Лекция 4
Криптосистемы Рабина,Уильямса, Голдвассера-Микали, Эль-Гамаля и Диффи-Хеллмана

Криптосистема Рабина
1979г.

Генерирование ключей

Эта процедура выполняется при помощи следующих шагов:

1) необходимо генерировать два простых числа p и q примерно одинаковой разрядности $\boldsymbol{p = q = 3 \,(mod\, 4)}$

2) вычислить $n = p \cdot q$

3) выбрать в качестве открытого ключа n, а в качестве закрытого – его множители p,q.

,

Шифрование

Если пользователь *B* хочет зашифровать сообщение *M* для пользователя *A*, то он выполняет следующие шаги:

1) получает открытый ключ *n* пользователя *A*;

2) представляет сообщение *M* в виде последовательности блоков такой длины, что сообщение из каждого блока может быть задано целым числом $M_i \in (0, 1, 2, ..., n-1)$;

3) вычисляет криптограмму $C_i = M_i^2 \bmod n, i = 1, 2, ...$

4) Отправляет **C** , пользователю *A*.

Дешифрование

1) вычисляют $\sqrt{a} \bmod p$, т. е. находят два корня $+r$, $-r$ по $\bmod p$;

2) аналогично вычисляют корни $-s$, $+s$ по $\bmod q$;

3) используя рассмотренный в разд. 2 алгоритм, находят числа c и d, такие, что $c \cdot p + d \cdot q = 1$;

4) рассчитывают $x = (r \cdot d \cdot q + s \cdot c \cdot p) \bmod n$, $y = (r \cdot d \cdot q - s \cdot c \cdot p) \bmod n$;

5) в качестве решения $\sqrt{a} \bmod n$ выбирают числа $\pm x (\bmod n)$, $\pm y (\bmod n)$.

Видно, что схема Рабина обеспечивает простое генерирование ключей, а также весьма простой алгоритм шифрования, но имеет сложный алгоритм дешифрования. Данный метод можно рекомендовать в тех случаях, где шифрование должно быть простым, а при дешифровании этого не требуется.

Истинное сообщение из 4-х возможных находится на основе анализа избыточности сообщения. При отсутствии избыточности она должна быть внесена в сообщение до его шифрования, например, путем повторения некоторых символов.

Дополнительные комментарии по алгоритму дешифрования

Дешифрование равносильно нахождению корня уравнения

$$r = \sqrt{a} \bmod p$$

Простое число p может быть представлено

либо как p=4k+3, либо как p=4k+1, где k положительное целое число.

В первом случае вычет находится просто:

-найти r=a^(p+1)/4modp,

-выдать в качестве ответа (r,-r).

Пример для 1-го случая.

r^2=3mod23

Находим 3^(24/4)=3^6mod23=16.

r=+16, r=-16.

Имея в своем распоряжении метод генерирования невычетов b, можно использовать следующую конструкцию для нахождения $\sqrt{a} \bmod p$ [2, 3]:

1) генерировать случайные числа $b \in Z_p$, $Z_p = \{0, 1, 2, 3, \ldots, p-1\}$, до тех пор, пока $b^2 - 4a$ не окажется квадратичным невычетом по *mod* p, т. е.

$$\left(\frac{b^2 - 4a}{p}\right) = -1$$

2) найти $r = x^{(p+1)/2} \bmod\left(x^2 - bx + a\right)$,

где $\left(x^2 - bx + a\right)$ - полином над полем $GF(p)$

3) выдать ответ: r, $-r$ – как решение задачи $\sqrt{a} \bmod p$.

Можно использовать алгоритм Чипполы (см. следующий слайд).

Второй способ решения квадратного уравнения

$$r = (b + \sqrt{b^2 - a})^{(p+1)/2} \bmod p$$

ПРИМЕР $r^2 = 10 \bmod 13$

Можно проверить, что значение символа Лежандра для 10 равно 1,т.е. в поле GF(13) корень из 10 существует.

Шаг 1. подбором находим число b такое, что b^2-10 оказывается невычетом. Например, b=2.

