Асимметричное шифрование

Проблема расространения ключей
Даффи-Хелман/Маркл

- Алгоритм общедоступен
- Ключ шифрования общедоступен
- Ключ расшифровки - секрет
- Обратное преобразование открытым ключом сложно

RSA

- Вычисление ключей
  - P, Q
  - N=P*Q - длина алфавита
  - fi=(P-1)(Q-1)
  - E -открытый ключ: взаимно простое с fi -> (E,N)
  - D -закрытый ключ: (E*D)mod fi = 1 -> (D,N)
- Шифрование
  - C=(M^E) mod N
- Расшифровка
  - M'=(C^D) mod N

Алгоритмы получения простых чисел

- [2;SQRT (P)]
- Решето Эратосфена
  2 **3** 4 **5** 6 **7** 8 9 10 **11** 12 **13** 14 15
- Теорема Рабина
- Тест Рабина-Миллера

Алгоритм Евклида
НОД (a,b) = НОД (b, a/b)

a=b*q1+r1
b=r1*q2+r2
r1=r2*q3+r3
....
rN-1=rN*qN

Расширенный алгоритм Евклида
r1=a+b(-q1)
r2=b+r1=r(-q2)=b+(a+b(-q1)(-q2)=a(-q2)+b(1+q1q2)
...
rN=a*S+b*T

a/b=q1+r1/b
b/r1=q2+r2/r1
r1/r2=q3+r3/r2
...
rN-1/rN=qN

a/b=q1+(q2+rr2/r1)-1=q1+(q2+(q3+(q4...(qN)-1)-1)-1)-1

ed=1+fi*k
ed-fi*k=1

Матричная реализация
E=1 0
  0 1
r=a mod b
q=a/b (целочисленное деление)
r=0?
E=E*(0 1
  1 -q)
a,b->b,r

d>0 -> N+d

Возведение в степень по модулю
(a^k)mod N:

r=1
(k>0)?
  ?k-нечетное -> r=(r*a)mod N
  a=(a^2) mod N
  k>>=1 (k=k/2)