КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

ЛЕКЦИЯ ЛР1. АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

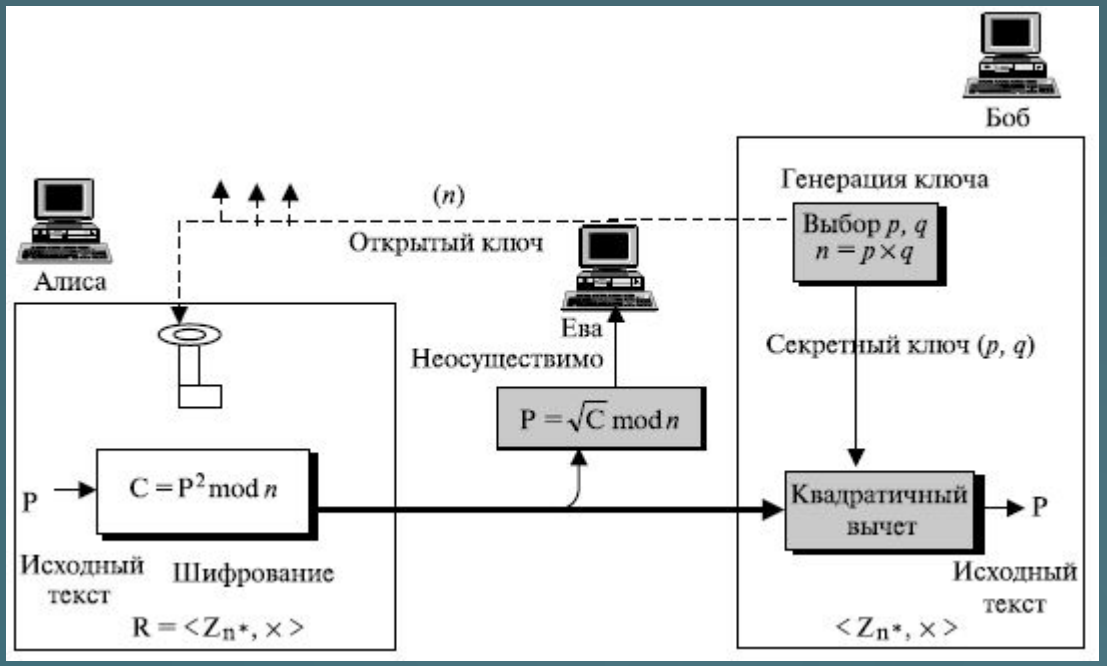
Профессор кафедры
доктор технических наук, старший научный сотрудник
ТУКЕЕВ Дмитрий Леонидович

УЧЕБНЫЕ ВОПРОСЫ

ЛИТЕРАТУРА

1. А.А. ВАРФОЛОМЕЕВ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Учебное пособие. Российский университет дружбы народов. – М.: 2008 С.

Криптосистема Рабина



Криптосистема Рабина (M.Rabin) является вариантом *криптосистемы* RSA. RSA базируется на возведении в степень сравнений. *Криптосистема* Рабина базируется на квадратичных сравнениях.

Безопасность схемы Рабина опирается на сложность поиска квадратных корней по модулю составного числа. Эта проблема аналогична разложению на множители.

ПРОЦЕДУРА ШИФРОВАНИЯ: выбираются два простых числа p и q, конгруэнтных 3 mod 4. Эти простые числа являются закрытым ключом, а их произведение n=pq - открытым ключом.

Для шифрования сообщения M (M должно быть меньше n), вычисляется $C = M^2 \bmod n$.

ДЕШИФРОВАНИЕ СООБЩЕНИЯ: Так как получатель знает p и q, вычисляется:

$m1=C^{(p+1)/4} \bmod p$; $m2=(p-C^{(p+1)/4}) \bmod p$; $m3=C^{(q+1)/4} \bmod q$; $m4=(q-C^{(q+1)/4}) \bmod q$.

После этого решается задача нахождения четырех возможных решений с помощью китайской теоремы об остатках для комбинаций:

