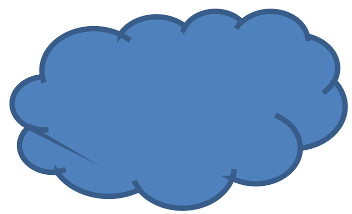
Лекция 4. Асимметричное шифрование

Модель асимметричного шифрования



в репозитарий

в репозитарий

Alice	Bob
$K^A_{откр}$ – открытый ключ	$K^B_{откр}$ – открытый ключ
$K^A_{закр}$ – закрытый ключ	$K^B_{закр}$ – закрытый ключ
M – открытый текст	M – открытый текст
$E(M, K^B_{откр}) = M'$ →	$D(M', K^B_{закр}) = M$
$D(M', K^A_{закр}) = M$	← $E(M, K^A_{откр}) = M'$

Историческая справка и особенности

- ✔Шифрование с открытым ключом было открыто двумя американцами, Диффи (Diffie) и Хеллманом (Hellman), в 1976 г
- ✔Два ключа, не нужно передавать ключ
- ✔Математический аппарат вместо перестановок и подстановок
- ✔ Различные области применения
- ✔Основаны на вычислительно сложных математических задачах

Алгоритм шифрования RSA (Rivest, Shamir и Adleman)

- ✔ Предложен 1977 году в мат. журнале
- ✔ Основывается на вычислительной сложности задачи факторизации больших целых чисел
- ✔ С 1993 года объявлен в стандарте PKCS1 v. 1.5
- ✔ Блочный шифр
- ✔ Широко исследован, считается абсолютно надежным при длине ключа больше 2048 бит
- ✔ Применяется как для шифрования, так и для цифровой подписи

Вспомогательные понятия

1. Делитель числа *n* – число которое делит *n* без остатка.

2. Простые числа – которые делятся без остатка только на себя и на единицу.

3. НОД(*m*,*n*) – наибольший общий делитель чисел *m, n* – наибольшее число которое делит без остатка *n* и *m.*

НОД(*70*,*105*)=35, НОД(5,35)=5

НОД(1678,49)=?

Алгоритм шифрования RSA. Создание пары ключей

1. Выбираются два простых числа **p** и **q**
2. Вычисляется их произведение **n = p*q, n – модуль шифрования**
3. Выбирается произвольное число **e (e<n)** такое, что

НОД(e,(p-1)(q-1)) = 1

Т.е. **e** должно быть взаимно простым с числом **(p-1)(q-1).**

4. Находится **d – взаимообратное с e по mod (p-1)(q-1).**

Для этого решается методом Евклида в целых числах уравнение

e*d+(p-1)(q-1)*y = 1, d и **y** – неизвестные.

5. Два числа **(e, n)** публикуются как открытый ключ.

6. Число **d** является закрытым (секретным) ключом.

Алгоритм шифрования RSA. Шифрование/дешифрование.

Шифрование:

1. Отправитель разбивает M на блоки, меньшие n.
2. $M' = M^e \pmod n$ (возводим M в степень e, делим на n и берем целый остаток от деления – это и есть зашифрованный результат)

Дешифрование:

1. $M = M'^d \bmod n$

Алгоритм шифрования RSA. Пример.

Шифрование:

1. Выбрали простые числа p=7 q=17.
2. Вычислили n = p*q = 7*17 = 119.
3. Вычислили e = 5.
4. Вычислили d = 77 (5*77=1 mod 96)
5. M = 19.
6. Результат шифрования вычисляется так:

$19^5 = 2476099 / 119 = 20807$ с остатком 66.

$M' = 19^5 \mod 119 = 66$

Дешифрование:

$66^{77} = 1{,}27 \cdot 10^{140} / 119 = 1.06 \cdot 10^{138}$ с остатком 19.

$M = 66^{77} \mod 119 = 19.$

Алгоритм Евклида.

Дано *a*, *b* задача - найти НОД*(a,b)*.

Пусть *a*=1071, *b*=462.

Для любых *a* и *b* можно выполнить: *a*=*b***q*+*r*

$1071=462*2+147$

$462=147*3+21$

$147=21*7+0$

НОД(1071, 462)=21

Алгоритм Евклида. Пример 2.

Пусть a=665, $b=548$.

Для любых a и b можно выполнить: $a=b*q+r$

*665=548*1+117*

…

НОД(665, 548)=?

Алгоритм Евклида. Пример 2.

Пусть *a*=665, *b=548*.

Для любых *a* и *b* можно выполнить: *a=b*q+r*

*665=548*1+117*

*548=117*4+80*

*117=80*1+37*

*80=37*2+6*

*37=6*6+1*

НОД(665, 548)=1

Нахождение коэффициентов Безу

$a*x+b*y$=НОД(a,b) – соотношение Безу, а и b всегда существуют

следовательно:

если a и b взаимно простые, то уравнение

$a*x+b*y=1$ всегда имеет решение.

Расширенный алгоритм Евклида. Пример 1.

$51*d=1 \bmod 110$, <u>задача - найти d</u>. Для этого решим уравнение:

$110*x+51*y=1$ ($d=y$)

i	a	b	r	q		x	$x_0=0,\ x_1=1$ **Для i=2,3…** $x_i=x_{i-2}-q_i*x_{i-1}$
						0	
1	110	51	8	2	*110=51*2+8*	1	
2	51	8	3	6	*51=8*6+3*	-6	-6=0-6*1
3	8	3	2	2	*8=3*2+2*	13	13=1-2*(-6)
4	3	2	1	1	*3=2*1+1*	-19	-19= -6-1*13

$110*(-19)+51*y=1$

$y = 41$

Проверка: $51*41=2091=1 \bmod 110$

Расширенный алгоритм Евклида. Пример 2.

$17*d=1 \bmod 77$, <u>задача - найти *d*</u>. Для этого решим уравнение:
$77*x+17*y=1$ ($d=y$)

				0
a	**b**	**r**	**q**	**x**
77	17	9	4	1
17	9	8	1	-1
9	8	1	1	2

*77=17*4+9*

*17=9*1+8*

*9=8*1+1*

$77*2+17*y=1$
$y = -9=68 \bmod 77$

Проверка: $17*68=1156=1 \bmod 77$

Расширенный алгоритм Евклида. Пример 3.

$79*d=1 \bmod 196$, <u>задача - найти *d*</u>*.* Для этого решим уравнение:
$196*x+79*y=1$ ($d=y$)

				0	
a	**b**	**r**	**q**	**x**	
196	79	38	2	1	*196=79*2+38*
.	.	.	.	.	

y =?

Расширенный алгоритм Евклида. Пример 3.

79*d=1 mod 196, <u>задача - найти d</u>. Для этого решим уравнение:
196*x+79*y=1 (d=y)

a	b	r	q	x	
				0	
196	79	38	2	1	*196=79*2+38*
79	38	3	2	-2	*79=38*2+3*
38	3	2	12	25	*38=3*12+2*
3	2	1	1	-27	*3=2*1+1*

196*(-27)+79*y=1
y = 67

Проверка: 79*67=5293=1 mod 196