

Obsah

Předmluva	ix
1 Diskrétní komunikační kanál	1
1.1 Bezpečný informační zdroj	4
1.2 Entropie	9
1.3 Bezpečný přenosový kanál	15
1.4 Vzájemná informace a podmíněná entropie	22
1.5 Podmíněná informace a podmíněná nezávislost	26
1.6 Stacionární informační zdroj	29
2 Kódování informačního zdroje	36
2.1 Kódy s pevnou délkou	37
2.2 Kódovací věta pro blokové kódy	40
2.3 Kódy s proměnlivou délkou	48
2.4 Konstrukce optimálních kódů	57
2.5 Kódovací věta pro kódy s proměnlivou délkou	69
3 Kódy detekující chyby a samoopravné kódy	74
3.1 Minimální vzdálenost kódu	75
3.2 Binární lineární kódy	77
3.2.1 Generující a kontrolní matice	80
3.2.2 Opravné tabulky	85
3.3 Perfektní kódy	90
3.3.1 Hammingovy kódy	94
3.3.2 Golayův kód	99
3.4 Obecné lineární kódy	101
3.4.1 Grupy a tělesa	101
3.4.2 Generující a kontrolní matice lineárních kódů	105
3.5 Cyklické kódy	107
3.5.1 Násobení a dělení polynomů	109
3.5.2 Generující a kontrolní polynomy cyklických kódů	111
4 Kódy pro sdílení utajované hodnoty	120
4.1 Rozdělení a sdílení utajované hodnoty	122
4.1.1 Nedokonalé a dokonalé rozdělení utajené hodnoty	122
4.1.2 Kvalifikované a nepřipustné skupiny	124
4.2 Přístupové struktury a schémata	126
4.2.1 Přístupové struktury	126
4.2.2 Formalizace popisu rozdělení hodnoty	131
4.2.3 Pravděpodobnostní schémata	134
4.3 Vlastnosti přístupových struktur	139
4.3.1 Souvislost přístupových struktur	139

4.3.2	Kódy na úplných strukturách	141
4.3.3	Velikost částečných údajů	143
4.4	Příklady rozdělení utajené hodnoty	145
4.4.1	Dokonalé rozdělení utajené hodnoty podle Shamira	145
4.4.2	Nedokonalé rozdělení utajené hodnoty podle Blakleyho	148
4.4.3	Schodová schémata	149
4.4.4	Další aplikace rozdělení utajené hodnoty	153
5	Bezeztrátová komprese dat	158
5.1	Základní pojmy	159
5.2	RLE – kódování proudů	161
5.3	Algoritmy Lempela a Ziva	164
5.3.1	LZ77	164
5.3.2	LZ78	166
5.3.3	LZW	169
5.4	Aritmetické kódování	172
5.5	PPM	176
5.6	Burrows–Wheelerova metoda	181
6	Digitální zpracování signálu	185
6.1	Analogový a digitální signál	185
6.2	Převod analogového signálu na digitální	187
6.2.1	Princip digitalizace	187
6.2.2	Určení vzorkovací frekvence	188
6.2.3	Převod spojité funkce na diskretní definiční obor	191
6.2.4	Kvantování	192
6.3	Rekonstrukce analogového signálu z digitálního	195
6.4	Lineární diskretní transformace	196
6.4.1	Diskretní Fourierova a diskretní kosinová transformace	199
6.4.2	Vlnková transformace a lifting schéma	201
6.5	Specifika obrazového signálu	206
6.5.1	Digitalizace obrazu	206
6.5.2	Reprezentace barev	206
6.5.3	Barevné systémy s paletou	209
7	Ztrátová komprese	210
7.1	Odstranění irelevance a měření ztrátovosti	211
7.2	Základní principy komprese	213
7.2.1	Prediktivní metody	214
7.2.2	Hierarchické metody	217
7.3	Komprese zvuku	218
7.3.1	Digitální zvukový signál	218
7.3.2	Psychoakustický model MP3	218
7.3.3	Zvuková komprese MP3	220
7.4	Komprese statických obrázků	222
7.4.1	Reprezentace statických obrázků	222
7.4.2	Snížení barevné hloubky	224
7.4.3	JPEG	225
7.5	Komprese videa	235

7.5.1	Rámec kódování videa	235
7.5.2	MPEG	236
7.5.3	Aplikace komprese videa	238
8	Základní metody šifrování	240
8.1	Vigenèrova substituční šifra	241
8.1.1	Kryptoanalýza s využitím koincidencí	245
8.1.2	Kasiského kryptoanalýza	247
8.1.3	Frekvenční kryptoanalýza při znalosti periody	248
8.1.4	Vernamova šifra	250
8.1.5	Enigma	251
8.2	Šifrový standard DES	252
8.2.1	Expanze klíčů	253
8.2.2	Šifrování	255
8.2.3	Dešifrování	260
8.2.4	Vlastnosti DES	261
8.2.5	Kryptoanalýza DES	261
8.3	Nový šifrový standard AES	262
8.3.1	Expanze klíčů	266
8.3.2	Šifrování	267
8.3.3	Dešifrování	269
8.3.4	Kryptoanalýza AES	269
8.4	Šifrování s veřejným klíčem – metoda RSA	270
8.4.1	Podstata a použití RSA-kryptosystému	270
8.4.2	Matematické principy – Eulerova věta	274
8.4.3	Generování velkých prvočísel	275
8.4.4	Určení veřejného a soukromého klíče	277
8.4.5	Faktorizace a kryptoanalýza RSA	280
8.5	Další metody šifrování s veřejným klíčem	283
8.5.1	Diffie-Hellmanova metoda výměny klíčů	283
8.5.2	Micaliho rozšíření	285
8.5.3	Kryptosystém ElGamal	287
8.5.4	Metoda založená na problému batohu	289
	Použitá a doplňující literatura	293
	Použité symboly	297
	Rejstřík	303