УКАЗАНИЕ К РЕШЕНИЮ ЗАДАЧИ № 31

В 1976 году была опубликована работа молодых американских математиков У. Диффи и М.Э. Хеллмана «Новые направления в криптографии», в ней они предложили конкретную конструкцию так называемого "открытого распределения ключей".

Цель алгоритма состоит в том, чтобы два участника могли безопасно обменяться ключом, который в дальнейшем может использоваться в каком-либо алгоритме симметричного шифрования. Сам алгоритм Диффи-Хеллмана может применяться только для обмена ключами. Алгоритм основан на трудности вычислений ***дискретных логарифмов***.

Безопасность обмена ключа в алгоритме Диффи-Хеллмана вытекает из того факта, что, хотя относительно легко вычислить экспоненты по модулю простого числа, очень трудно вычислить дискретные логарифмы. Для больших простых чисел задача считается неразрешимой.

Предположим, что двум абонентам необходимо провести конфиденциальную переписку, а в их распоряжении нет первоначально оговоренного секретного ключа. Однако между ними существует канал, защищенный от модификации, то есть данные, передаваемые по нему, могут быть прослушаны, но не изменены (такие условия имеют место довольно часто). В этом случае две стороны могут создать одинаковый секретный ключ, ни разу не передав его по сети, по следующему алгоритму.

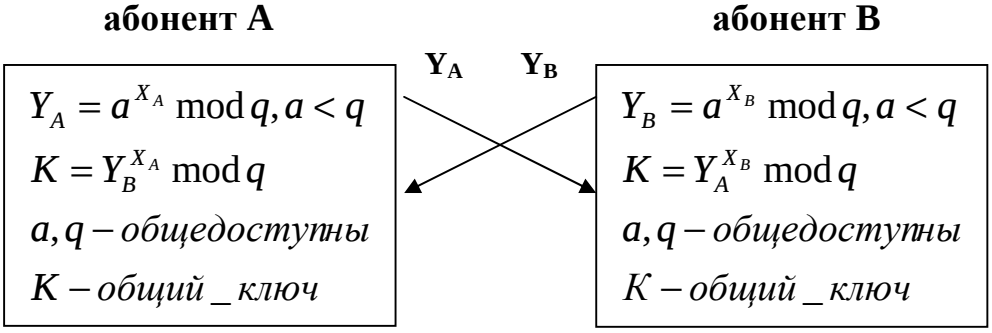

Рис. 9.1.Обмен ключами по схеме Диффи - Хеллмана.

Алгоритм заключается в следующем:

1. Глобальные открытые элементы:

   q - простое число

   a - первообразный корень q
2. Вычисление ключа абонентом А:

   - выбирается секретное число X_A ($X_A < q$)
   - вычисление открытого значения Y_A: $Y_A = a^{X_A} (\mathrm{mod}\, q)$
3. Вычисление ключа абонентом В:

   - выбирается секретное число X_B ($X_B < q$)
   - вычисление открытого значения Y_B: $Y_B = a^{X_B} (\mathrm{mod}\, q)$
4. Вычисление секретного ключа абонентом А:

   $K = (Y_B)^{X_A} (\mathrm{mod}\, q)$
5. Вычисление секретного ключа абонентом В:

   $K = (Y_A)^{X_B} (\mathrm{mod}\, q)$

Необходимо еще раз отметить, что алгоритм Диффи-Хеллмана работает только на линиях связи, надежно защищенных от модификации. Если бы он был применим на любых открытых каналах, то давно снял бы проблему распространения ключей и, возможно, заменил собой всю асимметричную криптографию.

Пример:

Пусть q = 97 и a = 5

Абонент А: Сгенерировал случайное число X_A = 36

Абонент В: Сгенерировал случайное число X_B = 58

Эти элементы они держат в секрете. Далее каждый из них вычисляет новый элемент: $Y_A = 5^{36} (\mathrm{mod}\, 97) = 50$, $Y_B = 5^{58} (\mathrm{mod}\, 97) = 44$

Потом они обмениваются этими элементами по каналу связи. Теперь абонент А, получив Y_B и зная свой секретный элемент X_A, вычисляет общий ключ: $K_A = 44^{36} (\mathrm{mod}\, 97) = 75$.

Аналогично поступает абонент В: $K_B = 50^{58} (\mathrm{mod}\, 97) = 75$