

Obsah

<i>Předmluva</i>	<i>xvii</i>
<i>Úvod</i>	<i>xix</i>
<i>I: Úvod do PGP</i>	<i>1</i>
<i>1: Úvod do PGP</i>	<i>3</i>
Proč PGP? Případ pro šifrování	4
Vaše pošta může zabloudit	7
Chraňte své soukromí	8
Odkud PGP pochází?	10
Základní terminologie PGP	11
Klíče: veřejné, tajné a pro seanci	11
Certifikáty klíčů	13
Kroužky na klíče	14
Vstupní fráze	15
Digitální podpisy	17
Podpisy na certifikátech klíčů	20
Jak PGP spustit	21
Rozhraní příkazového řádku	21
Nápověda (volba -h)	22
Specifikace argumentů příkazového řádku	23
Používání „brnění“ ASCII (volba -a)	24
Šifrování a podepisování e-mailu (volby -e a -s)	25
Extenze souborů PGP	27

PGP proměnné prostředí	28
PGP proměnné konfigurace	29
Jazykový soubor PGP	30
PGP a jeho konkurenti	31
Certifikace klíče v PGP	32
2: Základy šifrování	33
Jak pracuje jednoduché šifrování?	33
Kódy	34
Šifry	35
Jednorázový blok	36
Klíč a délka klíče	39
Narušení kódu	39
Šifrování soukromým klíčem	42
Algoritmy soukromých klíčů	43
Případ soukromého klíče	44
Problémy šifrování soukromým klíčem	45
Centrum distribuce klíčů	46
Vyhlídka pro soukromé klíče	47
Šifrování veřejným klíčem	47
Systémy veřejných klíčů	49
Výhody systémů veřejných klíčů	51
Digitální podpisy	51
Společné používání šifrování veřejným a soukromým klíčem	51
Jak dobré je šifrování?	51
Silný a slabý	52
Případy pro slabost	54
Co šifrování neumí	54
Omezení Spojených států v oblasti kryptografie	56
Kryptografie a patentový systém Spojených států	56
Šifrování a řízení vývozu	57

II: Historie šifrování a politiky	59
3: Šifrování před PGP	61
Kryptografie v dějinách	61
Národní bezpečnost a Úřad pro národní bezpečnost	62
Lucifer a DES	64
Národní úřad pro normalizaci	65
Bezpečnost DES	66
Narušení DES	67
Alternativy DES	68
Šifrování veřejným klíčem	69
Puzzle Raloha Merkla	69
Multiuživatelská technika Diffie-Hellman	71
Diffie-Hellmanova exponenciální výměna klíče	72
Zrození RSA	73
Vzestup a pád batohů	78
Uvedení veřejného klíče na trh	80
4: Báječná historie PGP	83
Phil Zimmermann: na cestě k PGP	83
Metamorfni systémy	85
Charlie Merritt	86
Phil Zimmermann se setkává s veřejným klíčem	88
Tváří v tvář Jimu Bidzosovi	88
Vzestup RSA Data Security	90
Spolupráce s Velkým Jimem	91
Opravdu skvělý program	92
Zrození PGP - verze 1.0	95
PGP roste	97
Bass-O-Matic	97
TO pravé - PGP verze 2.0	98
Cypherpunks	99
PEM, RSAREF a RIPEM	99
ViaCrypt	101

Nastupuje MIT	101
Vypuštění PGP do světa	104
Vyšetřování Zimmermanna na federální úrovni	106
Kam s PGP?	107
RSA-129 vyřešena!	108
5: Soukromí a veřejný život	111
Odposlouchávání a vláda Spojených států	112
Digitální telefonický plán FBI	115
Obrovské náklady Digital Telephony	116
Návrat Digital Telephony	117
Kde je zakopaný pes?	119
Informační superdálnice je „zapojena pro zvuk“	119
NSA čip Clipper	120
Čip Clipper obsahuje	121
Kdo získá klíče?	122
Bitva o Clipper a EES	124
Problémy s Clipperem	125
6: Šifrovací patenty a vývoz	127
Patenty a politika	127
Export: 40 bitů nestačí!	129
Norma digitálního podpisu	130
Bitva o DSS	130
DSS a patenty	131
Soumrak PKP?	132
Soudní spor Cylink	132
Schlaflyho soudní spor	134
III: Používání PGP	137
7: Zabezpečte své soubory	139
Šifrování a dešifrování souborů	140
Zašifrování souboru	140

