# Асимметричное шифрование

Проблема распространения ключей

М: Е(М,К1) ->С

С: D(C,K2) ->M’

-алгоритм публичен

-ключ шифрования общедоступен

-ключ расшифровки секретен

-расшифровка/получение ключа расшифровки, имея ключ шифрования очень сложно

Riverst

Shamir

Aldman

RSA

Вычисление ключей

P и Q – простые числа

N=P\*Q – длина алфавита (зашифрованного)

Fi(N)=(P-1)(Q-1) – Функция Эйлера

E – открытый ключ: взаимно простое с Fi(N)

D – секретный ключ: **(E\*D)mod (Fi(N))=1** -> E\*D=1+k\*Fi(N)=1+k\*(P-1)(Q-1)

Шифрование

С=(М^E)mod N

Расшифровка

M’=(C^D)mod N

M=(M^E)^D=M^(E\*D)=M\*M^Fi(N)=M

Гибридная схема:

- генерация симметричного ключа

- отправка ключа через асимметричное шифрование

- расшифровка симметричного ключа

- симметричное шифрование большого объема данных/потока

Решето Эратосфена

**1 2** **3** ~~4~~ **5** ~~6~~ **7** ~~8~~ ~~9~~ ~~10~~ **11** ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ **17**

Теорема Рабина

Алгоритм Миллера-Рабина (вероятностный)

Быстрое возведение в степень

R=A^K mod N

R=1

? K>0

? K – нечетное : R=(R\*A)mod N

K=K/2

A=(A\*A) mod N

110000**101**

Алгоритм Евклида

А и В

**B**=A mod B

A=B

Расширенный алгоритм Евклида

A\*X+B\*Y=НОД(A,B)=1

E( 1 0=x (D)

0 1)

R=A mod B

? R = 0

E=E\*(0 1

1 -q=A/B)

**B**=A mod B

A=B