FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Ing. Pavel Přibáň
Katedra informatiky a výpočetní techniky
Fakulta aplikovaných věd
Technická 8, 301 00 Plzeň
Tel.: (+420) 377 63 2151
E-mail: pribanp@ntis.zcu.cz

Posudek oponenta bakalářské práce

Štěpán Červenka
Klient-server aplikace pro výměnu šifrovaných dat

Obsah Práce
Práce se zabývá návrhem a vytvořením aplikace (framework), která dovoluje ověřovat správnost implementace kryptografických algoritmů. Hlavní motivací této práce je umožnit vytvořenou aplikací automatické testování semestrálních prací z předmětu KIV/BIT.

V první části práce autor krátce popisuje protokoly pro síťovou komunikaci TCP a UDP a jejich použití v programovacím jazyce JAVA spolu s názornými příklady zdrojového kódu. Následně autor popisuje základní pojmy, úlohy a algoritmy z oblasti kryptografie jako jsou šifrování, integrita dat nebo digitální podpis.

V teoretické části práce mi chybí detailnější popis a porovnání zmíněných protokolů TCP a UDP jinak je podle mého názoru teoretická část dostačující a nenašel jsem v ní žádné závažné nedostatky.

Ve druhé části je uveden popis implementace programu a jednotlivých tříd serverové a klientské části aplikace. Autor detailně popisuje jednotlivé části (třídy) aplikace, ale místy je popis velmi neintuitivní a pro pochopení některých odstavců je potřeba je několikrát opakovaně přečíst. Popis implementace je vhodně doplňován zdařilými UML diagramy.

V práci mi naopak chybí kapitola nebo část, ve které by autor souhrnně popsal návrh a architekturu vytvořené aplikace. Některé tyto informace je možné částečně odvodit z popisu implementace, ale očekával bych je popsané v samostatné kapitole. Nesouhlasím s tvrzením na str. 37, a to „Nejvhodnějším způsobem komunikace ... je možnost odesílat celé objekty“, tento způsob komunikace není nejvhodnější ale nejjednodušší.

Struktura práce a řazení kapitol je logické (kromě chybějící kapitoly návrhu). Místy se v práci vyskytují překlepy nebo výrazy, které jsou pro technický dokument nevhodné, např. str. 10 “*jakýmsi spojením*”, str. 17 “*Stále slušná přenositelnost*”, “*rozumné množství dat*” apod.

Většina obrázků a diagramů je vektorová, pouze obr. 3.1 a 3.2 jsou rastrové, ale jejich kvalita je dostačující (snadno by je bylo možné nakreslit jako vektorové obrázky).

Kvalita řešení a dosažených výsledků
Zdrojový kód bylo možné bez problémů přeložit přiloženými ANT skripty a následně spustit. Kód je místy komentován, ale metody rozhraní, které studenti budou implementovat, komentovány nejsou. Aplikace je poměrně dobře dekomponována do jednotlivých tříd a rozhraní. Práce obsahuje přiložené návody s příklady, na kterých je názorně ukázáno jak aplikaci používat. Pokud jsem správně pochopil z textu práce a z přiložených návodů úkolem studenta (uživatele) je implementovat jak kryptografické algoritmy, tak i jejich testy. Z povahy práce bych předpokládal, že student bude implementovat pouze kryptografické algoritmy a jejich ověření (testy) již bude připraveno.

Data jsou šifrována pouze při přenosu ze serveru na klienta a v testech není implementována kontrola dešifrování, tj. testy neověřují, zda uživatelská (studentova) implementace dokáže data opět správně dešifrovat.

V metodě `execute` třídy `RequestExecutor` autor používá pro zjištění typu dotazu operátor `instanceof`, což by jistě šlo vyřešit mnohem lépe.

Za největší slabinu vytvořené aplikace považuji zvolený způsob komunikace mezi serverem a klientem, tj. pomocí serializace a přenášení celých JAVA objektů. Se serverem je možné komunikovat pouze v jazyce JAVA a studenti tak budou nuceni vypracovávat semestrální práce pouze v tomto jazyce.

Formální úroveň
Formální úroveň práce je v pořádku. Dokument bakalářské práce je vysázen v LaTeX a dokument neobsahuje typografické chyby. V textu jsem objevil několik překlepů a gramatických chyb. I přes některé nedostatky si autor dal na práci záležet.

Práce s literaturou
Citovaná literatura je vzhledem k tématu bakalářské práce relevantní a citace v textu jsou v pořádku. V seznamu literatury není u žádné z použitých referencí uvedeno ISBN nebo ISSN i přesto, že některé citované zdroje je mají přiřazené.

Splnění zadání
Pokud bych zadání práce interpretoval naprosto doslovně, pak by se dalo považovat za částečně nesplněné, protože data jsou šifrovaná pouze při přenosu ze serveru na klienta a nejedná se přímo o šifrovaný přenos. I přesto považuji zadání za splněné, protože hlavní motivací podle mě bylo umožnit automatizaci kontroly semestrálních prací předmětu KIV/BIT, což implementovaná aplikace ve větší míře dovoluje.

Dotazy k práci

1. Co by bylo potřeba v aplikaci upravit, aby bylo možné se serverem komunikovat jiným způsobem než pomocí objektů jazyka JAVA ?
2. Jak náročné by bylo provést tyto úpravy na serveru, aby s ním bylo možné komunikovat jiným způsobem, např. implementací REST API, které zmiňujete v závěru ?
3. Proč neověřujete i správnost implementace dešifrování ? (viz str. 60)

Navrhuji hodnocení známkou **dobře** a práci doporučuji k obhajobě.

V Plzni dne 29. května 2020

Ing. Pavel Přibáň
(oponent BP)