

# Posudek práce

předložené na Přírodovědecké fakultě JU

- posudek vedoucího  
 bakalářské práce
- posudek oponenta  
 diplomové práce

Autor/ka: **Petr Kopecký**  
Název práce: Praktická implementace Vernamovy šifry  
Studijní program a obor: Aplikovaná informatika  
Rok odevzdání: 2011

Jméno a tituly vedoucího/oponenta: ing. Petr Břehovský  
Pracoviště: Ústav aplikované informatiky  
Kontaktní e-mail: petrbreh@gmail.com

## Odborná úroveň práce:

- vynikající  velmi dobrá  průměrná  podprůměrná  nevyhovující

## Věcné chyby:

- téměř žádné  vzhledem k rozsahu přiměřený počet  méně podstatné četné  závažné

## Výsledky:

- originální  původní i převzaté  netriviální kompilace  citované z literatury  opsané

## Rozsah práce:

- veliký  standardní  dostatečný  nedostatečný

## Grafická, jazyková a formální úroveň:

- vynikající  velmi dobrá  průměrná  podprůměrná  nevyhovující

## Tiskové chyby:

- téměř žádné  vzhledem k rozsahu a tématu přiměřený počet  četné

## Celková úroveň práce:

- vynikající  velmi dobrá  průměrná  podprůměrná  nevyhovující

**Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:**

Praktických cílů práce bylo dosaženo. Popisná část je však příliš stručná a popis problematiky je bez konzultování dalších zdrojů pro neznalého čtenáře hůře pochopitelný. Chybí popis a analýza „bezpečnosti“ samotné aplikace.

I přes výhrady je práce vhodným úvodem do problematiky velmi bezpečné komunikace a dobrým základem pro praktickou implementaci téměř neprolomitelné šifry.

**Případné otázky při obhajobě a náměty do diskuze:**

Doporučoval byste data z random.org k praktickému použití?  
Navrhněte metody zabezpečení klíče.

**Práci**

doporučuji

nedoporučuji

uznat jako diplomovou/bakalářskou.

**Navrhuji hodnocení stupněm:**

výborně  velmi dobře  dobře  neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích , 15.1. 2012

