ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению лабораторных работ

по дисциплине

Многоканальные цифровые системы передачи и средства их защиты

для студентов очной и заочной форм обучения
Направление подготовки 11.03.02
Инфокоммуникационные технологии и системы связи
профиль Защищенные системы и сети связи

Ростов-на-Дону

2019

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ по дисциплине

Многоканальные цифровые системы передачи и средства их защиты

Составитель: П.С Шевчук, проф. кафедры ИТСС

Рассмотрено и одобрено
на заседании кафедры ИТСС
Протокол от «26» августа 2019 г. № 1

- Лабораторная работа №7

ИССЛЕДОВАНИЕ АЛГОРИТМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ВАРИАНТЕ RSA

Важной услугой безопасности информационных систем становится в последнее время аутентификация информации, которая понимается как установление подлинности и неизменности сообщения, установления и доказуемости авторства сообщения, доказательства факта приема сообщения. Особенно важна эта услуга в сфере финансового и юридического электронного документооборота. Для решения задачи аутентификации информации сегодня используется концепция электронной цифровой подписи (ЭЦП). ЭЦП – это набор методов, которые позволяют перенести свойства рукописной подписи под документом в область электронного документооборота. Реальная подпись обладает следующими свойствами:

1. достоверностью, утверждающей, что пользователь сознательно подписал документ;
2. неподдельностью, доказывающей, что конкретный пользователь, а никто другой за него подписал документ;
3. невозможностью повторного использования подписи под одним документом для подписи другого;
4. неизменностью подписанного документа;
5. материальностью подписи, не дающей возможности подписавшему впоследствии отказаться от нее и от документа.

Такими же свойствами должна обладать электронная цифровая подпись, для чего в ее основу положены криптографические методы. Рассмотрим вариант реализации электронной цифровой подписи, построенной на алгоритме RSA (рис. 7.1).

В отличие от алгоритма шифрования, отправителем здесь является владелец пары закрытый/открытый ключ. Процедура формирования электронной подписи *sign* под сообщением схожа с шифрованием документа, но в степень закрытого ключа d по вычету n возводится не само сообщение или его части, а дайджест сообщения h. Неотъемлемой частью алгоритмов ЭЦП является хэширование информации, на рисунке оно обозначено через H.

Сообщение m с подписью *sign* будет однозначно аутентифицировано. Авторство сообщения может быть установлено и доказано по паре ключей (d, e) с использованием. Злоумышленник не сможет подменить сообщение m (точнее,ему будет очень трудно это сделать), поскольку ему необходимо вместо сообщения m подставить другое сообщение m', удовлетворяющее его и имеющее такое же

значение хэш-функции, что и у *m*, что является на сегодня вычислительно трудной задачей. По этой же причине злоумышленник не сможет применить перехваченную подпись *sign* для подписи другого документа, поскольку для другого документа будет получено иное значение хэш-функции *h*,а оно лежит в основе подписи. Таким образом, все необходимые свойства подписи описанным алгоритмом обеспечиваются, что же касается криптостойкости метода ЭЦП, то онаопределяется криптостойкостью используемого асимметричного криптографического метода и функции однонаправленного шифрования.

