ïÐÉÓÁÎÉÅ GNU Privacy Guard

ïÐÉÓÁÎÉÅ GNU Privacy Guard

Copyright © 1999 The Free Software Foundation
Copyright © 2000 ðÁ×ÅÌ ûÁÊÄÏ. ðÅÒÅ×ÏÄ

òÁÚÒÅÛÁÅÔÓÑ ËÏÐÉÒÏ×ÁÎÉÅ, ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÅ É/ÉÌÉ ÍÏÄÉÆÉËÁÃÉÑ ÜÔÏÇÏ ÄÏËÕÍÅÎÔÁ ÎÁ ÕÓÌÏ×ÉÑÈ GNU Free Documentation License, Version 1.1 ÉÌÉ ÌÀÂÏÊ ÄÒÕÇÏÊ ÂÏÌÅÅ ÐÏÚÄÎÅÊ ×ÅÒÓÉÉ, ÏÐÕÂÌÉËÏ×ÁÎÎÏÊ Free Software Foundation; ÂÅÚ éÎ×ÁÒÉÁÎÔÏÙÈ ÒÁÚÄÅÌÏ×, ôÅËÓÔ× ÐÅÒÅÄÎÅÊ ïÂÌÏËÉ É ôÅËÓÔ× úÁÄÎÅÊ ïÂÌÏËÉ. ëÏÐÉÑ ÌÉÃÅÎÚÉÉ ÎÁÈÏÄÉÔÓÑ × ÐÒÉÌÏÅÎÉÉ "GNU Free Documentation License".

îÁÐÒÁ×ÌÑÊÔÅ ×ÏÐÒÏÓÙ, ÏÐÉÓÁÎÉÑ ÏÛÉÂÏË É ÐÒÅÄÌÏÖÅÎÉÑ ÐÏ ÓÏÄÅÒÖÁÎÉÀ ÄÁÎÎÏÇÏ ÒÕËÏ×ÏÄÓÔ×Á ÍÁÊËÕ üÛÌÉ (Mike Ashley) (<jashley@acm.org>). (üÔÏ ÏÔÎÏÓÉÔÓÑ Ë ÁÎÇÌÉÊÓËÏÊ ×ÅÒÓÉÉ)

úÁÍÅÞÁÎÉÑ É ÐÒÅÄÌÏÖÅÎÉÑ ÏÔÎÏÓÉÔÅÌØÎÏ ÐÅÒÅ×ÏÄÁ ÎÁÐÒÁ×ÌÑÊÔÅ ðÁ×ÌÕ ûÁÊÄÏ (<zwon@e-mail.ru>).

äÒÕÇÉÅ ËÏÎÔÒÉÂØÀÔÏÒÙ ÄÁÎÎÏÇÏ ÒÕËÏ×ÏÄÓÔ×Á íÜÔØÀ ëÏÕÐÌÜÎÄ (Matthew Copeland), êÏÒÇÅÎ çÒÜÎ (Joergen Grahn), äÜ×ÉÄ á. ÷ÉÌÅÒ (David A. Wheeler). J Horacio MG ÐÅÒÅ×ÅÌ ÜÔÏÔ ÄÏËÕÍÅÎÔ ÎÁ ÉÓÐÁÎÓËÉÊ.

1. âÙÓÔÒÙÊ ÓÔÁÒÔ 13
1.1. çÅÎÅÒÁÃÉÑ ÎÏ×ÏÊ ÐÁÒÙ ËÌÀÞÅÊ 13
1.1.1. óÏÚÄÁÎÉÅ ÏÔÚÙ×ÁÀÝÅÇÏ ÓÅÒÔÉÆÉËÁÔÁ 16
1.2. ïÂÍÅÎ ËÌÀÞÁÍÉ 16
1.2.1. üËÓÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ 17
1.2.2. éÍÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ 17
1.3. úÁÛÉÆÒÏ×ÁÎÉÅ É ÒÁÓÛÉÆÒÏ×ÁÎÉÅ ÄÏËÕÍÅÎÔÏ× 19
1.4. ðÏÄÐÉÓÉ É ÉÈ ÐÒÏ×ÅÒËÁ 21
1.4.1. ðÒÏÚÒÁÞÎÏ ÐÏÄÐÉÓÁÎÎÙÅ(Clearsigned) ÄÏËÕÍÅÎÔÙ 22
1.4.2. ïÔÄÅÌÅÎÎÁÑ ÐÏÄÐÉÓØ 22
2. Concepts 25
2.1. óÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ 25
2.2. ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ 26
2.3. óÍÅÛÁÎÎÙÅ ÛÉÆÒÙ 28
2.4. ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ 29
3. õÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ 33
3.1. õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÐÁÒÏÊ ËÌÀÞÅÊ 33
3.1.1. ãÅÌÏÓÔÏÓÔØ ËÌÀÞÁ. 35
3.1.2. äÏÂÁ×ÌÅÎÉÅ É ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ 36
3.1.3. ïÚÙ× ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ 38
3.1.4. éÚÍÅÎÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ 40
3.2. ðÒÏ×ÅÒËÁ ÄÏÓÏ×ÅÒÏÓÔÉ ËÌÀÞÅÊ × ÷ÁÛÅÊ Ó×ÑÚËÅ 41
3.2.1. äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ 42
3.2.2. éÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏ×ÅÒÉÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÏ×ÅÒÏÓÔÉ ËÌÀÞÅÊ 44
3.3. òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÅÊ 47
4. åÖÅÄÎÅ×ÎÏÅ ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG 51
4.1. ïÐÒÅÄÅÌÅÎÉÅ ÷ÁÛÉÈ ÔÒÅÂÏ×ÁÎÉÊ Ë ÚÁÝÉÔÅ 51
4.1.1. ÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ 52
4.1.2. úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ 53

4.1.3. ÷ÙÂÏÒ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ É ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏÐÏÎÎÉÔÅÌØÎÙÈ ËÌÀÞÅÊ 55
4.1.4. õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ. 57
4.2. ðÏÓÔÒÏÅÎÉÅ ÷ÁÛÅÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ 58
4.3. úÁËÏÎÎÏÓÔØ ÉÓÐÌØÚÏ×ÁÎÉÑ GnuPG 60
5. ÒÁÚÌÉÞÎÙÅ ×ÏÐÒÏÓÙ 61
5.1. îÁÐÉÓÁÎÉÅ ÐÎØÚÏ×ÂÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ 61
I. óÐÉÓÏË ËÎÍÁÎÄ 65
sign 67
detach-signature 67
encrypt 68
symmetric 69
decrypt 69
clearsign 70
verify 71
gen-key 71
gen-revoke 72
send-keys 73
recv-keys 73
list-keys 74
list-public-keys 75
list-secret-keys 75
list-sigs 76
check-sigs 77
fingerprint 78
import 78
fast-import 79
export 80
export-all 80
export-secret-keys 81
edit-key 82
sign-key 86
lsign-key 87

delete-key 88
delete-secret-key 88
store 89
export-ownertrust 90
import-ownertrust 90
update-trustdb 91
print-md 92
gen-random 92
gen-prime 93
version 94
warranty 94
help 95
II. óÐÉÓÏË ÏÐÃÉÊ 97
keyserver 99
output 99
recipient 100
default-recipient 100
default-recipient-self 101
no-default-recipient 102
encrypt-to 103
no-encrypt-to 103
armor 104
no-armor 105
no-greeting 105
no-secmem-warning 106
batch 107
no-batch 107
local-user 108
default-key 109
completes-needed 109
marginals-needed 110
load-extension 111
rfc1991 112

allow-non-selfsigned-uid 112
cipher-algo 113
compress-algo 114
z 115
verbose 115
no-verbose 116
quiet 117
textmode 117
dry-run 118
interactive 119
yes 119
no 120
always-trust 121
skip-verify 121
keyring 122
secret-keyring 123
no-default-keyring 123
homedir 124
charset 125
no-literal 126
set-filesize 126
with-fingerprint 127
with-colons 128
with-key-data 128
lock-once 129
lock-multiple 130
passphrase-fd 130
force-mdc 131
force-v3-sigs 132
openpgp 132
utf8-strings 133
no-utf8-strings 134
no-options 135
debug 135

debug-all 137
status-fd 137
logger-fd 138
no-comment 139
comment 139
default-comment 140
no-version 141
emit-version 141
notation-data 142
set-policy-url 143
set-filename 143
use-embedded-filename 144
max-cert-depth 145
digest-algo 146
s2k-cipher-algo 146
s2k-digest-algo 147
s2k-mode 148
disable-cipher-algo 148
disable-pubkey-algo 149
throw-keyid 150
not-dash-escaped 151
escape-from-lines 151
A. GNU Free Documentation License 153
0. PREAMBLE 153
1. APPLICABILITY AND DEFINITIONS 153
2. VERBATIM COPYING 155
3. COPYING IN QUANTITY 155
4. MODIFICATIONS 156
5. COMBINING DOCUMENTS 158
6. COLLECTIONS OF DOCUMENTS 159
7. AGGREGATION WITH INDEPENDENT WORKS 159
8. TRANSLATION 160
9. TERMINATION 160

10. FUTURE REVISIONS OF THIS LICENSE.....161
How to use this License for your documents.....161

3-1. ðÒÉÍÅÒ ÓÅÔÉ ÄÏ×ÅÒÉÑ 46

1. âÙÓÔÒÙÊ ÓÔÁÒÔ

GnuPG - ÉÎÓÔÒÕÍÅÎÔ ÄÌÑ ÚÁÝÉÔÙ ËÏÍÍÕÎÉËÁÃÉÊ. üÔÁ ÇÌÁ×Á ËÏÒÏÔËÏ ÏÐÉÓÙ×ÁÅÔ ÏÓÎ×Ù ÒÁÂÏÔÙ Ó GnuPG, ×ËÌÀÞÁÑ ÓÏÚÄÁÎÉÅ ÐÁÒ ËÌÀÞÅÊ, ÏÂÍÅÎ ËÌÀÞÁÍÉ É ÉÈ ÐÒÏ×ÅÒÕ, ÚÁÛÉÆÒÏ×ËÕ É ÒÁÓÛÉÆÒÏ×ËÕ ÄÏËÕÍÅÎÔÏ×, ÚÁ×ÅÒÅÎÉÅ ÄÏËÕÍÅÎÔÏ× ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓØÀ. ïÎÁ ÎÅ ÏÐÉÓÙ×ÁÅÔ × ÄÅÔÁÌÑÈ ÐÒÉÎÃÉÐÙ ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÛÉÆÒÏ×ÁÎÉÑ É ÃÉÆÒÏ×ÙÈ ÐÏÄÐÉÓÅÊ. üÔÉ ×ÏÐÒÏÓÙ ÒÁÓÍÁÔÒÉ×ÁÀÓÑ × ÇÌÁ×Å 2. úÄÅÓØ, ÔÁËÖÅ, ÎÅ ÒÁÓÍÁÔÒÉ×ÁÀÔÓÑ ÔÏÎËÏÓÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG. üÔÉ ×ÏÐÒÏÓÙ ÒÁÓÍÁÔÒÉ×ÁÀÔÓÑ × ÇÌÁ×ÁÈ 3 É 4.

