POSUDEK BAKALÁŘSKÉ PRÁCE "KRYPTOGRAFICKÁ SCHÉMATA POUŽÍVAJÍCÍ DISKRÉTNÍ LOGARITMUS"

TOMÁŠE KADLČKA

Problém diskrétního logaritmu spočívá v nalezení exponentu α jsou-li dány dva prvky g a g^α cyklické abelovy grupy G prvočíselného řádu p. S diskrétním logaritmem souvisí Diffie-Hellmanův problém, který ve své základní verzi spočívá v nalezení prvku $g^{\alpha\beta}$ jsou-li známy prvky g, g^α a g^β z G. První kapitola práce je krátkým úvodem, ve druhé jsou rozebrány různé varianty Diffie-Hellmanova problému a jsou studovány případy ve kterých lze tyto varienty vzájemně převádět (v polynomiálním čase). Ve třetí kapitole je načrtnuta teorie eliptických křivek nad konečným tělesem, je definována třídová grupa divisorů a jsou popsána Weilovo a Tateovo párování. Ve čtvrté kapitole je podán přehled metod šifrování založených na teoretických principech studovaných v předchozích kapitolách, od klasických, jako ElGamal schéma, až po nejnovější. V páté kapitole jsou posány útoky na některé z těchto metod. Poslední, šestá kapitola, je shrnutím.

Práce je čistě kompilační bez originálních výsledků. Udává však rozsáhlý přehled studované problematiky, což potvrzuje i množství článků ze kterého student čerpal. Rozsáhlost práce je vykoupena neúplností a drobnou nepřesností argumentů a místy značení, což je však patrně styl obvyklý v kryptografii. V některých místech, např. v části 3.2 nebo v popisu zranitelnosti ElGamalova schématu vůči CCA2 (v části 5.2.2), jenž je evidentně nesprávný, si proto nejsem jist nakolik student pospisovanou problematiku chápe. Množství formálních chyb nepřesahuje únosnou mez.

Práci navrhuji uznat jako práci diplomovou a hodnotit ji známkou výborně, však za předpokladu, že student během obhajoby přesvědčí o dokonalém porozumění všem popisovaným skutečnostem.

V Praze dne 28. 8. 2008, Pavel Růžička

[redacted]