**ЭЦП\_DSA** (учебная хеш-функция)

**Тест\_1 -** файл пуст **-- H(m)= H0 = 100. Не совсем корректные значения: q=29, p=59**

**q=** **433**

**p=19919** (p-1=19918=2\*23\*433)

**h= 2,** тогда **g=8489, h** принадлежит **[2,p-2],** при этом **g>1.**

**x**=**11**, **x** принадлежит **[1,q-1],** тогда **y=gx**mod p

**Открытый ключ - p, q, y, закрытый - x.**

**k= 17, k** принадлежит **[1,q-1].**

**ЭЦП: r= 5** (gk mod p) mod q

**s= 111** k-1(h(m)+x\*r) mod q

**Проверка: v = r= 5**

**w=** s-1 mod q

**u1=** h(m)\*w mod q

**u2=** r\*w mod q

**v=** (gu1 \* yu2mod p) mod q

====================================================================

**Тест\_2 - файл BSUIR** (66,83,85,73,82) -- **H(m)= 74**

**q=** **593**

**p=** **3559** **(p-1=**3558=2\*3\*593**)**

**h= 3,** тогда **g=** **729 , h** принадлежит **[2,p-2],** при этом **g>1.**

**x**=**17**, **x** принадлежит **[1,q-1]**, тогда **y= 2201**

**k= 23, k** принадлежит **[1,q-1].**

**ЭЦП: r= 250**

**s= 188**

**Проверка: v = r= 250**

**==================================================================**

**ЭЦП\_DSA (Sha1)**

**Тест\_1 – файл BSUIR**

(66,83,85,73,82) -- **H(m) = 1162611392931174794535682367744230140359207005311**

Не верные p и q: **q=** **107464843, p= 35742549198872617291353508656626642567**

**q= 1193447034984784682329306571139467195163334221569**

**p= 89884656743115796742429711405763364460177151692783429800884652449310979263752253529349195459823881715145796498046459238345428121561386626945679753956400077352882071663925459750500807018254028771490434021315691357123734637046894876123496168716251735252662742462099334802433058472377674408598573487858308054417**

**h= 3,** тогда **g=**

**x**= **11934**, **x** принадлежит **[1,q-1].**

**k= 6274, k** принадлежит **[1,q-1].**

**ЭЦП: r= 763684579901334190290064024368121408692171318083**

**s= 191461125111786128975219616823573183032301959481**

**Проверка: v = r =**

**=======================================================**

**Тест\_2 - файл пуст** - **H(m)= 1245845410931227995499360226027473197403882391305**

**q и p** те же

**h= 3,**

**x= 11934**

**k= 6274**

**ЭЦП: r= 763684579901334190290064024368121408692171318083**

**s= 991924682209964961688430603309572736794551733110**