**Задание 10. Асиметрични криптографски алгоритми. Алгоритъм Diffie -Hellman.**

Име: Станислав Стоянов

Фак.номер: 471218066

Група: 76

ФПМИ, ИСН

Легенда: Зелено – верен отговор, Червено – грешен отговор

1. Посочете верния отговор относно същността на алгоритъма Diffie - Hellman:

а) той е симетричен алгоритъм, защото шифроването и дешифрирането се извършва с един и същи ключ;

**б) алгоритъмът е асиметричен, защото за всеки потребител се изчислява двойка ключове - публичен и секретен;**

в) алгоритъмът се отнася към самостоятелна група алгоритми, тъй като двойката ключове не се използва за шифроване и дешифриране.

2. Посочете кои са несекретните параметри в алгоритъма:

**α, q, публичните ключове - YA, YB**

3. Определете в кои от изброените по-долу варианти на стойностите за реализация на алгоритъма има грешка и посочете в какво се състои тя:

а) q = 47; a = 12;

**б) q = 56; a = 9; => защото q не е просто число**

**в) q = 31; a = 51; => защото a трябва да бъде в интервала [0, q-1], т.е [0, 30]**

**г) q = 148; a = 17. => защото q не е просто число**

4. Надеждността на алгоритъма Diffie - Hellman зависи от:

а) размера на параметъра “q”;

б) стойността на параметъра “a”;

в) запазването в секретност на xA и xB;

**г) верни са всички отговори.**

5. Параметърът *q* в алготитъма е:

а) случайно число, генерирано от източника на съобщение;

**б) просто число, изчислено от двойката участници в комуникациите;**

**в) число, за което е в сила изискването “(q-1)/2” да е просто число;**

г) няма верен отговор