (2.1.1):
3. Сторона А выбирает секретный ключ , согласно исходным данным . Проверим условие (2.1.2), что НОД:

61 5771

61 37

24 37

24 13

11 13

11 2

3 2

1. 2

1 0

Условие выполняется.

1. Сторона А вычисляет открытый ключ по формуле (2.1.3):

Сначала найдем значение после чего приступим к вычислению отрицательной степени:

Далее избавимся от отрицательной степени с помощью формулы:

(2.1.8)

где - функция Эйлера, которая рассчитывается по формулам:

а) Если с – составное число:

б) Если с – простое число: .

в) В RSA:

Воспользуемся третьей формулой:

Следовательно:

Рассчитаем данное значение*:*

Получим, что открытый ключ имеет значение:

1. Сторона А выбирает случайное число *r*, удовлетворяющее условию (2.1.4). Согласно исходным данным, для трех этапов идентификации Проверим, удовлетворяют ли заданные значения *r* вышеуказанному условию.

а) Для :

Удовлетворяет.

б) Для :

Удовлетворяет.

в) Для :

Удовлетворяет.

1. Процесс идентификации:
   1. Первый этап идентификации ():

Сторона А отправляет стороне В значения *r,N, .*

Сторона В вычисляет значение по формуле (2.1.5):

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации .

Сторона А вычисляет значение *y* по формуле (2.1.6) :

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.1.7):

Первый этап идентификации прошел успешно.

* 1. Второй этап идентификации ():

Сторона А отправляет стороне В значения *r,N, .*

Сторона В вычисляет значение по формуле (2.1.5):

Сторона В отправляет стороне А значение . Согласно исходным данным, для второго этапа идентификации .

Сторона А вычисляет значение по формуле (2.1.6) :

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.1.7):

Второй этап идентификации прошел успешно.

* 1. Третий этап идентификации ():

Сторона А отправляет стороне В значения *r,N, .*

Сторона В вычисляет значение по формуле (2.1.5):

Сторона В отправляет стороне А значение . Согласно исходным данным, для третьго этапа идентификации .

Сторона А вычисляет значение по формуле (2.1.6):

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.1.7):

Третий этап идентификации прошел успешно.

*Задание 2. Протокол Шнорра*

Описание:

Стороны А и В выбирают простые секретные числа *p* и *q*, которые должны удовлетворять условию:

(2.2.1)

Сторона А выбирает секретный ключ с условием:

(2.2.2)

Выбирает значение , таким, что:

(2.2.3)

Затем сторона А вычисляет открытый ключ (сертификат) по формуле:

(2.2.4)

Сторона А выбирает случайное число *r*, исходя из условия:

(2.2.5)

Сторона А вычисляет значение :

(2.2.6)

Сторона А передает стороне В значения , α, . Сторона В передает стороне А значение x, которое должно удовлетворять условию:

(2.2.7)

После этого сторона А вычисляет значение y по формуле:

(2.2.8)

Сторона А отправляет стороне В вычисленное значение *y.* После чего сторона В вычисляет по формуле:

(2.2.9)

Если стороны А совпадает с стороны В, то идентификация прошла успешно.

Выполним процедуру идентификации для трех циклов аккредитации в соответствии с протоколом Шнорра:

1. Согласно исходным данным Выполним проверку условия (2.2.1):

Условие выполняется.

1. Сторона А выбирает секретный ключ , который согласно исходным данным равен . Проверим, выполняется ли условие (2.2.2):

Условие (2.2.2) выполняется.

1. Сторона А выбирает значение , которое удовлетворяет условию (2.2.3).

Пусть , тогда проверим, что :

Рассчитаем данное значение:

Получим, что

Условие (2.2.3) не выполняется.

Пусть , тогда проверим, что :

Рассчитаем данное значение:

Получим, что

Условие (2.2.3) выполняется.

1. Сторона А вычисляет открытый ключ по формуле (2.2.4):

Сначала найдем значение после чего приступим к вычислению отрицательной степени:

Получим .

Далее избавимся от отрицательной степени с помощью формулы (2.1.8). . Так как 149 – простое число:

Следовательно:

Рассчитаем данное значение*:*

Получим, что открытый ключ имеет значение:

1. Сторона А выбирает случайное число *r*, удовлетворяющее условию (2.2.5). Согласно исходным данным, для трех этапов идентификации Проверим, удовлетворяют ли заданные значения *r* вышеуказанному условию.

а) Для :

Удовлетворяет.

б) Для :

Удовлетворяет.

в) Для :

Удовлетворяет.

1. Процесс идентификации:
   1. Первый этап идентификации ():

Сторона А вычисляет значение по формуле (2.2.6):

Сторона А отправляет стороне В значения *α, , .*

Сторона В отправляет стороне А значение удовлетворяющее условию (2.2.7). Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.2.7):

Сторона А вычисляет значение *y* по формуле (2.2.8) :

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.2.9):

Получим:

Первый этап идентификации прошел успешно.

