АБВГДЕЖЗИК
ЕЖЗИКЛМНОП

БАБА
ЖЕЖЕ

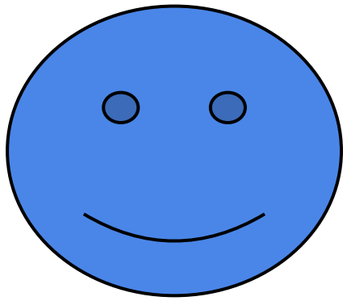
Симметричное шифрование

КЛЮЧ МОГУТ ПЕРЕХВАТИТЬ

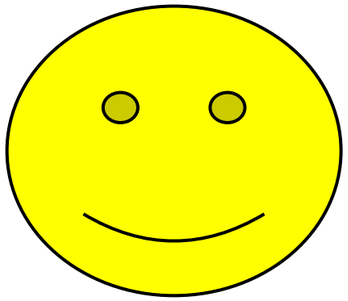
Абсолютное шифрование

один ключ и на расшифровку и не дешифровку

ключ = 5 (длина сдвига)



КЛЮЧ



КЛЮЧ

Ассимметричное шифрование

RSA (простые числа)

Эллиптические кривые

кричишь на всю улицу

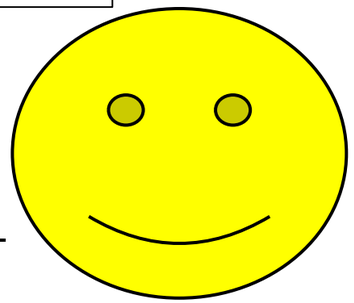
КЛЮЧ1- зашифровки сообщений p*q

11

13

P

Q



КЛЮЧ1- зашифровки сообщений m*n

КЛЮЧ2 - расшифровки сообщений (m-1)*(n-1)

public key

private key

КЛЮЧ1- зашифровки сообщений p*q=143

КЛЮЧ2 - расшифровки сообщений (p-1)*(q-1)=120

КЛЮЧ1- зашифровки сообщений