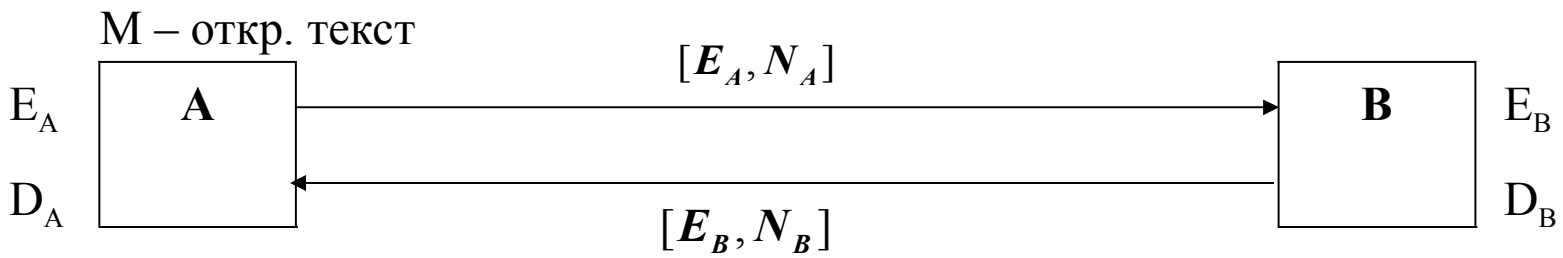
RSA

1. Формирование ключа
   1. p и q – большие простые целые числа;
   2. $N=p\times q$
   3. $\varphi(N)=(p-1)\times(q-1)$ – функция Эйлера;
   4. Выбор открытого ключа $E<N$, такого, что $НОД(E, \varphi(N))=1$
   5. Определение закрытого ключа D:
      $E \cdot D \equiv 1 \bmod \varphi(N)$
      $НОД(D, \varphi(N))=1$



$p_A, q_A;$

$N_A = p_A \cdot q_A;$

$\varphi(N_A) = (p_A - 1)(q_A - 1);$

$E_A \cdot D_A \equiv 1 \bmod \varphi(N_A).$

$p_B, q_B;$

$N_B = p_B \cdot q_B;$

$\varphi(N_B) = (p_B - 1)(q_B - 1);$

$E_B \cdot D_B \equiv 1 \bmod \varphi(N_B).$

$$(M)^{E_B} = C \bmod N_B \Rightarrow C = \left[(M)^{E_B}\right]^{D_B} = (M)^{E_B \cdot D_B \equiv 1 \bmod \varphi(N_B)} = M \bmod N_B$$

Отправитель А

С – шифрованный текст

Получатель В

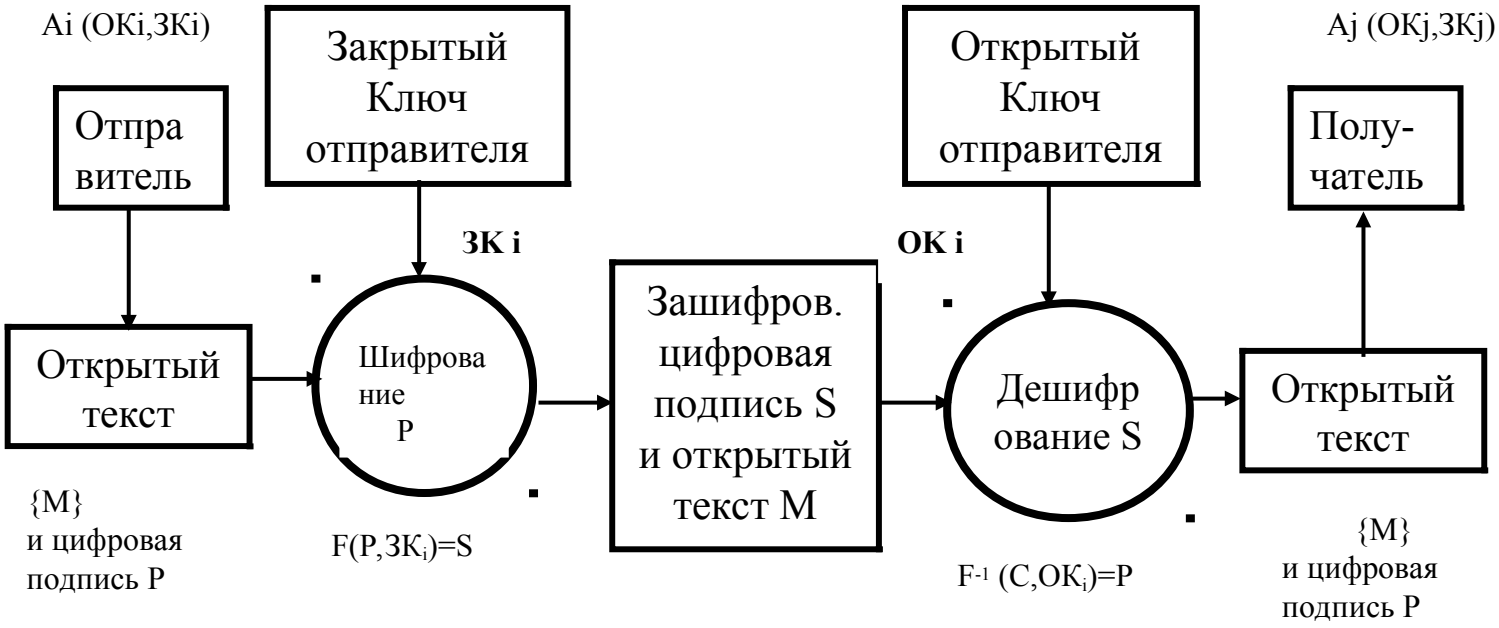
p и q – простые большие числа, например 100-разрядные. p и q - нечетные числа.