* 1. Второй этап идентификации ():

Сторона А вычисляет значение по формуле (2.2.6):

Сторона А отправляет стороне В значения *α, , .*

Сторона В отправляет стороне А значение удовлетворяющее условию (2.2.7). Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.2.7):

Сторона А вычисляет значение *y* по формуле (2.2.8) :

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.2.9):

Получим:

Второй этап идентификации прошел успешно.

* 1. Третий этап идентификации ():

Сторона А вычисляет значение по формуле (2.2.6):

Сторона А отправляет стороне В значения *α, , .*

Сторона В отправляет стороне А значение удовлетворяющее условию (2.2.7). Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.2.7):

Сторона А вычисляет значение *y* по формуле (2.2.8) :

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.2.9):

Рассчитаем данное значение*:*

Получим:

Таким образом:

Третий этап идентификации прошел успешно.

*Задание 3. Протокол Окамото*

Описание:

Стороны А и В выбирают простые секретные числа *p* и *q*, которые должны удовлетворять условию:

(2.3.1)

Сторона А выбирает секретный ключ , сторона В выбирает секретный ключ с условием:

(2.3.2)

Стороны выбирают значения , такими, что:

(2.3.3)

Затем сторона А вычисляет открытый ключ (сертификат) по формуле:

(2.3.4)

Сторона А выбирает случайные числа , исходя из условия:

(2.3.5)

Сторона А вычисляет значение :

(2.3.6)

Сторона А передает стороне В значения , , . Сторона В передает стороне А значение x, которое должно удовлетворять условию:

(2.3.7)

После этого сторона А вычисляет значения и по формуле:

, (2.3.8)

Сторона А отправляет стороне В вычисленные значения и *.* После чего сторона В вычисляет по формуле:

(2.3.9)

Если стороны А совпадает с стороны В, то идентификация прошла успешно.

Выполним процедуру идентификации для двух циклов аккредитации в соответствии с протоколом Окамото:

1. Согласно исходным данным Выполним проверку условия (2.3.1):

Условие выполняется.

1. Сторона А выбирает секретный ключ , которые согласно исходным данным равны: . Проверим, выполняется ли условие (2.3.2):

Условие (2.3.2) выполняется в обоих случаях.

1. Сторона А выбирает значение , которые удовлетворяют условию (2.2.3).

Пусть , тогда проверим, что :

Рассчитаем данное значение:

Получим, что

Условие (2.3.3) не выполняется.

Пусть , тогда проверим, что :

Рассчитаем данное значение:

Получим, что

Условие (2.3.3) выполняется.

Пусть , тогда проверим, что :

Рассчитаем данное значение:

Получим, что

Условие (2.3.3) выполняется.

Получили

1. Сторона А вычисляет открытый ключ по формуле (2.3.4):

Получим .

Далее избавимся от отрицательных степеней с помощью формулы (2.1.8). .

Так как 139 – простое число:

Следовательно:

Получим данное значение:

Получим данное значение:

Откуда:

Получим, что открытый ключ имеет значение:

1. Сторона А выбирает случайное число *r*, удовлетворяющее условию (2.3.5). Согласно исходным данным, для двух этапов идентификации Проверим, удовлетворяют ли заданные значения *r* вышеуказанному условию.

а) Для :

Удовлетворяет.

б) Для :

Удовлетворяет.

1. Процесс идентификации:
   1. Первый этап идентификации ():

Сторона А вычисляет значение по формуле (2.3.6):

Сторона А отправляет стороне В значения *, , .*

Сторона В отправляет стороне А значение удовлетворяющее условию (2.2.7). Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.3.7):

Сторона А вычисляет значения и по формуле (2.3.8):

Сторона А отправляет стороне В значения и

Сторона В производит вычисление по формуле (2.3.9):

Рассчитаем данное значение:

Получим:

Первый этап идентификации прошел успешно.

* 1. Второй этап идентификации ():

Сторона А вычисляет значение по формуле (2.3.6):

Сторона А отправляет стороне В значения *, , .*

Сторона В отправляет стороне А значение удовлетворяющее условию (2.2.7). Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.3.7):

Сторона А вычисляет значения и по формуле (2.3.8):

Сторона А отправляет стороне В значения и

Сторона В производит вычисление по формуле (2.3.9):

Получим:

Второй этап идентификации прошел успешно.

*Задание 4. Протокол GQ (Гиллу-Кискатр)*

Описание:

Стороны А и В выбирают простые секретные числа *p* и *q* и вычисляют открытое число *N* по формуле:

(2.4.1)

Стороны выбирают открытое число , такое, что удовлетворяет условию:

(2.4.2)

Выбирают секретный ключ (не простое число) с условием:

НОД (2.4.3)

Затем сторона А вычисляет открытый ключ по формуле:

(2.4.4)

При этом . Сторона А выбирает случайное число *r*, исходя из условия:

(2.4.5)

Сторона А отправляет стороне В значения *, N, ,* при чем значение сторона А вычисляет по формуле:

(2.4.6)

Сторона В отправляет стороне А значение x, которое должно удовлетворять условию:

(2.4.7)

После этого сторона А вычисляет значение y по формуле:

(2.4.8)

Сторона А отправляет стороне В вычисленное значение *y.* После чего сторона В вычисляет по формуле:

(2.4.9)

Если стороны А совпадает с стороны В, то процесс идентификации прошел успешно.

