Садржај:

Увод у криптографију

Комуникација се јавила врло рано у историји људских бића, развијала се, и развија се и данас непревазиђеном брзином. Међутим, увек је постојао проблем приватности у комуникацији. Неке поруке су важне са аспекта људске интиме, друге пак са аспекта економије, сигурности или науке, и потребно је обезбедити да поруке буду достављене само онима којима су и послате, у неизмењеном стању и са гаранцијом идентитета пошиљаоца.

Данас, у информатичкој ери, Интернет, и поред фантастичне предности коју нам пружа као средство у свакодневној комуникацији, постоје одређени ризици у домену заштите података, јер постоји реална могућност да неко прати комуникацију између два корисника, пресреће поруке и чита их, евентуално мења њихов садржај, а да ни пошиљалац, ни примаоц не примете ништа. Такође, неко може да се лажно представи у комуникацији (на пример лажирајући да је поруке послао пословни партнер) да би у размени докумената прибавио поверљиве податке.

Да би се смањили ризици савременог пословања на Интернету било је потребно пронаћи механизам који ће обезбедити да прималац електронске поруке зна ко је послао поруку и да ли је садржај поруке у изворном облику, односно да није промењен након што га је пошиљалац послао. С друге стране пошиљалац мора бити сигуран у идентитет примаоца пре слања поруке и мора имати доказ да је порука примљена, како прималац касније не би могао да порекне пријем поруке.

Механизам заштите мора обезбедити заштиту тајности информација (спречавање откривања њиховог садржаја), интегритет информација (спречавање неовлашћене измене информација), и аутентичност информација (дефинисање и провера идентитета пошиљаоца).

То је урађено системом шифровања података криптографијом чији су основни елементи:
Шифровање – поступак трансформације читљивог текста у облик нечитљив за онога коме није намењен
Дешифровање – поступак враћања шифрованог текста у читљив облик

Тешко би било остварити заштиту приватности и аутентификацију без две кључне предности модерне криптографије: енкрипције и дигиталног потписа. Ова два једноставна концепта модерном човеку олакшавају живот, омогућавајући му обављање сигурних банковних трансакције са даљине, очување приватности комуникације, било путем Интернета или мобилне телефоније, заштиту приступа установама високе сигурности итд.
Криптографија има две области: симетричну и асиметричну криптографију, тј криптографију са тајним и јавним кључем.