Шаг 2. вычисляем $(b + \sqrt{b^2 - a}) = 2 + \sqrt{4 - 10} = 2 + \sqrt{-6}.$

Далее находим

$$(2+\sqrt{-6})^7 \bmod 13 = (2+\sqrt{-6})^2 (2+\sqrt{-6})^2 (2+\sqrt{-6})^2 (2+\sqrt{-6}) \bmod 13$$

$$= (-2+4\sqrt{-6})(-2+4\sqrt{-6})(-2+4\sqrt{-6})(2+\sqrt{-6}) \bmod 13 =$$

$$= (9+2\sqrt{-6})(2+\sqrt{-6}) \bmod 13 = 6$$

Стойкость КС Рабина

Ясно, что если злоумышленник сможет факторизовать n, то он становится «легальным» пользователем, однако задача факторизации является сложной и не имеет пока полиномиальных решений. Таким образом, выбором, скажем, $l(n) = 768$ (или для большей стойкости $l(n) = 1024$) обеспечивается невозможность факторизации. Кроме того, для системы Рабина можно доказать и обратное утверждение.

Теорема [3]. Пусть $n = p \cdot q$ где p и q – простые числа, и пусть существует алгоритм R, который для каждого целого числа C, которое заведомо является квадратом некоторого числа x по $\bmod n$ (т.е. $x^2 = C \bmod n$), находит решение этого уравнения x при помощи $F(n)$ битовых операций. Тогда существует вероятностный алгоритм, который факторизует n со средним числом битовых операций $2\left(F(n) + O\left(\lg^2 n\right)\right)$.

Пояснение к оценке стойкости схемы Рабина

Прямая теорема

Если решена задача факторизации за полиномиальное время, то есть известно, что n=pq, то уравнение x^2=c modn решается за полиномиальное время.

Обратная теорема

Если уравнение x^2=c modn решается за полиномиальное время, то за полиномиальное время может быть решена задача факторизации n=pq.

Доказательство. Выберем случайное целое число m, $0 < m < n$, и найдем $C = m^2 \bmod n$. Решим уравнение используя алгоритм R извлечения корня при помощи $F(n)$ операций. Обозначим через k найденные решения. Имеется четыре возможности (примем вероятность каждой из них $1/4$):

а) $k = +m \bmod p$ и $k = +m \bmod q$;
б) $k = +m \bmod p$ и $k = -m \bmod q$;
в) $k = -m \bmod p$ и $k = +m \bmod q$;
г) $k = -m \bmod p$ и $k = -m \bmod q$;

Для решения задачи факторизации подходят случаи б) и в). Тогда факторизацию можно выполнить, вычисляя для этих случаев:

б) $\gcd(k - m, n) = p$;

в) $\gcd(k - m, n) = q$;

Замечание. Для а) , г) следует, что k=m mod n. Следовательно, НОД(k-m,n)=n

Итак, при каждом случайном выборе m приходим к возможности факторизации n с вероятностью $\frac{1}{2}$.Так как известно, что сложность нахождения gcd требует $O(\lg^2 n)$ операций, то, учитывая сложность $F(n)$ выполнения алгоритма R, получаем $2(O(\lg^2 n)+F(n))$ операций, необходимых для факторизации.

Если алгоритм R запускается t раз, причем каждый раз выбирается новое значение C, то вероятность не нахождения решения на превышает $1/2^t$

Таким образом, стойкость КС Рабина строго эквивалентна задаче факторизации и поэтому ее можно назвать *доказуемо секретной криптосистемой*. Заметим, что КС Рабина, так же как и КС РША, имеет побочные атаки (при малом количестве сообщений, при использовании общих модулей и т. д.) [3].

Криптосистема M^2 Уильямса (Williams) 1980

- Криптосистема Рабина имеет недостаток, заключающийся в неоднозначности дешифрования криптограммы. Этот недостаток преодолевается в M^2 Уильямса.

Генерирование ключей:

- 1) необходимо генерировать два простых числа p и q примерно одинаковой разрядности $\boldsymbol{p} \equiv 3 (mod\, 8), \boldsymbol{q} \equiv 7 (mod\, 8)$;
- 2) вычислить $\boldsymbol{N} = \boldsymbol{pq}$
- 3) выбрать в качестве открытого ключа $(\boldsymbol{N}, 2)$,а в качестве закрытого d.