m1	**m1**	**m2**	**m2**
m3	**m4**	**m3**	**m4**

Криптосистема Рабина

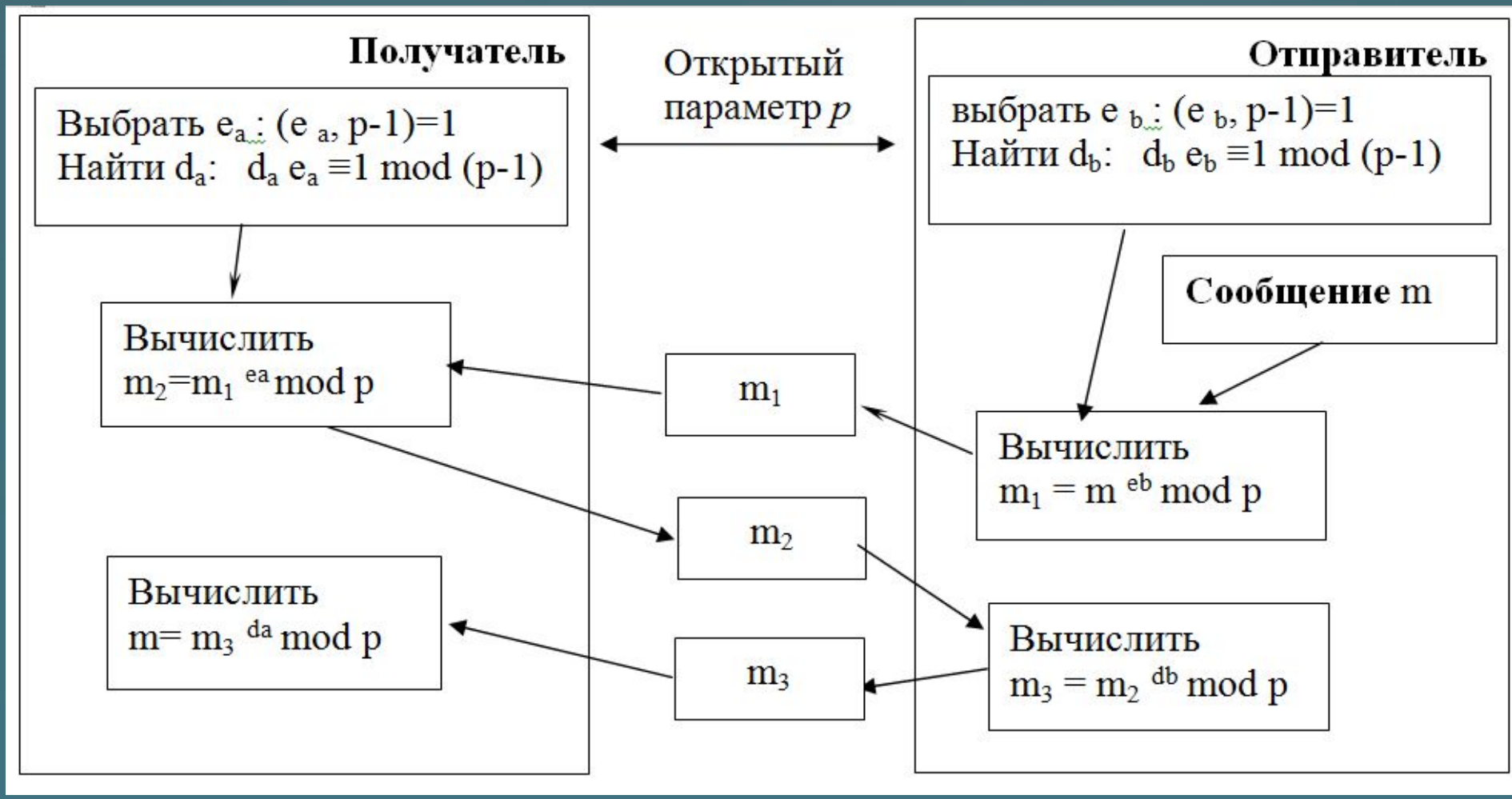
p=	23	M	24	20	19	14	22	31	39
q=	7								
n=p*q=	161		576	400	361	196	484	961	1521
		C	93	78	39	35	1	156	72
			6,5E+11	2E+11	4E+09	2E+09	1	1E+13	1E+11
		m1=	1	3	4	9	1	8	16
			-6E+11	-2E+11	-4E+09	-2E+09	22	-1E+13	-1E+11
		m2=	22	20	19	14	22	15	7
			8649	6084	1521	1225	1	24336	5184
		m3=	4	1	2	0	1	4	4
			-8642	-6077	-1514	-1218	6	-24329	-5177
		m4=	3	6	5	0	6	3	3

Криптосистема Рабина

		Китайская теорема об остатках													
1 ПАРА	m1	1	mod	23											
	m3	4	mod	7											
		MMo=	161												
		MM1=	7		7	*	Y	СООТВ	1	mod	23		Y1=	10	70
		MM2=	23		23	*	Y	СООТВ	4	mod	7		Y2=	2	46
															116
2 ПАРА	m1	1	mod	23											
	m4	3	mod	7											
		MMo=	161												
		MM1=	7		7	*	Y	СООТВ	1	mod	23		Y1=	10	70
		MM2=	23		23	*	Y	СООТВ	3	mod	7		Y2=	5	115
															24
3 ПАРА	m2	22	mod	23											
	m3	4	mod	7											
		MMo=	161												
		MM1=	7		7	*	Y	СООТВ	22	mod	23		Y1=	13	91
		MM2=	23		23	*	Y	СООТВ	4	mod	7		Y2=	2	46
															137
4 ПАРА	m2	22	mod	23											
	m4	3	mod	7											
		MMo=	161												

