АКАДЕМИЈА ТЕХНИЧКО-УМЕТНИЧКИХ СТРУКОТВНИХ СТУДИЈА БЕОГРАД

ОДСЕК ВИСОКА ШКОЛА ЕЛЕКТРОТЕХНИКЕ И РАЧУНАРСТВА

**Миленковић Ђорђе**

**ЈЕДНА ИМПЛЕМЕНТАЦИЈА СИСТЕМА ЗА ЧУВАЊЕ ЛОЗИНКИ НА ПАМЕТНИМ КАРТИЦАМА**

**- мастер рад -**



Београд, ххх 2021.

Кандидат: **Миленковић Ђорђе**

Број индекса: **РИН-65/17**

Студијски програм: **Рачунарско инжењерство**

Тема: **Једна имплементација система за чување лозинки на паметним картицама**

Основни задаци:

**1. Преглед у област истраживанја**

**2. Пројектовање система за чување лозинки**

**3. Имплементација система за чување лозинки**

Београд, ххх 2021. године. Ментор:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Др Немања Мачек, проф. ВИШЕР

**РЕЗИМЕ:**

ХХХХХХХХХХХХХХХххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххх

**Кључне речи:** ХХХХХХххххххххххххххххххх

**ABSTRACT:**

Ххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххх

**Key words:** Хххххххххххххххххххххх

САДРЖАЈ

# Увод

Кроз целу историју човечанства, постојала је потреба за сигурном разменом информација. Проблемом сигурне комуникације бавили су се већ Египћани и Индијци пре више од 3000 година и од тада до данас основна идеја се није променила – пренети неку поруку са једног места на друго што је сигурније могуће, тј. направити алгоритам који би омогућио скривање оригиналне поруке тако да буде потпуно (у идеалном случају) неразумљива особама које би неовлашћено дошле у њен посед.

Главна предност смарт картица у односу на друге медијуме за чување података, као што су меморијске картице, је та што омогућавају сигурно чување поверљивих података. Да би се подаци из сигурне меморије на смарт картици прочитали, неопходно је успоставити сигуран канал комуникације између картице и терминала.

Циљ овог рада је приказати један систем за сигурно чување поверљивих података као што су кориснички налози и њихове лозинке на паметним картицама.

# Опис паметних картица

Паметне картице представљају једну од најмањих рачунарских платформи која се данас користи. Иако су веома малих димензија, памерне картице функционишу слично као персонални рачунари јер могу да складиште податке, манипулишу подацима и обављају функције као што су математичке операције, криптографске операције итд. Паметне картице се могу поделити у две форме: контактне и безконтактне. Контактне паметне картице захтевају уметање или дирактан контакт са читачем паметних картица док безконтактне функционишу на принципу магнетног поља и могу да се користе када су прислоњене близу безконтактног читача картица. Паметне картице су највише заступљене у следећим индустријама:

* Телекомуникације (78%)
* Банкарство (7%)
* Здравство (3%)
* Саобраћај и транспорт (2%)
* Остало (10%)

Паметне картице су израђене у потпуности од пластике, осим малог дела предвиђеног за чип картице. Интегрисана кола, или чипови, за паметне картице се производе од силицијумских плочица, баш као и други рачунарски чипови. Ови чипови су везани за алиминијумске површине (да би се обезбедила читљивост) и обложени су у епокси смолом пре уграђивања у пластику картице.

Пошто паметне картице садрже централну процесорску јединицу (ЦПУ), оперативни систем и различите типове меморије на њеном чипу, њихова анатомија је веома слична персоналним рачунарима.

## Централна процесорска јединица (ЦПУ)

Централна процесорска јединица чипа паметне картице тумачи и извршава инструкције добијене од оперативног система.

## Реад онл РОМ