$$\boldsymbol{d} = \frac{(\boldsymbol{p}-1)(\boldsymbol{q}-1)}{4} + 1$$

Шифрование

Пусть сообщение M удовлетворяет условию:

$$2(2\boldsymbol{M}+1) \le N, \textbf{\textit{если символ Якоби}} \left(\frac{2\boldsymbol{M}+1}{\boldsymbol{N}}\right) = -1$$

$$4(2\boldsymbol{M}+1) \le N, \textbf{\textit{если символ Якоби}} \left(\frac{2\boldsymbol{M}+1}{\boldsymbol{N}}\right) = 1$$

Шифрование выполняется в два шага:

1.

$$\boldsymbol{M}' = \boldsymbol{E}_1(\boldsymbol{M}) = \begin{cases} 2(2\boldsymbol{M}+1), \textbf{\textit{если символ Якоби}} \left(\frac{2\boldsymbol{M}+1}{\boldsymbol{N}}\right) = -1 \\ 4(2\boldsymbol{M}+1), \textbf{\textit{если символ Якоби}} \left(\frac{2\boldsymbol{M}+1}{\boldsymbol{N}}\right) = 1 \end{cases}$$

2. $\boldsymbol{C} = \left(\boldsymbol{M}'\right)^2 \bmod \boldsymbol{N}$

Дешифрование

Действия выполняются в обратном порядке:

1. $M' = C^d \bmod N$
2. $$M = \begin{cases} \dfrac{M'/4 - 1}{2}, \text{если } M' \equiv 0 \bmod 4 \\ \dfrac{(N - M')/4 - 1}{2}, \text{если } M' \equiv 1 \bmod 4 \\ \dfrac{M'/2 - 1}{2}, \text{если } M' \equiv 2 \bmod 4 \\ \dfrac{(N - M')/2 - 1}{2}, \text{если } M' \equiv 3 \bmod 4 \end{cases}$$

Показано, что стойкость криптосистемы Уильямса эквивалентна разложению N на множители.

Дополнения

Бывают криптосистемы :

- Рабина M^3 с соотношением 9:1 между открытыми текстами и шифротекстами.
- Уильямса M^3, которая устраняет эту проблему.

Криптосистема Голдвассера-Микали

КС РША относится к детерминированным системам. Открытый ключ фиксирован и некоторое заданное сообщение M всегда в результате шифрования преобразуется в фиксированную криптограмму.

Недостатки детерминированных криптосистем:

1. Они не безопасны для произвольных распределений вероятностей исходных сообщений. Например в РША сообщения 0 и 1 всегда преобразуются в самих себя.

2. Легко можно получить некоторую информацию о p и q:

Например, если последняя цифра n равна 3, то последнии цифры p и q либо 1и 3, либо 7 и 9.

183= 3*61, 253 = 11·23
203= 7·29, 303 = 3·101
213= 3·71, 323 = 17·19.

3. легко определить, что некоторое сообщение было отправлено дважды.

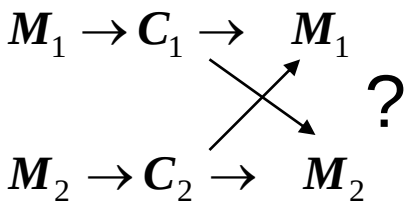
Понятие о вероятностном шифровании

Вероятностное шифрование позволяет добиться более высокого уровня безопасности.

Основные понятия:

Полиномиальная безопасность

1. *Пусть M1 и M2 два открытых текста и C1 и C2 две криптограммы им соответствующие. Криптосистема называется обеспечивающей полиномиальную безопасность, если нарушитель, перехватив C1 и C2, не может за полиномиальное время отличить какая криптограмма какому сообщению соответствует с вероятностью существенно большей 1\2.*



- **2. Семантическая безопасность**.
- *Криптосистема называется обеспечивающей семантическую безопасность, если при любом распределении вероятностей на множестве открытых текстов нарушитель не может за полиномиальное время отличить криптограмму, соответствующую открытому сообщению от «криптограммы» как случайной последовательности.*
- Криптосистема обеспечивает семантическую безопасность, если криптограмма не позволяет получить никакой информации об открытом тсоощении за полиномиальное время. Криптосистема обеспечивает семантическую безопасность, тогда и только тогда, когда она обеспечивает полиномиальную безопасность,

$$\begin{matrix} M \to C \\ X = \quad C \end{matrix} ?$$

Символ Якоби

Обозначим Q_N множество квадратичных вычетов по модулю N, $\bar{Q}_N$ множество квадратичных невычетов по модулю N, Если a вычет и НОД(a,N)=1, то существует решение квадратного уравнения $x^2 = a(mod\ N)$

Задача о квадратичном вычете:

Даны натуральные числа a и N, определить

верно ли утверждение $a \in Q_N$*?*

Считается, что решение задачи о квадратичном вычете эквивалентно решению задачи о разложении *N* на множители и

Следовательно эта задача является вычислительно неразрешимой.