GnuPG ÉÓÐÏÌØÚÕÅÔ ËÒÉÐÔÏÇÒÁÆÉÀ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. ëÁÖÄÙÊ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÅÅÔ ÐÁÒÕ ËÌÀÞÅÊ (keypair), ÓÏÓÔÏÑÝÕÀ ÉÚ *ÓÅËÒÅÔÎÏÇÏ (private)* É *ÏÔËÒÙÔÏÇÏ (public)* ËÌÀÞÅÊ. óÅËÒÅÔÎÙÊ ËÌÀÞ Ñ×ÌÑÅÔÓÑ ÓÅËÒÅÔÎÏÍ ÐÏÌØÚÏ×ÁÔÅÌÑ É ÎÅ ÍÏÖÅÔ ÂÙÔØ ÐÒÅÄÁÎ ÄÒÕÇÏÍÕ ÌÉÃÕ, ÎÉ ÐÒÉ ËÁËÉÈ ÏÂÓÔÏÑÔÅÌØÓÔÁÈ. ïÔËÒÙÔÙÊ ËÌÀÞ ÐÒÅÄÁÅÔÓÑ ×ÓÅÍ ÌÀÄÑÍ, Ó ËÏÔÏÒÙÍÉ ÐÏÌØÚÏ×ÁÔÅÌØ ÂÕÄÅÔ ÏÂÍÅÎÉ×ÁÔØÓÑ ÓÏÌÁŸÅÎÉÑÍÉ. GnuPG ÉÓÐÏÌØÚÕÅÔ ÎÅÓËÏÌØËÏ ÂÏÌÅÅ ÈÉÔÒÏÕÍÕÔÀ ÓÈÅÍÕ, ÐÒÉ ËÏÔÏÒÏÊ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÅÅÔ ÐÅ×ÉÞÎÕÀ ÐÁÒÕ ËÌÀÞÅÊ É, ×ÚÍÏÖÎÏ, ÄÏÐÏÌÎÉÔÅÌØÎÏ ÎÅÓËÏÌØËÏ ÐÏÄÞÉÎÅÎÎÙÈ. ðÅÒ×ÉÞÎÁÑ É ÐÏÄÞÉÎÅÎÎÙÅ ÐÁÒÙ ÏÂßÄÉÎÅÎÙ, ÄÌÑ ÕÐÒÏŸÅÎÉÑ ÉÈ ÉÓÐÏÌØÚÏ×ÁÎÉÑ, É ÜÔÁ Ó×ÑÚËÁ, ÚÁÞÁÓÔÕÀ, ÍÖÅÔ ÒÁÓÍÁÔÒÉ×ÁÔØÓÑ ÐÒÏÓÔÏ, ËÁË ÏÄÎÁ ÐÁÒÁ ËÌÀÞÅÊ.

1.1. çÅÎÅÒÁÃÉÑ ÏÌ×ÏÊ ÐÁÒÙ ËÌÀÞÅÊ

äÌÑ ÓÏÚÄÁÎÉÑ ÐÅÒ×ÉÞÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--gen-key`

```
alice% gpg --gen-key
gpg (GnuPG) 0.9.4; Copyright (C) 1999 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
```

```
Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (4) ElGamal (sign and encrypt)
Your selection?
```

GnuPG ÍÏÖÅÔ ÓÏÚÄÁ×ÁÔØ ÎÅÓËÏÌØËÏ ÒÁÚÎÙÈ ÔÉÐÏ× ËÌÀÞÅÊ, ÎÏ ÐÅÒ×ÉÞÎÙÊ ËÌÀÞ ÄÏÌÖÅÎ ÂÙÔØ ÐÒÉÇÏÄÅÎ ÄÌÑ ÓÏÚÄÁÎÉÑ ÐÏÄÐÉÓÉ (signature). ðÏÜÔÏÍÕ ÅÓÔØ ÔÌØËÏ ÔÒÉ ×ÁÒÉÁÎÔÁ. ÷ÁÒÉÁÎÔ 1 ÓÏÚÄÁÅÔ Ä×Å ÐÁÒÙ ËÌÀÞÅÊ. DSA - ÐÅÒ×ÉÞÎÁÑ, ÉÓÐÏÌØÚÕÅÍÁÑ ÔÏÌØËÏ ÄÌÑ ÐÏÄÐÉÓÉ. ElGamal - ÐÏÄÞÉÎÅÎÎÁÑ, ÉÓÐÏÌØÚÕÅÍÁÑ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ÷ÁÒÉÁÎÔ 2 ÐÏËÏÖ, ÎÏ ÓÏÚÄÁÅÔ ÔÌØËÏ ÐÁÒÕ DSA. ÷ÁÒÉÁÎÔ 4[1] ÓÏÚÄÁÅÔ ÔÌØËÏ ÐÁÒÕ ElGamal, ÉÓÐÏÌØÚÕÅÍÕÀ É ÄÌÑ ÐÏÄÐÉÓÉ É ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ÷ ÌÀÂÏÍ ÓÌÕÞÁÅ, ÐÏÚÖÅ ÍÏÖÎÏ ÓÏÚÄÁÔØ ÄÏÐÏÎÉÔÅÌØÎÙÅ ÐÁÒÙ ËÌÀÞÅÊ ÄÌÑ ÐÏÄÐÉÓÉ É ÛÉÆÒÏ×ÁÎÉÑ. âÏÌØÛÉÎÓÔ×Õ ÐÏÌØÚÏ×ÁÔÅÌÅÊ ÐÏÄÏÊÄÅÔ ×ÁÒÉÁÎÔ 1.

ôÁËÖÅ ÷Ù ÄÏÌÖÎÙ ×ÙÂÒÁÔØ ÒÁÚÍÅÒ ËÌÀÞÁ. òÁÚÍÅÒ ËÌÀÞÁ DSA ÄÏÌÖÅÎ ÂÙÔØ ÍÅÖÄÕ 512 É 1024 ÂÉÔ. ëÌÀÞ ElGamal ÍÏÖÅÔ ÂÙÔØ ÌÀÂÏÇÏ ÒÁÚÍÅÒÁ. ïÂÙÞÎÏ, GnuPG ÔÒÅÂÕÅÔ ËÌÀÞÉ ÎÅ ËÏÒÏÞÅ 768 ÂÉÔ. ôÁËÉÍ ÏÂÒÁÚÏÍ, ÅÓÌÉ ÷Ù ×ÙÂÒÁÌÉ ×ÁÒÉÁÎÔ 1 É ÒÁÚÍÅÒ ËÌÀÞÁ ÂÏØÛÅ 1024 ÂÉÔ, ÔÏ ËÌÀÞ ElGamal ÂÕÄÅÔ ÉÍÅÔØ ÕËÁÚÁÎÎÕÀ ÒÁÚÍÅÒ, Á ËÌÀÞ DSA - 1024 ÂÉÔÁ.

```
About to generate a new ELG-E keypair.
              minimum keysize is  768 bits
              default keysize is 1024 bits
    highest suggested keysize is 2048 bits
What keysize do you want? (1024)
```

âÏÌØÛÉÊ ÒÁÚÍÅÒ ËÌÀÞÁ ÄÁÅÔ ÂÏØÛÕÀ ÚÁÝÉÔÕ ÏÔ ×ÚÌÏÍÁ, ÎÏ ÒÁÚÍÅÒ ÐÏ ÕÍÏÌÞÁÎÉÀ ÄÏÓÔÁÔÏÞÅÎ ÐÒÁËÔÉÞÅÓËÉ ÄÌÑ ÌÀÂÙÈ ÃÅÌÅÊ. âÏØÛÁÑ ÄÌÉÎÁ ËÌÀÞÁ ÚÁÍÅÄÌÑÅÔ ÚÁÛÉÆÒÏ×ËÕ É ÒÁÓÛÉÆÒÏ×ËÕ É ÍÏÖÅÔ ÏÔÒÁÚÉÔØÓÑ ÎÁ ÄÌÉÎÅ ÓÉÇÎÁÔÕÒÙ. òÁÚÍÅÒ ËÌÀÞÁ ÎÅÌØÚÑ ÂÕÄÅÔ ×ÐÏÌÅÄÓÔ×ÉÉ ÉÚÍÅÎÉÔØ.

îÁËÏÎÅÃ, ÷Ù ÄÏÌÖÎÙ ÕËÁÚÁÔØ ÓÒÏË ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ. ÷ ÓÌÕÞÁÅ ×ÁÒÉÁÎÔÁ 1, ÕËÁÚÁÎÎÙÊ ÓÒÏË ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÏÂÏÉÈ ËÌÀÞÅÊ.

```
Please specify how long the key should be valid.
         0 = key does not expire
```

```
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
```

âÏÌØÛÉÎÓÔ×Õ ÐÏÌØÚÏ×ÁÔÅÌÅÊ ÐÏÄÏÊÄÅÔ ÂÅÓÓÒÏÞÎÙÊ ËÌÀÞ. óÒÏË ÄÅÊÓÔ×ÉÑ ÓÌÅÄÕÅÔ ×ÙÂÉÒÁÔØ Ó ÏÓÔÏÒÏÖÎÓÔØÀ; ÈÏÔÑ ÍÏÖÎ ÉÚÍÅÎÉÔØ ÓÒÏË ÄÅÊÓÔ×ÉÑ ÐÏÓÌÅ ÓÏÚÄÁÎÉÑ ËÌÀÞÁ, ÎÅ ÉÓËÌÀÞÅÎÙ ÐÒÏÂÌÅÍÙ Ó ÐÅÒÅÄÁÞÅÊ ÉÚÍÅÎÅÎÉÊ ÔÅÍ ÐÏÌØÚÏ×ÁÔÅÌÑÍ, Õ ËÏÔÏÒÙÈ ÕÖÅ ÉÍÅÅÔÓÑ ÷ÁÛ ÏÔËÒÙÔÙÊ ËÌÀÞ.

÷ ÄÏÐÏÌÎÉÔÅÌØÎÏÍ ÐÒÉÍÅÒÅ ÷Ù ÄÏÌÖÎÙ ÕËÁÚÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ. éÄÅÎÔÉÆÉËÁÔÏÒ ÎÕÖÅÎ, ÞÔÂÙ Ó×ÑÚÁÔØ ÓÏÚÄÁÎÎÙÊ ËÌÀÞ Ó ËÏÎËÒÅÔÎÙÍ ÌÉÃÏÍ.

```
äÌÑ ÉÄÅÎÔÉÆÉËÁÃÉÉ ËÌÀÞÁ ÎÅÏÂÈÏÄÉÍ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ; ÐÒÏÇÒÁÍÍÁ
ËÏÎÓÔÒÕÉÒÕÅÔ ÅÇÏ ÉÚ ÐÏÌÎÏÇÏ ÍÍÅÎÉ ÐÏÌØÚÏ×ÁÔÅÌÑ, ËÏÍÐÁÎÉÏÁÌÅÑ É ÁÄÒÅÓÁ email × ×ÉÄÅ:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name:
```

ðÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÓÏÚÄÁÅÔÓÑ ÔÏÌØËÏ ÏÄÎÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÎÏ ×ÏÚÍÏÖÎÏ ÓÏÚÄÁÎÅÁ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ×, ÅÓÌÉ ÷Ù ÈÏÔÉÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ ËÌÀÞ × ÎÅÓËÏÌØËÉÈ ËÏÎÔÅËÓÔÁÈ; ÎÁÐÒÉÍÅÒ, ËÁË ÉÎÖÅÎÅÒ ÎÁ ÒÁÂÏÔÅ É ËÁË ÐÏÉÔÉÞÅÓËÉÊ ÄÅÑÔÅÌØ ÐÏÓÌÅ ÎÅÅ. éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÎÅ ÍÖÅÔ ÂÙÔØ ÏÔÒÅÄÁËÔÉÒÏ×ÁÎ ÐÏÓÌÅ ÓÏÚÄÁÎÉÑ.

GnuPG ÚÁÐÒÏÓÉÔ ÐÁÒÏÌØ ÄÌÑ ÚÁÝÉÔÙ ÐÅÒ×ÉÞÎÏÇÏ É ÐÏÄÞÉÎÅÎÎÏÇÏ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ, ËÏÔÏÒÙÅ ÷Ù ÂÕÄÅÔÅ ÄÅÒÖÁÔØ × ÎÅÄÏÓÔÕÐÎÏÍ ÄÌÑ ÄÒÕÇÉÈ ÍÅÓÔ.

```
You need a Passphrase to protect your private key.

Enter passphrase:
```

îÁ ÄÌÉÎÕ ÐÁÒÏÌÑ ÎÅÔ ÏÇÒÁÎÉÞÅÎÉÊ, É ÅÇÏ ÓÌÅÄÕÅÔ ×ÙÂÉÒÁÔØ ÔÝÁÔÅÌØÎÏ. ó ÔÏÞËÉ ÚÒÅÎÉÑ ÂÅÚÏÐÁÓÏÓÔÉ, ÐÁÒÏÌØ ÄÌÑ ÚÁÝÉÔÙ ËÌÀÞÁ ÏÐÅÒÁÖÉÏ × GnuPG (É ÄÒÕÇÉÈ ÓÉÓÔÅÍÁÈ Ó ÎÔËÒÙÔÙÍ ËÌÀÞÏÍ), Ô.Ë. ÜÔÏ ÷ÁÛÁ ÄÄÉÎÓÔ×ÅÎÎÁÑ ÚÁÝÉÔÁ × ÓÌÕÞÁÅ, ÅÓÌÉ ÷ÁÛ ÓÅËÒÅÔÎÙÊ

ËÌÀÞ ÐÏÐÁÄÅÔ × ÞÕÖÉÅ ÒÕËÉ. îÅ ÓÌÅÄÕÅÔ ÂÒÁÔØ ÓÌÏ×Á ÉÚ âóü, ÞÅÒÅÄÕÊÅ ÒÅÇÉÓÔÒ ÂÕË× É ÉÓÐÏÌØÚÕÊÔÅ ÎÅÁÌÆÁ×ÉÔÎÅ ÓÉÍ×ÏÌÙ. èÏÒÏÛÉÊ ÐÁÒÏÌØ ËÒÉÔÉÞÅÎ ÄÌÑ ÎÁÄÅÖÎÏÓÔÉ GnuPG.

1.1.1. óÏÚÄÁÎÉÅ ÏÔÚÙ×ÁÀÝÅÇÏ ÓÅÒÔÉÆÉËÁÔÁ

ðÏÓÌÅ ÓÏÚÄÁÎÉÑ ÐÁÒÙ ËÌÀÞÅÊ, ÷ÁÍ ÓÌÅÄÕÅÔ ÓÏÚÄÁÔØ ÏÔÚÙ×ÁÀÝÉÊ ÓÅÒÔÉÆÉËÁÔ (revokation certificate) ÄÌÑ ÐÅÒ×ÉÞÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÉÓÐÏÌØÚÕÑ ËÏÍÁÎÄÕ `--gen-revoke`. åÓÌÉ ÷Ù ÚÁÂÕÄÅÔÅ ÐÁÒÏÌØ, ÌÉÂÏ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÂÕÄÅÔ ÐÏÉÝÅÎ ÉÌÉ ÕÔÅÒÑÎ, ÜÔÏ ÓÅÒÔÉÆÉËÁÔ ÍÏÅÔ ÂÙÔØ ÒÁÚÏÓÌÁÎ ÄÌÑ Õ×ÅÄÏÌÅÎÑ Ï ÔÏÍ, ÞÔÏ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÅÌØÚÑ ÂÏÌØÛÅ ÉÓÐÏÌØÚÏ×ÁÔØ. ïÔÏÚ×ÁÎÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÐÒÏ×ÅÒÏÞÎÙÈ ÷ÁÍÉ ÐÏÄÐÉÓÅÊ É ÄÁÌØÛÅ, ÎÉ ÏÎ ÎÅ ÍÏÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÓÏÎÂÝÅÎÉÊ ÄÌÑ ÷ÁÓ. ôÁËÖÅ ÷Ù ÓÏÈÒÁÎÑÅÔÅ ×ÏÚÍÏÖÎÏÓÔØ ÒÁÓÛÉÆÒÏ×ËÉ ÐÏÌÁÎÎÙÈ ÷ÁÍ ÓÏÎÂÝÅÎÉÊ, ÐÒÉ ÎÁÌÉÞÉÉ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ.

```
alice% gpg --output revoke.asc --gen-revoke mykey
[...]
```

áÒÇÕÍÅÎÔ **`mykey`** - ÉÄÅÎÔÉÆÉËÁÔÏÒ ÷ÁÛÅÊ ÐÒ×ÉÞÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ ÉÌÉ ÌÀÂÁÑ ÞÁÓÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÎØÚÏ×ÁÔÅÌÑ ÷ÁÛÅÊ ÐÁÒÙ ËÌÀÞÅÊ. óÇÅÎÅÒÉÒÏ×ÁÎÎÙÊ ÓÅÒÔÉÆÉËÁÔ ÂÕÄÅÔ ÓÏÈÒÁÎÅÎ × ÆÁÊÌÅ *`revoke.asc`*. åÓÌÉ ÏÐÃÉÑ `--output` ÏÐÕÝÅÎÁ, ÒÅÚÕÌØÔÁÔ ÐÏÍÝÅÝÅÔÓÑ × ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ. ÷Ù ÍÏÖÅÔ ×Ù×ÅÓÔÉ ÓÅÒÔÉÆÉËÁÔ ÍÁ ÐÒÉÎÔÅÒ É ÈÒÁÎÉÔØ ÅÇÏ ÇÄÅ-ÎÉÂÕÄØ × ÎÁÄÅÖÎÏÍ ÍÅÓÔÅ (ÂÁÎËÏ×ÓËÉÊ ÓÅÊÆ ÐÏÄÏÊÄÅÔ). åÓÌÉ ÓÅÒÔÉÆÉËÁÔ ÐÏÐÁÄÅÔ × ÞÕÖÉÅ ÒÕËÉ É ÂÕÄÅÔ ÏÐÕÂÌÉËÏ×ÁÎ, ÔÏ ÏÔËÒÙÔÙÊ ËÌÀÞ ÕÔÒÁÔÉÔ Ó×ÏÅ ÄÅÊÓ×ÉÅ.

1.2. ïÂÍÅÎ ËÌÀÞÁÍÉ

äÌÑ ÏÂÝÅÎÉÑ Ó ËÅÍ-ÌÉÂÏ, ×Ù ÄÏÌÖÎÙ ÏÂÍÅÎÑÔØÓÑ ËÌÀÞÁÍÉ. ðÒÏÍÏÔÒÅÔØ

ÓÐÉÓÏË ÉÍÅÀÝÉÈÓÑ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ, ÍÏÖÎÏ ÉÓÐÏÌØÚÕÑ ËÏÍÁÎÄÕ `--list-keys`.

```
alice% gpg --list-keys
/users/alice/.gnupg/pubring.gpg
------------------------------------
pub  1024D/BB7576AC 1999-06-04 Alice (Judge) <alice@cyb.org>
sub  1024g/78E9A8FA 1999-06-04
```

1.2.1. üËÓÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ

ðÅÒÅÄ ÔÅÍ ËÁË ÐÏÓÌÁÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ ËÏÍÕ-ÌÉÂÏ, ÷Ù ÄÏÌÖÎÙ ÅÇÏ ÜËÓÐÏÒÔÉÒ×ÁÔØ. äÌÑ ÜÔÏÇÏ ÉÓÐÏÌØÚÕÊÔÅ ËÏÍÁÎÄÕ `--export`. åÊ ÔÒÅÂÕÅÔÓÑ, ÄÏÐÏÌÎÉÔÅÌØÎÏ, ÁÒÇÕÍÅÎÔ, ÉÄÅÎÔÉÆÉËÁÔÏÒ ÜËÓÐÏÒÔÉÒÕÅÍÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, ËÁË É `--gen-revoke`.

```
alice% gpg --output alice.gpg --export alice@cyb.org
```

ëÌÀÞ ÜËÓÐÏÒÔÉÒÕÅÔÓÑ × Ä×ÏÉÞÎÎÍ ÆÏÒÍÁÔÅ, ÞÔÏ ÂÙ×ÁÅÔ ÎÅÕÄÏÂÎÏ. GnuPG ÉÍÅÅÔ ÏÐÃÉÀ ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÉ `--armor`, ËÏÔÏÒÁÑ ÕËÁÚÙ×ÁÅÔ ÎÁ ÎÅÏÂÈÏÄÉÍÏÓÔØ ×Ù×ÏÄÁ × ÆÏÒÍÁÔÅ ASCII. ðÒÁËÔÉÞÅÓËÉ ÌÀÂÏÊ ×Ù×ÏÄ GnuPG, Ô.Å. ËÌÀÞÉ, ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÏËÕÍÅÎÔÙ, ÐÏÄÐÉÓÉ, ÍÏÖÅÔ ÐÒÏÐÕÓËÏÄÉÔØ × ÆÏÒÍÁÔÅ ASCII.[2]

```
alice% gpg --armor --export alice@cyb.org
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v0.9.7 (GNU/Linux)
Comment: For info see http://www.gnupg.org

[...]
-----END PGP PUBLIC KEY BLOCK-----
```

1.2.2. éÍÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ

ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÄÏÂÁ×ÌÅÎ Ë ÍÎÏÖÅÓÔ×Õ ÷ÁÛÉÈ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÐÒÉ ÐÏÍÏÝÉ ËÏÍÁÎÄÙ `--import`.

```
alice% gpg --import blake.gpg
```

```
gpg: key 9E98BC16: public key imported
gpg: Total number processed: 1
gpg:               imported: 1
alice% gpg --list-keys
/users/alice/.gnupg/pubring.gpg
---------------------------------------
pub  1024D/BB7576AC 1999-06-04 Alice (Judge) <alice@cyb.org>
sub  1024g/78E9A8FA 1999-06-04

pub  1024D/9E98BC16 1999-06-04 Blake (Executioner) <blake@cyb.org>
sub  1024g/5C8CBD41 1999-06-04
```

äÏÓÔÏ×ÅÒÎÏÓÔØ ÉÍÐÏÒÔÉÒÏ×ÁÎÎÏÇÏ ËÌÀÞÁ ÄÏÌÖÎÁ ÂÙÔØ ÐÏÄÔ×ÅÒÖÄÅÎÁ. GnuPG ÉÓÐÏÌØÚÕÅÔ ÇÉÂËÕÀ É ÍÏÝÎÕÀ ÍÏÄÅÌØ ÐÒÏ×ÅÒËÉ ÐÏÄÌÉÎÎÏÓÔÉ, ÎÅ ÔÒÅÂÕÀÝÕÀ, ÞÔÏÂÙ ÷Ù ÌÉÞÎÏ ÐÒÏ×ÅÒÑÌÉ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÁÖÄÏÇÏ ÉÍÐÏÒÔÉÒÏ×ÁÎÎÏÇÏ ËÌÀÞÁ. ôÅÍ ÎÅ ÍÅÎÅÅ, ÄÏÓÔÏ×ÅÒÎÏÓÔØ ÎÅËÏÔÏÒÙÈ ËÌÀÞÅÊ ÷ÁÍ ÐÒÉÄÅÔÓÑ ÐÒÏ×ÅÒÉÔØ ÓÁÍÏÍÕ. óÎÁÞÁÌÁ ÐÒÏ×ÅÒÑÀÔÓÑ ÏÔÐÅÞÁÔËÉ(fingerprint) ËÌÀÞÁ, ÚÁÔÅÍ ÏÎ ÚÁ×ÅÒÑÅÔÓÑ ÐÏÄÐÉÓØÀ, ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÔÏÇÏ, ÞÔÏ ËÌÀÞ ÄÏÓÔÏ×ÅÒÅÎ. ïÔÐÅÞÁÔËÉ ËÌÀÞÁ ÍÏÖÎÏ ÂÙÓÔÒÏ ÐÒÏÓÍÏÔÒÅÔØ ËÏÍÁÎÄÏÊ `--fingerprint`, ÎÏ ÄÌÑ ÚÁ×ÅÒÅÎÉÑ ËÌÀÞÁ ÷Ù ÄÏÌÖÎÙ ÏÔÒÅÄÁËÔÉÒÏ×ÁÔØ ÅÇÏ.

```
alice% gpg --edit-key blake@cyb.org

pub  1024D/9E98BC16  created: 1999-06-04 expires: never      trust: -/q
sub  1024g/5C8CBD41  created: 1999-06-04 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Command> fpr
pub  1024D/9E98BC16 1999-06-04 Blake (Executioner) <blake@cyb.org>
             Fingerprint: 268F 448F CCD7 AF34 183E  52D8 9BDE 1A08 9E98 BC16
```

ïÔÐÅÞÁÔËÉ ËÌÀÞÁ ÐÒÏ×ÅÒÑÀÔÓÑ ÅÇÏ ×ÌÁÄÅÌØÃÅÍ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÓÄÅÌÁÎÏ ÐÒÉ ÌÉÞÎÏÊ ×ÓÔÒÅÞÅ, ÐÏ ÔÅÌÅÆÏÎÕ, ÉÌÉ ÌÀÂÙÍ ÄÒÕÇÉÍ ÓÐÏÓÏÂÏÍ, ÇÁÒÁÎÔÉÒÕÀÝÉÍ, ÞÔÏ ÷Ù ÏÂÝÁÅÔÅÓØ Ó ×ÌÁÄÅÌØÃÅÍ ËÌÀÞÁ. åÓÌÉ ÏÔÐÅÞÁÔËÉ ÐÏÌÕÞÅÎÎÙÅ ÷ÁÍÉ ÓÏ×ÐÁÄÁÀÔ Ó ÕËÁÚÁÎÎÙÍÉ ×ÌÁÄÅÌØÃÅÍ ËÌÀÞÁ, ÔÏ ÍÏÖÅÔÅ ÂÙÔØ Õ×ÅÒÅÎÙ, ÞÔÏ ÏÂÌÁÄÁÅÔÅ ÄÏÓÔÏ×ÅÒÎÏÊ ËÏÐÉÅÊ ËÌÀÞÁ.