Выполним процедуру идентификации для трех циклов аккредитации в соответствии с протоколом GQ:

1. Согласно исходным данным
2. Рассчитаем N по формуле (2.4.1):
3. Сторона А выбирает открытое число . Согласно исходным данным . Проверим условие(2.4.2). Для этого вычислим значение по формуле

61 8364

61 7

5 7

5 2

1 2

1 0

(2.1.8). Так как 8549 – это составное число, то:

Условие выполняется

1. Выберем секретный ключ , чтоб он удовлетворял

21 8549

21 2

2 1

0 1

условию (2.4.3), что НОД. Пусть

Условие выполняется.

1. Сторона А вычисляет открытый ключ по формуле (2.4.4):

Сначала найдем значение

Рассчитаем данное значение:

Получим:

Далее избавимся от отрицательной степени с помощью формулы(2.1.8).

Получим:

Следовательно:

Рассчитаем данное значение*:*

Получим, что открытый ключ имеет значение:

1. Сторона А выбирает случайное число *r*, удовлетворяющее условию (2.4.5). Согласно исходным данным, для трех этапов идентификации Проверим, удовлетворяют ли заданные значения *r* вышеуказанному условию.

а) Для :

Удовлетворяет.

б) Для :

Удовлетворяет.

в) Для :

Удовлетворяет.

1. Процесс идентификации:
   1. Первый этап идентификации ():

Сторона А отправляет стороне В значения *r,N, , γ.* При этом сторона А вычисляет значение *γ* по формуле (2.4.6):

Рассчитаем данное значение:

Получим:

Таким образом:

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.4.7):

Условие выполняется.

Сторона А вычисляет значение *y* по формуле (2.4.8):

Таким образом:

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.4.9):

Рассчитаем значения и :

Получим:

Получим:

Первый этап идентификации прошел успешно.

* 1. Второй этап идентификации ():

Сторона А отправляет стороне В значения *r,N, .* При этом сторона А вычисляет значение *γ* по формуле (2.4.6):

Рассчитаем данное значение:

Получим:

Таким образом:

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.4.7):

Условие выполняется.

Сторона А вычисляет значение *y* по формуле (2.4.8):

Таким образом:

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.4.9):

Рассчитаем значения и :

Получим:

Второй этап идентификации прошел успешно.

* 1. Третий этап идентификации ():

Сторона А отправляет стороне В значения *r,N, .* При этом сторона А вычисляет значение *γ* по формуле (2.4.6):

Рассчитаем данное значение:

Получим:

Таким образом:

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.4.7):

Условие выполняется.

Сторона А вычисляет значение *y* по формуле (2.4.8):

Таким образом:

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.4.9):

Получим:

Третий этап идентификации прошел успешно.

*Задание 5. Протокол GQ (Гиллу-Кискатр) с ключами, зависящими от идентификатора*

Описание:

Стороны А и В выбирают простые секретные числа *p* и *q* и вычисляют открытое число *N* по формуле:

(2.5.1)

Стороны выбирают открытое число , такое, что удовлетворяет условию:

(2.5.2)

Выбирают значение секретного числа d, так чтоб удовлетворяло условию:

(2.5.3)

Сторона А имеет свой идентификатор, а именно его хэш-функцию .

Сторона А выбирает секретный ключ по формуле:

(2.5.4)

Затем сторона А вычисляет открытый ключ по формуле:

(2.5.5)

При этом, если , то все выполнено верно.

Процесс идентификации:

1. Сторона А выбирает случайное число *r*, исходя из условия:

(2.5.6)

И затем отправляет стороне В свой идентификатор и значение *,* при чем значение сторона А вычисляет по формуле:

(2.5.7)

1. Сторона В отправляет стороне А значение x, которое должно удовлетворять условию:

(2.5.8)

1. Сторона А вычисляет значение y по формуле:

(2.5.9)

Проверка:

Сторона А отправляет стороне В вычисленное значение *y.* После чего сторона В вычисляет по формуле:

(2.5.10)

Если стороны А совпадает с стороны В, то процесс идентификации прошел успешно.

Выполним процедуру идентификации для трех циклов аккредитации в соответствии с протоколом GQ с ключами, зависящими от идентификаторов:

1. Согласно исходным данным
2. Рассчитаем N по формуле (2.5.1):
3. Сторона А выбирает открытое число . Согласно исходным данным . Проверим условие(2.5.2). Для этого вычислим значение по формуле

31 7176

31 15

1 15

1 0

(2.1.8). Так как 7379– это составное число, то:

Условие выполняется

1. Выбирают значение секретного числа d, так чтоб удовлетворяло условию (2.5.3):

Путем подбора величины d, получили, что Проверим условие (2.5.3):

Условие выполняется.

