Испит из Заштите података (13E113ZP, 13S114ZP) – колоквијум 20.08.2020.

1. (**10п**) Алекса је направио поруку M и за њу је генерисао дигитални потпис ДП1 коришћењем *DSS* алгоритма. Алекса је затим послао (M, ДП1) Бранки. После неког времена за исту поруку M коју Алекса није мењао, генерисао је дигитални потпис ДП2 коришћењем истог алгоритма, те истог глобалног, јавног и приватног кључа. Поруку и потпис (M, ДП2) је послао Весни. Установио је да је нови потпис ДП2 различит од ДП1. Ако је Алекса сигуран да је софтвер за генерисање дигиталних потписа исправан и да његови кључеви потребни за дигитално потписивање нису компромитовани, из горе наведених чињеница исправно је да Алекса закључи следеће (одредити могући одговор или одговоре и детаљно образложити):

   а) да је неко променио поруку M у времену између два генерисања потписа

   б) да ће и Бранка и Весна моћи исправно да утврде да је управо Алекса потписао поруку M

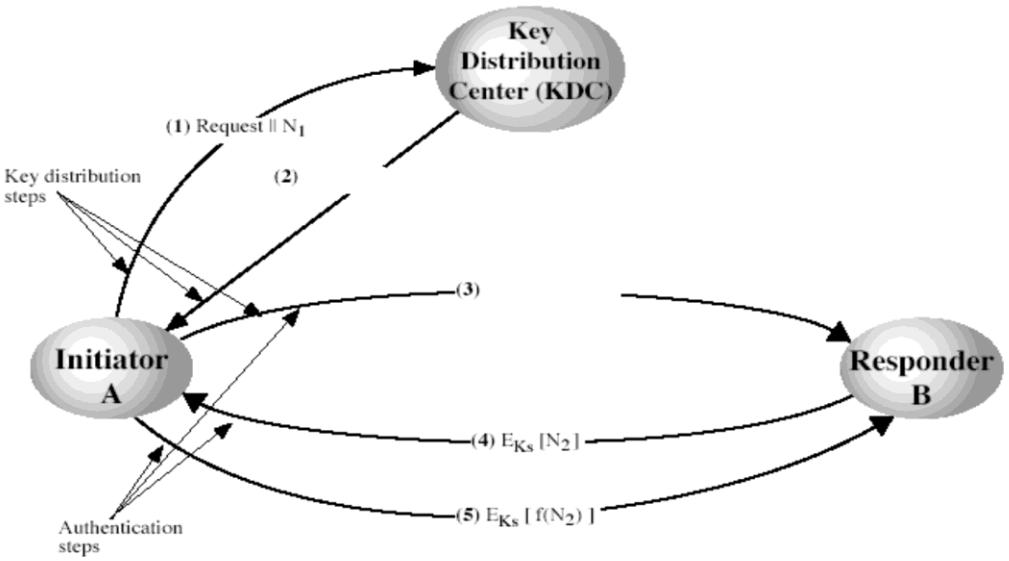
   в) да ће Бранка посумњати у аутентичност поруке

   г) да ће Весна посумњати у аутентичност поруке

2. (**10п**) Наведите какав би изабрани оригинални текст користили у нападу на *Vigenère* шифру да би најбрже одредили кључ. Објасните разлог за избор таквог оригиналног текста.

3. (**10п**) За шифровање неке поруке *Hill*-овим алгоритмом на располагању су следећи кључеви: BATA, MEDA, BRDA. За сваки од кључева навести да ли могу или не могу да се употребе и образложити зашто. Претпоставити да се користе слова енглеског алфабета и да се слово A кодира вредношћу 0.

4. (**15п**) Допунити сценарио централизоване дистрибуције кључева приказан на слици порукама које недостају и укратко објаснити кључне елементе тих порука. Скицирати и укратко описати улогу хијерархије KDC-ова у великим мрежама.



Напомена: *На колоквијуму нису дозвољена никаква помоћна средства, ни калкулатори ни литература. Колоквијум траје 70 минута.*

1. **(14/9п)** Биткоин тип блокчејна је формиран тако да сваки блок садржи 1024 трансакције. Тежина рударења одређена тако да хеш блока мора да има 20 водећих нула. У блокчејну се користи хеш функција *SHA-256*. Изглед једног блока је дат на слици. Одредити:

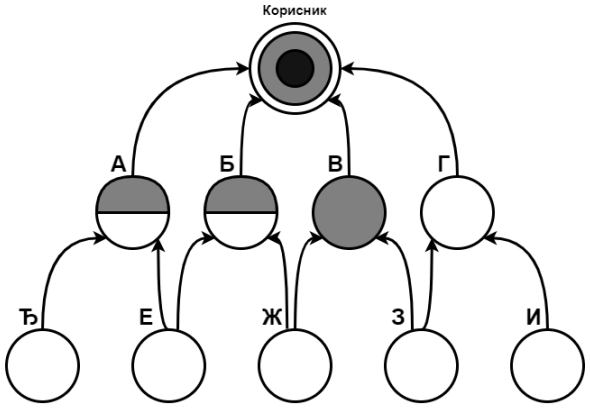
   а) (9п) рачунску комплексност исказану као укупан број израчунавања хеш функција потребних за формирање и потврду једног блока,

   б) (5п) рачунску комплексност напада на блокчејн у којем би нападач желео да промени садржај једне своје раније извршене трансакције која је регистрована у већ потврђеном блоку, а да та промена прође недетектована (на пример, у тренутку посматрања је потврђено 100 блокова, а трансакција која се мења је у блоку бр. 80).

   Одговоре образложити.

2. **(14/9п)** Објасните како се у комуникацији између *Kerberos realm*-ова обезбеђује приступ клијента из једног *realm*-а сервису из другог *realm*-а. Наведите сваки корак у аутентикацији и ауторизацији. Ако је у току рада потребно прићи сервису из неког трећег *realm*-а, да ли је потребно поново се улоговати?

3. **(11/6п)** На слици је представљена шема *PGP* прстена јавних кључева са коришћењем поверења. Чворови стабла представљају улазе у прстен, док стрелице означавају потписе (стрелица од чвора Е ка чвору Б означава да је јавни кључ корисника Е потписан јавним кључем корисника Б). Корисник В је потпуно поверљив, док су корисници А и Б делимично поверљиви са тежинском сумом 1/2. За све улазе одредити вредност поља легитимитета кључа. За сваки специфичан случај образложити поступак.



4. **(11/6п)** Скицирати модел хијерархије улога и модел ограничења који припадају концептуалним моделима којима се контролише приступ помоћу улога. Укратко објаснити основхе елементе ова два модела.

Напомена: *На испиту нису дозвољена никаква помоћна средства, ни калкулатори ни литература. Испит траје 70 минута.*