Символ Якоби $\left(\frac{x}{N}\right)$ определен для любого $x \in Z_N$ и принимает значения $\{1,-1\}$

Если N- простое число, то $a \in Q_N \Leftrightarrow \left(\frac{a}{N}\right) = 1$ (символ Якоби совпадает с символом Лежандра).

Если N- составное число, то $a \in Q_N \Rightarrow \left(\frac{a}{N}\right) = 1$

$$a \in Q_N \xleftarrow{?} \left(\frac{a}{N}\right) = 1$$

$$a \in \bar{Q}_N \Leftarrow \left(\frac{a}{N}\right) = -1$$

Таким образом, если *N* составное, то *a* может не принадлежать $\bar{Q}_N$ даже если $\left(\frac{a}{N}\right) = 1$.

Пусть $J_N = \{ a \in (Z_N)^* : \left(\frac{a}{N}\right) = 1 \}$

Обозначим, $\tilde{Q}_N = J_N - Q_N$ т.е. множество чисел, для которых символ Якоби равен 1, но они не являются вычетами. Назовем это множество множеством всех псевдоквадратов по модулю N.

Криптосистема Голдвассера-Микали

Генерирование ключей

1) генерируем два больших простых числа p и q, состоящих из β бит,

2) вычисляем $N = pq$,

3) Выбираем $y \in \tilde{Q}_N$ и $\left(\frac{y}{N}\right) = 1$,

то есть, y является псевдоквадратом по модулю N),

4) Открытый ключ (N,y) , закрытый (p,q).

шифрование

Для того , чтобы отправить сообщение корреспонденту. А корреспондент. В выполняет:

1. Получает от А открытый ключ (N,y),
2. Представляет сообщение m в виде битовой строки

$$m = m_1, m_2, \cdots, m_k,$$ длиной k,

3. Для *i* от 1 до k выполняет:

- выбирает случайным образом $x_i \in (Z_N)^{\bullet}$, $Z^*_N = \{a \in Z_N : НОД(a, N) = 1\}$

мультипликативная группа,

- вычисляет $$c_i = \begin{cases} x_i^2 \bmod N, & \text{если } m_i = 0, \\ yx_i^2 \bmod N, & \text{если } m_i = 1 \end{cases},$$

в первом случае получаем квадрат, а во втором псевдоквадрат по модулю N,

4. Посылает $c = c_1, c_2, \cdots, c_k,$ корр. А. (Размер криптограммы $k(2\beta)$)

Расшифрование

Корр. А выполняет следующие действия:

1. Для *i* от 1 до k вычисляет символ Лежандра: $e_i' = \left(\frac{c_i}{p} \right)$,
2. Вычисляет m_i

$$m_i = \begin{cases} 0, \textit{если } e_i' = 1 \\ 1, \textit{в противном случае} \end{cases}$$

то есть, $m_i = 0$ если $c_i \in Q_N$ (вычет) , $m_i = 1$ в противном случае,

3. Выводит расшифрованное сообщение $m = m_1, m_2, \cdots, m_k,$

Криптостойкость КС Голдвассера-Микали

- Данный алгоритм использует при шифровании псевдослучайные числа и основывается на вычислительной неразрешимости задачи о квадратичном вычете.
- Данный алгоритм вероятностного шифрования обеспечивает семантическую безопасность.

- Недостаток – существенное увеличение длины криптограммы
- (в 2β раз, где β - количество разрядов в числах p и q).

КС Эль-Гамаля

Это некоторая модификация КС РША, стойкость которой не связана непосредственно с проблемой факторизации. Она широко используется в стандартах цифровой подписи и допускает естественное обобщение на случай КС, построенных на основе использования эллиптических кривых, что будет рассмотрено далее.