ðÏÓÌÅ ÐÒÏ×ÅÒËÉ ÏÔÐÅÞÁÔËÏ× ÷Ù ÍÏÖÅÔÅ ÐÏÄÐÉÓÁÔØ ËÌÀÞ. ôÁË ËÁË ÐÒÏ×ÅÒËÁ ËÌÀÞÁ ÓÌÁÂÏÅ Ú×ÅÎÏ × ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ,

ÔÏ ÷Ù ÄÏÌÖÎÙ ÂÙÔØ ÓÏ×ÅÒÛÅÎÎÏ Õ×ÅÒÅÎÙ × ËÌÀÞÅ ÐÅÒÅÄ ÔÅÍ, ËÁË ÅÇÏ ÐÏÄÐÉÓÙ×ÁÔØ, É ×*ÓÅÇÄÁ* ÐÒÏ×ÅÒÑÊÔÅ ÏÔÐÅÞÁÔËÉ.

```
Command> sign

pub  1024D/9E98BC16  created: 1999-06-04 expires: never      trust: -/q
             Fingerprint: 268F 448F CCD7 AF34 183E  52D8 9BDE 1A08 9E98 BC16

     Blake (Executioner) <blake@cyb.org>

Are you really sure that you want to sign this key
with your key: "Alice (Judge) <alice@cyb.org>"

Really sign?
```

ðÏÄÐÉÓÁ× ËÌÀÞ, ÷Ù ÍÏÖÅÔÅ ÐÒÏÍÏÔÏÒÅÔØ ÓÐÉÓÏË ÐÏÄÐÉÓÅÊ ÎÁ ËÌÀÞÅ É Õ×ÉÄÅÔØ ÔÁÍ ÄÏÂÁ×ÌÅÎÎÕÀ ÷ÁÍÉ. ëÁÖÄÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏØÚÏ×ÁÔÅÌÑ ËÌÀÞÁ ÐÏÄÐÉÓÁÎ ÜÔÉÍ ËÌÀÞÏÍ É ËÁÖÄÙÍ ÐÏØÚÏ×ÁÔÅÌÅÍ, ÚÁ×ÅÒÉ×ÛÉÍ ÜÔÏÔ ËÌÀÞ.

```
Command> check
uid  Blake (Executioner) <blake@cyb.org>
sig!       9E98BC16 1999-06-04   [self-signature]
sig!       BB7576AC 1999-06-04   Alice (Judge) <alice@cyb.org>
```

1.3. úÁÛÉÆÒÏ×ÁÎÉÅ É ÒÁÓÛÉÆÒÏ×ÁÎÉÅ ÄÏËÕÍÅÎÔÏ×

ïÔËÒÙÔÙÊ É ÓÅËÒÅÔÎÙÊ ËÌÀÞÉ, ÉÇÒÁÀÔ ËÁÖÄÙÊ Ó×ÏÀ ÒÏÌØ ÐÒÉ ÚÁÛÉÆÒÏ×ËÅ É ÒÁÓÛÉÆÒÏ×ËÅ ÄÏËÕÍÅÎÔÏ×. ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÎÏ ÐÒÅÄÓÔ×ÉÔØ ËÁË ÏÔËÒÙÔÙÊ ÓÅÊÆ. ëÏÇÄÁ ËÏÒÒÅÓÐÏÎÄÅÎÔ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÎÁÝÅÎÉÅ ÐÒÉ ÐÍÍÝÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÜÔÏ ÓÏÎÂÝÅÎÉÅ ÐÍÅÝÁÅÔÓÑ × ÓÅÊÆ É ÓÅÊÆ ÚÁËÒÙ×ÁÅÔÓÑ. óÏÎÔ×ÅÔÓ×ÕÀÝÉÊ ÚÁËÒÙÔÙÊ ËÌÀÞ - ËÍÍÂÉÎÁÃÉÑ, ÎÅÏÂÈÏÄÉÍÁÑ ÄÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÏÔËÒÙÔØ ÓÅÊÆ É ÐÌÕÞÉÔØ ÄÏËÕÍÅÎÔ. äÒÕÇÉÍÉ ÓÌ×ÁÍÉ, ÔÌØËÏ ÏÀÌÄÁÔÅÌØ ÚÁËÒÙÔÏÇÏ ËÌÀÞÁ ÍÏÖÅ ×ÏÓÓÔÁÎÏ×ÉÔØ ÄÏËÕÍÅÎÔ, ÚÁÛÉÆÒÏ×ÁÎÙÊ ÓÏÎÔ×ÅÔÓ×ÕÀÝÉÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ.

åÓÌÉ ÷Ù ÈÏÔÉÔÅ ÐÏÓÌÁÔØ ÓÏÏÂÝÅÎÉÅ ÄÒÕÇÏÍ, ÔÏ ÚÁÛÉÆÒÏ×Ù×ÁÅÔÅ ÅÇÏ ÐÒÉ ÐÏÍÏÝÉ ÏÐËÒÙÔÏÇÏ ËÌÀÞÁ ÄÒÕÇÁ, Á ÔÏÔ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ ÅÇÏ ÐÒÉ ÐÏÍÏÝÉ Ó×ÏÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ. åÓÌÉ ÄÒÕÇ ÚÁÈÏÞÅÔ ÷ÁÍ ÏÔ×ÅÔÉØ, ÔÏ ÏÎ ÚÁÛÉÆÒÕÅÔ ÏÔ×ÅÔ ÐÒÉ ÐÏÍÏÝÉ ÷ÁÛÅÇÏ ÏÐËÒÙÔÏÇÏ ËÌÀÞÁ, Á ÷Ù ÒÁÓÛÉÆÒÕÅÔÅ ÅÇÏ Ó×ÏÉÍ ÓÅËÒÅÔÎÙÍ.

äÌÑ ÚÁÛÉÆÒÏ×ÁÎÉÑ ÄÏÐÏÎÉÔÅÌØÎÏÊ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--encrypt`. ÷Ù ÄÏÌÖÎÙ ÉÍÅÔØ ÏÐËÒÙÔÙÅ ËÌÀÞÉ ÐÒÅÄÐÏÁÇÁÅÍÙÅ ÐÏÕÞÁÔÅÌÅÍ. ðÒÏÇÒÁÍÍÁ ÏÐÅÄÅÌÑÅÔ × ËÁÞÅÓÔ×Å ÐÁÒÁÍÅÔÒÁ ÉÍÑ ÛÉÆÒÕÅÍÏÇÏ ÄÏËÕÍÅÎÔÁ ÉÌÉ, × ÓÌÕÞÁÅ ÅÇÏ ÏÔÓÕÔÓÔ×ÉÑ, ÛÉÆÒÕÅÔ ÓÔÁÎÄÁÒÔÎÙÊ ××ÏÄ. úÁÛÉÆÒÏ×ÁÎÎÙÊ ÒÅÚÕÌØÔÁÔ ÐÏÅÝÁÅÔÓÑ × ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ, ÅÓÌÉ ÎÅ ÕËÁÚÁÎ ÏÐÃÉÑ `--output`. äÌÑ ÐÏ×ÙÛÅÎÉÑ ÚÁÝÉÔÙ ÄÏËÕÍÅÎÔ ÄÏÐÏÎÉÔÅÌØÎÏ ÓÖÉÍÁÅÔÓÑ.

```
alice% gpg --output doc.gpg --encrypt --recipient blake@cyb.org doc
```

ïÐÃÉÑ `--recipient` ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ËÁÖÄÏÇÏ ÐÏÌÕÞÁÔÅÌÑ É ÉÍÅÅÔ ÁÒÇÕÍÅÎÔ, ÉÄÅÎÔÉÆÉÃÉÒÕÀÝÉÊ ÏÐËÒÙÔÙÊ ËÌÀÞ, ËÏÔÏÒÙÍ ÄÏÌÖÅÎ ÂÙÔØ ÚÁÛÉÆÒÏ×ÁÎ ÄÏËÕÍÅÎÔ. úÁÛÉÆÒÏ×ÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÍÏÖÅÔ ÂÙÔØ ÒÁÓÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÔÅÍ, ÞÅÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÓÏÏÔ×ÅÔÓÔ×ÕÅÔ ÏÄÎÏÍÕ ÉÚ ÕËÁÚÁÎÎÙÈ ÏÐËÒÙÔÙÈ ËÌÀÞÅÊ. ÷ ÞÁÓÔÎÏÓÔÉ, ÷Ù ÎÅ ÍÏÖÅÔÅ ÒÁÓÛÉÆÒÏ×ÁÔØ ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÷ÁÍÉ ÄÏËÕÍÅÎÔ, ÅÓÌÉ ÎÅ ×ËÌÀÞÉÌÉ Ó×ÏÊ ÏÐËÒÙÔÙÊ ËÌÀÞ × ÓÐÉÓÏË ÐÏÌÕÞÁÔÅÌÅÊ.

äÌÑ ÒÁÓÛÉÆÒÏ×ÁÎÉÑ ÓÏÏÂÝÅÎÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--decrypt`. ÷ÁÍ ÎÕÖÅÎ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÄÌÑ ËÏÔÏÒÏÇÏ ÜÔÏ ÓÏÏÂÝÅÎÉÅ ÂÙÌÏ ÚÁÛÉÆÒÏ×ÁÎÏ. äÌÅÓÍÅÎÔ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÎÁ ×ÈÏÄÅ ÐÒÏÇÒÁÍÍÙ, ÒÁÓÛÉÆÒÏ×ÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÎÁ ×ÙÈÏÄÅ.

```
blake% gpg --output doc --decrypt doc.gpg

You need a passphrase to unlock the secret key for
user: "Blake (Executioner) <blake@cyb.org>"
1024-bit ELG-E key, ID 5C8CBD41, created 1999-06-04 (main key ID 9E98BC16)

Enter passphrase:
```

äÏÅÓÍÅÎÔÙ, ÔÁËÖÅ, ÍÏÖÎÏ ÚÁÛÉÆÒÏ×Ù×ÁÔØ ÂÅÚ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ÷ÍÅÓÔ ÜÔÏÇÏ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÉÍÂÏÌÛ ÛÉÆÒ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ

ÄÏËÕÍÅÎÔÁ. ëÌÀÞ, ÉÓÐÏÌØÚÕÅÍÙÊ ÐÒÉ ÚÁÛÉÆÒÏ×ÁÎÉÉ, ÏÂÒÁÚÕÅÔÓÑ ÉÚ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ, ÚÁÐÒÁÛÉ×ÁÅÍÏÊ ÐÅÒÅÄ ÚÁÛÉÆÒÏ×ÁÎÉÅÍ. äÌÑ ÂÏÌØÛÅÊ ÂÅÚÏÐÁÓÎÏÓÔÉ ÜÔÏ ÐÁÒÏÌØ ÎÅ ÄÏÌÖÅÎ ÓÏ×ÐÁÄÁÔØ Ó ÔÅÍ, ËÏÔÏÒÙÊ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ ÄÌÑ ÚÁÝÉÔÙ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ. óÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ ÐÒÉÍÅÎÉÍ, ËÏÇÄÁ ÎÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ ÏÂÍÅÎÉ×ÁÔØÓÑ ËÌÀÞÅ×ÏÊ ÆÒÁÚÏÊ. äÌÑ ÉÓÐÏÌØÚÏ×ÁÎÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ ÐÒÉÍÅÎÑÅÔÓÑ ËÏÍÁÎÄÁ `--symmetric`.

```
alice% gpg --output doc.gpg --symmetric doc
Enter passphrase:
```

1.4. ðÏÄÐÉÓÉ É ÉÈ ÐÒÏ×ÅÒËÁ

ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÕÄÏÓÏÏ×ÅÒÑÅÔ ÓÏÚÄÁÔÅÌÑ É ÄÁÔÕ ÓÏÚÄÁÎÉÑ ÄÏÐÏÌÎÉÔÅÌØÎÏÊ ÎÕÖÎÏÊ ÉÎÆÏÒÍÁÃÉÉ. åÓÌÉ ÄÏÐÏÌÎÉÔÅÌØÎÁÑ ÎÕÖÄÁÅÔÓÑ É ÄÁÎÎÏÊ ÐÒÏ×ÅÒËÅ ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓÉ ×ÙÄÁÓÔ ÏÛÉÂËÕ. ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ × ÔÅÈ ÖÅ ÃÅÌÑÈ, ÞÔÏ É ÏÂÙÞÎÁÑ ÐÏÄÐÉÓØ. éÓÐÏÌÎÙÅ ÔÅËÓÔÙ GnuPG, ÎÁÐÒÍÅÒ, ÐÏÄÐÉÓÁÎÙ, É ÷Ù ÍÏÖÅÔ ÕÂÅÄÉÔØÓÑ, ÞÔÏ ÏÎÉ ÄÏÛÌÉ ÄÏ ÷ÁÓ ÎÅÉÚÍÅÎÎÙÍÉ.

óÏÚÄÁÎÉÅ É ÐÒÏ×ÅÒËÁ ÐÏÄÐÉÓÅÊ ÏÔÎÉÞÁÅÔÓÑ ÏÔ ÚÁÛÉÆÒÏ×ÁÎÉÑ/ÒÁÓÛÉÆÒÏ×ÁÎÉÑ. ðÒÉ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÁ ÉÓÐÏÌØÚÕÅÔÓÑ ÚÁËÒÙÔÙÊ ËÌÀÞ ÐÏÄÐÉÓÙ×ÁÀÝÅÇÏ, Á ÐÒÏ×ÅÒÑÅÔÓÑ ÐÏÄÐÉÓØ Ó ÉÓÐÏÌØÚÏ×ÁÎÉÅÍ ÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. îÁÐÒÉÍÅÒ, Alice ÉÓÐÏÌØÚÕÅÔ Ó×ÏÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÞÔÏÂÙ ÐÏÄÐÉÓÁÔØ Ó×ÏÀ ÎÏ×ÕÀ ÓÔÁÔØÀ × ÖÕÒÎÁÌ. òÅÄÁËÔÏÒ, ÐÏÕÞÉ× ÐÉÓØÍÏ, ÉÓÐÏÌØÚÕÅÔ ÏÔËÒÙÔÙÊ ËÌÀÞ Alice, ÞÔÏÂÙ ÐÒÏ×ÅÒÉÔØ, ÞÔÏ ÐÉÓØÍÏ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÏÔ Alice É ÎÅ ÂÙÌÏ ÉÚÍÅÎÅÎÏ ÚÁ ×ÒÅÍÑ ÐÅÒÅÓÙÌËÉ.

äÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÏ× ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--sign`. äÏËÕÍÅÎÔ ÄÌÑ ÐÏÄÐÉÓÉ ÎÁ ×ÈÏÄÅ É ÐÏÄÐÉÓÁÎÎÙÊ ÎÁ ×ÙÈÏÄÅ.

```
alice% gpg --output doc.sig --sign doc

You need a passphrase to unlock the private key for
user: "Alice (Judge) <alice@cyb.org>"
```

```
1024-bit DSA key, ID BB7576AC, created 1999-06-04

Enter passphrase:
```

äÏËÕÍÅÎÔ ÓÖÉÍÁÅÔÓÑ ÐÅÒÅÄ ÐÏÄÐÉÓØÀ É ×Ù×ÏÄÉÔÓÑ × Ä×ÏÉÞÎÍ ÆÏÒÍÁÔÅ.

éÍÅÑ ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ, ÷Ù ÍÏÖÅÔÅ ÌÉÂÏ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ÌÉÂÏ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ É ×ÏÓÓÔÁÎÏ×ÉÔØ ÉÓÈÏÄÎÙÊ ÄÏËÕÍÅÎÔ. äÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ ÉÓÐÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--verify`. äÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ É ÉÚ×ÌÅÞÅÎÉÑ ÄÏËÕÍÅÎÔÁ ÉÓÐÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--decrypt`. ðÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÎÁ ×ÈÏÄ É ÐÒÏ×ÅÒÅÎÎÙÊ É ×ÏÓÓÔÁÎÏ×ÌÅÎÎÙÊ ÎÁ ×ÙÈÏÄ.

```
blake% gpg --output doc --decrypt doc.sig
gpg: Signature made Fri Jun  4 12:02:38 1999 CDT using DSA key ID BB7576AC
gpg: Good signature from "Alice (Judge) <alice@cyb.org>"
```

1.4.1. ðÒÏÚÒÁÞÎÏ ÐÏÄÐÉÓÁÎÎÙÅ(Clearsigned) ÄÏËÕÍÅÎÔÙ

ïÂÙÞÎÏ ÃÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ ÐÒÉÍÅÎÑÀÔÓÑ ÐÒÉ ÐÏÄÐÉÓÉ ÓÏÏÂÝÅÎÉÊ usenet É e-mail. ðÒÉ ÜÔÏÍ ÎÅÖÅÌÉÔÅÌØÎÏ ÓÖÉÍÁÔØ ÐÏÄÐÉÓÙ×ÁÅÍÙÅ ÄÏËÕÍÅÎÔÙ. ëÏÍÁÎÄÁ `--clearsign` ÄÏÂÁ×ÌÑÅÔ Ë ÄÏËÕÍÅÎÔÕ ÃÉÆÒÏ×ÕÀ ÐÏÄÐÉÓØ × ÆÏÒÍÁÔÅ ASCII, ÎÏ ÎÅ ÉÚÍÅÎÑÅÔ ÓÁÍ ÄÏËÕÍÅÎÔ.

```
alice% gpg --clearsign doc

You need a passphrase to unlock the secret key for
user: "Alice (Judge) <alice@cyb.org>"
1024-bit DSA key, ID BB7576AC, created 1999-06-04

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

[...]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v0.9.7 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iEYEARECAAYFAjdYCQoACgkQJ9S6ULt1dqz6IwCfQ7wP6i/i8HhbcOSKF4ELyQB1
oCoAoOuqpRqEzr4kOkQqHRLE/b8/Rw2k
=y6kj
-----END PGP SIGNATURE-----
```

1.4.2. ïÔÄÅÌÅÎÎÁÑ ÐÏÄÐÉÓØ

ðÒÉÍÅÎÅÎÉÅ ÐÏÄÐÉÓÁÎÎÙÈ ÄÏËÕÍÅÎÔÏ× ÏÇÒÁÎÉÞÅÎÎÏ. ðÏÌÕÞÁÔÅÌØ ÄÏÌÖÅÎ ×ÏÓÓÔÁÎÁ×ÌÉ×ÁÔØ ÄÏËÕÍÅÎÔ ÉÚ ÐÏÄÐÉÓÁÎÎÏÊ ×ÅÒÓÉÉ, É ÄÁÖÅ × ÓÌÕÞÁÅ ÐÒÏÚÁÞÎÏÊ ÐÏÄÐÉÓÉ, ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÄÏÌÖÅÎ ÂÙÔØ ÏÔÒÅÄÁËÔÉÒÏ×ÁÎ ÄÌÑ ÐÌÕÞÅÎÉÑ ÒÉÇÉÎÁÌÁ. ðÏÜÔÏÍÕ ÉÍÅÅÔÓÑ ÔÒÅÈ ÍÅÔÏÄ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÏ×, ËÏÔÏÒÙÊ ÓÏÚÄÁÅÔ ÏÔÄÅÌÅÎÎÕÀ ÐÏÄÐÉÓØ (detached signature). ïÔÄÅÌÅÎÎÁÑ ÐÏÄÐÉÓØ ÓÏÚÄÁÅÔÓÑ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ËÏÍÁÎÄÙ `--detach-sig`.

```
alice% gpg --output doc.sig --detach-sig doc

You need a passphrase to unlock the secret key for
user: "Alice (Judge) <alice@cyb.org>"
1024-bit DSA key, ID BB7576AC, created 1999-06-04

Enter passphrase:
```

äÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ ÎÅÏÂÈÏÄÉÍÙ É ÏÔÄÅÌÅÎÎÁÑ ÐÏÄÐÉÓØ, É ÄÏËÕÍÅÎÔ. äÌÑ ÐÒÏ×ÅÒËÉ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--verify`.

```
blake% gpg --verify doc.sig doc
gpg: Signature made Fri Jun  4 12:38:46 1999 CDT using DSA key ID BB7576AC
gpg: Good signature from "Alice (Judge) <alice@cyb.org>"
```

1. ÷ÁÖÉÁÎÔ 3 ÇÅÎÅÒÉÒÕÅÔ ÐÁÒÕ ElGamal, ËÏÔÏÒÁÑ ÎÅ ÐÒÉÇÏÄÎÁ ÄÌÑ ÐÏÄÐÉÓÉ.
2. íÎÏÇÉÅ, ÞÁÓÔÏ ÉÓÐÏÌØÚÕÅÍÙÅ, ÏÐÃÉÉ ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÉ ÍÏÇÕÔ ÂÙÔØ ÕÓÔÁÎÏ×ÌÅÎÙ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.

2. Concepts

GnuPG ÉÓÐÏÌØÚÕÅÔ ÎÅÓËÏÌØËÏ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÍÅÔÏÄÏ×, ×ËÌÀÞÁÑ *ÓÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ*, *ÛÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ*, É *ÏÄÎÎÔÁÐÒÁ×ÌÅÎÎÅ ÈÜÛÉÒÏ×ÁÎÉÅ*. ÷Ù ÍÏÖÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ ÏÓÎÏ×ÎÙÅ ÆÕÎËÃÉÉ GnuPG ÂÅÚ ÉÚÕÞÅÎÉÑ ÜÔÉÈ ÍÅÔÏÄÏ×, ÎÏ ÄÌÑ ÂÎÌÅÅ ÒÁÚÕÍÎÏÇÏ ÐÒÉÍÅÎÅÎÉÑ ÖÅÌÁÔÅÌØÎÏ, ×ÓÅ ÖÅ, ËÏÅ-ÞÔÏ ÚÎÁÔØ.

üÔÁ ÇÌÁ×Á - ××ÅÄÅÎÉÅ × ÏÓÎÏ×ÎÙÅ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÅ ÍÅÔÏÄÙ, ÉÓÐÏÌØÚÕÅÍÙÅ × GnuPG. âÎÅÅ ÐÏÄÒÏÂÎÏ ÜÔÉ ×ÏÐÒÏÓÙ ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ × ÄÒÕÇÉÈ ÉÓÔÏÞÎÉËÁÈ. èÏÒÏÛÁÑ ËÎÉÇÁ, ÄÌÑ ÄÁÌØÎÅÊÛÅÇÏ ÉÚÕÞÅÎÉÑ: Bruce Schneier (http://www.counterpane.com/schneier.html) “Applied Cryptography” (http://www.counterpane.com/applied.html).