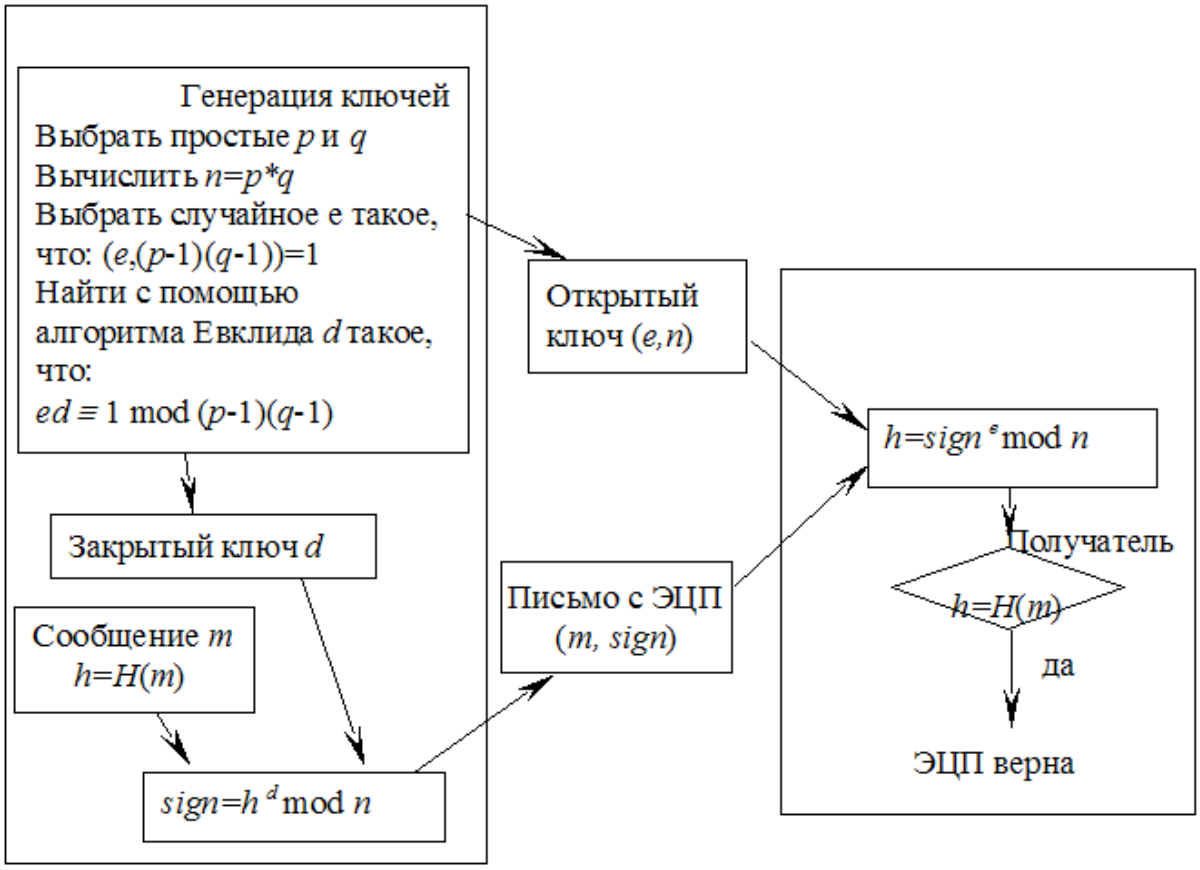

Рисунок 7.1 – Схема ЭЦП на основе RSA

Необходимо отметить также, что само сообщение *m* передается в открытом виде. Для того, чтобы обеспечить конфиденциальность передаваемой в нем информации, требуется использование дополнительного шифрования по симметричной или асимметричной схеме (при этом шифрование на ключе *d* конфиденциальности не обеспечит, поскольку сообщение может быть расшифровано открытым ключом *e*).

Очень популярными являются схемы ЭЦП на основе алгоритма ЭльГемаля, что обусловлено как надлежащей стойкостью алгоритма, так и лучшей по сравнению с RSA скоростью вычислений. В частности, в стандарте национального института стандартов США DSS (Digital Signature Standard) используется

алгоритм DSA (Digital Signature Algorithm), который является вариацией алгоритма ЭЦП ЭльГемаля в модификации Шнорра. В алгоритме используются следующие открытые параметры:

- p - простое число в диапазоне от 512 до 1024 бит;
- q -160-битовое простое число, делитель p-1;
- v – любое число, $v < p$-1, такое, что $v^{(p-1)/q} \bmod p > 1$;
- $g = v^{(p-1)/q} \bmod p$;
- $y = g^x \bmod p$.

Секретным ключом является любое 160-разрядное число x,$x < q$.

Алгоритм ЭЦП DSA в графической форме представлен на рис.7.2.