Алгоритм Месси-Омуры

Алгоритм **Месси-Омуры** позволяет передать сообщение по открытому каналу связи без предварительной передачи какой бы то ни было ключевой информации. Алгоритм является аналогом ящика, запираемого на один или два замка. Вместо замков абоненты используют ключи (d_a, e_a), (d_b , e_b). Для их организации используется открытый параметр – большое простое число p. Алгоритм генерации ключей приведен на рисунке



Алгоритм Месси-Омуры

A и B	Договариваются об использовании в качестве открытого параметра сеанса простого числа N такого, что N-1 имеет большой простой делитель. Пусть N=19. Число Nпубликуется в общедоступном месте.
A	1) Выбирает случайным образом в качестве своего секретного параметра простое число E=5 из диапазона 1..N-1 2) Вычисляет мультипликативно обратное к нему число D: $D=E^{-1}$ mod (N-1) т.е. удовлетворяющее равенству (D*E mod (N-1))=1. D= **11** 3) Имея открытые данные X=8, вычисляет промежуточный параметр $C=(X^E \bmod N)= (8^{11} \bmod 19)=12$ и отправляет его приемнику B.
B	1) Выбирает случайным образом в качестве своего секретного параметра простое число E'=7 из диапазона 1..N-1. 2) Вычисляет мультипликативно обратное к нему число D': $D'=(E'^{-1} \bmod (N-1))$. D'= **13** 3) Получив от источника C=12, вычисляет $C'=(C^{E'}N)=(12^7 \bmod 19)=12$ и отправляет его отправителю A.
A	Снимает свой ключ, вычисляя $X'=(C'^D \bmod N)=(12^5 \bmod 19)=8$ и передает результат B.
B	Снимает свой ключ, вычисляя $X=(X'^{D'} \bmod N)=(8^{13} \bmod 19)=8$. Таким образом, B получил исходные секретные данные.

Алгоритм Месси-Омуры

В результате всех пересылок по открытому каналу, злоумышленнику известно:

$N = 19$, $C = (X^E \bmod N) = 12$, $C' = ((X^E)^{E'} \bmod N) = 12$, $X' = (((X^E)^{E'})^D, \bmod N) = 8$.

Для восстановления X ему необходимо решить задачу дискретного логарифмирования, простого решения которой на сегодняшний день не существует.

Алгоритм Месси-Омуры

Пусть E — эллиптическая кривая порядка n, а e — некоторое целое , причем, $(e,n)=1$, $1<e<n$. Используя алгоритм инвертирования, найдем

$$d \equiv e^{-1} (\mathrm{mod}\, n). \qquad (7.2)$$

Используем то свойство, что законы модулярной арифметики над целыми числами и над точками эллиптической кривой идентичны. Любую точку P эллиптической кривой можно вычислить по формулам

$$Q = eP,$$
$$R = dQ.$$

Очевидно, что $Q = P$. Протокол Месси-Омуры основан на этой идее, реализуемой с учетом трудности решения проблемы определения скалярного множителя, соответствующего данной точке эллиптической кривой относительно базовой точки, умножаемой на этот скаляр, т.е. на проблеме дискретного логарифма для эллиптических кривых.

Обмен ключами между пользователями A и B можно провести по следующей схеме:

1) сторона A выбирает целое число $e_A < n$ и вычисляет по формуле (7.2) d_A. Это число e_A будет личным ключом шифрования участника A. Число d_A будет личным ключом расшифрования участника A. Затем участник A помещает свое сообщение m в некоторую точку P_m эллиптической кривой и умножая на свое секретное значение e_A получает точку (генерирует открытый ключ)

$$P_A = e_A P_m;$$

Алгоритм Месси-Омуры

2) сторона B выбирает аналогично e_B и d_B, которые являются личными ключами шифрования и расшифрования, соответственно, участника B. Затем участник B, умножая свое секретное значение e_B на открытый ключ P_A получает точку (генерирует открытый ключ)

$$P_B = e_B P_A;$$

3) это значение отсылается участнику A;
4) участник A вычисляет

$$P_O = d_A P_B$$

5) и отсылает полученную точку B;
6) умножая полученную точку на свой секретный ключ расшифрования d_B, участник B получает точку P_m, соответствующую сообщению m участника A:

$$P_m = d_B P_O.$$

Вычисляя P_O, участник A снимает действие своего ключа шифрования :

$$P_O = d_A P_B = d_A(e_B P_A) = d_A(e_B(e_A P_m)) = e_B(d_A(e_A P_m)) = e_B P_m.$$

Следовательно, участник B получает

$$d_B P_O = d_B(d_A P_m) = P_m.$$

Сообщение m может быть использовано в качестве ключа традиционной криптосистемы. 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.