1, 2, 3, кодирај ! - Активност циклуса 4 - Пројект « Криптографија » - Час 5: Како комуницирати без размене кључа

Доминантна дисциплина	Математика
Резиме	Ученици праве модел размена између 2 саговорника помоћу катанца и кључа. Упознају слабе тачке више метода шифрирања: размена шифри; сазнају да употреба више шифри омогућује решење проблема, познато као принцип асиметричног шифрирања.
Појмови	« Информације » • Цезарево и шифрирање моно-алфабетском супституцијом је познато још и под називом "симетрично" шифрирање јер користе исти кључ за шифрирање и дешифрирање • Размена кључа између саговорника је слаба тачка сваког метода симетричног шифрирања (користи се исти кључ за шифрирање и дешифрирање)
Матријал	За сваку групу: • 1 коверат • 2 катанца са кључевима. Ако је могуће, користите катнце у различитим бојама, и с одговрајућим кључевима.

Полазна ситуација

Ученици се подсећају оног што су научили из криптографије:

- Цезарево шифрирње се врло лако открива, јер је мали број могућих кључева (могуће их је све врло брзо тестирати) а применљива је анализа фреквенција;
- Шифрирање моно-алфабетском супституцијом поседује велики број кључева, али се лако откривају (за довољно дуге поруке) помоћу анализе фреквенције;
- Постоје методе шифрирања које је тешко открити анализом фреквенције (оне код којих се исто слово може шифрирати с више рзличитих слова).

Наставник наглашава да све методе имају слабу тачку, која се односи на трансмисију кључа. Јер, да би прималац могао да дешифрује поруку потребан му је кључ шифрирања. Пита ученике како је могуће да се договре саговорници у вези кључа, па одељење испитује слабе тачке метода предложених од стране ученика:

- Бележење кључа на папиру који се шаље саговорнику може бити лако откривено. (У свакој земљи постоје службе задужене да прате комуникације између одговарајућих институција или појединаца).
- Слање кључа непосредном разменом између саговорника захтева да се он запамти. Данас се комуникација остварује веома брзо између удаљених саговорника тако да је непосредна трансмисија кључа немогућа. На пример, за функционисање црвеног телефона је неопходно да се пре сваке нове комуникације да нови кључ кокји се размењује дипломатским путем (то захтева доста времена и изузетно обезбеђење). Битно је да кључ буде врло дуг (приближно као и дужина шифриране поруке) и да је за сваку нову поруку нови кључ. Овакво шифрирање је тешко открити али је оно веома скупо, тако да само важне комуникације оправдавају овакав трошак.
- Кључ је потребно често мењати. Предност: онај ко је открио кључ може га користити само за ту али не и за следећу поруку. Недостаци: кључеве није потребно бележити и слати… па се суочавамо с већ поменутм потешкоћама.
- …

Истраживање (по групама)

Наставник предлаже ученицима да направе модел комуникације између 2 саговорника помоћу коверте (у коју се ставља порука коју шаљемо) и катанца (који симболизује методе шифрирања). Можемо користити више метода шифрирања (тј. кристимо више катанаца). Свака група добија коверт и 2 катанца, а сваки катанас има свој кључ.

Ситуација је следећа: Алиса хоће да пошаље поруку Бобу, а да при том Ева није у могућности да до ове поруке дође.

Ученици испитују операције које је потребно реализовати (и којим редом) да би Алиса и Боб коректно дешифровали долазну поруку.

Научна напомена:
Аиса, Боб и Ева су ликови уведени од стране Ron Rivest, 1978 године, у раду који описује систем асиметричне криптографије- RSA (детаљнији опис је дат у Радном листу-B09). Од тада се ова 3 имена обично користе при илустрцији криптогрфских метода.