1. Выберем секретный ключ по формуле (2.5.4), при чем согласно исходным данным, уникальный идентификатор стороны А . Получим выражение:

Вычислим значение :

Получим:

Избавимся от отрицательной степени с помощью формулы(2.1.8).

Получим, что

1. Сторона А вычисляет открытый ключ по формуле (2.5.5):

Сначала найдем значение

Рассчитаем данное значение:

Получим:

Далее избавимся от отрицательной степени с помощью формулы(2.1.8).

Получим:

Следовательно:

1. Сторона А выбирает случайное число *r*, удовлетворяющее условию (2.5.6). Согласно исходным данным, для трех этапов идентификации Проверим, удовлетворяют ли заданные значения *r* вышеуказанному условию.

а) Для :

Удовлетворяет.

б) Для :

Удовлетворяет.

в) Для :

Удовлетворяет.

1. Процесс идентификации:
   1. Первый этап идентификации ():

Сторона А отправляет стороне В свой идентификатор h(A) и значение *γ.* При этом сторона А вычисляет значение *γ* по формуле (2.5.7):

Рассчитаем данное значение:

Получим:

Таким образом:

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.5.8):

Условие выполняется.

Сторона А вычисляет значение *y* по формуле (2.5.9):

Таким образом:

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.5.10):

Получим:

Первый этап идентификации прошел успешно.

* 1. Второй этап идентификации ():

Сторона А отправляет стороне В свой уникальный идентификатор и значение *γ.* При этом сторона А вычисляет значение *γ* по формуле (2.5.7):

Рассчитаем данное значение:

Получим:

Таким образом:

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.5.8):

Условие выполняется.

Сторона А вычисляет значение *y* по формуле (2.5.9):

Таким образом:

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.5.10):

Получим:

Второй этап идентификации прошел успешно.

* 1. Третий этап идентификации ():

Сторона А отправляет стороне В своего уникального идентификатора и значение *γ.* При этом сторона А вычисляет значение *γ* по формуле (2.5.7):

Рассчитаем данное значение:

Получим:

Таким образом:

Сторона В отправляет стороне А значение . Согласно исходным данным, для первого этапа идентификации . Проверим условие (2.5.8):

Условие выполняется.

Сторона А вычисляет значение *y* по формуле (2.4.8):

Таким образом:

Сторона А отправляет стороне В значение

Сторона В производит вычисление по формуле (2.5.10):

Получим:

Третий этап идентификации прошел успешно.

*Задание 6. Параллельная схема с нулевой передачей знаний*

Описание:

В данном алгоритме стороны А и В выбирают два простых числа *p* и *q.* Затем определяют значение *N* по формуле:

(2.6.1)

Сторона А выбирает k различных чисел , где является квадратичным вычетом:

(2.6.2)

Также следует отметить, что является открытым ключом стороны А.

Далее определяются секретные ключи , такие что:

(2.6.3)

Следует отметить, что при выборе и обязательно выполнение условий, что .

Процесс идентификации:

1. Сторона А передает стороне В свой открытый ключ и значение γ, которое вычисляется по формуле:

, (2.6.4)

где r – случайное число, удовлетворяющее условию:

(2.6.5)

1. Сторона В передает стороне А значения , где .
2. Сторона А передает стороне В вычисленное значение y:

(2.6.6)

1. Сторона В выполняет проверку:

(2.6.7)

Выполним процедуру идентификации для двух циклов аккредитации, используя параллельную схему с нулевой передачей знаний:

1. Согласно исходным данным
2. Определим значение *N* по формуле (2.6.1):
3. Сторона А выбирает k различных чисел , где является квадратичным вычетом по формуле (2.6.2):

Сведем значения , полученные выше, в *таблицу 2.1*, куда также запишем значения .

Таблица 2.1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 4 | 9 | 16 | 25 | 36 | 64 | 81 | 100 | 2 | 50 | 106 | 18 | 86 | 43 | 8 | 53 | 30 | 15 | 67 | 72 | 60 | 93 | 32 |
|  | 1 | 30 | 53 | 67 | 100 | 43 | 106 | 72 | 25 | 60 | 50 | 64 | 86 | 18 | 36 | 15 | 9 | 4 | 8 | 16 | 81 | 2 | 32 | 93 |
|  | 1 | 25 | 23 | 30 | 10 | 20 | 15 | 32 | 5 | 37 | 13 | 8 | 18 | 16 | 6 | 27 | 3 | 2 | 22 | 4 | 9 | 11 | 44 | 39 |

Приведем расчеты всех значений , воспользовавшись формулой (2.1.8):

1. Далее определим секретные ключи по формуле (2.6.3). Рассчитаем данные значения вычислением корня значений из табл. 2.1, те значения, у которых не является целым значением, найдем методом подбора. Полученные значения запишем в табл. 2.1.

Следует отметить, что при выборе и обязательно выполнение условий, что . Значения, которые удовлетворяют всем условиям запишем в табл. 2.2.