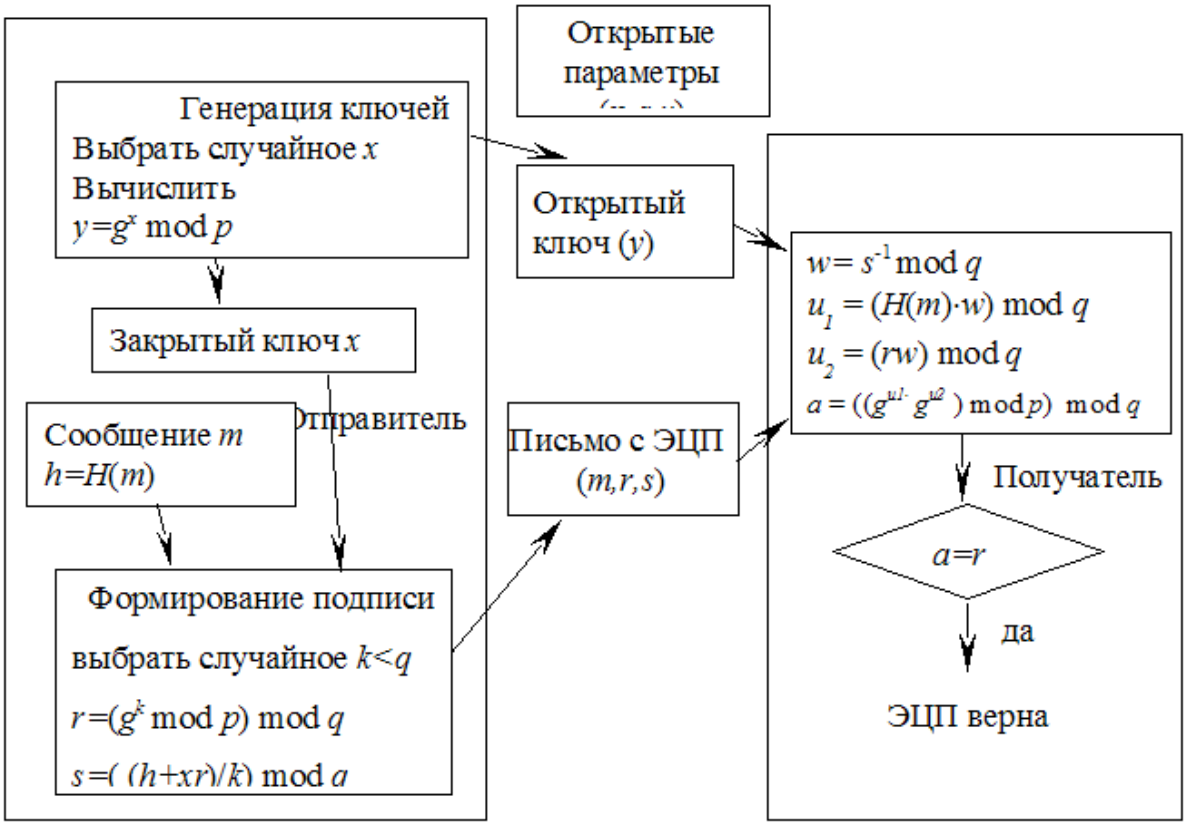

Рисунок 7.2 – Схема алгоритма ЭЦП DSA

Существует множество модификаций схемы ЭльГемаля. Одним из типов модификации стал перенос вычислений в группу, образованную эллиптическими кривыми. Рассмотрим свойства эллиптических кривых подробнее.

Для практического применения в криптографии используются эллиптические кривые (ЭК), заданные над полями Галуа. Пусть задано простое число $p > 3$.

Тогда эллиптической кривой E, определенной над простым конечным полем F_p, называется множество пар чисел (x, y),x, $y \in F_p$, которые удовлетворяют тождеству:

$$y^2 = x^3 + ax + b \bmod p,$$

где a, $b \in F_p$ и $(4a^3 + 27b^2) \neq 0 \bmod p$. Кроме того, к эллиптической кривой добавляется бесконечно удаленная точка I. Таким образом, точки, удовлетворяющие уравнению кривой E, и точка I образуют конечную абелеву группу. Геометрическое представление эллиптической кривой изображено на рис. 7.3.

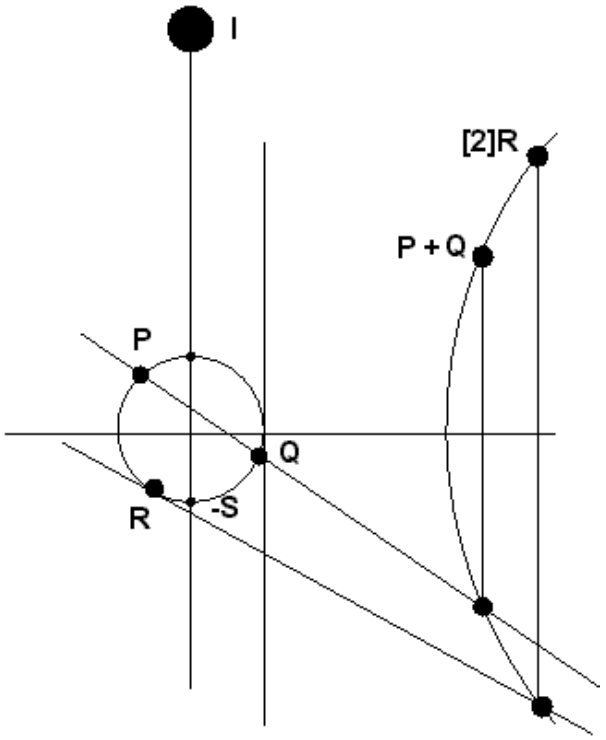

Рисунок 7.3.– График эллиптической кривой

Для точек эллиптической кривой определена операция сложения. Для двух точек, принадлежащих кривой E, $P(x_p, y_p)$ и $Q(x_p, y_p)$, точка, являющаяся их суммой, также будет лежать на эллиптической кривой. Координаты точки $S = P+Q$ определяются следующими выражениями:

