Криптографија

Вања Никитовић

Јун 2026.

Sažetak

Криптографија представља једну од кључних области информационе безбедности. Њен задатак је да обезбеди сигуран пренос и складиштење података, тако да информације буду доступне само овлашћеним корисницима. У овом кратком академском тексту приказани су основни појмови, подела алгоритама, математичка основа, као и значај криптографије у савременим комуникационим системима.

Sadržaj

1 Увод

Криптографија се бави методама заштите података од неовлашћеног приступа, измене и злоупотребе. У савременом дигиталном окружењу она има важну улогу у областима као што су електронско пословање, интернет комуникација, заштита лозинки и безбедна размена кључева.

Основни циљеви криптографије су:

Тајност спречава неовлашћене особе да приступе садржају поруке и прочитају је.

Интегритет гарантује да порука није измењена, избрисана или модификована током преноса.

Аутентичност потврђује стварни идентитет пошиљаоца, чиме се спречава лажно представљање.

2 Основни појмови

2.1 Шта је криптографија?

Криптографија је наука о методама шифровања и дешифровања података. Њен циљ је да се порука претвори у облик који је нечитљив неовлашћеним лицима, а разумљив само ономе ко поседује одговарајући кључ.

Дефиниција 2.1. Криптографски систем је уређен скуп алгоритама и правила који омогућавају шифровање и дешифровање порука употребом једног или више кључева.

2.2 Подела криптографских алгоритама

Најчешћа подела је на:

1. симетричне алгоритме,
2. асиметричне алгоритме.

Симетрични алгоритми користе исти кључ за шифровање и дешифровање.
Асиметрични алгоритми користе пар кључева: јавни и приватни.

3 Математичка основа

Један од најпознатијих формалних записа у науци и техници је:

$$E = mc^2$$

У криптографији се често користе и функције облика:

$$C = E_K(P)$$

где је:

P отворени текст,

C шифрован текст,

K кључ,

E_K функција шифровања.

Такође, за дешифровање важи:

$$P = D_K(C)$$

Лема 3.1. *Ако је алгоритам шифровања коректно дефинисан, онда за сваки отворени текст P и кључ K важи:*

$$D_K(E_K(P)) = P$$

Dokaz. По дефиницији коректног криптосистема, поступак дешифровања представља инверзну операцију поступка шифровања за исти кључ K. Зато се применом дешифровања на шифровану поруку поново добија почетни текст P. □

Теорема 3.2. *Сваки практично употребљив криптографски систем мора да обезбеди бар један од следећих захтева: тајност, аутентичност или интегритет, а у савременим системима пожељно је обезбедити сва три захтева истовремено.*

Dokaz. Уколико систем не обезбеђује ниједан од наведених захтева, онда подаци могу бити прочитани, измењени или лажно представљени без могућности откривања напада. Такав систем се не може сматрати безбедним у реалном окружењу. □

4 Примери и примена

4.1 Табеларни приказ алгоритама

Tabela 1: Поређење основних криптографских алгоритама

Алгоритам	**Тип**	**Основна намена**
AES	Симетрични	Брзо шифровање података
RSA	Асиметрични	Размена кључева, дигитални потпис
DSA	Асиметрични	Дигитални потпис
SHA-256	Хеш функција	Провера интегритета података

4.2 Практични примери и сигурносни механизми

Slika 1: Симболички приказ заштите

Савремена имплементација криптографских заштитних механизама заснива се на строгим математичким протоколима. Да би шифровање у пракси било успешно, цео процес се мора одвијати кроз тачно дефинисане кораке који осигуравају безбедност података на мрежи.

Кораци у процесу асиметричног шифровања:

1. Корисник А генерише пар кључева (јавни и приватни).
2. Корисник А јавно дели свој јавни кључ са осталим учесницима.
3. Корисник Б шифрује поруку помоћу јавног кључа корисника А.
4. Корисник А дешифрује примљену поруку својим тајним приватним кључем.

Додатни захтеви за сигурне канале комуникације:

- Употреба заштићених дигиталних сертификата.
- Редовна замена криптографских кључева.
- Имплементација двофакторске аутентификације корисника.

5 Закључак

Криптографија је темељ безбедне дигиталне комуникације и њена примена је видљива у свакодневном животу, на пример, сваки пут када приступамо веб сајту путем заштићеног HTTPS протокола. Кроз правилну примену шифровања, дигиталних потписа и хеш функција могуће је значајно повећати ниво сигурности у савременим информационим системима.
С друге стране, важно је нагласити да јаки алгоритми морају бити ефикасни и отпорни на познате нападе. У пракси, **лош избор параметара** или **небезбедно чување кључева** може потпуно угрозити и изнутра срушити и иначе математички савршен криптографски систем.