### Задание 12. Асиметричен алгоритъм DSA

Име: Станислав Стоянов

Фак.номер: 471218066

Група: 76

ФПМИ, ИСН

Легенда: Зелено – верен отговор, Червено – грешен отговор

1. Избройте несекретните параметри в алгоритъма DSA:

**p, q и g, h и публичните ключове на всички потребители**

2. Посочете кои от следните твърдения са верни:

а) алгоритъмът DSA може да се използва както в системи за шифроване, така и в системи за автентификация;

**б) публичният ключ се изчислява на основата на предварително дефиниран секретен ключ;**

**в) алгоритъмът DSA принадлежи към алгоритмите, които се използват в системи за генериране на електронен подпис с приложение;**

г) в алгоритъма не се използват параметри, които отговарят на изискването да бъдат прости числа.

3. Криптографският ключ в DSA може да бъде с размер:

**а)  1024 бита**; б) 1092 бита; в) 4096 бита; г) 2048 бита.

4. ЕП, генериран с DSA, се отхвърля ако:

а) r < s;  б) r > s;  **в) r = 0;  s > 0**;  **г) r > 0;  s = 0**.

5. Параметърът *q* в DSA служи за:

**а) определяне на областта на допустимите стойности на SK ;**

б) изчисляване на един от криптографските ключове;

**в) определяне на областта на допустимите стойности на *k*;**

**г) проверка на ЕП**.