- $k = ((y_q-y_p)/(x_q-x_p)) \bmod p$
- $x_s = (k^2-x_q-x_p) \bmod p$
- $y_s = (k(x_q-x_p)-y_p) \bmod p$

Точку S можно получить графически путем несложных построений. Для этого на графике проводится прямая через точки P и Q, и точка пересечения этой прямой с ЭК зеркально отображается относительно оси OX (см. рис 7.3).

Если точки P и Q совпадают, то мы получаем точку $S = 2*Q$. Тогда ее координаты определяются иначе:

- $k = ((3*x_q^2+a)/(2*y_q)) \bmod p$
- $x_s = (k^2-2x_q) \bmod p$
- $y_s = (k(x_q-x_s)-y_p) \bmod p$

Графически удвоение точки можно получить, построив касательную к точке и отразив точку пересечения касательной с эллиптической кривой относительно

оси OX (см. точки R и $2R$ на рис.7.3). Отсюда очевидно, что можно определить операцию умножения некоторой точки эллиптической кривой на целое число, которая позволяет определить точку $Q = k*P$ (точка P, умноженная на целое число k, обращается в точку Q). Скалярное умножение осуществляется посредством нескольких комбинаций сложения и удвоения точек эллиптической кривой. Например, точка $25*P$ может быть представлена, как $25*P = 2*(2*(2*(2*P)) + 2*(2*(2*P))) + P$. С операцией умножения точки ЭК на целое число напрямую связана идея, надёжность и криптостойкость эллиптической криптографии. Дело в том, что задача ECDLP (Elliptic Curve Discrete Logarithm Problem - задача дискретного логарифма на эллиптической кривой), суть которой заключается в отыскании целого числа k по известным точкам P и $Q = k*P$, является трудноразрешимой. Помимо уравнения, важным параметром кривой является базисная (генерирующая) точка G, выбираемая для каждой кривой отдельно. Секретным ключом в соответствии с технологией ЭК является большое случайное число k, а сообщаемым открытым ключом - произведение k на базисную точку G.

На криптостойкость алгоритма существенное влияние оказывает правильный выбор как самой кривой (коэффициентов a, b, p), так и базисной точки G.

Не каждая кривая обеспечивает требуемую криптостойкость, и для некоторых из них задача ECDLP решается довольно эффективно. Поскольку неудачный выбор кривой может повлечь за собой снижение обеспечиваемого уровня безопасности, организации по стандартизации выделяют целые блоки кривых, обладающих необходимой надёжностью. Использование стандартизированных кривых рекомендуется и потому, что становится возможной лучшая совместимость между различными реализациями протоколов информационной безопасности.

Выбор базисной точки обусловлен тем соображением, чтобы ее порядок был достаточно большим $2254 < q < 2256$. Точка $P \in E$ называется точкой порядка q, если $qP = I$.

На эллиптических кривых построен алгоритм проверки ЭЦП ГОСТ Р 34.10 – 2001, являющийся на сегодня стандартом РФ в области ЭЦП. Схема этого алгоритма приведена на рис. 7.4.

Основным достоинством криптосистем на основе ЭК является то, что они обеспечивают надежность, адекватную классическим криптосистемам (RSA, ЭльГемаль) на существенно меньших по длине ключах, что положительно отражается на времени кодирования и декодирования. Криптосистемы цифровой подписи на основе эллиптических кривых с длиной ключа 160 бит имеют одинаковую стойкость с криптосистемами DSA и Эль-Гамаля с длиной ключа 1024 бита. Ожидается, что в ближайшем будущем данные системы займут

доминирующее положение в криптографии с открытым ключом. Однако, это повлечет более серьезные исследования свойств этих криптоалгоритмов, что может привести к появлению новых, более эффективных алгоритмов решения проблемы дискретного логарифма в группе точек эллиптических кривых.

