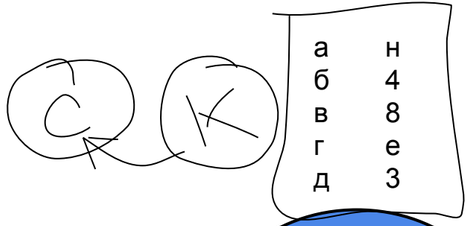
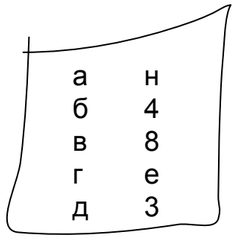


Симметричное шифрование

КЛЮЧ МОГУТ ПЕРЕХВАТИТЬ

КЛЮЧ



КЛЮЧ

Ассимметричное шифрование **RSA 1970**, SSH, SSL
эллиптических кривых

кричишь на всю улицу

КЛЮЧ1- зашифровки сообщений p*q

P

Q

КЛЮЧ1- зашифровки сообщений p*q PUBLIC

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

?

P 1

Q 1

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

КЛЮЧ1- зашифровки сообщений p1*q1

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

простые числа 2,3,5,7,11,13,17,19,...

481478912789412378418177 7

312468912398419811239084 1

312893789126378127831278387162783612783612631231682132689 7