Генерирование ключей

Пользователь A проделывает следующие операции для генерирования ключей:

1) генерирует простое число p и примитивный элемент $\alpha \in GF(p)$;
2) выбирает случайное число a такое, что $1 \le a \le p-2$, и вычисляет число α^a;
3) в качестве открытого ключа выбирает набор: $\left(p, \alpha, \alpha^a \bmod p\right)$, а в качестве закрытого ключа – число a.

Шифрование

Пользователь B выполняет следующие шаги для шифрования сообщения M, предназначенного пользователю A:

1) получает открытый ключ A;

2) представляет сообщение M в виде цепочки чисел M_i, каждое из которых не превосходит $p-1$;

3) выбирает случайное число k такое, что $1 \le k \le p-2$;

4) вычисляет $\gamma = \alpha^k \bmod p$, $\delta = M_i \cdot \left(\alpha^a\right)^k \bmod p$;

5) посылает криптограмму $C = (\gamma, \delta)$ пользователю *A*.

Дешифрование

Пользователь *A* выполняет следующие шаги для дешифрования сообщения, полученного от пользователя *B*:

1) используя свой закрытый ключ, вычисляет $\gamma^{-a} \bmod p$;

2) восстанавливает сообщение $M_i = \gamma^{-a}\delta \bmod p$.

Действительно $\gamma^{-a}\delta = \alpha^{-ak} M_i \alpha^{ak} = M_i \bmod p$.

Особенностью схемы Эль-Гамаля является то, что она относится к так называемым схемам *рандомизационного шифрования*, поскольку при шифровании в ней используется дополнительная случайность в виде числа *k*.

(Считается, что рандомизационное шифрование более стойко по отношению к некоторым методам криптоанализа, например к таким как статистические атаки [3].)

Шифрование-дешифрование (второй вариант)

Шифрование

- Пользователь *B* выполняет следующие шаги для шифрования сообщения *M*, предназначенного пользователю *A*:
- получает открытый ключ *A*;
- представляет сообщение *M* в виде цепочки чисел , каждое из которых не превосходит $p-1$;
- выбирает случайное число *k* такое, что $1 \le k \le p-2$;
- вычисляет $\gamma = \alpha^k \bmod p$, $\delta = \boldsymbol{M_i}(\alpha^{\boldsymbol{a}})^{-\boldsymbol{k}} \, mod \, \boldsymbol{p}$;
- посылает криптограмму $C = (\gamma, \delta)$ пользователю *A*.

Дешифрование

- используя свой закрытый ключ, вычисляет $\gamma^{\boldsymbol{a}} \, mod p$;
- восстанавливает сообщение $\boldsymbol{M_i} = \gamma^{\boldsymbol{a}} \cdot \delta \, mod p$.
- Действительно, $\gamma^{\boldsymbol{a}} \cdot \delta = \alpha^{\boldsymbol{ak}} \cdot \boldsymbol{M_i}(\alpha^{\boldsymbol{a}})^{-\boldsymbol{k}} \, mod \, \boldsymbol{p} = \boldsymbol{M_i}$.

Первый вариант имеет меньшую сложность шифрования, второй – меньшую сложность дешифрования, из-за отсутствия операции обращения элемента по модулю

Преимущество КС Эль-Гамаля состоит также и в том, что тогда все пользователи в сети могут выбирать одинаковые α и p, что невозможно для КС РША. Кроме того, как будет показано далее, эта схема может быть естественным образом распространена на случай эллиптических кривых.

Существенным недостатком схемы является то, что длина криптограммы в ней в 2 раза больше длины сообщения.

Стойкость КС Эль-Гамаля

Проблема восстановления сообщения M по заданным p α , α^a, δ и γ при неизвестном a эквивалентна решению задачи Диффи–Хеллмана.

Ясно также, что если будет решена проблема нахождения дискретного логарифма, то криптосистема Эль-Гамаля будет вскрыта. При выборе p с разрядностью 768 бит (для повышенной стойкости – до 1024 бит), стойкость КС Эль-Гамаля будет такой же, как и у КС РША при выборе в последней тех же параметров для модуля.

Важно отметить, что для шифрования различных сообщений M_i, M_j необходимо использовать различные значения чисел k, поскольку в противном случае $\frac{\delta_1}{\delta_2} = \frac{M_i}{M_j}$, и тогда сообщение M_j может быть легко найдено, если известно сообщение M_i .