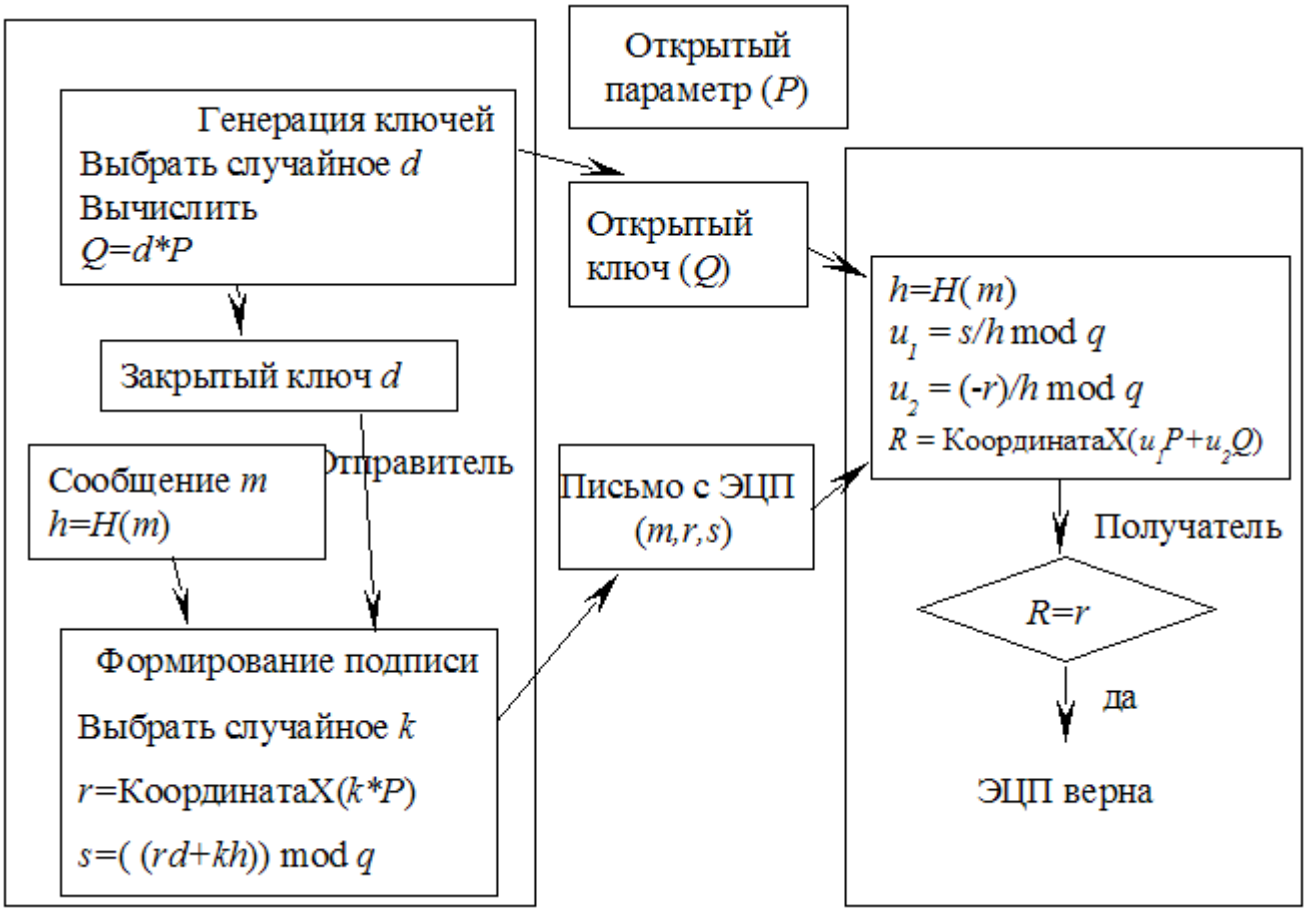

Рисунок 7.4 – Схема алгоритма ЭЦП ГОСТ Р 34.10-2001

Еще одним подходом к формированию ЭЦП является использование симметричных алгоритмов шифрования. Однако, известные на сегодня алгоритмы этого класса представляют скорее теоретический интерес, поскольку эффективность их реализации по времени или по объему требуемых вычислений очень невысока. Например, предложенная Диффи и Хелманом система ЭЦП на симметричном шифре позволяет подписывать только один бит информации, что на практике потребует формирования отдельной подписи для каждого бита передаваемого сообщения, причем подпись бита имеет размер ключа блочного шифра, и каждый новый бит требует генерации своего ключа подписи. Поэтому системы подобного класса пока не нашли широкого применения.

Асимметричные алгоритмы

Для симметричной криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В

асимметричных криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Алгоритм Диффи-Хелмана

Алгоритм Диффи-Хелмана (1976 год) использует функцию дискретного возведения в степень.

1. Сначала генерируются два больших простых числа **n** и **q**. Эти два числа не обязательно хранить в секрете.