2.1. óÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ

óÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ ÜÔÏ ÛÉÆÒ ÉÓÐÏÌØÚÕÀÝÉÊ ÏÄÉÎ ËÌÀÞ ÄÌÑ ÚÁÛÉÆÒÏ×ÁÎÉÑ É ÒÁÓÛÉÆÒÏ×ÁÎÉÑ. óÔÏÒÏÎÙ, ÏÂÝÁÀÝÉÅÓÑ ÐÒÉ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ, ÄÏÌÖÎÙ ÄÏÇÏ×ÏÒÉÔØÓÑ Ï ËÌÀÞÅ ÄÏ ÎÁÞÁÌÁ ÏÂÍÅÎÏÍ ÓÏÂÝÅÎÉÑÍÉ. ðÏÓÌÅ ÔÏÇÏ ËÁË ÏÎÉ ÄÏÇÏ×ÏÉÌÉÓØ, ÏÔÐÒÁ×ÉÔÅÌØ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÂÝÅÎÉÅ, ÉÓÐÏÌØÚÕÑ ËÌÀÞ, ÏÔÐÒÁ×ÌÑÅÔ ÐÏÕÞÁÔÅÌÀ, É ÐÏÕÞÁÔÅÌØ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÂÝÅÎÉÅ, ÉÓÐÏÌØÚÕÑ ÔÏÔ ÖÅ ÓÁÍÙÊ ËÌÀÞ. îÁÐÒÉÍÅÒ, ÎÅÍÃËÁÑ Enigma - ÓÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ, ÅÖÅÄÎ×ÎÙÅ ËÌÀÞÉ ÒÁÓÐÒÏÓÔÒÁÎÑÉÓØ ËÁË ËÎÉÇÉ ËÏÄ×. ëÁÖÄÙÊ ÄÅÎØ ÐÏÓÙÌÁÀÝÉÊ ÉÌÉ ÐÒÉÎÉÍÁÀÝÉÊ ÒÁÄÉÓÔ ÄÏÖÅÎ ÂÙÌ ÎÁÊÔÉ × Ó×ÏÅÊ ËÏÐÉÉ ËÎÉÇÉ ËÏÄ×Ï ÍÁ ÔÅÕÝÉÊ ÄÅÎØ. òÁÄÉÏÇÒÁÍÍÙ × ÜÔÏÔ ÄÅÎØ ÚÁÛÉÆÒÏ×Ù×ÁÌÉÓØ É ÒÁÓÛÉÆÒÏ×Ù×ÁÌÉÓØ ÜÔÉÍ ËÌÀÞÏÍ. óÏ×ÒÅÍÅÎÎÙÅ ÐÒÉÅÒÙ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ×: 3DES, Blowfish, IDEA É çïóô.

èÏÒÏÛÉÊ ÛÉÆÒ ÚÁËÌÀÞÅÔÓÀ ×ÓÀ ÚÁÝÉÔÕ × ËÌÀÞÅ, ÎÏ ÎÅ × ÁÌÇÏÒÉÔÍÅ. äÒÕÇÉÉ ÓÌÏ×ÁÍÉ, ÚÎÁÎÉÅ ÉÓÐÏÌØÚÕÅÍÏÇÏ ÁÌÇÏÒÉÔÍÁ ÎÅ ÄÁÌÏÎÏ ÐÍÍÞØ

×ÚÌÏÍÝÉËÕ. úÎÁÎÉÅ ÁÌÇÏÒÉÔÍÁ ÐÏÍÁÄÏÂÉÔÓÑ ÅÍÕ, ÔÏÌØËÏ ËÏÇÄÁ ÏÎ ÐÏÌÕÞÉÔ ËÌÀÞ. ûÉÆÒÙ, ÉÓÐÏÌØÚÕÅÍÙÅ × GnuPG, ÏÂÌÁÄÁÀÔ ÜÔÉÍ Ó×ÏÊÓÔ×ÏÍ.

ôÁË ËÁË ×ÓÑ ÚÁÝÉÔÁ ÚÁËÌÀÞÅÎÁ × ËÌÀÞÅ, ÔÏ ÏÞÅÎØ ×ÁÖÎÏ, ÞÔÏÂÙ ÅÇÏ ÂÙÌÏ ÔÒÕÄÎÏ ÐÏÄÏÂÒÁÔØ. äÒÕÇÉÉ ÓÌÏ×ÁÍÉ, ÍÎÏÖÅÓÔ×Ï ×ÏÚÍÏÖÎÙÈ ËÌÀÞÅÊ, Ô.Å. *ÐÒÏÓÔÒÁÎÓÔ×Ï ËÌÀÞÅÊ*, ÄÎÏÖÎÏ ÂÙÔØ ÄÏÓÔÁÔÏÞÎÏ ×ÅÌÉËÏ. âÕÄÕÞÉ × ìÏÓ áÌÁÍÏÓÅ, òÉÞÁÒÄ æÅÊÍÁÎ ÐÒÏÓÌ×ÉÌÓÑ ÕÍÅÎÉÅÍ ×ÓËÒÙ×ÁÔØ ÓÅÊÆÙ. äÌÑ ÐÏÄÄÅÒÖÁÎÉÑ ÍÉÓÔÉÆÉËÁÃÉÉ ÏÎ ÄÁÖÅ ÐÒÉÎÏÓÉÌ Ó ÓÏÂÏÊ ÎÁÂÏÒ ÉÎÓÔÒÕÍÅÎÔÏ×, ×ËÌÀÞÁÑ ÓÔÁÒÙÊ ÓÔÅÔÏÓËÏÐ. ÷ ÄÅÊÓÔ×ÉÔÅÌØÎÏÓÔÉ, ÏÎ ÉÓÐÏÌØÚÏ×ÁÌ ÎÁÂÏÒ ÕÌ×ÏË ÄÌÑ ÕÍÅÎØÛÅÎÉÑ ÞÉÓÌÁ ËÏÍÂÉÎÁÃÉÊ, Á ÚÁÔÅÍ ÐÒÏÓÏ ÐÏÄÂÉÒÁÌ ÐÒÁ×ÉÌØÎÕÀ. ðÒÏÝÅ ÇÏ×ÏÒÑ, ÏÎ ÕÍÅÎØÛÁÌ ÒÁÚÍÅÒ ÐÒÏÓÔÒÁÎÓÔ×Á ËÌÀÞÅÊ.

âÒÉÔÁÎÉÑ ÉÓÐÏÌØÚÏ×ÁÌÁ ÍÁÛÉÎÙ ÄÌÑ ÐÏÄÂÏÒÁ ËÌÀÞÅÊ, ×Ï ×ÒÅÍÑ ÷ÔÏÒÏÊ íÉÒÏ×ÏÊ ×ÏÊÎÙ. Britain used machines to guess keys during World War 2. îÅÍÅÃÇÁÑ Enigma ÉÍÅÌÁ ÏÞÅÎØ ÂÏÌØÛÏÅ ÐÒÏÓÔÒÁÎÓÔ×Ï ËÌÀÞÅÊ, ÎÏ áÎÇÌÉÞÁÎÅ ÐÏÓÔÒÏÉÌÉ ÓÐÅÃÉÁÌØÎÙÅ ×ÙÞÉÓÌÉÔÅÌØÎÙÅ ÍÅÈÁÎÉÚÍÙ, "Bombes", ËÏÔÒÙÅ ÐÅÒÅÂÒÁÌÉ ËÌÀÞÉ ÐÏËÁ ÎÁ ÎÁÈÏÄÉÌÉ ÎÕÖÎÙÊ. éÎÏÇÄÁ ÏÎÉ ÎÁÈÏÄÉÌÉ ËÌÀÞ ÎÁ ÔÅËÕÝÉÊ ÄÅÎØ ÞÅÒÅÚ ÎÅÓËÏÌØËÏ ÞÁÓÏ× ÐÏÓÌÅ ÎÁÞÁÌÁ ÅÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ, Á ÉÎÏÇÄÁ ÎÅ ÎÁÈÏÄÉÌÉ ÓÏ×ÓÅÍ. "Bombes" ÎÅ Ñ×ÌÑÌÉÓØ ËÏÍÐØÀÔÅÒÁÍÉ, ÎÏ ÂÙÌÉ ÉÈ ÐÒÅÄÛÅÓÔ×ÅÎÎÉËÁÍÉ.

óÏ×ÒÅÍÅÎÎÙÅ ËÏÍÐØÀÔÅÒÙ ÍÇÕÔ ÐÅÒÅÂÉÒÁØ ËÌÀÞÉ Ó ÏÇÒÏÍÎÏÊ ÓËÏÒÏÓØÀ, ÐÏÜÔÍÕ ÒÁÚÍÅÒ ËÌÀÞÁ ÔÁË ×ÁÖÅÎ × ÓÏ×ÒÅÍÅÎÎÙÈ ËÒÉÐÔÏÓÉÓÔÅÍÁÈ. ûÉÆÒ DES ÉÓÐÏÌØÚÕÅÔ ËÌÀÞ ÄÌÉÎÏÊ 56 ÂÉÔ, Ô.Å. ÓÕÝÅÓÔ×ÕÅÔ 2^{56} ×ÏÚÍÖÎÙÈ ËÌÀÞÅÊ. 2^{56} ÜÔÏ 72,057,594,037,927,936 ËÌÀÞÅÊ. íÎÏÇÏ, ÎÏ ÏÂÙÞÎÙÊ ËÏÍÐØÀÔÅÒ ÍÖÅÔ ÐÅÒÅÂÒÁÔØ ÉÈ ÚÁ ÓÞÉÔÁÎÙÅ ÄÎÉ, Á ÓÐÅÃÉÁÌÉÚÉÒÏ×ÁÎÎÙÊ ÚÁ ÞÁÓÙ. ó ÄÒÕÇÏÊ ÓÔÒÏÎÙ, ÂÏÌÅ ÐÏÚÄÉÅ ÁÌÇÏÒÉÔÍÙ - 3DES, Blowfish É IDEA ÉÓÐÏÌØÚÕÀÔ ËÌÀÞÉ ÄÌÉÎÏÊ 128 ÂÉÔ, ÞÔÏ ÏÚÎÁÞÁÅÔ 2^{128} ×ÏÚÍÖÎÙÈ ËÌÀÞÅÊ. üÔÏ ÎÁÍÎÏÇÏ ÂÏØÛÅ, É, ÄÁÖÅ, ÅÓÌÉ ×ÓÅ ËÏÍÐØÀÔÅÒÙ ÎÁ ÎÁÛÅÊ ÐÌÁÎÅÔÅ ÏÂßÅÄÉÎÉÔØ, ÉÍ ÐÏÔÒÅÂÕÅÔÓÑ ×ÒÅÍÅÎÉ ÂÏØÛÅ, ÞÅÍ ×ÏÚÒÁÔ ×ÓÅÌÅÎÎÏÊ, ÄÌÑ ÎÁÈÏÄÅÎÉÑ ËÌÀÞÁ.

