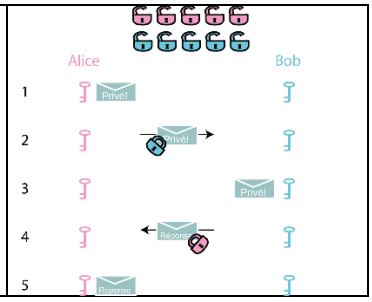
Радни лист – B09
Историја криптографије и јавних кључева

Развој информатике је, у 1960-тим годинама, отворио нове могућности. Криптографија, до тада резервисана само за владине агенције, постаје доступна и другим заинтересованим. Јер двоје људи, који жели да комуницира тајно, мора да се договори о кључ који ће им омогућити да шифрирају и дешифрирају поруке. Размена тих кључева је одувек била проблем криптографије а посебно сад када се она на неки начин демократизовала.

Whitfield Diffie и Martin Hellman су овај проблем решили 1976, у раду под насловом Нови успешни правци криптографије. Ова два математичара су показала да је могуће тајно комуницирати користећи асиметрично шифрирање. У овом типу шифрирања се користе два кључа, један јавни, и други приватни. Јавни кључ омогућује шифрирање поруке коју само приватни кључ може да дешифрује.



Ron Rivest, Adi Shamir и Leonard Adleman су, две године касније, ову идеју допунили креацијом алгоритма RSA (названом по њиховим именима). Алгоритам RSA користи, као поједностављење, врло велики број, N, који можемо да разложимо на производ 2 проста броја p и q, N=pxq. N је јавни кључ, док су p и q констиутенти приватног кључа. N омогућује шифрирање поруке, али је за операцију дешифрирања неопходно познавати p и q. Сигурност RSA се базира на чињеници да је врло тешко израчунати делитеље неког врло великог броја (познато још и као « факторизација » броја, дељење најмањим простим бројем). Ако је број веома велик онда су и најбољим компјутерима потребне године да га факторизују. RSA алгоритам шифрирања се управо из тих разлога највише користи.

RSA је врло сигурана шифра али захтева изузетне прорачуне. Paul Zimmermann је решио овај проблем 1991 креацијом софтвера познатог под именом PGP (pretty good privacy) је нека врста компромиса између « класичног » шифрирања приватним кључем и RSA шифрирања. PGP је омогућио демократизацију криптографије тиме што је она постала доступна и PC компјутерима које користи већина људи. Америчка влада је управо због тога и легализовала криптографију. Неке владе су, настојећи да ограниче употребу криптографије, наставиле да прате комуникације. Уопштени захтеви се своде на:

• Било на ограничење величине коришћених кључева: кључ « средње » величине се тешко открива класичним компјутером, али не и суперкомпјутером. Поверљивост је тако осигурана за мале кориснике, али не и за владине агенције нити за предузећа која поседују суперкомпјутере.

• Било на депоновање приватних кључева у « сеф » који је заштићен од стране организације « од поверења » (на пример, нека владина агенција). Комуникације су на тај начин тајне за све изузев за оне који имају приступ сефу.

Криптографију, дуго времена резервисану за армије и дипломате, данас користе бројни сервиси: банке (банкарске картице, сигурносне транскације на интернету), електронска трговина, електронске поруке (SIM картице, e-mail…), медицинске услуге (здравствене књижице…), електронско гласање, итд.