Таблица 2.2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 4 | 9 | 16 | 25 | 36 | 64 | 81 | 100 | 2 | 106 | 86 | 43 | 8 | 53 | 30 | 15 | 67 | 72 | 60 | 93 | 32 |
|  | 30 | 53 | 67 | 100 | 43 | 106 | 72 | 25 | 60 | 64 | 18 | 36 | 15 | 9 | 4 | 8 | 16 | 81 | 2 | 32 | 93 |
|  | 25 | 23 | 30 | 10 | 20 | 15 | 32 | 5 | 37 | 8 | 16 | 6 | 27 | 3 | 2 | 22 | 4 | 9 | 11 | 44 | 39 |

Для первого этапа идентификации сторона А выбирает из и 6 значений: и . Для второго этапа идентификации сторона А выбирает из и 7 значений: и .

На этом процесс формирования открытых и закрытых ключей окончен.

Процесс идентификации:

Первый этап идентификации (r=20):

* 1. Сторона А передает стороне В свой сертификат и значение γ, которое вычисляется по формуле (2.6.4), при чем r должно удовлетворять условию (2.6.5):

Условие (2.6.5) выполняется. Вычислим γ:

* 1. Сторона В передает стороне А значения , где . Согласно исходным данным, x=43. Переведем число 43 в двоичную форму:

Получим, что .

* 1. Сторона А передает стороне В вычисленное по формуле (2.6.6) значение y:

8.1 Сторона В выполняет проверку по формуле (2.6.7):

Первый этап идентификации прошел успешно.

Второй этап идентификации (r=21):

* 1. Сторона А передает стороне В свой сертификат и значение γ, которое вычисляется по формуле (2.6.4), при чем r должно удовлетворять условию (2.6.5):

Условие (2.6.5) выполняется. Вычислим γ:

* 1. Сторона В передает стороне А значения , где . Согласно исходным данным, x=122. Переведем число 122 в двоичную форму:

Получим, что .

* 1. Сторона А передает стороне В вычисленное по формуле (2.6.6) значение y:

8.1 Сторона В выполняет проверку по формуле (2.6.7):

Второй этап идентификации прошел успешно.

**Часть 3 – Протоколы распределения ключей**

*Задание 1. Протокол Диффи-Хеллмана*

Описание:

Стороны А и В договариваются о некотором значении *p* ( *p* – простое число). После чего выбирают число , которое удовлетворяет условию:

(3.1.1)

Каждый из пользователей выбирает свой секретный ключ: сторона А выбирает , а сторона В . При чем эти секретные ключи должны удовлетворять условиям:

(3.1.2)

(3.1.3)

Затем каждый из пользователей вычисляет свои открытые ключи:

(3.1.4)

(3.1.5)

Стороны обмениваются открытыми ключами. После чего вычисляют сеансовый ключ:

(3.1.6)

(3.1.7)

Если и совпали, значит все верно.

Выполним процедуру выработки общего ключа протоколом Диффи-Хеллмана:

1. Согласно исходным данным *p = 199*, и *a = 69.* Проверим условие (3.1.1):

Условие (3.1.1) выполняется.

1. Каждый из пользователей выбирает свой секретный ключ: сторона А выбирает , а сторона В . Согласно исходным данным , а . Проверим условия (3.1.2) и (3.1.3):

Оба эти условия выполняются.

1. Затем каждый из пользователей вычисляет свои открытые ключи по формулам (3.1.4) для стороны А и (3.1.5) для стороны В:
2. Стороны обмениваются открытыми ключами. После чего сторона А вычисляет сеансовый ключ по формуле (3.1.6) , а сторона В вычисляет сеансовый ключ по формуле (3.1.7):

и совпали, следовательно, все верно.

*Задание 2. Протокол Шамира-Ривеста-Адлемана*

Описание:

Данный протокол предназначен не для распределения ключей, а для передачи ключа. Для выполнения процедуры передачи ключа стороны А и В должны выбрать простое число p. Каждая из сторон должна иметь свой секретный ключ, сторона А ключ , сторона В ключ . Также у стороны А должен быть ключ , который она хочет передать. Для расчетов необходимо рассчитать значения по формулам:

(3.2.1)

(3.2.2)

Процесс передачи происходит следующим образом:

1. Сторона А передает стороне В свой открытый ключ , вычисленный по формуле:

(3.2.3)

1. Сторона В передает стороне А свой открытый ключ , вычисленный по формуле:

(3.2.4)

1. Сторона А передает стороне В некое значение C, которое является секретным ключом, преобразованным в некий зашифрованный вид по формуле:

(3.2.5)

1. Сторона В получает непосредственно сам ключ преобразованием:

(3.2.6)

Если все расчеты верны, то изначальное значение стороны А должно совпасть со значением , полученным стороной В.

