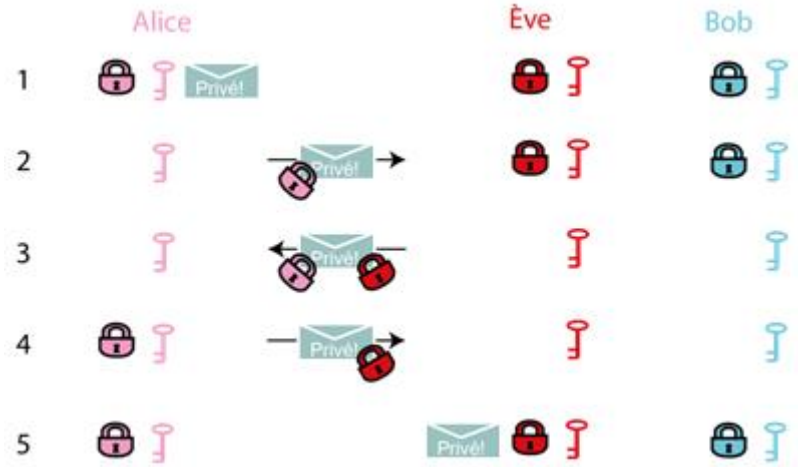
1, 2, 3, кодирај ! - Активност циклуса 4 - Пројект « Криптографија » - Час 6: Јавна и приватна шифра

Доминантна дисциплина	Математика
Резиме	Ученици усавршавају свој алгоритам асиметричног шифрирања користећи јавне шифре (које се користе за шифрирање) и приватне шифре (које се користе за дешифрирање).
Појмови	« Информације » • Diffie et Helmann су, 1976, показали да се проблем размене кључева може решити употребом 2 кључа: један кључ је јавни (користи се за шифрирање поруке) а један је приватни (којим се порука дешифрује), у питању је асиметрично шифрирање. • Употреба асиметричног шифрирања гарантује поверљивост комуникације, и осигурава идентитет кореспондената. • Бројна оруђа, данас, омогућују сигурну комуникацију специфичним предузећима.
Матријал	За сваку групу: • 1 коверат • 3 катанца са кључевима. Ако је могуће, користите катнце у различитим бојама, и с одговрајућим кључевима. За сваког ученика: • Радни лист-B09

Полазна ситуација

Наставник тражи од 2 ученика да демонстрирају, пред одељењем, метод размене кључева који је реализован на претходном часу.

Пита ученике да ли могу да идентификују слабу тачку те размене. Ако то ученици нису у могућности да ураде усмерава их питајући шта се дешава ако Ева (која покушава да открије тајну кореспонденцију између Алисе и Боба) прочита поруку (етапа 2, у претходном приказу).
Ако поруку не прими Боб, а прими је Ева која сад може да се предстви као Боб без његовог знања (он чак и не зна да је Алиса покушала са њим да комуницира). Ева преузима Бобов идентитет, ставља свој катанац и шаље га Алиси. Алиса мисли да је то Бобов одговор и повлачи свој катанац. У следећој етапи Ева може да прими поруку и да је дешифрује. Ово можемо представити на следећи начин:



