

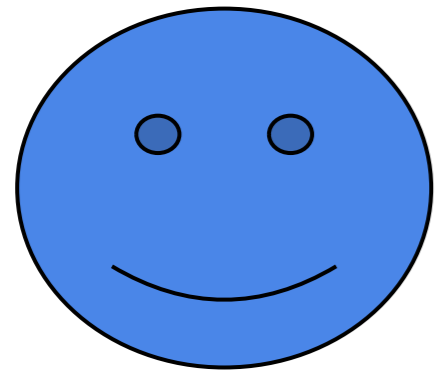


а н
б 4
в 8
г е
д з

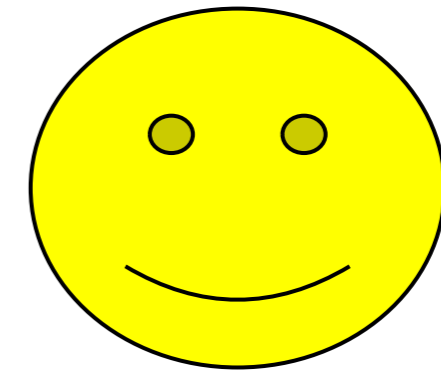
Симметричное шифрование

КЛЮЧ МОГУТ ПЕРЕХВАТИТЬ

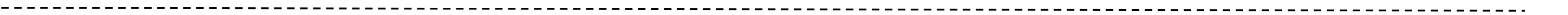
а н
б 4
в 8
г е
д з



КЛЮЧ



КЛЮЧ



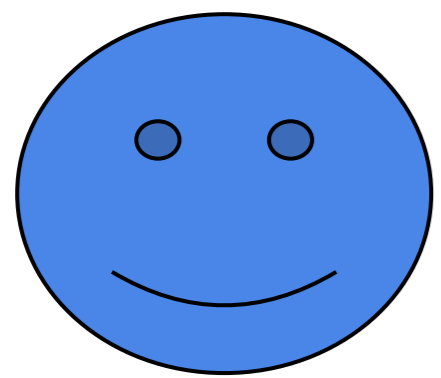
Ассиметричное шифрование RSA 1970, эллиптических кривых

кричишь на всю улицу

КЛЮЧ1- зашифровки сообщений $p \cdot q$

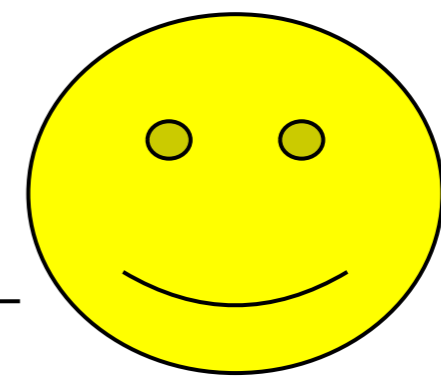
P
Q

P
1
Q
1



КЛЮЧ1- зашифровки сообщений $p \cdot q$

КЛЮЧ2 - расшифровки сообщений $(p-1) \cdot (q-1)$



~~КЛЮЧ2 - расшифровки сообщений $(p-1) \cdot (q-1)$~~

КЛЮЧ1- зашифровки сообщений $p \cdot q$

КЛЮЧ2- зашифровки сообщений $(p-1) \cdot (q-1)$