2. Далее один из партнеров **P1** генерирует случайное число **x** и посылает другому участнику будущих обменов **P2** значение $\mathbf{A = q^x \bmod n}$

3. По получении **A** партнер **P2** генерирует случайное число **y** и посылает P2 вычисленное значение

$\mathbf{B = q^y \bmod n}$

4. Партнер **P1,** получив **B,** вычисляет $\mathbf{K_x = B^x \bmod n,}$

5. Партнер **P2,** получив **A** вычисляет $\mathbf{K_y = A^y \bmod n.}$

6. Алгоритм гарантирует, что числа $\mathbf{K_y}$ и $\mathbf{K_x}$ равны и могут быть использованы в качестве секретного ключа для шифрования.

Даже «перехватив» числа A и B, вычислить $\mathbf{K_x}$ или $\mathbf{K_y}$ невозможно.

Пример. Представим итерации алгоритма в виде последовательности действий партнеров в табличной форме, таблица 7.1.

Таблица 7.1

пп	Действия партнеров	
	Партнер P1	Партнер P2
	Генерация двух больших простых чисел и обмен ими. Пусть n=17, q=11	
	Генерируем случайное число **x, x=5.** Вычисляем $\mathbf{A = q^x \bmod n = 11^5 \bmod 17 = 10}$ Посылаем значение **A** партнеру	Получено **A = 10** Генерируем случайное число **y, y=7.** Вычисляем $\mathbf{B = q^y \bmod n = 11^7 \bmod 17 = 3}$ Посылаем значение **B** партнеру
	Получено **B = 3** Вычисляем $\mathbf{K_x = B^x \bmod n = 3^5 \bmod 17 = 5}$	Получено **A = 10** Вычисляем $\mathbf{K_y = A^y \bmod n = 10^7 \bmod 17 = 5}$
	Сравниваем $\mathbf{K_y}$ и $\mathbf{K_x}$, **5=5**	Сравниваем $\mathbf{K_y}$ и $\mathbf{K_x}$, **5=5**
	Ключем для шифрования является 5	

Криптосистема шифрования данных RSA предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Последовательность действий пользователя:

1.Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $N=pq$; $M=(p-1)(q-1)$.

*2.*Получатель выбирает целое случайное число d, которое является взаимопростым со значением M, и вычисляет значение e из условия $(ed) \bmod M = 1$.

3.d и N публикуются как открытый ключ, e и M являются закрытым ключом.

4.Если S –сообщение и его длина: $1<\text{Len}(S)<N$, то зашифровать этот текст можно как $S'=S^d \bmod N$, то есть шифруется открытым ключом.

5.Получатель расшифровывает с помощью закрытого ключа: $S=S'^e \bmod N$.

Пример. Далее представлены шаги алгоритма:

1. *p=19, q=13, N=pq=247, M=(p-1)(q-1)=18*12=216.*

2.Выбираем целое случайное число *d,* которое взаимно простое с *M. d=35.* (*d* и *M* не имеют общих делителей *35=7*5, 216=2*2*2*3*3*3*). Вычисляем *e* такое, что $ed \bmod M = 1$. *e=179*.

3. *(d,N)* открытый ключ, т.е. *(35,247), (e,M)* – закрытый ключ *(179, 216).*

4. Шифрование сообщения *2 3 1* **,** используя открытый ключ

$S'=S^d \bmod N$

$2 \rightarrow 2^{35} \bmod 247 = 124$

$3 \rightarrow 3^{35} \bmod 247 = 165$

$1 \rightarrow 1^{35} \bmod 247 = 1$

Шифрованное сообщение *124 165 1*.

5.Расшифровка сообщения *124 165 1*, используя закрытый ключ

$S=S'^e \bmod N$

$124 \rightarrow 124^{179} \bmod 247 = 2$

$165 \rightarrow 165^{179} \bmod 247 = 3$

$1 \rightarrow 1^{179} \bmod 247 = 1$

Расшифрованное сообщение *2 3 1.*

Задания для выполнения

1. Используя алгоритм Диффи-Хелмана сгенерируйте ключ для симметричного алгоритма криптографии.

.2. Сгенерировать открытый и закрытые ключи для алгоритма RSA. Передать открытый ключ следующему по списку студенту. Таблица простых числе в интервале [1; 200] приведена в таблице 7.2.

3. Составить последовательность цифр для шифрования из столбца чисел таблицы 1, определяемого по последней цифре номера варианта. Выполнить шифрование последовательности цифр, используя открытый ключ, полученный от другого студента п 7.3. Передать шифрограмму адресату.

