а б в г д н 4 8 е 3

Симметричное шифрование

КЛЮЧ МОГУТ ПЕРЕХВАТИТЬ

а б в г д н 4 8 е 3

КЛЮЧ

КЛЮЧ

Ассимметричное шифрование RSA 1970, эллиптических кривых

кричишь на всю улицу

КЛЮЧ1- зашифровки сообщений p*q

P

Q

КЛЮЧ1- зашифровки сообщений p*q

КЛЮЧ2 - расшифровки сообщений (p-1)*(q-1)

?

КЛЮЧ2 - расшифровки сообщений (p-1)*(q-1)

P 1

Q 1

КЛЮЧ1- зашифровки сообщений p1*q1

КЛЮЧ2- зашифровки сообщений (p1-1)*(q1-1)