Педагошке напомене

- Мала је вероватноћа да ученици могу сами да нађу алгоритам. Насумични покушаји ће им помоћи да размисле о решењу пре него што наставник почне да их усмерава.
- Један од начина вођења ученика би могао бити по угледу на игру « вук/коза/купус »: Чамџија мора да пребаци с обале на обалу реке вука, козу и купус, међутим ограничен је постојањем само једног места у чамцу. Осим тог, ако су вук и коза сами на истој обали, вук ће појести козу. Иста ситауција је с козом и купусом. Шта урадити? У питњу је проблем сличан ограничењима при путовању. Овде се несме дозволити да вук и коза остану сами, или коза и купус. У нашем случају не смемо да пошаљемо кофер а да га не закључамо, тј. ставимо катнац.

Наставник, после десетак минута утрошених на насумичне покушаје, објашњава ученицима да је проблем размене кључа у томе што 2 саговорника користе исти кључ.
Предлаже им да размотре ситуацију у којој сваки саговорник поседује свој сопствени катанац и кључ. Ученици насумично покушавају поново да упознају овако дефинисан проблем:

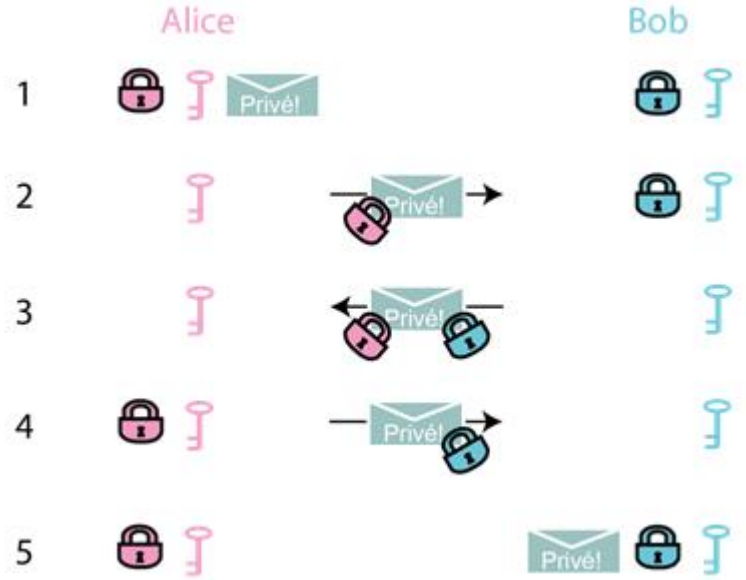
- Алиса поседује катанац и кључ (који отвара само њен катанац)
- Исто је и са Бобом
- Морају да пошаљу коверту која је увек закључана катанцем, који може да се отвори (од стране Боба).

Заједничко представљање

Наставник организује заједничко представљање током ког ће неколико група представити свој метод о коме ће се развити дискусија.

Метод који функционише (или пак изгледа да функционише, како ћемо видети на следећем часу) је:

- Етапа 1: полазна ситуација: Алиса је управо послала поруку Бобу. Свако поседује свој катнац и кључ (свој алгоритам шифрирања)
- Етапа 2: Алиса ставља свој катанац и шаље шифрирану поруку Бобу.
- Етапа 3: Боб није у могућности да откључа Алисин катанац (нема Алисин кључ): ставља свој катнац и враћа поруку (коју су истовремено шифрирали Алиса и Боб) Алиси
- Етапа 4: Алиса узима свој катанац (дешифрује поруку помоћу кључа) и поново је шаље Бобу
- Етапа 5: Боб сад може да откључа катнац (јер је његов и за њега има кључ!) прочита садржај поруке у коверти.



Наставник нагалашава да су Алиса и Боб успели да тајно комуницирају … и то без икаквог слања кључа!

Вежба

Свака група понавља овај поступак више пута док сви ученици не схвата о чему је реч.

Научне напомене

- Овај метод има слабу тачку о којој ће бити више речи на следећем часу.
- Катанци представљају математичке функције шифрирања (а кључеви омогућују дешифрирање). Овај метод комуникације без размене кључева претпоставља да су употребљене комутативне методе шифрирања (дакле математичке функције).
