РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ ПО ОТКРЫТЫМ КАНАЛАМ

1 Введение

Рассмотрим ряд протоколов, криптографическая стойкость которых основана на трудности решения проблемы дискретного логарифма и проблемы Диффи-Хеллмана. Проблема дискретного логарифма возникает в каждом случае, когда задана некоторая циклическая группа, известна степень $y = g^x$ некоторого её элемента (если группа мультипликативная) или кратное $y = x * g$ (в аддитивной группе) и требуется найти значение показателя степени или коэффициент кратности x (дискретный логарифм элемента y по основанию g).

В одних случаях, например для аддитивной группы, заданной на множестве Z_n вычетов по модулю простого числа p, эта проблема легко решаема с использованием алгоритма, подобного алгоритму Евклида, в других случаях, например, для мультипликативной группы конечного поля известны субэкспоненциальные алгоритмы для этой проблемы.

Для группы точек эллиптической кривой проблема дискретного логарифма заключается в определении числа k по известным точке P данной эллиптической кривой и точке $Q = kP$. Сложность этой проблемы не меньше сложности проблемы дискретного логарифма для поля, над которым определена кривая. Для несуперсингулярных кривых неизвестны субэкспоненциальные алгоритмы решения проблемы дискретного логарифма.

Классическая проблема Диффи-Хеллмана формулируется применительно к мультипликативной группе конечного поля. Она заключается в вычислении элемента α^{xy} по элементам α, α^x и α^y. Не известно, возможно ли ее решение без предварительного вычисления индексов x и y, то есть минуя проблему дискретного логарифма. Применительно к циклической подгруппе группы точек эллиптической кривой эта проблема заключается в том, чтобы при известных точке $P \in \mathcal{EF}$ и двух ее кратных k_AP и k_BP найти точку k_Ak_BP. Также неизвестно, можно ли это сделать без предварительного вычисления констант k_A и k_B, то есть не решая проблему дискретного логарифма для эллиптических кривых. Не доказана и гипотеза об эквивалентности проблем дискретного логарифма и Диффи-Хеллмана для эллиптических кривых.

2 Распределение ключей для классической криптосистемы (протокол Диффи-Хеллмана)

Заметим, что в качестве ключа классической криптосистемы можно использовать неизвестную посторонним (секретную) случайную точку $(x, y) \neq O$ группы точек эллиптической кривой $\mathcal{EF}$, если условиться, как конвертировать ее в натуральное число, например, одну из координат, скажем, x считать двоичной записью натурального числа[1].

Для получения такой секретной точки на двух терминалах открытого канала связи можно использовать модификацию протокола Диффи-Хеллмана. [2]

Допустим, что $\mathcal{E}$ – эллиптическая кривая и P – предварительно согласованная и опубликованная точка этой кривой. Абонент A выбирает, сохраняя в секрете случайное число k_A(секретный ключ A), вычисляет координаты точки k_AP (свою «половинку» ключа) и пересылает их абоненту B. Аналогично B выбирает секретный ключ k_B, вычисляет и пересылает абоненту A «половинку» k_BP ключа. Общим ключом является точка $P = k_Ak_BP$. A вычисляет ее умножая на свой секретный ключ k_A «половинку» ключа, вычисленную B, а B вычисляет эту же точку, умножая сообщение, поступившее от A на свой секретный ключ k_B. Ввиду того, что группа точек эллиптической кривой абелева, результат не зависит от порядка вычисления и, следовательно, A и B имеют координаты секретной точки[3] $k_A(k_BP) = k_B(k_A)P = k_Ak_BP = (x, y)$ и могут использовать x в качестве ключа симметричной криптосистемы (при условии

[1] В общем случае следует иметь в виду некоторое инъективное отображение из $\mathcal{EF} \setminus \{O\}$ в множество натуральных чисел N.

