Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Posudek vedoucího diplomové práce

Jméno studenta:	Petr KNAP, Bc.
Téma práce:	Zabezpečená výměna dat mezi počítači v nezabezpečeném prostředí
Cíl práce:	Cílem práce byl návrh a implementace zabezpečeného spoje mezi počítači.

Slovní hodnocení:

Obsah a naplnění cíle práce:

Po stručném úvodu do síťové komunikace autor v úvodních kapitolách provedl rešerše nejvíce používaných metod pro bezpečnou výměnu dat a též metod a způsobů obcházení a prolamování těchto zabezpečení. Čtvrtá kapitola obsahuje stručný popis generátorů náhodných čísel nutných pro tvorbu šifrovacích klíčů. Pátá kapitola obsahuje popis kvantových počítačů a jejich využití v kryptografii. Závěrečné čtyři kapitoly jsou implementační. Šestá kapitola obsahuje význam, popis a práci s autorem navrženou knihovnou JavaCry, která obsahuje třídy určené pro bezpečenou komunikaci. V dalších dvou kapitolách autor odděleně popisuje synchronizační službu a příklad realizace klienta této služby. V poslední deváté kapitole jsou prezentovány klíčové návrhy změn a zhodnocena navrhovaná řešení.

Obsah práce je v souladu se zadáním. Autor práci vytvořil zcela sám a dané cíle splnil.

Logická stavba, srozumitelnost, jazyková a stylistická úroveň práce:

V kap. 6.3 autor v některých případech nešťastně používá pojem objekty namísto třídy poskytované knihovnou.

V práci jsou dodrženy zásady DTP. Práce je zpracována přehledně, obsahuje všechny potřebné náležitosti a je v požadovaném rozsahu. Práce má na některých místech poškozen text vinou nedokonalého tisku.

Metody a technologie uplatněné v práci:

Vlastní navržená knihovna JavaCry jako zjednodušující rozhraní mezi Java SE Security a aplikací. Databáze SQLite, JavaFX, JavaScript, jQuery, JSON, HTML, CSS. Sockety.

Prokázání správnosti navrženého řešení problému:

Aplikace je funkční a splňuje zadání. Výsledky práce by bylo třeba více otestovat a zhodnotit, a tím prokázat správnost řešení.

Dotazy a připomínky k DP:

Jak bezpečně předat - obdržet tajný- privátní klíč u asymetrického šifrování?

V práci není občas zřejmé (není zdůrazněno), které třídy jsou přímo převzaty z Java SE Security a které byly autorem modifikovány či přímo vytvořeny. Oceňuji autorovu volbu řešené problematiky.

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **výborně minus**

Posudek vypracoval:

Jméno, tituly: Zdeněk Šilar, Ing., Ph.D.
Zaměstnavatel: Univerzita Pardubice, FEI

V Pardubicích dne: 5. 6. 2014 Podpis: