**Лекция. Основы криптографии. Криптография с асимметричными ключами.**

**Алгоритм Диффи — Хеллмана**

[http://ru.wikipedia.org/wiki/Алгоритм\_Диффи-Хеллмана](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B8%D1%84%D1%84%D0%B8-%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0)

Алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены канал связи.

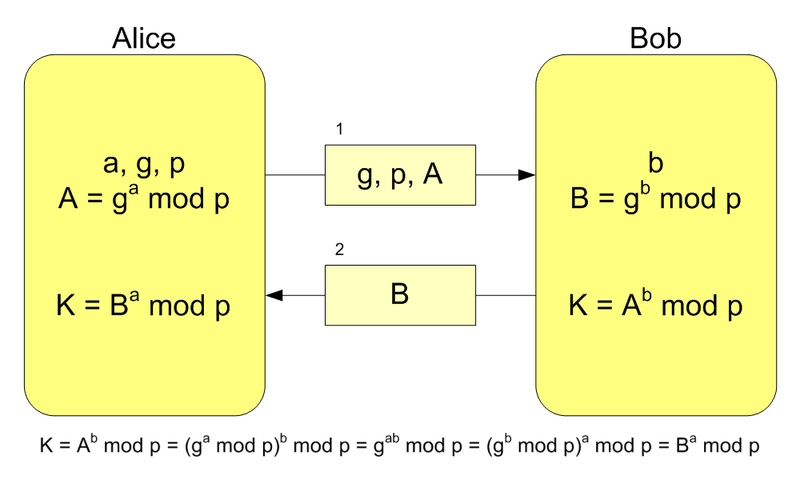
[](https://moodle.kstu.ru/pluginfile.php/40236/mod_page/content/29/800PX-~1.PNG)

Рис. Получение симметричного ключа на алгоритме Диффи — Хеллмана

Алгоритм:

* 1. генерируются ***закрытые ключи a и b****(случайное натуральное число)*
  2. генерируются***открытые******параметры*** ***p*** и ***g***и передаются другой стороне

***p*** - случайное простое число

***g*** - первообразный корень по модулю ***p (***находится из условия***g*φ(*p*) mod *p* ≡1  где φ(*p*) функция Эйлера, существует множество корней)**

* 1. вычисление ***открытых ключей* *A и B***

***A = ga mod p***

***B = gb mod p***

* 1. обмен ***открытыми ключами***
  2. вычисляется ***общий секретный ключ* *K***

***K = Ba mod p***

***K = Ab mod p***

*ключ****К*** равный с обеих сторон, потому что:

***Ba mod p = (gb mod p)a mod p = gab mod p = (ga mod p)b mod p = Ab mod p***

**Пример:**

Ева - криптоаналитик. Она читает пересылку Боба и Алисы, но не изменяет содержимого их сообщений.

открытая - закрытая

* K = секретный ключ. K = 2
* g = открытое простое число. g = 5
* p = открытое простое число. p = 23
* a = секретный ключ Алисы. a = 6
* A = открытый ключ Алисы. A = ga mod p = 8
* b = секретный ключ Боба. b = 15
* B = открытый ключ Боба. B = gb mod p = 19

В случае (5**6** mod 23 = 8) , 8-это остаток деления 56/23

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Алисы** | | | знает | не знает | | p = 23 | **b** = **?** | | g = 5 (522**mod *23* =1**) |  | | **a** = **6** |  | | A = 5**6** mod 23 = 8 |  | | B = 5**b** mod 23 = 19 |  | | **K** = 19**6** mod 23 = **2** |  | | **K** = 8**b** mod 23 = **2** |  | | **K** = 19**6** mod 23 = 8**b** mod 23 |  | | **K** = **2** |  | | |  |  | | --- | --- | | **Боба** | | | знает | не знает | | p = 23 | **a** = **?** | | g = 5 |  | | **b** = **15** |  | | B = 5**15** mod 23 = 19 |  | | A = 5**a** mod 23 = 8 |  | | **K** = 8**15** mod 23 = **2** |  | | **K** = 19**a** mod 23 = **2** |  | | **K** = 8**15** mod 23 = 19**a** mod 23 |  | | **K** = **2** |  | | |  |  | | --- | --- | | **Ева** | | | знает | не знает | | p = 23 | **a** = **?** | | g = 5 | **b** = **?** | |  | **K** = **?** | | A = 5**a** mod 23 = 8 |  | | B = 5**b** mod 23 = 19 |  | | **K** = 19**a** mod 23 |  | | **K** = 8**b** mod 23 |  | | **K** = 19**a** mod 23 = 8**b** mod 23 |  | |

 Получив симметричные ключи шифруются сообщения симметричным алгоритмом.

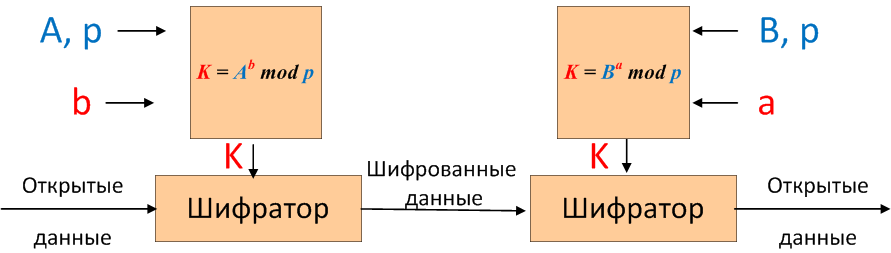


Рис. Получение симметричных ключей из ассиметричных

**Алгоритм RSA**

<http://ru.wikipedia.org/wiki/RSA>

Алгоритм генерации пары ассиметричных ключей RSA:

1. генерируются два различных случайных простых числа **p** и **q** заданного размера (например, 1024 бита каждое).
2. вычисляется их произведение **n=pq** , которое называется модулем.
3. вычисляется значение функции Эйлера от числа ***n***:  
   **φ(n)=(p-1)(q-1)**
4. **p и q**уничтожаются.
5. выбирается целое число (открытая экспонента)**e(1<e<φ(n))** , взаимно простое со значением функции **φ(n)**.
6. вычисляется число (закрытая экспонента) **d**,  
   **d** это первообразный корень по модулю **φ(*n*)   e·d mod φ(*n*) ≡1**.  
   ***d***находится с помощью расширенного алгоритма Евклида ([http://ru.wikipedia.org/wiki/Расширенный\_алгоритм\_Евклида](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%95%D0%B2%D0%BA%D0%BB%D0%B8%D0%B4%D0%B0))  
   как коэффициент уравнения **φ(*n*)·s+e·d=1**Расширенный алгоритм Евклида для нахождения НОД и коэффициентов s и d.  **r1 = φ(*n*) − q0e  
   r2 = e − q1 r1 = e − q1 (φ(*n*) − q0 e) = −q1 φ(*n*) + (1 + q1 q0 )e  
   r3 = r1 − q2 r2 = φ(*n*) − q0 e − q2 (−q1 φ(*n*) + (1 + q1 q0 )e) = (1 + q1 q2 )φ(*n*) − (q0 + q2 (1 + q1 q0 ))e**

**..........................................................................................................................  
  
ri - остатки от деления.**В случае если**r2=1**(найден НОД), получим

**d=(1 + q1 q0 )**

В случае если**r3=1**(коэффициент со знаком "-"), получим

**d=− (q0 + q2 (1 + q1 q0 )+φ(*n*)**

1. число**φ(n)**- уничтожается.
2. пара ***e, n*** публикуется в качестве **открытого ключа RSA**
3. пара ***d, n*** играет роль **секретного ключа RSA**

Предположим, сторона **B** хочет послать стороне **A** сообщение **M**.

Алгоритм шифрования:

* взять ***открытый ключ (e,n)*** стороны **A**
* взять открытый текст **M**
* зашифровать сообщение **PA(M)=Memod n .**

Алгоритм расшифровки:

* принять зашифрованное сообщение  **С=PA(M)**
* применить свой ***секретный ключ (d,n)*** для расшифровки сообщения **SA(C)=Cdmod n .**

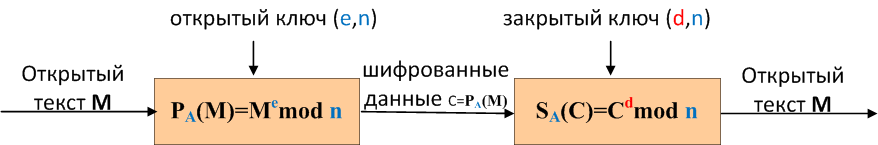


 Рис. Шифрование и расшифровка RSA

**Пример:**

* генерируем два числа**p и q  
  p=61 и q=53**.
* вычислим **n=pq   
  n = 61 · 53 = 3233.**
* вычислим **φ(n)  
  φ(3233)=φ(n)=(p-1)(q-1)=(61-1)(53-1)=3120**.
* выберем число из **1<e<3120  
  e=17**.
* вычислим **d**   
  **r1 = φ(*n*) − q0e= 3120-183\*17=9  
  r2 = e − q1 r1 = e − q1 (φ(*n*) − q0 e) = −q1 φ(*n*) + (1 + q1 q0 )e=17-9\*1=-3120\*1+(183\*1+1)\*17=8  
  r3 = r1 − q2 r2 = φ(*n*) − q0 e − q2 (−q1 φ(*n*) + (1 + q1 q0 )e) = (1 + q1 q2 )φ(*n*) − (q0 + q2 (1 + q1 q0 ))e=9-8\*1=3120\*(1+1\*1)-(183+1\*(1+1\*183))\*17=3120\*2-367\*17=1  
    
  коэффициенты уравнения φ(*n*)·s+e·d=1  
  s=2 и d=-357  
    
  d = -367+φ(*n*)=-367+3120= 2753**
* открытый ключ (**n=3233, e=17**)
* закрытый ключ  (**n=3233**, **d=2753**)
* зашифруем текст **m=65**
* зашифруем **C=PA(M)=Memod n=6517mod 3233=2790** .
* расшифруем  **SA(C)=Cdmod n=27902753mod 3233=65**