Выполним процедуру передачи ключа протоколом Шамира-Ривеста-Адлемана:

1. Согласно исходным данным .
2. Секретный ключ стороны А , стороны В (согласно исходным данным).
3. Ключ, который необходимо передать .
4. Произведем расчет значений по формулам (3.2.1) и (3.2.2) соответственно:

Рассчитаем значение по формуле (2.1.8):

1. Выполним процесс передачи ключа следующим образом:
   1. Сторона А передает стороне В свой открытый ключ , вычисленный по формуле (3.2.3):

5.2 Сторона В передает стороне А свой открытый ключ , вычисленный по формуле (3.2.4):

5.3 Сторона А передает стороне В некое значение C, которое является секретным ключом, преобразованным в некий зашифрованный вид по формуле(3.2.5):

5.4 Сторона В получает непосредственно сам ключ преобразованием (3.2.6):

Изначальное значение стороны А совпало со значением , полученным в пункте 5.4.

*Задание 3. Протокол MTI*

Описание:

Стороны договариваются о некотором простом числе . После чего выбирают значение , такое, что удовлетворяет условию:

(3.3.1)

Каждая сторона выбирает свой секретный ключ соответственно сторона А и В. Затем каждая сторона вычисляет свой открытый ключ:

Сторона А по формуле:

(3.3.2)

Сторона В по формуле:

(3.3.3)

Сторона А выбирает значение , и на основании этого значения вычисляет по формуле:

(3.3.4)

Сторона В выбирает значение , и на основании этого значения вычисляет по формуле:

(3.3.5)

Стороны обмениваются своими открытыми ключами и значениями и . После чего каждый вычисляет сеансовый ключ:

(3.3.6)

(3.3.7)

Выполним процедуру выработки общего ключа протоколом MTI:

1. Согласно исходным данным Проверим условие (3.3.1), для этого вычислим значение по формуле (2.1.8). Так как 233 – это простое число, то:

Условие (3.3.1) выполняется.

1. Секретный ключ стороны А согласно исходным данным , а секретный ключ стороны В согласно исходным данным .
2. Сторона А вычисляет свой открытый ключ по формуле (3.3.2):
3. Сторона B вычисляет свой открытый ключ по формуле(3.3.3):
4. Значение стороны А согласно исходным данным . Вычислим значение по формуле (3.3.4):
5. Значение стороны B согласно исходным данным . Вычислим значение по формуле (3.3.5):
6. Стороны обмениваются своими открытыми ключами и значениями и . После чего каждый вычисляет сеансовый ключ по формулам (3.3.6) и (3.3.7) соответственно:

Вычислим значение

Вычислим значение

Получим значение :

Рассчитаем значение сеансового ключа стороны В:

Вычислим значение

Вычислим значение

Получим значение :

Так как ключи и совпали, значит все верно рассчитано.

*Задание 4. Протокол KEA (Key Exchange Algorithm)*

Описание:

Стороны договариваются о некоторых простых числах . После чего выбирают значение , такое, что удовлетворяет условию:

(3.4.1)

Каждая сторона выбирает свой секретный ключ соответственно сторона А и В. Затем каждая сторона вычисляет свой открытый ключ:

Сторона А по формуле:

(3.4.2)

Сторона В по формуле:

(3.4.3)

Сторона А выбирает значение , и на основании этого значения вычисляет по формуле:

(3.4.4)

Сторона А передает стороне В свой открытый ключ и значение . Сторона В выполняет проверку условий для:

(3.4.5)

(3.4.6)

Если условия выполняются, сторона В выбирает значение , и на основании этого значения вычисляет по формуле:

(3.4.7)

Сторона В передает стороне А свой открытый ключ и значение . Сторона А выполняет проверку условий для:

(3.4.8)

(3.4.9)

Если условия выполняются, то каждый вычисляет сеансовый ключ:

(3.4.10)

(3.4.11)

Выполним процедуру выработки общего ключа протоколом KEA:

1. Согласно исходным данным .
2. Значение выберем таким, чтоб удовлетворялось условие (3.4.1). Пусть . Проверим условие (3.4.1):

Условие (3.4.1) выполняется.

1. Согласно исходным данным секретный ключ стороны А , а секретный ключ стороны В .
2. Сторона А вычисляет свой открытый ключ по формуле(3.4.2):
3. Сторона B вычисляет свой открытый ключ по формуле(3.4.3):
4. Сторона А выбирает значение , которое согласно исходным данным . На основании этого значения вычислим по формуле:
5. Сторона А передает стороне В свой открытый ключ и значение . Сторона В выполняет проверку условий для, используя формулы (3.4.5) и (3.4.6):

Первое условие выполняется.

Второе условие также выполнятся.

1. Сторона В выбирает значение , которое согласно исходным данным . На основании этого значения вычислим по формуле (3.4.7):
2. Сторона В передает стороне А свой открытый ключ и значение . Сторона А выполняет проверку условий для, используя формулы (3.4.8) и (3.4.9):

Первое условие выполняется.

Второе условие также выполнятся.

1. Сторона А вычисляет сеансовый ключ по формуле (3.4.10):

Вычислим значение :

Вычислим значение :

Получим значение :

1. Сторона В вычисляет сеансовый ключ по формуле (3.4.11):

Вычислим значение :

Вычислим значение :

Получим значение :

Так как ключи и совпали, значит все верно рассчитано.

*Задание 5. Протокол MQV*

Описание:

Стороны договариваются о некоторых простых числах , где – простой делитель числа . После чего выбирают значение , такое, что удовлетворяет условию:

(3.5.1)

Каждая сторона выбирает свой секретный ключ соответственно сторона А и В. Секретные ключи должны удовлетворять условию:

(3.5.2)

Затем каждая сторона вычисляет свой открытый ключ:

Сторона А по формуле:

(3.5.3)

Сторона В по формуле:

(3.5.4)

Сторона А выбирает значение , которое должно удовлетворять условию:

(3.5.5)

На основании этого значения вычисляет по формуле:

(3.5.6)

Для упрощения дальнейших расчетов необходимо рассчитать:

(3.5.7)

(3.5.8)

Сторона А передает стороне В свой открытый ключ и значение . Затем сторона В выбирает значение , которое должно удовлетворять условию:

(3.5.9)

На основании этого значения вычисляет по формуле:

(3.5.10)

Для упрощения дальнейших расчетов необходимо рассчитать:

(3.5.11)

(3.5.12)

Сторона В передает стороне А свой открытый ключ и значение .

Каждая сторона вычисляет сеансовый ключ:

(3.5.13)

(3.5.14)

Если , то все выполнено верно.

Выполним процедуру выработки общего ключа протоколом MQV:

1. Согласно исходным данным . Проверим, является ли простым делителем числа :

Действительно, число 37 является простым делителем числа 148.

1. Значение выберем таким, чтоб удовлетворялось условие (3.5.1). Пусть . Проверим условие (3.5.1):

Условие (3.5.1) выполняется.

1. Согласно исходным данным секретный ключ стороны А , а секретный ключ стороны В . Проверим условие (3.5.2) для каждого секретного ключа:

Условие (3.5.2) выполняется в обоих случаях.

1. Сторона А вычисляет свой открытый ключ по формуле(3.5.3):
2. Сторона В вычисляет свой открытый ключ по формуле(3.5.4):
3. Сторона А выбирает значение , которое согласно исходным данным . Проверим условие (3.5.5):

Условие (3.5.5) выполняется.

1. На основании этого значения вычисляет по формуле (3.5.6):
2. Для упрощения дальнейших расчетов вычислим следующие значения:

по формуле (3.5.7):

Вычислим по формуле (2.1.8), так как 37 – простое число:

по формуле (3.5.8):

1. Сторона А передает стороне В свой открытый ключ и значение .
2. Сторона B выбирает значение , которое согласно исходным данным . Проверим условие (3.5.9):

Условие (3.5.9) выполняется.

1. На основании этого значения вычисляет по формуле (3.5.10):
2. Для упрощения дальнейших расчетов вычислим следующие значения:

по формуле (3.5.11):

по формуле (3.5.12):

1. Сторона В передает стороне А свой открытый ключ и значение .
2. Сторона А вычисляет сеансовый ключ по формуле (3.5.13):

Рассчитаем значение :

Вычислим значение :

Получим, что:

1. Сторона В вычисляет сеансовый ключ по формуле (3.5.14):

Рассчитаем значение :

Вычислим значение :

Получим, что:

Так как , то все выполнено верно.

*Задание 6. Протокол Girault*

Описание:

Стороны А и В договариваются о двух простых числах . Находят их произведение по формуле:

(3.6.1)

Выбирают число , которое должно удовлетворять условию:

(3.6.2)

Стороны выбирают число , после чего выбирают число , исходя из условия:

(3.6.3)

Каждая сторона выбирает себе идентификатор *А* и *В* соответственно. Также каждая сторона выбирает пару случайных чисел: секретный ключ и случайное число . Затем каждая сторона вычисляет свой открытый ключ:

Сторона А по формуле:

(3.6.4)

Сторона B по формуле:

(3.6.5)

В данной схеме обмена данными кроме стороны А и стороны В есть еще сервер Т, который выполняет роль удостоверяющего центра. После вычисления открытых ключей сторона А передает серверу Т свой открытый ключ и свой идентификатор , сторона В передает серверу Т свой открытый ключ и свой идентификатор .

Сервер Т вычисляет значения по формулам:

(3.6.6)

(3.6.7)

Стороны А и В для удостоверения в том, что сервер Т – это действительно он выполняет проверку полученных значений. Сторона А вычисляет значение:

(3.6.8)

Если вычисленное значение совпадет со значением , то все в порядке. Сторона В вычисляет значение:

(3.6.9)

Если вычисленное значение совпадет со значением , то все в порядке. Далее между сторонами А и В происходит обмен данными. Сторона А передает стороне В значения , которое было вычислено предварительно по формуле:

(3.6.10)

Сторона B передает стороне A значения , которое было вычислено предварительно по формуле:

(3.6.11)

После обмена стороны вычисляют сеансовый ключ по формулам:

(3.6.12)

(3.6.13)

Если ключи и совпадут, значит все выполнено верно.

Схема процесса обмена данными между всеми тремя участниками изображена на рис.3.1.

N, d

A, и

B, и

A,

B,

Сторона

В

Сторона

А

Сервер

Т

p, q, α, e, d, B, ,

p, q, α, e, d, A, ,

Рисунок 3.1 – Схема обмена данными между участниками процесса открытого распределения ключей протоколом Girault

Выполним процедуру открытого распределения ключей протоколом Girault:

1. Согласно исходным данным , . Вычислим их произведение по формуле (3.6.1):
2. Выберем число которое должно удовлетворять условию (3.6.2). Пусть . Проверим условие (3.6.2):

Вычислим :

Условие (3.6.2) выполняется.

1. Согласно исходным данным число . Выберем число методом подбора величины исходя из условия (3.6.3). Пусть , проверим условие (3.6.3) для данного значения:

Найдем значение , воспользовавшись формулой (2.1.8). Так как число 8413 – составное, тогда:

Тогда:

Условие (3.6.3) выполнятся.

1. Согласно исходным данным идентификатор стороны А , а идентификатор стороны В .
2. Согласно исходным данным, секретный ключ стороны А , а число . Секретный ключ стороны В , а число .
3. Сторона А вычисляет свой открытый ключ по формуле (3.6.4):
4. Сторона В вычисляет свой открытый ключ по формуле (3.6.5):
5. Сторона А передает серверу Т свой открытый ключ и свой идентификатор , сторона В передает серверу Т свой открытый ключ и свой идентификатор .
6. Сервер Т вычисляет значения по формулам (3.6.6) и (3.6.7):

Таким образом, . Аналогично рассчитаем :

Таким образом, .

1. Стороны А и В для удостоверения в том, что сервер Т – это действительно он выполняет проверку полученных значений. Сторона А вычисляет значение по формуле (3.6.8):

Рассчитаем значение :

Получим:

Полученное значение совпадает со значением .

1. Стороны А и В для удостоверения в том, что сервер Т – это действительно он выполняет проверку полученных значений. Сторона А вычисляет значение по формуле (3.6.9):

Рассчитаем значение :

Получим:

Полученное значение совпадает со значением .

1. Сторона А передает стороне В значения , которое было вычислено предварительно по формуле (3.6.10):
2. Сторона B передает стороне A значения , которое было вычислено предварительно по формуле (3.6.11):
3. Сторона А вычисляет сеансовый ключ по формуле (3.6.12):

Выражение было рассчитано ранее: . Вычислим значение

Вычислим значение :

Получим:

1. Сторона В вычисляет сеансовый ключ по формуле (3.6.13):

Выражение было рассчитано ранее: . Вычислим значение

Вычислим значение :

Получим:

Так как и совпали, значит все выполнено верно.

*Задание 7. Протокол Диффи-Хеллмана на эллиптических кривых*

Описание:

Стороны А и В договариваются об определенном уравнении эллиптической кривой, записанной в виде:

(3.7.1)

Также стороны договариваются о точке , которая принадлежит данной эллиптической кривой. Для того, чтоб проверить, принадлежит ли точка кривой необходимо воспользоваться уравнением:

(3.7.2)

Каждый из пользователей выбирает свой секретный ключ: сторона А выбирает , а сторона В .

Затем каждый из пользователей вычисляет свои открытые ключи:

(3.7.3)

(3.7.4)

Чтоб выполнить умножение какого-либо числа на точку , необходимо поочередно выполнять сложение всех точек по 2 точки (А и В). Результирующая точка будет иметь координаты:

, (3.7.5)

где значение рассчитывается следующим образом:

* Если :

(3.7.6)

* Если :

(3.7.7)

Стороны обмениваются открытыми ключами. После чего вычисляют сеансовый ключ:

(3.7.8)

(3.7.9)

Если и совпали, значит все верно.

Выполним процедуру выработки общего ключа протоколом Диффи-Хеллмана на эллиптических кривых (ЭК):

1. Согласно исходным данным уравнение ЭК имеет вид . Точка на ЭК выбрана . Проверим, принадлежит ли точка кривой . Для этого воспользуемся уравнением (3.7.2):

Действительно, точка принадлежит ЭК .

1. Согласно исходным данным, секретный ключ стороны А , а секретный ключ стороны В .
2. Сторона А вычисляет свой открытый ключ по формуле (3.7.3):

Вычислим значение точки, которая получится в результате суммирования , то есть :

Вычислим значение λ для данного случая, воспользовавшись формулой (3.7.7), так как мы суммируем две одинаковые точки:

Для облегчения дальнейших расчетов возьмем полученное значение по модулю :

По формуле (2.1.8):

Найдем значение . Так как 199 – простое число, то:

Тогда:

Вычислим значение :

Таким образом:

Рассчитаем координаты получившейся в результате суммирования (29,1)+(29,1) точки по формуле (3.7.5):