**Эль Гамаль**

**Тест1:**

Исходный текст: **BSUIR**

**p=911(910=2\*5\*7\*13), g=17(первообразный корень по модулю 911), x=9(1<x<p-1),**

**k=17 (1<x<p-1, взаимно простое с p-1)**

**Шифротекст: 836,518 836,541 836,115 836,849 836,754**

**Расшифровка: 66 83 85 73 82**

**Тест2:**

Исходный текст: **BSUIR**

**p=431(430=2\*5\*43), g=7, x=429, k=41**

**Шифротекст: 68,39 68,147 68,109 68,337 68,166**

**Расшифровка: 66 83 85 73 82**

**Тест3:**

Исходный текст: **BSUIR**

**p=431(430=2\*5\*43), g=7, x=5, k=7**

**Шифротекст: 333, 172 333, 151 333, 326 333, 138 333, 279**

**Расшифровка: 66 83 85 73 82**

**Тест4:**

Исходный текст: **BSUIR**

**p=257(256=2\*2\*2\*2\*2\*2\*2\*2), g=3 , x=5, k=7**

**Шифротекст: 131, 197 131, 18  131, 133 131, 214 131, 89**

**Расшифровка: 66 83 85 73 82**

**Теорема 1:**

Первообразные корни по модулю *m* существуют, если *m* = 2, 4, *p*α или 2*p*α, где *p* – простое нечетное число, α>=1 целое.

**Теорема 2:**

Количество первообразных корней по модулю *m*, если они существуют, есть φ(φ(*m*)).

**Пример:**

Определить количество первообразных корней по модулю 10.

10 = 2·5=2*р*. Первообразные корни существуют. Найдем их количество:

φ(φ(10))=φ(4)=2.