### Задание 13. Автентификация със сертификати

Име: Станислав Стоянов

Фак.номер: 471218066

Група: 76

ФПМИ, ИСН

Легенда: Зелено – верен отговор, Червено – грешен отговор

1. Посочете кои от следните твърдения са верни:

**а) публичният ключ в** [**RSA**](https://fpmi.bg/moodle/mod/resource/view.php?id=6180) **се изчислява на основата на секретния ключ;**

**б) схемата за автентификация с групов електронен подпис (ЕП) може да се реализира с всеки асиметричен алгоритъм;**

в) алгоритъмът DSA принадлежи към алгоритмите, които се използват в системи за генериране на ЕП с възстановяване на съобщението;

г) всички отговори са верни.

 2 Информация за кои алгоритми се съдържа в сертификат за публичен ключ, издаден съгласно стандарта X.509 v. 3?

**RSA, хеш-алгоритмите**

***идентификатор на асиметричния алгоритъм****,* в който ще се използва сертифицираният ключ; ***идентификатор на асиметричния алгоритъм за ЕП,*** който се използва от ЦС за подписване на издадения сертификат.

3. Ако за i-тия потребител в една система на основата на [RSA](https://fpmi.bg/moodle/mod/resource/view.php?id=6180" \o "RSA) е дефинирана двойката ключове PKi /SKi, за кой от криптографските ключове трябва да се издаде сертификат?

**PKi**

4. Публичният ключ в DSA се използва за:

а) шифроване на съобщения;

**б) генериране на ЕП;**

**в) проверка на ЕП;**

**г) в системите за автентификация със сертификати.**

 5. Посочете кои са основните части в структурата на един сертификат:

**информационна; асиметричен алгоритъм и публичен ключ; електронен подпис на Центъра, издал сертификата**

6. LDAP-протоколът се използва за:

**а) достъп до сертификатите на потребителите;**

**б) достъп до CRL-списъците;**

**в) достъп до сертификатите на центровете за сертификация;**

г) достъп до хешираните пароли на потребителите.

7. Компонентите в една PKI система формират няколко нива. Техният брой е:

а) 3;      б) 6;      **в) 5**     г) няма верен отговор.

8. Секретният ключ в асиметричния алгоритъм служи за:

**а) дешифриране на криптирани съобщения;**

б) проверка на ЕП;

в) проверка за достоверност на източника;

**г) генериране на ЕП.**

 9. Кой от изброените алгоритми не може да бъде използван в системи за автентификация?

а) [RSA](https://fpmi.bg/moodle/mod/resource/view.php?id=6180);  б) DSA;  **в) Diffie-Hellman**;  **г) Rabin-Miller**.

10)  СRL-списъкът съдържа:

а) информация за издадените сертификати;

б) публичните ключове на регистрираните потребители;

**в) информация за анулираните сертификати;**

г) всички отговори са верни.