ШИФРИРАЊЕ И ДЕШИФРИРАЊЕ

Шифрирање је трансформација оригиналне поруке помоћу одговарајућег поступка у нечитљиву форму за све, сем за корисника снабдевеног механизмом за дешифрирање. У поступку шифрирања, у механизам шифрирања улази оригинална порука и специфичан садржај који се зове кључ.

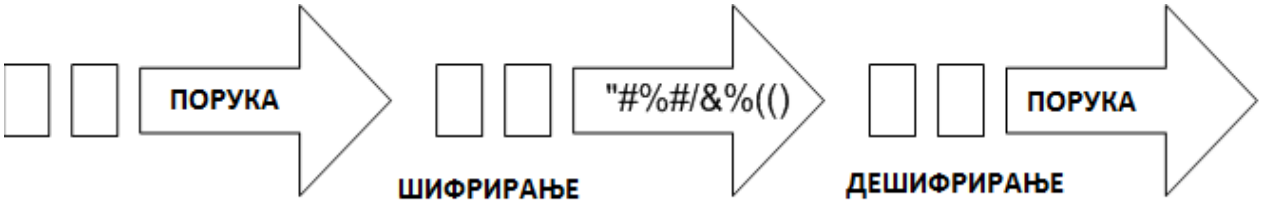
Дешифрирање је инверзна трансформација којом се од шифроване поруке уз помоћ кључа и механизма за шифровање добија поново оригинални или изворни облик поруке.

Две основне врсте шифрирања и дешифрирања су:

1. Симетрично (де)шифрирање
2. Асиметрично (де)шифрирање

СИМЕТРИЧНО ШИФРИРАЊЕ И ДЕШИФРИРАЊЕ

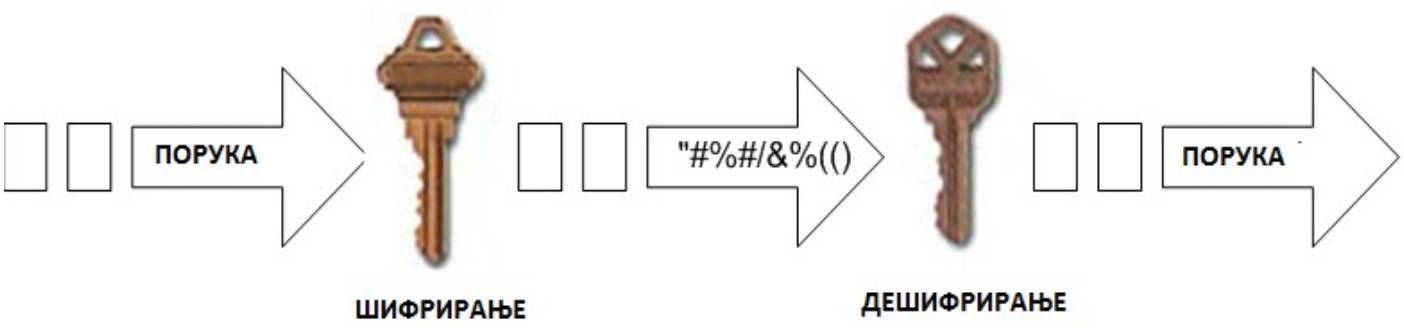
Симетрично - шифрирање и дешифрирање врши се истим кључем Ако желимо да сачувамо тајност поруке, кључ наравно мора бити познат само пошиљаоцу и примаоцу, зато се и зове тајни кључ. Проблем који се у овом случају јавља је дистрибуција тајног кључа удаљеном учеснику комуницирања.



СИМЕТРИЧНО ШИФРИРАЊЕ И ДЕШИФРИРАЊЕ

АСИМЕТРИЧНО ШИФРИРАЊЕ И ДЕШИФРИРАЊЕ

Асиметрично - шифрирање и дешифрирање врши се помоћу два кључа. Пошиљалац поруку шифрира једним кључем, а она се дешифрира другим. Један од кључева, познат само власнику, зове се тајни кључ, а други који је доступан свима са којима власник комуницира, зове се јавни кључ. Мада постоји математичка веза између ова два кључа, у коначном времену, са постојећом комерцијалном рачунарском опремом, практично је немогуће реконструисати тајни кључ на основу размењених порука и познатог јавног кључа.



АСИМЕТРИЧНО ШИФРИРАЊЕ И ДЕШИФРИРАЊЕ

ШИФРИРАЊЕ ПОРУКА ЈАВНИМ И ТАЈНИМ КЉУЧЕМ

Сигурносна инфраструктура заснована на употреби јавних кључева најчешћа је технологија која се примењује за заштиту при преносу података, на пример у електронској трговини. Техника позната као шифрирање јавним кључем у ствари се заснива на употреби пара кључева: тајном - приватном, и јавном кључу власника доступном свима. Веома је важно да тајни кључ зна само власник, а јавни кључ, како му само име каже, не представља никакву тајну и може се преносити на различите, чак и небезбедне начине.

Техника коришћења јавног и приватног кључа одвија се у следећим корацима:

Сваки корисник, као власник система шифрирања, на свом рачунару генерише пар кључева - јавни и тајни; тајни чува само за себе. Корисници размењују своје јавне кључеве када желе да међусобно комуницирају. Ако неко неауторизовано дође до ових јавних кључева, то не представља никакву опасност јер они служе само за шифрирање порука, а могу их прочитати само власници пириватних кључева.

Порука која се шаље одговарајућем кориснику прво се шифрира - "закључа" његовим јавним кључем. Ради провере идентитета пошиљаоца и обезбеђења веродостојности поруке, често се користи и додатни механизам дигиталног потписа, о чему ће бити више речи у следећем одељку.

"Закључану" поруку прималац дешифрира употребом свог тајног кључа. "Откључавањем", порука се враћа у изворни облик. Уколико је порука дигитално потписана, откључавањем се проверава идентитет пошиљаоца и веродостојност поруке.