Метод распределения ключей Диффи–Хеллмана

Недостатком всех КС с открытым ключом является относительная сложность шифрования и дешифрования по сравнению с симметричными КС, что приводит к большим затратам времени при выполнении таких процедур. Это особенно существенно при шифровании больших объемов информации (например, содержащейся на жестких дисках компьютеров или в больших базах данных).

Преимуществом же КС с открытым ключом является простой метод распределения ключей. Для объединения положительных свойств симметричных и несимметричных КС используют так называемые *гибридные КС*, в которых распределение ключей осуществляется при помощи несимметричного алгоритма, а собственно шифрование – при помощи симметричного алгоритма.

Так как обновление ключей требуется сравнительно редко, то гибридная система обеспечивает практически такую же скорость шифрования/дешифрования, как и симметричная КС.

Для распределения ключей можно использовать любую КС ОК, например РША или Рабина. Тогда гибридная КС будет иметь вид, показанный на рис. 3.3.

На таком принципе построена, например, система PGP, используемая для шифрования электронной почты [7].

Однако для решения задачи только по распределению ключей к симметричным шифрам можно применить другой асимметричный алгоритм, называемый распределением ключей *Диффи–Хеллмана*.

Перед выполнением этого алгоритма пользователи A и B согласуют открытые параметры $\alpha \in Z_p$ и p, где p – простое число. Далее выполняется протокол, показанный на рис. 1.