.4. Произвести дешифрование полученного сообщения. Для дешифрования использовать сгенерированный вами закрытый ключ (п. 7.3).

Замечание: Некоторые простейшие ключи для алгоритма RSA представлены в таблице 7.3.

Таблица 7.2. – Таблица простых чисел от 1 до 200

Номера столбцов таблицы									
1	2	3	4	5	6	7	8	9	0
Простые числа в интервале от 1 до 200									
1	2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61	67
71	73	79	83	89	97	101	103	107	109
113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199			

Таблица 7.3. – Простейшие ключи для алгоритма RSA.

пп	Открытый ключ	Закрытый ключ	№ пп	Открытый ключ	Закрытый ключ	№ пп	Открытый ключ	Закрытый ключ
	(35,21)	(11,12)	8	(35,35)	(11,24)	15	(35,221)	(11,192)
	(15,15)	(7,8)	9	(77,77)	(53,60)	16	(35,247)	(179,216)
	(35,119)	(11,96)	10	(35,91)	(35,72)	17	(35,323)	(107,288)
	(21,33)	(21,20)	11	(35,161)	(83,132)	18	(35,437)	(215,396)
	(15,85)	(47,64)	12	(35,133)	(71,108)	19	(15,391)	(47,352)
	(35,65)	(11,48)	13	(77,209)	(173,180)	20	(35,299)	(83,264)
	(21,55)	(21,40)	14	(21,187)	(61,160)	21	(15,69)	(3,44)

Лабораторная работа №8

МЕТОДЫ ВЗЛОМА ШИФРОВ, ОСНОВАННЫЕ НА ДИСКРЕТНОМ ЛОГАРИФМИРОВАНИИ

Для обычных положительных действительных чисел логарифм является функцией, обратной возведению в степень. Аналогичная функция существует и в арифметике классов вычетов.

Свойства обычного логарифмирования. Логарифм числа определяется как степень, в которую нужно возвести значение положительного основания (не равного 1), чтобы получить данное число, т.е. для заданного основания x и произвольного y: y = xlog x(y).

Далее перечислены основные свойства логарифмов:

log x(1)=0,

log x(x)=1,

log x(yz)= log x(y)+ log x(z),

log x(yr)=rlog x(y).

Определение и свойства дискретного логарифмирования. Рассмотрим первообразный корень некоторого простого числа p (подобные аргументы могут быть использованы и в случае с числами, не являющимися простыми). В этом случае степени числа a с показателями от 1 до (p – 1) порождают каждое целое число от 1 до (p – 1) в точности по одному разу. Также известно, что любое целое число b можно представить в форме

$$b \equiv r \pmod p, \text{ где} 1 \le r \le (p-1)$$

в классах вычетов. Отсюда вытекает, что для любого целого числа b и любого первообразного корня a простого числа p можно найти ровно один показатель степени i, для которого

$$b \equiv a^i \pmod p, \text{ где} 1 \le i \le (p-1).$$

Значение этого показателя называют индексом числа b по модулю p при основании a. Записывается это значение как inda,p(b).

Необходимо обратить внимание на следующий момент:

$\text{ind}_{a,p}(1)= 0$, поскольку $a^0 \pmod p = 1 \pmod p = 1$,

$\text{ind}_{a,p}(a)= 1$, поскольку $a1 \pmod p = a$.

Теперь рассмотрим:

$$x = a^{ind_{a,p}(x)} \bmod p$$
$$y = a^{ind_{a,p}(y)} \bmod p$$
$$xy = a^{ind_{a,p}(xy)} \bmod p$$

Воспользовавшись правилами умножения по модулю сравнения, получим

$$a^{ind_{a,p}(xy)} \bmod p = (a^{ind_{a,p}(x)} \bmod p)(a^{ind_{a,p}(y)} \bmod p) =$$
$$= a^{ind_{a,p}(x)+ind_{a,p}(y)} \bmod p$$

Теперь применим теорему Эйлера, которая утверждает, что для любых взаимно простых каждого a и n имеет место формула

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod} n).$$

Любое положительное целое число z может быть представлено в виде $z = q + k\varphi(n)$. Поэтому по теореме Эйлера имеем

$$a^z \equiv a^q (\mathrm{mod}\ n), \text{ если } z = q (\mathrm{mod}\ \varphi(n)).$$

Используя это соотношение совместно с предыдущим, получим равенство

$$\mathrm{ind}_{a,p}(xy) = [\mathrm{ind}_{a,p}(x) + \mathrm{ind}_{a,p}(y)] \mathrm{mod}\ \varphi(p),$$

обобщив которое, получаем

$$\mathrm{ind}_{a,p}(y^r) = [r\mathrm{ind}_{a,p}(y)] \mathrm{mod}\ \varphi(p).$$

Это указывает на аналогию между обычными логарифмами и индексами — по этой причине последние часто называют дискретными логарифмами.

