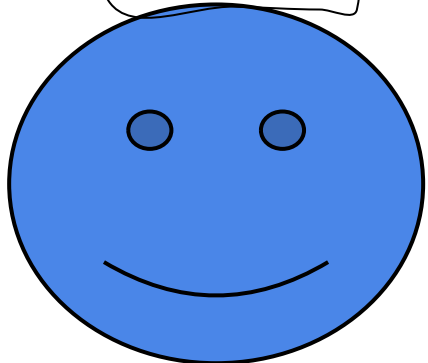


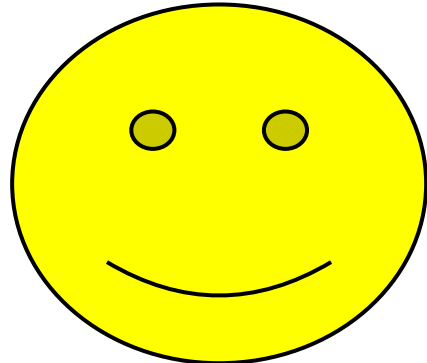


Симметричное шифрование

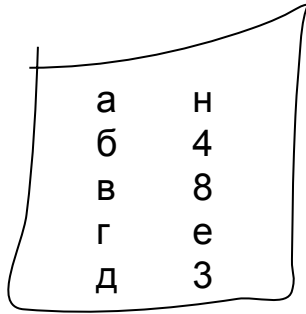
КЛЮЧ МОГУТ ПЕРЕХВАТИТЬ



КЛЮЧ



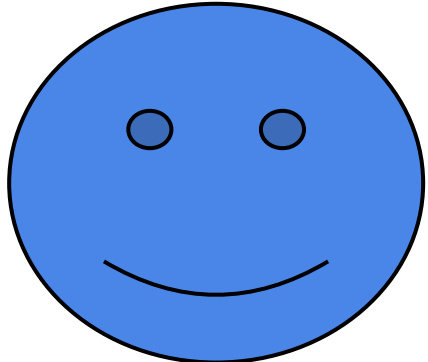
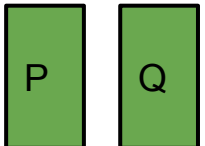
КЛЮЧ



Ассиметричное шифрование RSA 1970, эллиптических кривых

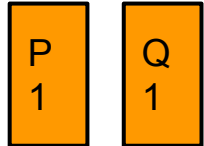
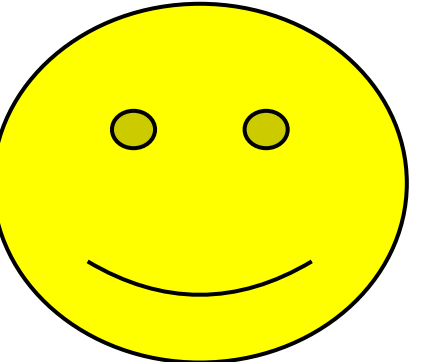
кричишь на всю улицу

КЛЮЧ1- зашифровки сообщений  $p \cdot q$



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  $(p-1) \cdot (q-1)$