Když uděláte chybu	143
Vymazání původního souboru (volba -w)	143
Obnovení vašeho zašifrovaného souboru (předdefinovaná volba)	144
Vstupní fráze	145
Musíte použít různé vstupní fráze pro každý soubor?	145
Jak vstupní frázi vybrat	145
Správná vstupní fráze	147
Proč používat dlouhou vstupní frázi?	148
8: Vytváření klíčů PGP	151
Aby mohlo šifrování veřejným klíčem pracovat	152
Teorie v pozadí klíčů	153
Vytvoření klíčů pomocí PGP (volba -kg)	154
Volba délky vašeho veřejného klíče	155
Zadání vašeho uživatelského identifikátoru (ID)	155
Výběr vaší vstupní fráze	157
Vytvoření náhodnosti	157
Co když PGP klíče negeneruje?	159
Kroužek na klíče PGP: místo pro vaše klíče	160
9: Správa klíčů PGP	161
Kroužky na veřejné a tajné klíče	162
Zobrazení klíčů (volba -kv)	163
Zobrazení klíčů na vašem kroužku veřejných klíčů	163
Zobrazení klíčů na vašem kroužku tajných klíčů	164
Zobrazení klíčů na jiném kroužku	165
Získání více informací o klíčích (volba -kvc)	166
Změna certifikátu vašeho klíče (volba -ke)	167
Změna vaší vstupní fráze	167
Změna vašeho uživatelského ID (volba -ke)	168
Úpravy pomocí voleb	170
Změna vašeho uživatelského ID (volby -ke a -kr)	170
Dejte svůj veřejný klíč každému	172
Kopírování kroužku veřejných klíčů	172

Vyjmutí vašeho veřejného klíče (volba -kx)	172
Vyjmutí tisknutelných klíčů s brněním ASCII (volba -kxa)	174
Použití režimu filtru (volba -f)	176
Vyjmutí více klíčů do jednoho souboru s „brněním“ ASCII	176
Přidání klíčů na kroužky klíčů (volba -ka)	178
Přidání něčího klíče na váš kroužek veřejných klíčů	178
Přidání klíče na zvolený kroužek na klíče	179
Duplikáty nejsou povoleny	180
Odstranění klíčů z kroužku na klíče (volba -kr)	181
Odstranění klíčů z vašeho kroužku veřejných klíčů	181
Odstranění klíče ze zvoleného kroužku na klíče	181
Pouštěcí sada veřejných klíčů	182
10: Šifrování elektronické pošty	185
Odesílání zašifrovaného e-mailu	186
Krok 1: Vytvoření zprávy	186
Krok 2: Získání veřejného klíče příjemce	188
Krok 3: Zašifrování zprávy (volba -e)	189
Krok 4: Odeslání zprávy	193
Udělejte to všechno najednou (volba -f)	194
Současné zašifrování a odeslání zprávy	194
Současný zápis, zašifrování a odeslání	195
Příjem zašifrovaného e-mailu	195
Dešifrování e-mailu	196
Změna souboru na výstupu (volba -o)	198
Zobrazení dešifrovaného souboru (volba -m)	198
Neznámý uživatel	199
Odesílání a příjem rozsáhlých dokumentů	199
Změna velikosti souboru v „brnění“	202
Odeslání zašifrovaného souboru do seznamu pošty	202
Zašifrování a odeslání více osobám	202
Přidání sebe sama do seznamu pošty	204
Automatické přidání sebe sama do seznamu	204

<i>11: Používání digitálních podpisů</i>	207
Jak pracují digitální podpisy	208
Funkce výtah zprávy MD5	208
Výtah zprávy a veřejný klíč	210
Digitální podpisy RSA	212
Digitální podpisy PGP	212
Podepsání zprávy (volba -s)	213
Ověření digitálního podpisu	215
Výběr z více tajných klíčů (volba -u)	217
Podepsání a zašifrování zprávy (volba -se)	218
Příjem podepsané zprávy	220
Vytvoření samostatných podpisů (volba -sb)	221
<i>12: Certifikace a distribuce klíčů</i>	223
Zfalšované klíče	224
Sít důvěry	225
Přidání klíče s podpisy (Volba -ka)	226
Přidání klíče Philovy Pretty Good Pizza	226
Přidání klíče váženého pana Terrence Talbota	231
Přidání klíče Sama Spadea	234
Zobrazení podpisů	235
Kontrola vašich klíčů a podpisů (volba -kc)	235
Kontrola vašich klíčů a podpisů (volba -kvv)	237
Kontrola všech otisků prstů vašich klíčů (volba -kvc)	237
Změna vaší důvěry k určité osobě (volba -ke)	238
Specifikace jiného kroužku na klíče	240
Podepsání klíče (volba -ks)	240
Podpis jiným tajným klíčem (volba -u)	242
Odstranění podpisu (volba -krs)	244
Neznámí podepsaní	245
Certifikace klíčů v souboru keys.asc (verze 2.6.1)	250

13: Zrušení, vypnutí a úprava klíčů	253
Zrušení vašeho veřejného klíče	253
Co to je certifikát zrušení klíče?	254
Vytvoření certifikátu zrušení klíče (volba -kd)	254
Problematika zrušení klíčů	257
Vypnutí veřejného klíče (volba -kd)	257
Systém manuálního uložení klíčů	258
Jednoduché uložení klíče	259
Rozdělené uložení klíče	260
 14: Konfigurační soubor PGP	 261
Co to je konfigurační soubor PGP?	261
Umístění konfiguračního souboru	262
Úprava konfiguračního souboru	262
Specifikace proměnných konfigurace v příkazovém řádku	263
Uvnitř konfiguračního souboru	264
Přehled proměnných konfigurace	268
 15: Servery Internetu pro klíče PGP	 275
Komunikace pomocí serveru klíče	276
Příkazy serveru klíče	276
Nápověda - Help	277
Jak zjistit kdo je na serveru	277
Přidání vašeho klíče na server	278
Jak získat veřejný klíč ze serveru	278
Jak získat sadu veřejných klíčů	280
Jak získat zaktualizované klíče	281
Kde jsou servery klíčů?	281
 IV: Přílohy	 283
 A: Jak získat PGP	 285
Jak získat PGP z MIT	286
Co mám zadat?	287

Jiné způsoby získání PGP	296
Hamburská univerzita: spousta kryptografických zdrojů	296
Kalifornská univerzita v Berkley: Cypherpunk	297
Netcom: PGP FAQ a další informace	297
Nadace Electronic Frontier	298
Jiné zdroje	298
<i>B: Instalace PGP na PC</i>	<i>299</i>
Volba adresáře	299
Rozbalení PGP	299
Ověření vaší kopie PGP	303
Nastavení proměnné prostředí PGP na PC	305
Proměnná prostředí PGPPATH	306
Proměnná prostředí TZ	307
Příklad souboru autoexec.bat	308
Vytvoření vaší dvojice veřejný/tajný klíč	308
<i>C: Instalace PGP v systému Unix</i>	<i>309</i>
Rozbalení PGP v Unixu	309
Získání kompilátoru C	311
Vytvoření knihovny RSAREF	311
Vytvoření PGP	313
Ověření vaší kopie PGP	317
Dokončení instalace PGP pod Unixem	320
Nebezpečí při používání PGP v multiuživatelském prostředí	322
<i>D: Instalace PGP na počítači Macintosh</i>	<i>325</i>
Jak získat MacPGP	325
Instalace MacPGP	326
Kopírování souboru	326
Dekódování souboru	326
Vytvoření složky pro nastavení	326
Vytvoření složky PGP	327
Zavedení MacPGP	328

Vytvoření vašich klíčů	328
Přidání klíčů na váš kroužek na klíče	329
MacBinarizace	330
Certifikace klíčů	332
<i>E: Verze PGP</i>	<i>335</i>
<i>F: Matematické problémy šifrování</i>	<i>341</i>
Funkce Diffie-Hellmanova algoritmu	341
Funkce RSA	343
Bezpečnost RSA	344
Jak velké je velmi velké?	344
Jak náhodná je náhoda?	346
Dr. Ron Rivest – Problémy rozkladu	346
Výtah	347
Algoritmy rozkladu	347
Náklady na výpočet	348
Výsledky	349
Závěry	349
Jak PGP volí prvočísla	350
<i>G: Glosář</i>	<i>353</i>
<i>Použitá literatura</i>	<i>363</i>
Knihy	363
Přednášky a ostatní publikace	364
Elektronické zdroje	365
<i>Rejstřík</i>	<i>367</i>