Predslov

Kryptografická ochrana spracovávaných, uchovávaných a prenášaných dát je jedným z kľúčových faktorov pri využívaní moderných informačno-komunikačných technológií. Využitie kryptografických metód nie je len výsadou drahých a zložitých systémov. Naopak, jednou z najdynamickejšie sa rozvíjajúcich oblastí je nasadenie kryptografických metód v lacných vstavaných (angl. embedded) systémoch. Príkladom sú napr. senzorové siete a ich využitie v rámci konceptu Internetu vecí (IoT – Internet of Things), kde je potrebné kryptografickú podporu integrovať do lacných vstavaných zariadení s relatívne obmedzenou výpočtovou kapacitou. Vo všeobecnosti je kryptografická ochrana vytváraná zo základných stavebných blokov (kryptografických primitív), ako sú symetrické a asymetrické šifry, hašovacie funkcie a generátory náhodných čísel.

Absolventi študijných programov zameraných na počítačové inžinierstvo, elektroniku a telekomunikačnú techniku sú tak konfrontovaní s potrebou uplatnenia základných znalostí z programovania v jazyku C, ktoré zvládli na začiatku štúdia, v oblasti programovania vstavaných systémov. Na to, aby boli pri ich programovaní dostatočne efektívni, musia pochopiť a zohľadniť špecifické nároky a obmedzenia vstavaných systémov. V prípade kryptografických blokov je potrebné tiež využiť pomerne špecializovaný matematický aparát a špecifické matematické vývojové nástroje, čo absolventov technických fakúlt často odrádza.

Učebnica vznikla na základe mojich skúseností vo výučbe predmetov Aplikovaná kryptografia, Programovanie vstavaných systémov a Mikroprocesorová technika na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach, a tiež aj výskumno-vývojových projektov, na ktorých dlhodobo pracujem. Hlavným cieľom učebnice je oboznámiť študentov so základnými technikami implementácie kryptografických stavebných blokov, ktoré sú využívané v moderných vstavaných systémoch, základnými metódami ich optimalizácie a nástrojmi pre ich efektívnu implementáciu a testovanie. Cieľom je poukázať na úzku súvislosť medzi teoretickými poznatkami z matematiky (teória čísel, algebra a štatistika) a efektívnou implementáciou kryptografických algoritmov v moderných vstavaných systémoch.

Na vybraných príkladoch kryptografických blokov sú naznačené možnosti využitia základného vývojového nástroja – jazyka C, s ktorým sa študenti stretávajú v základných predmetoch štúdia. Využijeme tiež efektívny matematický nástroj (softvérový balík Magma), ktorý umožňuje výrazne zvýšiť efektivitu testovania pri vývoji a implementácii moderných kryptografických algoritmov a protokolov. Hlav-

ným cieľom je prehĺbiť znalosti z algoritmizácie a programovania v tejto špecifickej oblasti, a čo najjednoduchšou formou poukázať na praktické využitie matematického aparátu, s ktorým sa študenti stretávajú počas štúdia len okrajovo. Tomuto cieľu je prispôsobený aj výber vývojových nástrojov, ktoré budeme v učebnici využívať. Všetky použité nástroje sú voľne dostupné aj v tzv. testovacích verziách, ktorých funkčnosť je pre náplň učebnice postačujúca.

V učebnici opisované algoritmy môžu tvoriť základ jednoduchých vstavaných kryptografických aplikácií, nie je však cieľom poskytnúť kompletné riešenia pre reálne aplikácie. Reálne aplikácie vyžadujú ďalšie dodatočné optimalizácie, ktoré sú nad rámec tejto učebnice a cieľov, ktoré učebnica sleduje. Nie je cieľom opisovať detailne jednotlivé implementované kryptografické algoritmy. Opisy budú obmedzené na nevyhnutné minimum potrebné na vysvetlenie využitých súvislostí a faktov potrebných pre programovú implementáciu. Na detailný opis kryptografických blokov môžu študenti využiť zdroje uvedené v zozname použitej literatúry. Do pozornosti dávam predovšetkým učebnicu [1], ktorá pokrýva oblasť kryptografických stavebných blokov a protokolov v dostatočnom rozsahu a je základnou učebnicou pre predmet Aplikovaná kryptografia na našej fakulte. Do učebnice som zahrnul aj niektoré nekryptografické algoritmy (CRC súčty a LZRW kompresiu) s cieľom ukázať príklady programových riešení aj ďalších praktických algoritmov často využívaných vo vstavaných systémoch.

Na záver sa chcem poďakovať recenzentom prof. Dušanovi Levickému z Technickej univerzity v Košiciach a prof. Viktorovi Fischerovi z Jean Monnet University v Saint-Etienne za pozorné prečítanie rukopisu a cenné pripomienky, ktoré umožnili zlepšiť čitateľnosť textu. Zároveň sa im chcem obom poďakovať za možnosť dlhoročnej spolupráce s nimi v pedagogickej a vedecko-výskumnej oblasti, a tiež aj za ich podporu v mojej profesionálnej kariére, bez ktorej by táto učebnica nevznikla. Za cenné rady, námety a pomoc pri zvládaní LaTeXu ďakujem RNDr. Jánovi Bušovi, CSc. Tiež ďakujem manželovi mojej dcéry Petrovi za pomoc pri prepise algoritmov do LaTeXu, synovi Tomášovi za prekreslenie obrázkov, dcére Janke za grafické spracovanie obálky učebnice a tiež aj všetkým ostatným, ktorí akoukoľvek mierou prispeli k napísaniu a vydaniu učebnice.

Košice, júl 2017 Miloš Drutarovský