2.2. ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ

ïÓÎÎ×ÎÁÑ ÐÒÏÂÌÅÍÁ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× - ÏÂÍÅÎ ËÌÀÞÁÍÉ. ïÔÐÒÁ×ÉÔÅÌØ É ÐÏÎÕÞÁÔÅÌØ ÄÎÌÖÎÙ ÏÂÍÅÎÑÔØÓÑ ËÌÀÞÁÍÉ, ËÏÔÏÒÙÅ ÂÕÄÕÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÚÁÝÉÝÅÎÎÏÇÏ ÏÂÍÅÎÁ ÉÎÆÏÒÍÁÃÉÅÊ, ÎÏ ËÁËÉÍ ÚÁÝÉÝÅÎÙÍ ËÁÎÁÌÏÍ ÏÎÉ ÍÏÇÕÔ ×ÏÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÏÂÍÅÁ ÓÁÍÉÍÉ ËÌÀÞÁÍÉ? ÷ ÞÁÓÔÏÓÔÉ, ×ÚÌÍÝÉËÕ ÍÏÅÔ ÂÙÔØ ÌÅÇÞÅ ÐÅÒÅ×ÁÔÉÔØ ËÌÀÞ, ÎÅÖÅÌÉ ÅÇÏ ÐÏÄÂÉÒÁÔØ. äÒÕÇÁÑ ÐÒÏÂÌÅÍÁ - ËÏÌÉÞÅÓÔ×Ï ÎÅÏÂÈÏÄÉÍÙÈ ËÌÀÞÅÊ. åÓÌÉ *n* ÞÅÌÏ×ÅË ÈÏÑÎÔ ÏÂÍÅÎ×ÁÔØÓÑ ÍÅÖÄÕ ÓÏÂÏÊ ÓÏÏÂÝÅÎÉÑÍÉ, ÔÏ ÎÅÏÂÈÏÄÉÍÏ *n(n-1)/2* ËÌÀÞÅÊ, ÐÏ ÏÂÎÍÕ ÄÌÑ ËÁÖÄÏÊ ÐÁÒÙ, ÕÞÁ×ÓÔ×ÕÀÝÅÊ × ÐÅÒÅÐÉÓËÅ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÐÒÉÅÍÌÅÍÏ ÄÌÑ ÎÅÂÏØÛÏÊ ÇÒÕÐÐÙ ÌÀÄÅÊ, ÎÏ ÓÔÁÎÅÔ ÎÅÕÄÏÂÎÙÍ ÐÒÉ ÅÅ Õ×ÅÌÉÞÅÎÉÉ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÂÙÌÉ ÐÒÉÄÕÍÁÎÙ, ÞÔÏÂÙ ÒÅÛÉÔØ ÐÒÏÂÌÅÍÕ Ó ÏÂÍÅÎÏÍ ËÌÀÞÁÍÉ. ûÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÉÓÐÏÌØÚÕÅÔ ÐÁÒÕ ËÌÀÞÅÊ ÄÌÑ ÏÔÐÒÁ×ËÉ ÓÏÏÂÝÅÎÉÊ. ä×Á ËÌÀÞÁ ÏÔÏÓÑÔÓÑ Ë ÌÉÃÕ ÐÒÉÎÉÁÀÝÅÍÕ ÓÏÏÂÝÅÎÉÅ. ïÄÉÎ ËÌÀÞ *ÏÔËÒÙÔÙÊ (public key)* É ÍÏÖÅÔ ÂÙÔØ ÐÅÒÅÄÁÎ ÌÀÂÏÍ. äÒÕÇÏÊ ËÌÀÞ *ÓÅËÒÅÔÎÙÊ (private key)* É ÈÒÁÎÉÔÓÑ ÔÏÌØËÏ Õ ×ÌÁÄÅÌØÃÁ. ïÔÐÒÁ×ÉÔÅÌØ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÏÂÝÅÎÉÅ ÏËÒÙÔÙÍ ËÌÀÞÏÍ ÐÏÌÕÞÁÔÅÌÑ, É ,ÂÕÄÕÞÉ ÚÁÛÉÆÒÏ×ÁÎ, ÓÏÏÂÝÅÎÉÅ ÍÏÖÅÔ ÂÙÔØ ÒÁÓÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÚÁËÒÙÔÙÍ ËÌÀÞÏÍ ÐÏÌÕÞÁÔÅÌÑ.

üÔÏ ÍÅÔÏÄ ÒÅÛÁÅÔ ÐÒÏÂÌÅÍÕ ÏÂÍÅÎÁ ËÌÀÞÁÍÉ, ÐÒÉÓÕÝÕÀ ÓÉÍÍÅÔÒÉÞÎÙÍ ÛÉÆÒÁÍ. ïÐÁÄÁÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔØ ÄÏÇÏ×ÏÒÅÎÎÏÓÔÉ Ï ËÌÀÞÅ ÍÅÖÄÕ ÏÔÐÒÁ×ÉÔÅÌÅÍ. ÷ÓÅ ÞÔÏ ÔÒÅÂÕÅÔÓÑ, ÜÔÏ ÞÔÏÂÙ ÏÔÐÒÁ×ÉÔÅÌØ ÄÏ ÎÁÞÁÌÁ ÓÅËÒÅÔÎÏÇÏ ÏÂÍÅÎÁ ÉÎÆÏÒÍÁÃÉÅÊ ×ÚÑÌ ËÏÐÉÌÏÛÏÇÏ ËÌÀÞÁ ÐÏÌÕÞÁÔÅÌÑ. ëÒÏÍÅ ÔÏÇÏ, ÏÄÉÎ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ×ÓÅÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍÉ ÐÏÌÕÞÁÔÅÌÑ. ôÁËÉÍ ÏÂÒÁÚÏÍ, ÔÏÌØËÏ *n* ÐÁÒ ËÌÀÞÅÊ ÎÅÏÂÈÏÄÉÍÏ ÄÌÑ *n* ÞÅÌÏ×ÅË, ÐÅÒÅÐÉÓÙ×ÁÀÝÉÈÓÑ ÄÒÕÇ Ó ÄÒÕÇÏÍ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÏÓÎÎ×ÁÎÙ ÎÁ ÏÄÎÓÔÒÏÎÎÉÈ ÆÕÎËÃÉÑÈ "c ÌÁÚÅËËÏÊ". ïÄÎÓÔÒÏÎÎÑÑ ÆÕÎËÃÉÑ ÜÔÏ ÆÕÎËÃÉÑ, ËÏÔÏÒÕÀ ÌÅÇËÏ ×ÙÞÉÓÌÉÔØ, ÎÏ ÔÒÕÄÎÏ ×ÙÞÉÓÌÉÔØ ÅÅ ÏÂÒÁÔÎÕÀ ÆÕÎËÃÉÀ, Ô.Å. ÐÏ

ÚÎÁÞÅÎÉÀ ÆÕÎËÃÉÉ ÎÁÊÔÉ ÚÎÁÞÅÎÉÅ ÁÒÇÕÍÅÎÔÁ. îÁÐÒÉÍÅÒ, ÌÅÇËÏ ×ÙÞÉÓÌÉÔØ ÐÒÏÉÚ×ÅÄÅÎÉÅ Ä×ÕÈ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, ÎÏ ÔÒÕÄÎÏ ÒÁÚÌÏÖÉÔØ ÜÔÏ ÐÒÏÉÚ×ÅÄÅÎÉÅ ÎÁ ÍÎÏÖÉÔÅÌÉ. ïÄÎÓÔÏÒÏÎÎÉÅ ÆÕÎËÃÉÉ "Ó ÌÁÚÅËËÏÊ" ÐÌÈÏÖÉ, ÎÏ ÉÍÅÀÔ ÌÁÚÅËÕ. ïÎÁ ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏ ÅÓÌÍ ÎÅËÏÔÒÁÑ ÞÁÓÔØ ÉÎÆÏÒÍÁÃÉÉ ÉÚ×ÅÓÔÎÁ, ÔÏ ×ÙÞÉÓÌÅÎÅ ÏÀÒÁÔÎÏÊ ÆÕÎËÃÉÉ ÓÔÁÎ×ÉÔÓÑ ÌÅÇËÉÍ. îÁÐÒÉÍÅÒ, ÅÓÌÉ ÷ÁÍ ÉÚ×ÅÓÔÎÏ ÏÄÎÏ ÉÚ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, × ÐÒÉÍÅÒÅ ×ÙÛÅ, ÔÏ, ÚÎÁÑ ÐÒÏÉÚ×ÅÄÅÎÉÅ, ÷Ù ÌÅÇËÏ ÎÁÊÄÅÔÅ ×ÔÏÒÏÅ ÞÉÓÌÏ. äÁÎÙÊ ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÏÓÎ×ÁÎ ÎÁ ÐÒÏÓÔÙÈ ÍÎÏÖÉÔÅÌÑÈ, ÏÔËÒÙÔÙÊ ËÌÀÞ ÓÏÄÅÒÖÉÔ ÐÒÏÉÚ×ÅÄÅÎÉÅ Ä×ÕÈ ÂÎØÛÉÈ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, ÁÌÇÏÒÉÔÍ ÛÉÆÒÏ×ÁÎÑ ÉÓÐÏÌØÚÕÅÔ ÜÔÏ ÞÉÓÌÏ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÓÏÎÂÝÅÎÑ. áÌÇÏÒÉÔÍ ÒÁÓÛÉÆÒÏ×ËÉ ÔÒÅÂÕÅÔ ÚÎÁÎÉÑ ÐÒÏÉÚ×ÅÄÅÎÉÑ ÐÅÒÖÉÓÌÅÔ, ÔÁË, ÒÁÓÛÉÆÒÏ×ËÁ ÓÔÁÎÏ×ÉÔÓÑ ÌÅÇËÏÊ, ÅÓÌÉ Õ ÷ÁÓ ÅÓÔØ ÓÅËÒÅÔÎÛÊ ËÌÀÞ, ÓÏÄÅÒÖÁÝÉÊ ÏÄÉÎ ÉÚ ÍÎÏÖÉÔÅÌÅÊ, ÎÏ ÞÒÅÚ×ÙÞÁÊÎÏ ÚÁÔÒÕÄÎÅÎÁ ÅÓÌÉ ÅÇÏ Õ ÷ÁÓ ÎÅÔ.

ëÁË É × ÓÌÕÞÁÅ ÓÉÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ×, ×ÓÑ ÚÁÝÉÔÁ ÈÏÒÏÛÅÇÏ ÛÉÆÒÁ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÚÁËÌÀÞÅÎÁ × ËÌÀÞÅ. ôÁËÖÅ, ÎÁÄÅÖÎÏÓÔØ ÚÁ×ÉÓÉÔ ÏÔ ÒÁÚÍÅÒÁ ËÌÀÞÁ, ÎÏ ÎÅÌØÚÑ ÓÒÁ×ÎÉ×ÁÔØ ÄÌÉÎÙ ËÌÀÞÅÊ ÓÉÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× É ÛÉÆÒÏ× Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ËÁË ÍÅÒÕ ÉÈ ÎÔÏÓÉÔÅÌØÎÏÎÊ ÎÁÄÅÖÎÏÓÔÉ. ðÒÉ ÇÒÕÂÏÍ ×ÚÌÏÍÅ ÓÉÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ Ó ËÌÀÞÏÍ ÄÌÉÎÏÊ 80 ÂÉÔ, ×ÚÌÏÝÉË ÄÏÌÖÅÎ ÐÅÒÅÂÒÁÔØ ÄÏ 2^{81}-1 ËÌÀÞÅÊ ÄÌÑ ÎÁÈÏÄÅÎÉÑ ÐÒÁ×ÉÌØÎÏÇÏ. ðÒÉ ×ÚÌÏÅ ÛÉÆÒÁ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ Ó ÄÌÉÎÏÊ ËÌÀÞÁ 512 ÂÉÔ, ×ÚÌÏÝÉË ÄÏÌÖÅÎ ÒÁÚÌÏÖÉÔØ ÎÁ ÍÎÏÖÉÔÅÌÉ ÞÉÓÌÏ ÚÁËÏÄÉÒ×ÁÎÎÅ × 512 ÂÉÔÁÈ (ÄÏ 155 ÄÅÓÑÔÉÞÎÙÈ ÚÎÁËÏ×). äÅÊÓÔ×ÉÑ ×ÚÌÏÝÉËÁ ÓÉÌØÎÏ ÒÁÚÌÉÞÁÀÔÓÑ × ÚÁ×ÉÓÉÍÏÔÉ ÏÔ ÛÉÆÒÁ. ðÏËÁ ÄÌÑ ÓÉÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× ÄÏÓÔÁÔÏÞÎÁ ÄÌÉÎÁ ËÌÀÞÁ 128 ÂÉÔ, ÄÌÑ ÓÅÇÏÄÎÑÛÎÉÈ ÔÅÌÌÏÇÉÊ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÒÅËÏÍÅÎÄÕÅÔÓÑ ÄÌÉÎÁ 1024 ÂÉÔÁ.

2.3. óÍÅÛÁÎÎÙÅ ÛÉÆÒÙ

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÎÅ ÐÁÎÁÃÅÑ. íÎÏÇÉÁ ÓÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ ÂÏÌÅÅ ÕÓÔÏÊÞÉ×Ù ÐÒÏÔÉ× ×ÚÌÏÍÁ, É, ËÒÏÍÅ ÔÏÇÏ ÚÁÛÉÆÒÏ×ÁÎÉÅ/ÒÁÓÛÉÆÒÏ×ÁÎÉÅ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÔÒÅÂÕÅÔ ÂÏØÛÉÈ

ÚÁÔÒÁÔ, ÞÅÍ ÁÎÁÏÏÇÉÞÎÙÅ ÏÐÅÒÁÃÉÉ × ÓÉÍÍÅÔÒÉÞÎÙÈ ÓÉÓÔÅÍÁÈ. ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÔÅÍ ÎÅ ÍÅÎÅÅ, ÜÆÆÅËÔÉ×ÎÙ ÐÒÉ ÒÁÓÐÒÏÓÔÒÁÎÅÉÉ ËÌÀÞÅÊ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× É ÉÍÅÎÎÏ ÔÁË ÏÎÉ ÉÓÐÏÌØÚÕÀÔÓÑ × ÓÉÓÔÅÍÁÈ ÓÏ ÓÍÅÛÁÎÎÙÍ ÛÉÆÒÏÍ.