Следует иметь в виду, что однозначно дискретные логарифмы по модулю n при основании a определяются, только когда a является первообразным корнем n.

Таблица У.3

Таблицы дискретных логарифмов по модулю 19

(а) Дискретные логарифмы по модулю 19 при основании2

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(б) Дискретные логарифмы по модулю 19 при основании 3

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(в) Дискретные логарифмы по модулю 19 при основании 10

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(г) Дискретные логарифмы по модулю 19 при основании 13

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(д) Дискретные логарифмы по модулю 19 при основании 14

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	14	9

(е) Дискретные логарифмы по модулю 19 при основании 15

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	12	9

Вычисление дискретных логарифмов. Рассмотрим уравнение

$$y \equiv g^x (\mathrm{mod}\, p).$$

Вычисление y при заданных g, x и p является простым делом. В самом худшем случае придется выполнить x повторных умножений, для чего имеются достаточно эффективные алгоритмы. Но если заданы y, g и p, то вычисление x из указанного выше соотношения — т.е. дискретное логарифмирование — является, вообще говоря, очень непростой задачей. По сложности эта задача сравнима с задачей разложения больших чисел на простые множители (что требуется для RSA) и имеет экспоненциальную сложность.

В настоящее время сложность наиболее быстрого из известных алгоритмов вычисления дискретных логарифмов по модулю простого числа оценивается величиной порядка $e^{((\ln p)^{1/3}\ln(\ln p))^{2/3}}$, что для больших простых чисел оказывается за пределами практических возможностей современных вычислительных средств.

Рекомендуемая литература

1. Криптографическая защита информации : учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2019. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-16-106001-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018903 (дата обращения: 24.01.2020)
2. Бабаш А.В., Шанкин Г.П. Криптография. Под редакцией В.П. Шерстюка, ЭЛ. Применко / А.В. Бабаш, Г.П. Шанкин. - М.: СОЛОН-ПРЕСС, 2007. - 512 с. - ISBN 5-93455-135-3
3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2005. – 229 с.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. - М.: Горячая линия - Телеком, 2001. – 120 с.
5. Анин Б.Ю. Защита компьютерной информации. СПб: БХВ-Петербург, 2000. 384 с.
6. Галатенко В. А. Основы информационной безопасности. Курс лекций. Учебное пособие. М: ИНТУИТ. РУ «Интернет-университет Информационных Технологий», 2004. 264 с.
7. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы комплексной безопасности. М.: Радио и связь, 2000. 192 с.
8. Шнайдер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.
9. Венбо Мао. Современная криптография. Теория и практика / Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 768 с.
10. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ-Петербург, 2005. – 288 с.
11. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных.
12. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
13. Санников В.Г. Введение в теорию и методы криптографической защиты информации: Учебное пособие. - М.: МТУСИ, 2009. – 36 с.
14. Вус М. А. Государственная тайна в Российской Федерации. Учебно-методическое пособие. Издание 2-е, перераб. и дополн. СПб.: Изд-во Санкт-Петербургского университета, 2000. 409 с.

15. Галатенко В. А. Стандарты информационной безопасности. М: Интернет-Университет Информационных Технологий ИНТУИТ.РУ 2004.

16. Грязное Е., Панасенко С. Безопасность локальных сетей // Мир и безопасность (Электрон. журнал). 2003. № 2. Режим доступа к журн.: http://daily.sec.ru.

17. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. Спб: БХВ-Петербург. 2000. 368 с.

18. Карпов Е.А., Котенко И.В., Котухов М.М., Марков А.С, Парр Г.А., Рунеев А.Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И.В. Котенко. СПб.: ВУС, 2000.

19. Касперский Е. Компьютерные вирусы, 2003. Электронная энциклопедия. – Режим доступа к энциклопедии: http://www. Viruslistcom /viruslistbooks.html.

20. Медведовский И.Д., Семьянов П.В., Леонов Д.Г., Лукацкий А.В. Атака из Internet. М.: Солон-Р, 2002.

21. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Лань. 2000.

22. Новиков Ю. В., Кондратенко С, В. Локальные сети: архитектура, алгоритмы, проектирование. М.: ЭКОМ, 2001.

23. Олифер В. Г., Олифер Н. А.. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2000.

24. Спортак М., Паппас Ф. Компьютерные сети и сетевые технологии. М.: ТИД «ДС», 2002.