**ЭЦП на базе RSA**

**Вариант 1**

**Тест 1.** Текст из шифруемого файла: **BSUIR.**

***p*= 41 и *q*= 59**; ***r*= *p·q*= 2419;**

3) вычислим **функцию Эйлера: *φ*(*r*) = (*p*–1)*·*(*q*–1) = 40*·*58 = 2320;**

4) выберем ***КО* = 157**; (2320, 157) = (157, 122) = (122, 35) = (35, 17) = 1;

5)найдем значение *КС*, для которого выполняется: 157*·KС*= 1 mod *φ*(*r*) =   
= 1 mod 2320. Положив *а* равным *φ*(*r*) и *b* равным *KО*, по расширенному алгоритму Евклида вычислим ***КС* = *y*1 = 133.**

Символам исходного текста соответствуют следующие десятичные ASCII-коды:

«B»: 66; «S»: 83; «U»: 85; «I»: 73; «R»: 82.

**Значение хеш-функции по упрощенной формуле при Н0=100:**

**H[5]= 133**

**ЭЦП= 1451**

**Тест 2.** Файл **ПУСТ**.

***p*= 41 и *q*= 59. *r*= *p·q*= 2419. *КС* = 133. *КО* = 157**;

**H= 100**

**ЭЦП= 2306**

**Тест 3 (для больших P и Q).** Шифруем «BSUIR»

**P = 1125899839733759, Q = 18014398241046527)**

**R= 20282408092494394779761211604993. Kc= 4398042316799**

Значение хеш-функции по упрощенной формуле при **Н0=100**:

**H[5] = 133.**

**ЭЦП= 79682028967134813641419574225**

**ЭЦП на базе RSA**

**Вариант 2**

**Тест1** Файл **пуст**

P= **35742549198872617291353508656626642567**

Q= **359334085968622831041960188598043661065388726959079837**

K (закрытый ключ) = **27644437**

**хеш файла в 10 с/сч = 1245845410931227995499360226027473197403882391305**

**хеш файла в 16 с/сч = da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709**

**R= 12843516246565424159612232119158450558500502533923843847710718949148609993889068965015621579**

K (открытый ключ) = **1728878421902762998097455220819211776576604992212759706380229508756002499918000451466532133**

**ЭЦП=**  **7345037292125510823276286389127972135531234553033461313272884518077480827286076372724115183**

**ЭЦП на базе RSA Вариант 2**

**Тест2** Шифруемый файл: BSUIR = 66 83 85 73 82

p = **35742549198872617291353508656626642567**

q **= 359334085968622831041960188598043661065388726959079837**

закрытый ключ = **27644437**

**хеш файла в 10 с/сч = 1162611392931174794535682367744230140359207005311**

**хеш файла в 16 с/сч = cba54c437b066da131714f0d5b89c916db03ac7f**

**R=**

**12843516246565424159612232119158450558500502533923843847710718949148609993889068965015621579**

открытый ключ =

**1728878421902762998097455220819211776576604992212759706380229508756002499918000451466532133**

Шифрование хеша сообщения с закрытым ключом =(27644437,12843516246565424159612232119158450558500502533923843847710718949148609993889068965015621579)

**ЭЦП = 9045771182161666665739716492938175492893813960492837870659374602890755999147583216880689382**

расшифрование цифровой подписи с открытым ключом =1728878421902762998097455220819211776576604992212759706380229508756002499918000451466532133

расшифрованное сообщение = 1162611392931174794535682367744230140359207005311

decrypted digest is equal to the original digest