óÍÅÛÁÎÎÙÊ ÛÉÆÒ ÉÓÐÏÌØÚÕÅÔ ÓÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ É ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍ. ïÎ ÒÁÂÏÔÁÅÔ ÉÓÐÏÌØÚÕÑ ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍ ÄÌÑ ÐÅÒÅÄÁÞÉ ËÌÀÞÁ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÁ. óÏÎÂÝÅÎÉÅ, ÚÁÔÅÍ, ÚÁÛÉÆÒÏ×Ù×ÁÅÔÓÑ ÜÔÉÍ ËÌÀÞÍ É ÐÏÓÙÌÁÅÔÓÑ ÁÄÒÅÓÁÔÕ. ôÁË ËÁË ÐÅÒÅÄÁÞÁ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ËÌÀÞÁ ÚÁÝÉÝÅÎÁ, ÔÏ ÄÌÑ ËÁÖÄÏÇÏ ÓÏÏÂÝÅÎÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ Ó×ÏÊ ÓÉÍÍÅÔÒÉÞÎÙÊ ËÌÀÞ, ÎÁÚÙ×ÁÅÍÙÊ ÉÎÏÇÄÁ ÓÅÁÎÓÏ×ÙÍ ËÌÀÞÍÍ.

é PGP É GnuPG ÉÓÐÏÌØÚÕÀÔ ÇÉÂÒÉÄÎÙÅ ÛÉÆÒÙ. óÅÁÎÓÏ×ÙÊ ËÌÀÞ, ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÛÉÆÒÏÍ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ, É ÓÏÏÂÝÅÎÅ, ÚÁÛÉÆÒÏ×ÁÎÎÅ ÓÉÍÍÅÔÒÉÞÙÍ ÛÉÆÒÏÍ, Á×ÔÍÁÔÉÞÅÓËÉ ÏÂßÅÄÉÑÀÔÓÑ ×ÍÅÓÔÅ. ðÌÌÕÞÁÔÅÌØ ÉÓÐÏÌØÚÕÅÔ Ó×ÏÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÓÅÁÎÓÏ×ÏÇÏ ËÌÀÞÁ É, ÚÁÔÅÍ, ÉÓÐÏÌØÚÕÅÔ ÐÌÕÞÅÎÎÙÊ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÓÏÏÂÝÅÎÉÑ.

óÍÅÛÁÎÎÙÊ ÛÉÆÒ ÎÅ ÕÓÔÏÊÞÉ×ÅÅ ÞÅÍ ÓÌÁÂÅÊÛÉÊ ÉÚ ÉÓÐÏÌØÚÕÅÍÙÈ ÉÍ ÛÉÆÒÏ×. ÷ PGP É GnuPG, ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ×ÅÒÏÑÔÎÏ, ÓÌÁÂÅÅ. ë ÓÞÁÓÔØÀ, ÅÓÌÉ ×ÚÌÏÍÝÉËÕ ÕÄÁÅÔÓÑ ÒÁÓÛÉÆÒÏ×ÁÔØ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ, ÏÎ ÍÏÖÅÔ ÅÇÏ ÉÓÐÏÌØÚÏ×ÁÔØ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÔÏÌØËÏ ÏÎÉ ÓÏÏÂÝÅÎÉÑ, ÚÁÛÉÆÒÏ×ÁÎÎÏÇÏ ÜÔÉÍ ËÌÀÞÏÍ. äÌÑ ÐÒÏÞÔÅÎÉÑ ÄÒÕÇÏÇÏ ÓÏÏÂÝÅÎÉÑ, ÅÍÕ ÐÒÉÄÅÔÓÑ ÎÁÞÁÔØ ×ÓÅ ÚÁÎÏ×Ï.

2.4. ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ

èÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ ÜÔÏ ÆÕÎËÃÉÑ "ÍÎÏÇÉÅ-Ë-ÏÄÎÏÍÕ", ÏÔÏÂÒÁÖÁÝÁÑ Ó×ÏÉ ÁÒÇÕÍÅÎÔÙ ÎÁ ÏÇÒÁÎÉÞÅÎÎÙÅ ÍÎÏÖÅÓÔ×Ï ÚÍÁÞÅÎÉÊ. ïÂÙÞÎÏ ÜÔÏ ÍÎÏÖÅÓÔ×Ï - ÄÉÁÐÁÚÏÎ ÎÁÔÕÒÁÌØÎÙÈ ÞÉÓÅÌ. ðÒÏÓÔÁÑ ÈÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ - $f(x) = 0$ ÄÌÑ ×ÓÅÈ ÃÅÌÙÈ x. âÏÌÅÅ ÉÎÔÅÒÅÓÎÁ ÆÕÎËÃÉÑ $f(x) = x \mod 37$, ËÏÔÏÒÁÑ ÏÔÏÂÒÁÖÁÅÔ $x \times$ ÏÓÔÁÔÏË ÏÔ ÄÅÌÅÎÉÑ x ÎÁ 37.

ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÄÏËÕÍÅÎÔÁ - ÒÅÚÕÌØÔÁÔ ÐÒÉÍÅÎÅÎÉÑ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ Ë ÄÏËÕÍÅÎÔÕ. äÌÑ ÔÏÇÏ ÞÔÏÂÙ ÂÙÔØ ÐÏÌÅÚÎÏÊ, ÈÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ ÄÏÌÖÎÁ ÕÄÏ×ÌÅÔ×ÏÒÑÔØ Ä×ÕÍ ×ÁÖÎÙÍ ÕÓÌÏ×ÉÑÍ. ÷Ï-ÐÅÒ×ÙÈ, ÎÁÈÏÄÅÅ Ä×ÕÈ ÄÏËÕÍÅÎÔÏ× Ó ÏÄÉÎÁËÏ×ÙÍ ÚÎÁÞÅÎÉÅÍ ÆÕÎËÃÉÉ ÄÏÌÖÎÏ ÂÙÔØ ÓÌÏÖÎÙÍ. ÷Ï-×ÔÒÙÈ, ÄÏÌÖÎÏ ÂÙÔØ ÓÌÏÖÎÙÍ ×ÏÓÓÔÁÎÏ×ÉÔØ ÄÏËÕÍÅÎÔ ÐÏ ÉÍÅÀÝÅÊÓÑ ÐÏÄÐÉÓÉ.

îÅËÏÔÒÙÅ ÛÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ [1] ÍÇÕÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÙ ÄÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÏ×. ðÏÄÐÉÓÙ×ÁÀÝÉÊ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÄÏËÕÍÅÎÔ Ó×ÏÉÍ *ÓÅËÒÅÔÎÙÍ* ËÌÀÞÏÍ. öÅÌÁÀÝÉÊ ÐÒÏ×ÅÒÉÔ ÐÏÄÐÉÓØ É Õ×ÉÄÅÔØ ÄÏËÕÍÅÎÔ, ÐÒÏÓÔÏ ÉÓÐÏÌØÚÕÅÔ ÏÔËÒÙÔÙÊ ËÌÀÞ ÐÏÄÐÉÓÁ×ÛÅÇÏ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÄÏËÕÍÅÎÔÁ. üÔÏ ÁÌÇÏÒÉÔÍ ÕÄÏ×ÌÅÔ×ÏÒÑÅÔ Ä×ÕÍ ÕÓÌÏ×ÉÑÍ, ÎÁÌÁÇÁÅÍÙÍ ÎÁ ÈÏÒÏÛÕÀ ÈÅÛÉÒÕÀÝÕÀ ÆÕÎËÃÉÀ, ÎÏ ÎÁ ÐÒÁËÔÉËÅ ÏÎ ÓÌÉÛËÏÍ ÍÅÄÌÅÎÎÏ

÷ ËÁÞÅÓÔ×Å ÁÌØÔÅÒÎÁÔÉ×Ù ÉÓÐÏÌØÚÕÀÔÓÑ ÈÅÛÉÒÕÀÝÉÅ ÆÕÎËÃÉÉ, ÕÄÏ×ÌÅÔ×ÏÒÑÀÝÉÅ ÜÔÉÍ Ä×ÕÍ ÕÓÌÏ×ÉÑÍ. SHA É MD5 ÐÒÉÍÅÒÙ ÔÁËÉÈ ÁÌÇÏÒÉÔÍ×. ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÄÁÎÎÏÇÏ ÁÌÇÏÒÉÔÍÁ, ÄÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÁ ×ÙÞÉÓÌÑÔÓÑ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ, É ÚÁÔÅÍ ÜÔÏ ÚÎÁÞÅÎÉÅ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÉÎÎÏÓÔÉ ÄÏËÕÍÅÎÔÁ. ðÏÌÕÞÁÔÅÌØ ÍÏÖÅÔ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ×ÙÞÉÓÌÑ ×ÓÐÏÍÏ× ÚÎÁÞÅÎÉÅ ÆÕÎËÃÉÉ ÄÌÑ ÄÏËÕÍÅÎÔÁ É ÓÒÁ×ÎÉ× ÅÇÏ ÓÏ ÚÎÁÞÅÎÉÅÍ, ×ÙÞÉÓÌÑÎÙÍ ÏÐÒÁ×ÉÔÅÌÅÍ ÄÌÑ ÎÁÓÔÏÑÝÅÇÏ ÄÏËÕÍÅÎÔÁ. åÓÌÉ ÏÎÉ ÓÏ×ÐÁÄÕÔ, ÔÏ ÐÏÞÔÉ ÎÁ×ÅÒÎÑÁ ÄÏËÕÍÅÎÔÙ ÉÄÅÎÔÉÞÎÙ.

ôÅÐÅÒØ ÐÒÏÂÌÅÍÁ ÓÏÓÔÉÔ × ÔÏÍ, ÞÔÏÂÙ ÐÒÅÄÏ×ÒÁÔÉÔØ ÉÚÍÅÎÅÎÉÅ ÐÏÄÐÉÓÉ ÚÌÏÕÍÙÛÌÅÎÎÏÍ. åÓÌÉ ÄÏËÕÍÅÎÔ É ÐÏÄÐÉÓØ ÐÏÓÙÌÁÀÔÓÑ ÎÅÚÁÛÉÆÒÏ×ÁÎÙÍ, ×ÚÌÍÝÉË ÍÏÅÔ ÉÚÍÅÎÉÔØ ÄÏËÕÍÅÎÔ É ×ÙÞÉÓÌÉÔØ ÓÏÎ×ÅÓÔ×ÕÝÅÅ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ, ÂÅÚ ×ÄÄÍÁ ÐÌÕÞÁÔÅÌÑ. åÓÌÉ ÚÁÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÄÏËÕÍÅÎÔ, ×ÚÌÍÝÉË ÍÏÅÔ ÉÚÍÅÎÉÔØ ÚÎÁÞÅÎÉÅ ÐÏÄÐÉÓÉ É ÐÏ×ÁÌÉÔØ ÅÅ ÐÒÏ×ÅÒÕ. ôÒÅÉÊ ÕÞÁÓÔÎÉË ÍÏÖÅÔ ×ÙÐÏÌÎÑÔØ ÔÏÌØËÏ ÄÏËÕÍÅÎÔÙ É ÄÏËÕÍÅÎÔÏ×. ïÐÒÁ×ÉÔØ ÉÓÐÏÌØÚÕÅÔ Ó×ÏÊ ÚÁËÒÙÔÙÊ ËÌÀÞ, É ÌÀÂÏÊ ÍÏÅÔ ×ÏÓÐÏÌØÚÏ×ÁÔØÓÑ ÅÇÏ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÄÏÌÖÎÏ ÐÏÄÐÉÓÉ É ÄÏËÕÍÅÎÔÁ. ú×ÕÉÔ ÎÅÐÏÈÏÄ, ÎÏ ÎÁ ÄÅÌÅ ÅÒÕÎÄ. åÓÌÉ ÜÔÏ ÁÌÇÏÒÉÔÍ ÄÅÊÓÔ×ÉÔÅÌØÎÏ

ÚÁÝÉÝÁÅÔ ÄÏËÕÍÅÎÔ, ÏÎ, ÔÁËÖÅ, ÚÁÝÉÝÁÅÔ ