Аутор: Данијел Јовановић

Асиметрично шифровање и дешифровање

Творци асиметричне криптографије су Whitefield Diffie и Martin Hellman који су 1976. године описали идеју криптографије која се темељи на два кључа, приватном (или често званим тајним) и јавном кључу.

У литератури појам асиметричног криптовања се поистовећује са термином **asymmetric-key** или **public-key** криптовањем.

Разлика између симетричних и асиметричних алгоритама је у томе што симетрични алгоритми користе исти кључ за криптовање и декриптовање док асиметрични алгоритми користе **различите кључеве** за криптовање односно декриптовање.

Информације које су криптоване јавним кључем могу се декриптовати само тајним кључем односно то може само особа која је власник тајног асиметричног кључа.

Оба кључа морају бити повезана помоћу јединствене једносмерне функције. Односно не сме се израчунати тајни кључ из јавног кључа или се барем не сме израчунати у разумном времену.

Алгоритми асиметричних криптосистема заснивају се на одређеним својствима бројева.

При криптовању се изворни текст третира као низ природних бројева који се одабраном функцијом криптовања и кључем прерачунавају у криптовани низ текста.

Функција криптовања мора бити таква да се из криптованог текста не може одредити изворни текст, чак ако је познат и кључ за криптовање $\mathbf{K_e}$.

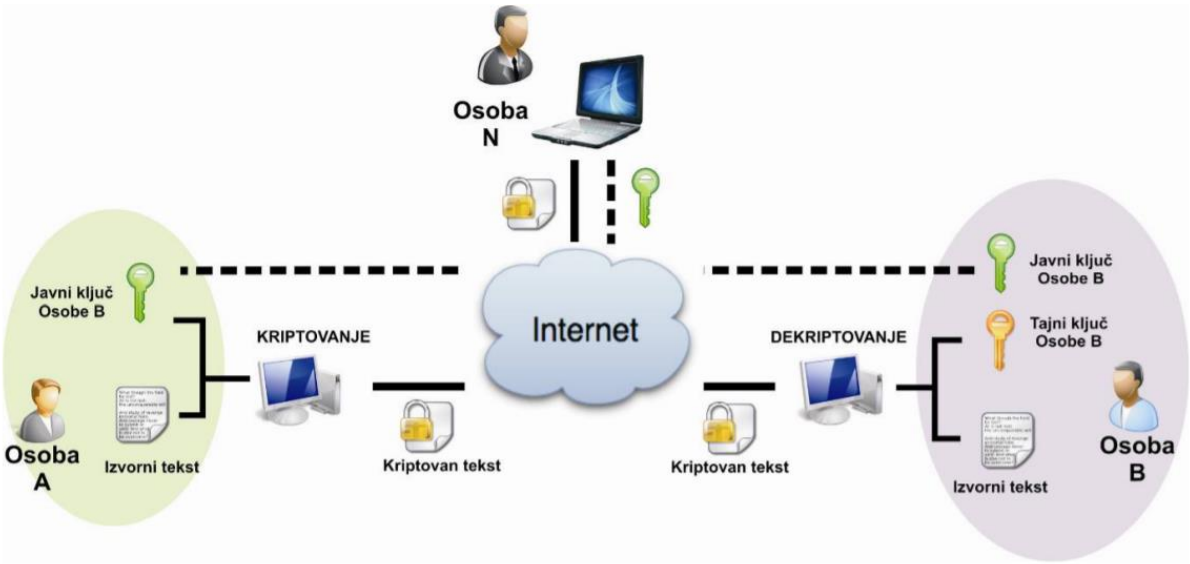
Међутим, уколико се зна кључ декриптовања $\mathbf{K_d}$ могуће је лако рачунање изворног текста.

Асиметрично криптовање представља јако сложен вид заштите података.

За његову реализацију сваки од саговорника мора поседовати два кључа (јавни и тајни).

Иако су различити, кључеви су међусобно повезани одређеним трансформацијама.

На Слици 1 је приказан пример асиметричног криптовања.



Слика 1: Асиметрично (де)криптовање

Ради једноставније анализе рада користићемо симболе A, B и N.

A је особа која жели да пошаље изворни текст, B представља особу која би требала да прими послати текст, а N је особа која неовлашћено жели да дође до сигурних података које особа A шаље особи B.

Сценарио асиметричног криптовања би изгледао овако:

1. Особа A кодира поруку ради слања особи B употребом јавног кључа особе B који је свима доступан (чак и особи N).

2. Особа A је јавни кључ је могла добити путем email-a, преузети са веб сајта и сл. Међутим било ко или особа N и поред тога што познаје јавни кључ не може открити садржај поруке.

Поруку може дешифровати само особа B коришћењем свог тајног кључа.

На овај начин порука је заштићена од трећег лица.

Основни недостатак овог начина криптовања је његова спорост и неприкладност за криптовање великих количина података.

Такође, остаје отворено питање аутентичности поруке, односно како да особа B буде сигурна да је поруку коју је примила уистину послала особа A.

Најчешће се користе следећи асиметрични алгоритми: RSA (енг. Rivest-Shamir-Adleman), Diffie-Hellman, ElGamal, Eliptic, Curves, Rabin, ...