

Meno:

Ing. Patrik Gallo



Ukončený stupeň štúdia:

Druhý, inžinier

Názov záverečnej práce:

Autentizácia na báze eliptických kriviek.
(Bezpečnosť sietí)

Abstrakt:

Kryptografické systémy založené na báze eliptických kriviek sa postupne dostali do popredia a stali sa úspešnou alternatívou ku tradičným kryptografickým systémom ako sú RSA, DSA či Diffie-Hellman. Poskytujú väčšiu bezpečnosť pri ekvivalentnej dĺžke kľúča ako hociktorý z vyššie spomínaných algoritmov, z čoho rezultujú menšie dĺžky kľúčov a teda rýchlejší výpočet a menšia náročnosť na spotrebu energie a pamäte. Na základe týchto faktov, umožňuje kryptografický systém vytvoriť rýchle, veľmi efektívne a flexibilné implementácie protokolov pre potreby autentizácie. Diplomová práca poskytuje, ako úvod do samotnej teórie eliptických kriviek, tak aj postup ako môžu byť eliptické krivky použité pre vytváranie bezpečných a výkonných kryptosystémov. Práca sa venuje aj problému riešenia diskretného logaritmu, keďže navrhnutá autentizačná metóda je založená práve na obtiažnosti riešenia tohto problému, a taktiež na overení hašovacieho kódu z určitej správy. Výsledky implementácie sú pojednávané na záver práce.

Meno:

Ing. Michaela Kreutzová



Ukončený stupeň štúdia:

Druhý, inžinier

Názov záverečnej práce:

Definovanie počítačových jazykov
prostredníctvom používateľských rozhraní

Abstrakt:

Súčasný postupy v softvérovom inžinierstve vedú k tvorbe aplikácií, v ktorých sú implicitné znalosti o doméne prepletené s hlavnou funkcionalitou. Je to tak aj v oblasti grafických používateľských rozhraní, ktoré sú pre používateľov najdôležitejšou časťou programu umožňujúcu interakciu. Táto diplomová práca sa zameriava na problém nedostatku výskumu v oblasti formalizácie jazykov v používateľských rozhraniach a snaží sa načrtnúť základné programátorské techniky pre tvorbu týchto rozhraní. Navrhuje softvérové riešenie umožňujúce definíciu doménovo-špecifického jazyka v grafických používateľských rozhraniach, zaznamenávanie používateľských úkonov na aplikácii a ich automatizáciu. Použitie softvérového riešenia je aplikované na príkladoch voľne dostupných aplikácií naprogramovaných v jazyku Java.

Meno:

Ing. Mária Virčíková



Ukončený stupeň štúdia:

Druhý, inžinier

Názov záverečnej práce:

Umelá inteligencia v humanoidných systémoch

Abstrakt:

Diplomová práca sa zaoberá použitím prostriedkov umelej inteligencie v humanoidnej robotike a konkrétne sa zameriava na spoločenskú robotiku a využitie interaktívnej evolúcie pre systém robotického tanca. V práci sú opísané základy a hlavné vlastnosti interaktívnych evolučných algoritmov nasledované prehľadom ich výskumu a aplikácií. Táto technika optimalizuje systém na základe subjektívneho hodnotenia používateľom. Algoritmus je aplikovaný na systém návrhu robotického tanca, kde evolučný algoritmus pomáha užívateľovi v procese tvorenia choreografie tanca robotov. Systém bol implementovaný v jazyku Python a v simulačnom prostredí Webots. Experimenty s niekoľkými ľudskými hodnotiteľmi dokázali, že prístup s použitím interaktívneho genetického algoritmu na navrhovanie choreografie robotického tanca je sľubný.