$\frac{10^{100} - 10^{99}}{2}$ - количество 100-разрядных нечетных чисел;

$\left[(10^{100} / \ln 10^{100}) - (10^{99} / \ln 10^{99})\right]$ - прибл. количество 100-разрядных простых чисел.

Вероятность успешного выбора одной пары 0,00868

3). Цифровая подпись (Аутентификация – подтверждение подлинности)

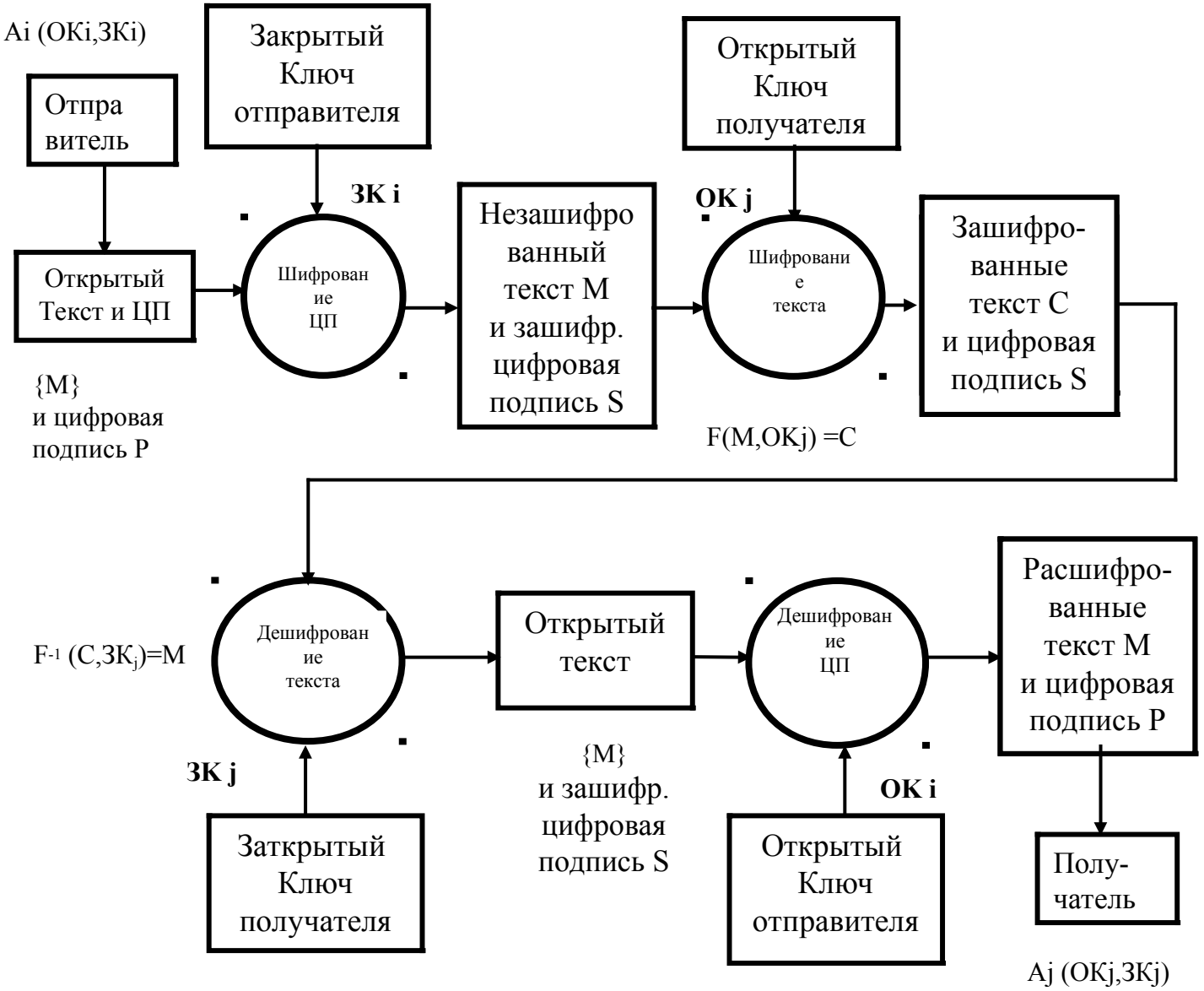


P –открытая цифровая подпись отправителя Ai;

S – зашифрованная цифровая подпись отправителя Ai

Привести пример использования стандарта RSA для электронной цифровой подписи для p=7 и q=13 при условии, сообщение было подписано открытой цифровой пдписью «12» (Это может быть вычисленная хеш-функция).

4). Раздельное шифрование текста и цифровая подпись. (Конфиденциальность и аутентификация)



5). Дайджест сообщения (проверка целостности сообщения) (хеш-функция – контрольная сумма, CRC и др.)