

# Obsah

Zoznam symbolov	ix
Zoznam skratiek	xii
Predslov	xiii
<b>1 Základné súvislosti a použité vývojové nástroje</b>	<b>1</b>
1.1 Velkosť operandov v kryptografických algoritmoch . . . . .	2
1.2 Ciele a metódy optimalizácie . . . . .	3
1.3 Použité vývojové nástroje . . . . .	5
1.3.1 Vývojové prostredie DEV C++ . . . . .	5
1.3.2 Program make . . . . .	5
1.3.3 Softvérový balík Magma . . . . .	7
1.3.4 Nástroj OpenSSL . . . . .	9
1.3.5 Vývojový nástroj MDK . . . . .	10
1.4 Ciele učebnice a odporúčaný postup . . . . .	11
<b>2 Modulárna aritmetika a jazyk C</b>	<b>13</b>
2.1 Implementácia modularnej aritmetiky v jazyku C . . . . .	13
2.2 Korekcia pretečenia čítača v modulo aritmetike . . . . .	17
2.3 Algoritmus RSA a modulárna aritmetika . . . . .	20
<b>3 Operácie s veľkými číslami</b>	<b>25</b>
3.1 Reprezentácia čísel v pamäti . . . . .	25
3.2 Celočíselná aritmetika s MP číslami . . . . .	27
3.2.1 Reprezentácia nezáporných MP čísel so základom $b$ . . . . .	28
3.2.2 Reprezentácia záporných MP čísel so základom $b$ . . . . .	29
3.2.3 Sčítanie dvoch MP čísel . . . . .	30
3.2.4 Odčítanie dvoch MP čísel . . . . .	30
3.2.5 Násobenie dvoch MP čísel . . . . .	30
3.2.6 Delenie dvoch MP čísel . . . . .	31
3.3 Modulárna aritmetika s MP číslami . . . . .	34
3.3.1 Modulárne sčítanie a odčítanie dvoch MP čísel . . . . .	34
3.3.2 Modulárne násobenie dvoch MP čísel . . . . .	34
3.3.3 Modulárna inverzia MP čísel . . . . .	35

<b>4</b>	<b>Techniky implementácie šifrovacieho štandardu AES</b>	<b>39</b>
4.1	Elementárne operácie v $\mathbb{GF}(2^8)$ . . . . .	40
4.1.1	Sčítanie prvkov v $\mathbb{GF}(2^8)$ . . . . .	40
4.1.2	Násobenie prvkov v $\mathbb{GF}(2^8)$ a funkcia <code>xtime()</code> . . . . .	41
4.1.3	Násobenie s pomocou logaritmických a exponenciálnych tabuliek . . . . .	44
4.2	Implementácia S-boxu v algoritme AES . . . . .	49
4.3	Implementácia algoritmu AES s využitím T-boxov . . . . .	55
4.4	Netradičné implementácie algoritmu AES . . . . .	58
4.4.1	Implementácia AES menšia ako S-box . . . . .	58
4.4.2	Inverzný AES so zdieľanou MixColumn transformáciou . . . . .	59
4.4.3	Tabuľková implementácia AES so zvýšenou ochranou voči DPA útoku . . . . .	60
4.5	Testovacie vektory a testovacia metóda Monte Carlo . . . . .	60
<b>5</b>	<b>Hašovacie funkcie</b>	<b>65</b>
5.1	Hašovacie funkcie z rodiny SHA . . . . .	65
5.2	Hašovacie funkcie s využitím blokovej šifry . . . . .	67
5.2.1	Konfigurácia typu Davies–Meyer . . . . .	68
5.2.2	Konfigurácia typu Matyas–Meyer–Oseas . . . . .	68
5.2.3	Konfigurácia typu Miyaguchi–Preneel . . . . .	69
5.2.4	Hiroseho konfigurácia s dvojnásobnou dĺžkou . . . . .	70
5.3	Hašovacie funkcie s využitím asymetrickej šifry . . . . .	71
<b>6</b>	<b>Pseudonáhodné generátory</b>	<b>73</b>
6.1	Funkcia RAND v štandardných knižniciach . . . . .	73
6.1.1	Lineárny kongruentný generátor . . . . .	74
6.1.2	Mitchellov a Moorov aditívny PRNG . . . . .	75
6.2	Kryptograficky bezpečné PRNG . . . . .	76
6.2.1	PRNG s využitím čítača . . . . .	77
6.2.2	Generátor BBS (Blum–Blum–Shub) . . . . .	78
6.2.3	Generátor RSA . . . . .	81
6.2.4	PRNG na báze SHA1 v knižnici OpenSSL . . . . .	82
6.3	Testovanie kvality náhodných generátorov . . . . .	85
6.3.1	Frekvenčný test . . . . .	86
6.3.2	Pokerový test . . . . .	86
6.3.3	Sériový test . . . . .	86
6.3.4	Test rovnakých reťazcov . . . . .	87
6.3.5	Autokorelačný test . . . . .	87
6.3.6	Štatistické testy FIPS . . . . .	87
6.3.7	Štatistické testy NIST . . . . .	91
<b>7</b>	<b>Optimalizácie výpočtu algoritmu RSA</b>	<b>93</b>
7.1	Využitie čínskej vety o zvyškoch . . . . .	93
7.2	Modulárne umocňovanie v Montgomeryho oblasti . . . . .	96
7.3	Umocňovanie s využitím Montgomeryho rebríka . . . . .	100

