**Задание 11. Асиметрични криптографски алгоритми. Алгоритъм RSA**

Име: Станислав Стоянов

Фак.номер: 471218066

Група: 76

ФПМИ, ИСН

Легенда: Зелено – верен отговор, Червено – грешен отговор

1. Криптографският ключ може да бъде с размер:

а)  512 бита; **б) 1024 бита**; **в) 4096 бита**; г) 128 бита.

2. Параметрите *p* и *q*.трябва да изпълняват следните изисквания:

а) стойностите им да са в интервала *[0*, *N-1];*

**б) стойността на *p*да е по-малка от тази на *q*; - не е задължително изискване**

**в) стойностите на *p*и *q* да не са равни;**

г) всички отговори са верни.

3. Посочете кои от следните твърдения са верни:

а) ако се компроментира секретният ключ се генерира нов, а публичният остава същият;

**б) алгоритъмът** [**RSA**](https://fpmi.bg/moodle/mod/resource/view.php?id=6180) **принадлежи към алгоритмите, които се използват в системи за генериране на електронен подпис с приложение;**

**в) единият от двойката ключове се изчислява от другия;**

**г) *p*и *q*са случайни цели прости числа.**

4. Надеждността на алгоритъма зависи от:

**а) размера на параметрите  *p*и *q*;**

б) запазване в тайна на стойностите на  *p*, *q* и *N*;

**в) спазване на изискванията и препоръките относно стойностите на секретните и несекретните параметри в алгоритъма.**

5. Ойлеровата функция на *N* :

**а) определя броя на простите множители на числото *N*;**

**б) е един от секретните параметри в алгоритъма;**

**в) служи за изчисляване на един от криптографските ключове.**

Общо точки: 7/9