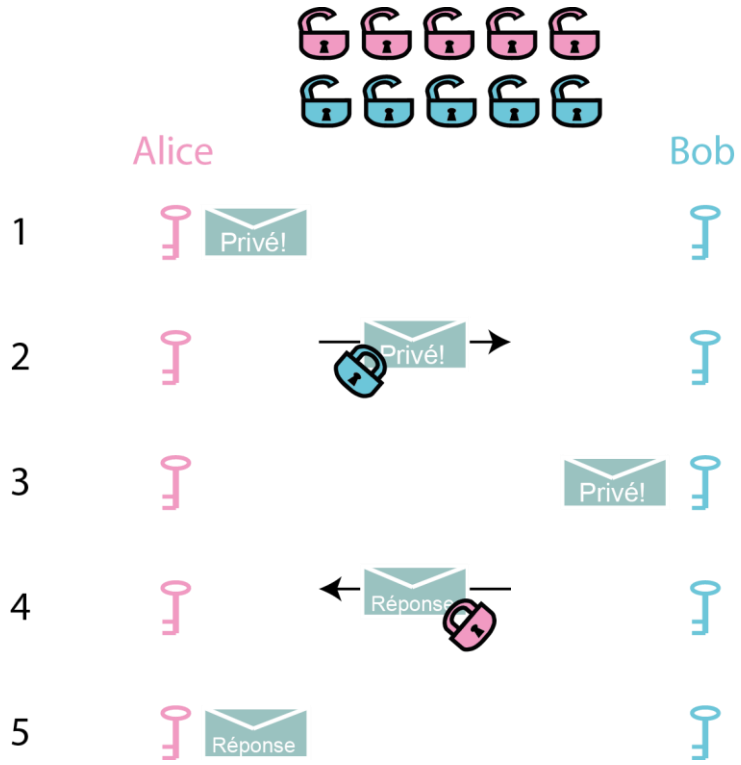
Употреба дуплог приватног кључа омогућује тајну комуникацију без потребе размене кључева, али зато постоји могућност да то открије неко трећи. Ниједан саговорник није у стању да верификује идентитет другог. Подсетимо да ма који корисник не « види » катанац (ни његову боју), него само ланац шифрираних карактера који изгледају као насумичан текст.

Увођење јавног кључа (заједнички)

Нставник објашњава да је овај проблем решен увођењем 2 кључа за сваког учесника у размени порука, један је јавни кључ (познат свима) а други је приватни кључ. Важно је нагалсити да ова дв кључа не раде исту ствар:

- Јавни кључ омогућује само шифрирање поруке;
- Приватни кључ омогућује само њено дешифрирање.

Овај метод користи асиметричне функције (продубљење у наставку). Настављајући аналогију катанца и кључева долазимо до закључка да је јавни кључ сличан отовреном катанцу (закључан катанац подразумева шифрирану поруку), док приватни кључ предствља кључ за катнац. Алиса и Боб су тако свима ставили на располагање своје катанце али не и своје кључеве.



Алиса, у овом случају, једноставно шаље своју поруку користећи Бобов катанац (њен кључ је јаван). Једино Боб поседују кључ који пружа могућност дешифровања ове поруке; он то чини и ако жели одговара Алиси користећи њен катанац.
Ева може да пресретне било коју поруку, али пошто нема кључеве Алисе или Боба, она неће моћи да дешифрује оригиналну поруку нити да одговара на њу.

Вежба

Ученици, као и на претходном часу, вежбају неколико минута асиметрично шифрирање.

Научне напомене

- Проблем са решењем без јавног кључа (*према* . претходном часу) се огледа у чињеници да Алиса и Боб не деле никакву информацију, никакву идентификацију, а да одједном све што Боб може да уради, ради и Ева која се представља као он, а Алиса није у могућности да сазна да ли

комуницира са стварним или лажним Бобом. Код система с јавним/приватним кључем и Алиса и Боб деле једну информацију (јавни кључ других). Алиса, дакле, зна да ако стави Бобов катанац на поруку, онда ће само он моћи да је дешифрује.

- Асиметрична криптографија омогућује не само шифрирање (дешифрирање) порука, него и самоидентификацију. Алиса може да шифрира свој потпис с приватним кључем и свако може да верификује (помоћу своје јавне шифре) да је потпис Алисин.

Петрага литературе (индивидуално)

Наставник расподељује Радни лист-B09 сваком ученику. Прво читају појединачно а затим дискуктују заједнички. Дискусија омогућује успостављање везе између расположивих могућности прорачуна и достигнутог нивоа сигурности (што је већа достигнута могућност прорачуна, захтева се и већа величина кључева с циљем да се оствари прихватљива сигурност). На крају се упознају с актуелним утицајем криптографије што је били разматрано у Радном листу-B08. Ове информације их припремају за дебату планирану за следећи час.