7.4	Umocňovanie s využitím tabuliek . . . . .	101
7.4.1	Umocňovanie s $w$ -bitovým oknom . . . . .	101
7.4.2	Umocňovanie s kľzavým oknom . . . . .	102
<b>8</b>	<b>Základné operácie v algoritmoch ECC</b>	<b>105</b>
8.1	Polia $\mathbb{GF}(p)$ optimalizované pre ECC . . . . .	107
8.2	Základné operácie s bodmi na eliptickej krivke . . . . .	110
8.3	Násobenie $kP$ bodu na eliptickej krivke . . . . .	117
8.4	Operácie s bodmi v projektívnych súradniciach . . . . .	119
<b>9</b>	<b>Podporné funkcie pre vstavané systémy</b>	<b>125</b>
9.1	Kontrolné CRC súčty . . . . .	125
9.1.1	Generačný polynóm a vytvorenie CRC súčtu . . . . .	126
9.1.2	Voľba generačného polynómu . . . . .	127
9.2	Implementácia výpočtu CRC v jazyku C . . . . .	129
9.3	Bezstratový kompresný algoritmus LZRW1 . . . . .	132
9.3.1	Základný princíp algoritmu LZRW1 . . . . .	133
9.3.2	Implementácia algoritmu LZRW1 v jazyku C . . . . .	135
<b>10</b>	<b>Vybrané kryptografické protokoly, algoritmy a aplikácie</b>	<b>139</b>
10.1	Parametre algoritmu Diffie-Hellman na výmenu kľúčov . . . . .	139
10.2	Násobenie v $\mathbb{GF}(2^{128})$ pre GCM mód blokovej šifry . . . . .	144
10.3	Digitálny podpis na báze ECC – algoritmus ECDSA . . . . .	149
10.4	Súbežné šifrovanie a autentizácia – algoritmus ECIES . . . . .	153
10.5	Zabezpečená aktualizácia MCU firmvéru . . . . .	155
	<b>Záver a ďalší odporúčaný postup</b>	<b>159</b>
<b>A</b>	<b>Magma – stručný úvod a základné ovládanie</b>	<b>161</b>
A.1	Spustenie programu a zadávanie príkazov . . . . .	162
A.2	Relačné operátory a riadenie slučiek . . . . .	164
A.3	Algebraické systémy – Galoisove polia a eliptické krivky . . . . .	167
	<b>Zoznam použitej literatúry</b>	<b>171</b>
	<b>Register</b>	<b>177</b>