[2] Классическая версия этого протокола основана на проблеме Диффи-Хеллмана для группы Z_p^*. Абоненты A и B, предварительно по открытому каналу уславливаются об использовании большого простого числа p и образующего элемента α мультипликативной группы Z_p^*. Для совместной выработки секретной точки они выбирают независимо друг от друга секретные числа $x \in Z_p^*$ и $y \in Z_p^*$, вычисляют «половинки» α^x и α^y и обмениваются ими по открытому каналу. После этого каждый из них вычисляет секретный ключ, возводя полученную «половинку» ключа в свою секретную степень: $(\alpha^x)^y = \alpha^{xy}$, $(\alpha^y)^x = \alpha^{yx} = \alpha^{xy}$.

[3] Предполагается, что полученная точка не есть O. Вероятность получить O при большом поряке поля F чрезвычайно мала, но тем не менее для логической завершенности следует осуществлять проверку и предусматривать возврат на этап выбора секретных ключей k_A и k_B.

достаточности длины этой двоичной записи, что зависит от порядка поля, над которым построена эллиптическая кривая, и при условии, что секретные ключи k_A и k_B были выбраны как случайные или как криптографически стойкие псевдослучайные числа). Теперь A и B имеют одинаковые копии искомой секретной точки эллиптической кривой.

Проблема, стоящая перед посторонним наблюдателем, имеющим намерение узнать секретный ключ, заключается в вычислении $k_A k_B P$ по известным $P,\ k_A P,\ k_B P$, но при неизвестных $k_A,\ k_B$, это и есть проблема Диффи-Хеллмана для эллиптических кривых.

Пример 2.1 Эллиптическая кривая

$$Y^2 + XY = X^3 + X^2 + 1$$

над полем $GF(2^{163})$ имеет порядок $2 \times P49$, где $P49$ – простое число, десятичное представление которого состоит из 49 десятичных знаков. Выберем неприводимый многочлен

$$1 + X + X^2 + X^8 + X^{163}$$

и возьмем точку этой эллиптической кривой

$P =$

(1011001001001000000101001011100001001001001001001101111110010
1010011011000111001110000001100001100010000100010011100101001
01101110001100111111001110001011001110101,
0011001110111000000110110110001100111100000000100100001100100
0111000111001010100100011001010000001101100001010100011000100
0010011101101001010011100010110010111 0011);

Проверим, что ее порядок не равен 2: $2P \neq O$. Значит, ее порядок равен порядку $2 \times P49$ группы или числу $P49$, и ее можно использовать для построения ключа.

Пусть $k_A = 12$, $k_B = 123$ (реально должны быть большие числа).

Тогда $k_A P =$

(1101101110011110111001101101110101110001111001010001110110 00
0000010000101101011101000111001010001010100110100100111110100
1001110011101110111100101000000111010010 11,
0011011011100101010000010111101111101101100011001110011111101
0100110001111001110011010100010111110000001011001011110100011
0111110110001001111010010100111010001001 1);

$k_B P =$

(0101101001100001001001110100001001100000000100010111100111000
0100011001111001000111000100101110001110101010001100110000011

110011100101110001001001001000010100010111,
1010011000011101001010001100111011110000100111111010111111101
0010101000101010110110100001111011100100010001110111111001010
00101100010111011000010101011101000011011);

$k_B k_A P = k_A k_B P =$
(1101110111100001101001100011011100110111100011000011111010001
0011000100110101100001000011110000111010011110101101111100010
10001000111101011011010001100001110010 1,
1111011001101000111111111011111101111000110101010001001111011 0
0011010100010110111000111011010110101010000000110110101001 01
010101101011001011110000111011110010 1).

В качестве ключа симметричной системы используется код

$x =$
0110001001101011000010000111100001110100111101011011111100010
100010001111010110110100011000011100101.

Заметим, что для выполнения этого протокола точное знание порядка эллиптической кривой не потребовалось.

3 Распределение ключей для классической криптосистемы (протокол Massey-Omura)

Протокола Massey-Omura позволяет передать сообщение от абонента A абоненту B по открытому каналу связи без предварительной передачи какой бы то ни было ключевой информации.

Мультипликативный вариант. Первоначально данный протокол был описан применительно к мультипликативной группе Z_p^*, где p – простое число как аналог передачи секрета с помощью ящиков, запираемых на один или два замка: абонент A запирает ящик с письмом своим ключом и пересылает ящик абоненту B, который запирает ящик своим ключом и отправляет его к A. Последний снимает свой замок и возвращает ящик к B, который снимает свой замок. Вместо механических замков абоненты (два или более) могут использовать электронные, то есть хранимые в компьютерной памяти ключи. Для их организации они выбирают как системный параметр большое простое число p. Затем абоненты A, и B выбирают случайные числа e_A и e_B, взаимно простые с $p-1$, и вычисляют числа d_A и d_B, обратные по модулю $\varphi(p)=p-1$ (φ – функция Эйлера) к выбранным ранее числам :

$$e_A \cdot d_A \equiv 1 \pmod{\varphi(p)},\ e_B \cdot d_B \equiv 1 \pmod{\varphi(p)}.$$

Пары чисел $(e_A, d_A),\ (e_B, d_B)$, представляют собой секретные ключи абонентов.

Отметим, что

$$m^{e_A \cdot d_A} = m \bmod p,$$

так как

$$m^{e_A \cdot d_A} = m^{j \cdot \varphi(p)+1} = m^{j \cdot \varphi(p)} \cdot m = m$$

(первый сомножитель равен 1 по теореме Эйлера).
Аналогично,

$$m^{e_B \cdot d_B} = m \bmod p.$$

Пусть абоненту A необходимо послать сообщение $m,\ 0 < m < p-1$, абоненту B (более длинные сообщения разбиваются на блоки). Абонент A шифрует сообщение своим первым ключом, то есть находит

$$m_1 = m^{e_A} \bmod p,\ 0 < m_1 < p,$$

и пересылает m_1 к абоненту B. Этот абонент «навешивает» свой первый замок на это сообщение и вычисляет

$$m_2 = m_1^{e_B} \bmod p = m^{e_A \cdot e_B} \bmod p,\ 0 < m_2 < p,$$

а потом пересылает m_2 обратно к A. Он снимает свой первый замок с помощью второго секретного ключа, вычисляя

$$m_3 = m_2^{d_A} \bmod p = m^{e_A \cdot e_B \cdot d_A} \bmod p,\ 0 < m_3 < p.$$

Это сообщение пересылается абоненту B, который снимает свой первый замок с помощью своего второго секретного ключа d_B :

$$m_4 = m_3^{d_B} \bmod p = m^{d_B \cdot e_A \cdot e_B \cdot d_A} \bmod p = m.$$

Таким образом, абоненту B доставлено секретное сообщение m от абонента A.

Эллиптический вариант протокола. Эллиптическая кривая имеет свойство приводить константы, на которые умножаются ее точки, по модулю ее порядка. Пусть $\mathcal{E}$ – эллиптическая кривая порядка N, e – целое, $1 < e < N$, взаимно простое с N. Используя алгоритм инвертирования, найдём

$$d \equiv e^{-1} (\mathrm{mod}\ N). \tag{1}$$

По определению сравнимости по модулю имеем $e \cdot d = jN + 1$. Поэтому для любой точки P эллиптической кривой $\mathcal{E}$ порядка N

$$(e \cdot d)Q = (j \cdot N + 1)P = (j \cdot N)P + P = jO + P = O + P = P,$$

то есть выполняется тождество

$$(e \cdot d)P = P. \tag{2}$$

Используя e и d из (1), и любую точку P эллиптической кривой, можно вычислить $Q = eP$, $R = dQ$.

Очевидно, что $R = P$.

В эллиптическом варианте протокола системными параметрами являются уравнение эллиптической кривой $\mathcal{E}$ и поле $\mathcal{F}$, над которым она построена (поле задается неприводимым многочленом). Этими параметрами определена группа $\mathcal{EF}$ точек эллиптической кривой и ее порядок, который также публикуется как системный параметр (хотя он может быть и вычислен по уравнению кривой и полю $\mathcal{F}$). Согласно этому протоколу после согласования системных параметров абонент A выбирает как ключ шифрования число e_A, взаимно простое с порядком N эллиптической кривой, и вычисляет по (1) обратное к a_A число d_A – ключ расшифрования. Аналогично, абонент B выбирает число e_B и вычисляет d_B, то есть создает свои ключи.

Абонент A помещает свое сообщение m в некоторую точку $M(m)$ эллиптической кривой и, умножая её на свое секретное значение e_A, получает точку

$$P_1 = e_A M.$$

Эту точку A посылает абоненту B.

Он вычисляет

$$P_2 = e_B P_1,$$

и посылает результат абоненту A, который снимает свой «замок», вычисляя

$$P_3 = d_A P_2,$$

и возвращает полученную точку абоненту B.

Последнему остается только расшифровать сообщение, зашифрованное на его ключе шифрования, то есть умножить полученную от A точку на свой секретный ключ расшифрования и найти

$$M = d_B P_3.$$

Действительно, с учетом коммутативности и ассоциативности операции группы

$$d_B P_3 = (d_B \cdot d_A) P_2 = (d_B \cdot d_A \cdot e_B) P_1 =$$

$$= (d_B \cdot d_A \cdot e_B \cdot e_A) M = (e_B \cdot d_B) \cdot (e_A \cdot d_A) M = M.$$

Сообщение m «вложенное» в точку M может быть использовано в качестве ключа симметричной криптосистемы.

Заметим, что в данном случае не требуется опубликования никакой информации о параметрах протокола, кроме самой эллиптической кривой. Платой за это является необходимость трехкратной передачи по открытым каналам.

Пример 3.1 Используем ту же несуперсингулярную эллиптическую кривую $\mathcal{E}$, что и в примерах двух предыдущих параграфов. Ее порядок есть
N =116920130986472233456294835071968966966582371481 26;
Пусть абоненты A и B выбрали следующие секретные числа в качестве ключей шифрования и расшифрования

$e_A = 12345,$

$d_A = e_A^{-1} \bmod N = 43652076445253181368980388403945319461237598230 63;$

$e_B = 54321,$

$d_B = e_B^{-1} \bmod N = 19993577009505358453922474236179741428776783356 15.$

Для передачи секретного сообщения m=987654321987654321 абоненту B абонент A размещает его в точке эллиптической кривой
$M(m) =$
(1111111111110101101101111001000110111100110011011011000011111110011010
0101011100010100001010100010001110101010000100111010110100101011101100011
0
00111101011011111,
0100110111100000101000011011100110110101111100100100010101011100101001
1000010000000001001010010000001011001100001010100011001011001110000100000111
11010101110011010l).

Затем он шифрует эту точку и пересылает результат
$P_1 = e_A M =$
(11110000101010011110111111001111101000000011110001110110000110110110010000
0010011110010011100000101110010110000011100010101010001001100000010010001111
100100001011,
01001101111000001010000110111001101101011111001001000101010111001010011000
0
1000000000100101001000000101100110000101010001100101100111000010000011111010
1011100110101)
абоненту B. Последний шифрует его своим ключом и возвращает результат
$P_2 = e_B P_1 =$
(10101011011111100000101110000101010111000000011000011110010010110001010001111
1001010110001110001001101111101000010010101110000110011001101110110000001011
101001111,
11000100111000110101000000111001111010111100001111101110110000000101100011
01
1001011110010110011010101111001110101100000010010111100111001111101010100101
101111011)
абоненту A, который осуществляет первичное расшифрование (снимает свой «замок») и осуществляет повторную пересылку результата
$P_3 = d_A P_2 =$
(0111101110000110111011000000100010101001011010100100010101001000011100111
01
0111001101010101011100101000010010110100100111011000101111011101001101010101
11000000101,
0111010100011111111111001011010100011011111001001010000110110001100101000000
0000110101110111110010100001100101100000000110010110110110010011000110010011
0
110001111);
абоненту B. Последний завершает расшифрование своим ключом, получая точку

$P_4 = d_B P_3 =$
(111111111111010110110111100100011011110011001101101100001111111001101001010
1110001010000101010001000111010101000010011101011010010101110110001100011110
1011011111,

0100110111100000101000011011100110110101111100100100010101011100101001100001
00000000100101001000000101100110000101010001100101100111000010000001111101010
11100110101)=M.

Заметим, что порядок использованной для передачи сообщения точки $M = N/2$.

4 Протокол распределения ключей Менезеса-Кью-Венстона (MQV-протокол)

Рассмотренные в Разделах 2 и 3 протоколы обладают тем недостатком, что некоторое третье лицо C может взять на себя функции посредника в передаче сообщений между двумя абонентами и завладеть при этом их секретом.

Действительно, если A и B взаимодействуют, например, по протоколу Диффи-Хеллмана, то посторонний наблюдатель C, перехватив передачу открытого ключа $k_A P$ абонента A, передаст абоненту B свой открытый ключ $k_C P$, абонент B передаст C свой открытый ключ $k_B P$, после чего B и C будут иметь общий закрытый ключ

$$(k_C \cdot k_B)P. \tag{3}$$

Далее, если C передаст свой открытый ключ также абоненту A, то C и A будут иметь общий секретный ключ $(k_A \cdot k_C)P$ (A вычислит этот ключ, используя $k_C \cdot P$ вместо $k_B P$)

Однако при хорошо замаскированных действиях C легальные абоненты A и B не будут знать, что имеется посредник, который, получая сообщение одного абонента, способен его расшифровать и вновь зашифровать с использованием другого закрытого ключа.

Для предотвращения таких действий активного криптоаналитика необходима аутентификация (авторизация) этих кратковременных ключей $k_A P$ и $k_B P$ (ключей одноразового использования), для чего используются публикуемые долговременные ключи $d_A P$ и $d_B P$ (ключи многоразового использования). При этом протокол организуется таким образом, что кратковременный открытый ключ связывается с долговременным и поэтому третье лицо, не имеющее долговременного ключа (не зарегистрированное на сервере, где такие ключи хранятся), не сможет стать посредником коммуникаций между двумя абонентами.

Использование кратковременного ключа обеспечивает невозможность использования раскрытого при одной из передач секрета для раскрытия секрета, вырабатываемого при последующих передачах.

Учитывая,что $kP = (k \bmod N)P$, вычисление константы k можно осуществлять как в модульной арифметике кольца Z_N, так и в кольце Z.

Соответственно, возможны две эквивалентные модификации протокола.

В первой используются модульная арифметика целых чисел, вторая основана на циклическом свойстве подгруппы точек эллиптической кривой.

В случае использования модульной арифметики над такими числами могут выполняться операции сложения и умножения по модулю n порядка эллиптической кривой, в случае использования арифметики эллиптической кривой на такие числа могут умножаться точки эллиптической кривой (тогда цикличность определяется порядком подгруппы точек эллиптической кривой и знание порядка эллиптической кривой или этой подгруппы для выполнения операций не требуется).

Во всех случаях абоненты A и B располагают точкой P эллиптической кривой порядка N, над которой и осуществляются все вычисления. Кроме того, они знают долговременные и кратковременные ключи друг друга: ключи абонента B

$$\begin{aligned} Q_B &= d_B P = (a_B, b_B), \\ R_B &= k_B P = (x_B, y_B) \end{aligned} \tag{4}$$

известны абоненту A, а ключи абонента A

$$\begin{aligned} Q_A &= d_A P = (a_A, b_A), \\ R_A &= k_A P = (x_A, y_A) \end{aligned} \tag{5}$$

известны абоненту B.

Рассмотрим описание и обоснование протокола с использованием как модульной арифметики, так и циклического свойства эллиптической кривой.

Протоколом предусматривается три этапа, симметрично выполняемых каждой из сторон.

На первом этапе A и B вычисляют числа

$$\begin{aligned} &s_A = (k_A + x_A a_A d_A) \bmod N \\ &(s_B = (k_B + x_B a_B d_B) \bmod N) \end{aligned} \tag{6}$$

(при этом они используют свои секретные данные k_A, d_A и k_B, d_B соответственно, а также *интерпретируемые как числа* координаты точек эллиптической кривой).

На втором этапе они вычисляют точки эллиптической кривой

$$\begin{aligned} U_A &= R_B + x_B(a_B Q_B), \\ U_B &= R_A + x_A(a_A Q_A) \end{aligned} \tag{7}$$

Здесь также используются конвертируемые в числовой формат координаты точек эллиптической кривой. На третьем этапе A и B вычисляют общую для них точку эллиптической кривой

$$W = s_A U_A = s_B U_B. \tag{8}$$

Действительно, в соответствии с использованными обозначениями (4)-(refequation6.13) получим на стороне A :

$$\begin{aligned} &s_A U_A = (k_A + x_A a_A d_A) \bmod N(R_B + x_B a_B Q_B) = \\ &= (k_A + x_A a_A d_A) \bmod N(k_B P + x_B a_B d_B P) = \\ &= (k_A + x_A a_A d_A) \bmod N(k_B + x_A a_B d_B)P = (k_A + x_A a_A d_A)(k_B + x_B a_B d_B)P. \end{aligned}$$

Аналогично получим для стороны B:

$$\begin{aligned} &s_B U_B = (k_B + x_B a_B d_B) \bmod N(R_A + x_A a_A Q_A) = \\ &= (k_B + x_B a_B d_B) \bmod N(k_A P + x_A a_A d_A P) = \\ &(k_B + x_B a_B d_B) \bmod N(k_A + x_A a_A d_A)P = (k_B + x_B a_B d_B)(k_A + x_A a_A d_A)P. \end{aligned}$$

Как видим, в рассмотренной интерпретации протокола модульная числовая арифметика сочетается с арифметикой эллиптической кривой: точка W вычисляется абонентом A, в конечном итоге, по формуле

$$W = ((k_A + x_A a_A d_A) \bmod N) U_A, \tag{9}$$

где используется точка U_A, вычисляемая по формуле (7). Абонент B получает точку W аналогично.

В варианте, не использующем модульную арифметику, та же точка W получается абонентом A по следующему алгоритму:

1. Вычислить точку U_A по формуле (7).
2. Вычислить точку W по формуле

$$W = k_A U_A + x_A(a_A(d_A U_A)).$$

Легко видеть, что с учетом модульного свойства умножения точки на константу эта формула эквивалентна формуле (9).

Действия абонента B аналогичны.

По окончании исполнения протокола A и B располагают секретной точкой W эллиптической кривой, координаты которой могут быть использованы для построения бинарного кода секретного ключа симметричной системы.

Пример 4.1 Рассмотрим имплементацию протокола с использованием той же эллиптической кривой, что и в Примере 2.1 и той же точки P в качестве системного параметра, учитывая, что порядок кривой (см. Разел **??**) есть $N =$11692013098647223345629483507196896696658237148126.

Пусть абоненты A и B выбрали числа

$$d_A = 345,\ d_B = 4567,$$

и зарегистрировали на сервере свои долговременные ключи

$$Q_A = 345P = (a_A, b_A),\ Q_B = 4567P = (a_B, b_B)$$

Пусть выбраны числа $k_A = 12$ и $k_B = 123$ и вычислены кратковременные ключи

$$R_A = k_A P = 12P = (x_A, y_A),\ R_B = k_B P = 123P = (x_B, y_B)$$

(приведены в Разделе 2), которыми абоненты обменялись. Они получили также долговременные ключи друг друга с сервера.

Затем они вычисляют W вторым из описанных выше способов и им потребуется конвертировать координаты точек в числовой формат.

Пример 4.2

5 Контрольные вопросы

1. Какие трудно решаемые задачи лежат в основе безопасности протокола распределения (согласования) ключей Диффи – Хеллмана?

Таблица 1: Пример исполнения MQV-протокола в поле малого порядка.

$\mathcal{EF}$	$Y^2 + XY = X^3 + X^2 + 1$
$p(X) =$	$1 + X + X^{15}$
$P =$	$(00001011111,$
	$1110101010011)$
$k_A =$	$12,$
$k_B =$	$123,$
$d_A =$	$345,$
$d_B =$	$4567,$
$Q_A = (a_A, b_A) = d_A P =$	$(010010101011101, 11111101001001)$
$Q_B = (a_B, b_B) = d_B P =$	$(01010011000101, 0100111000011)$
$R_A = (x_A, y_A) = k_A P =$	$(101110000111111, 111010010001001)$
$R_B = (x_B, y_B) = k_B P =$	$(001000011011101, 101110010001011)$
$(a_A Q_A) =$	$(010111010000111, 100100100100001)$
$x_A(a_A Q_A) =$	$(0111011100101, 100111011011)$
$(a_B Q_B) =$	$(001011010101011, 101000001101)$
$x_B(a_B Q_B) =$	$(0101011000111, 1110101000111)$
$U_A = R_B + x_B(a_B Q_B) =$	$(111111010111001, 1111000001111)$
$U_B = R_A + x_A(a_A Q_A) =$	$(001001101110111, 10101001101)$
$U_A =$	$(111111010111001, 1111000001111)$
$d_A U_A =$	$(1010101010011, 11001001010001)$
$k_A U_A =$	$(100010001011011, 001110101100011)$
$Q_A = (a_A, b_A) = d_A P =$	$(010010101011101, 11111101001001)$
$Q_B = (a_B, b_B) = d_B P =$	$(01010011000101, 0100111000011)$
$x_A d_A U_A =$	$(1111101101111, 111011110101001)$
$a_A x_A d_A U_A =$	$(110010111001101, 000110001111001)$
$U_B =$	$(001001101110111, 10101001101)$
$d_B U_B =$	$(000101110000011, 00110111110111)$
$k_B U_B =$	$(001100011111111, 10110011110101)$
$x_B d_B U_B =$	$(001111110000101, 00101011111101)$
$a_B x_B d_B U_B =$	$(00000110100011, 110101111001101)$
$W_A = k_A U_A + x_A a_A d_A U_A =$	$(101110011100011, 11000100010111)$
$W_B = k_B U_B + x_B a_B d_B U_B =$	$(101110011100011, 11000100010111)$

2. Каким образом активный злоумышленник может завладеть ключами, которые согласуются двумя участниками по протоколу Диффи – Хеллмана?

3. В чем состоит неудобство протокола Месси – Омуры?

4. Каким образом блокируется атака злоумышленника на протокол Диффи – Хеллмана в протоколе Менезеса – Кью – Венстоуна?

Литература.

1. Болотов А.А., Гашков С.Б., Фролов А.Б. Криптографические протоколы на эллиптических кривых.– М: Издательский дом МЭИ, 2007.

2.Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптограыию. Протоколы криптографии на эллиптических кривых. Криптографические протоколы на эллиптических кривых.– М: Издательский дом МЭИ, 2007.