Криптографија – основе за почетнике

Никола Лазаревић
57/2025

14. februar 2026.

Sadržaj

1 Увод

Криптографија представља **науку о заштити информација** од неовлашћеног приступа. У савременом друштву велики број података се размењује путем интернета, па је потребно обезбедити њихову поверљивост и сигурност.

2 Основни појмови

2.1 Дефиниција криптографије

Дефиниција 1. *Криптографија је дисциплина која проучава методе трансформације података у облик који је нечитљив свима осим овлашћеним учесницима комуникације.*

2.2 Модел комуникације

Најједноставнији модел подразумева пошиљаоца, поруку и примаоца. Додавањем процеса шифровања и дешифровања обезбеђује се сигурност комуникације. Овакви системи се данас користе у банкарству, електронској пошти и заштити лозинки.

3 Типови криптографије

3.1 Симетрична

Користи се један тајни кључ за оба процеса. Ова метода је **веома брза** и погодна за велике количине података.

3.2 Асиметрична

Користе се јавни и приватни кључ. Иако је спорија, омогућава већу флексибилност у комуникацији.

3.3 Карактеристике

- заштита поверљивости
- очување интегритета
- аутентичност корисника

3.4 Особине

1. генерисање кључа
2. шифровање поруке
3. дешифровање поруке

4 Математичка основа

Криптографија се у великој мери ослања на математику. На пример, једноставан приказ функције шифровања може бити:

$$C = E(K, P)$$

где је P оригинална порука, K кључ, а C шифровани текст.

Лема 1. *Уколико је кључ тајан, нападач без његовог познавања не може у разумном времену доћи до оригиналне поруке.*

Теорема 1. *Безбедност криптографског система директно зависи од јачине кључа и алгоритма који се користи.*

5 Примена алгоритама

Алгоритам	Тип	Примена
AES	симетрични	заштита датотека
RSA	асиметрични	дигитални потпис
SHA	хеш	лозинке

Tabela 1: Примери криптографских алгоритама

6 Закључак

Криптографија има кључну улогу у савременом информационом друштву. Комбинацијом различитих метода омогућава се висок ниво сигурности података и поверење у дигиталну комуникацију.