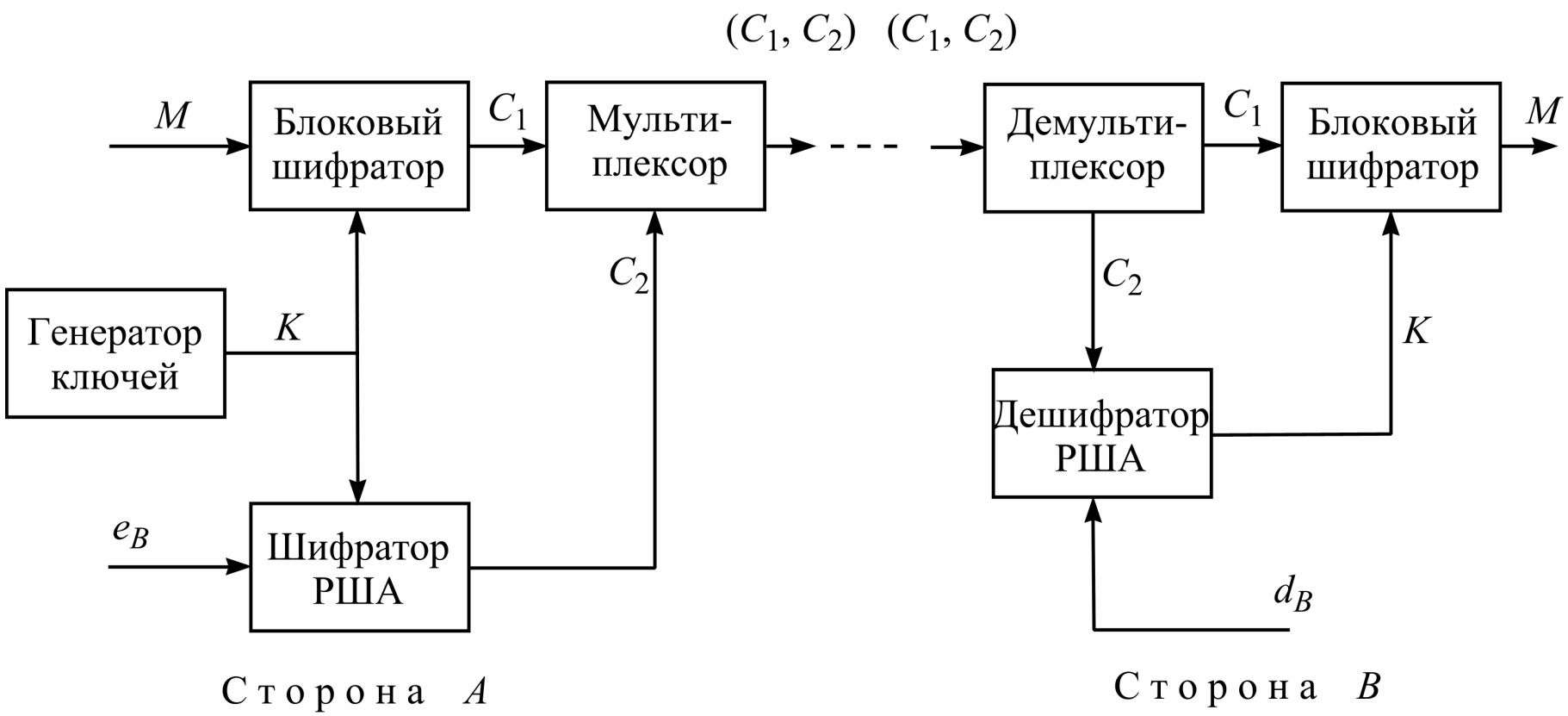


Рис. 1. Гибридная криптосистема

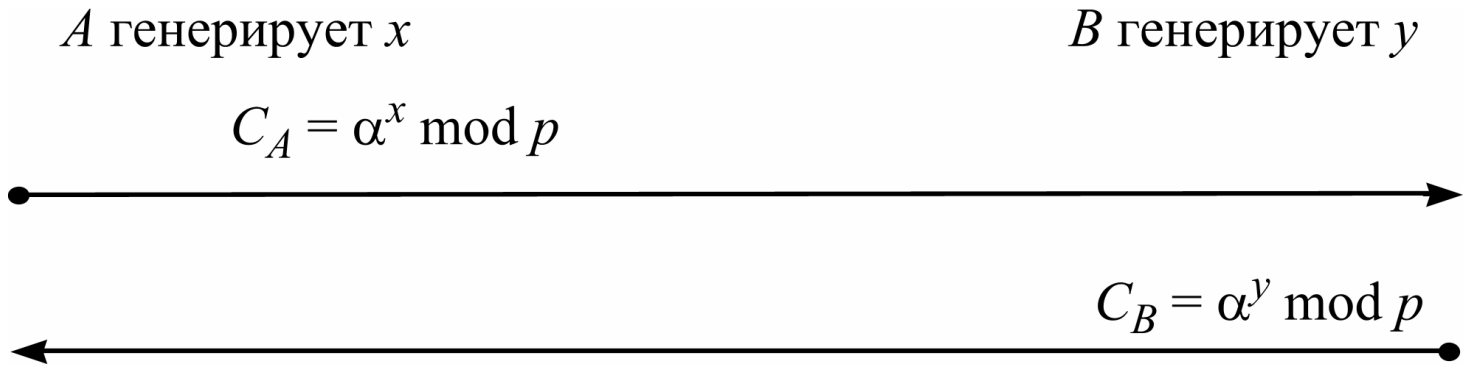


Рис. 2. Распределение ключей по методу Диффи–Хеллмана

После получения соответственно C_A и C_B пользователи A и B вычисляют общий ключ K следующим образом:

$$\begin{cases} K_A = C_B^x \bmod p = \left(\alpha^y\right)^x \bmod p = \alpha^{xy} \bmod p; \\ K_B = C_A^y \bmod p = \left(\alpha^x\right)^y \bmod p, \; K = K_A = K_B. \end{cases}$$

Стойкость КС Диффи–Хеллмана

Если злоумышленник умеет в обозримое время вычислять дискретный логарифм, то он может найти и секретный ключ *A* или *B*, поскольку $x = \log_{\alpha} C_A \bmod p$.

Однако поскольку задача дискретного логарифмирования является трудной, данный способ при больших величинах *p* нереализуем. Вместе с тем стойкость КС Диффи–Хеллмана не эквивалентна задаче факторизации, а соответствует так называемой *проблеме Диффи–Хеллмана*, которая формулируется следующим образом: *зная* p, α, $\alpha^x \bmod p, \alpha^y \bmod p$ *нужно найти* $\alpha^{xy} \bmod p$. (Впрочем, последняя задача по сложности несущественно уступает задаче дискретного логарифмирования.)

Важно отметить, что метод распределения ключей Диффи–Хеллмана может быть полностью скомпрометирован активными злоумышленниками, выдающими себя за пользователей *A* или *B*. Если этот факт подмены (или имитации) величин C_A, C_B не будет обнаружен, то вырабатывается совместный ключ не между *A* и *B*, а между злоумышленником и одним из пользователей.

Таким образом, для КС Диффи–Хеллмана, так же как и для всех КС ОК, необходимо обеспечивать подлинность открытых данных (т. е. обеспечить решение задач аутентификации).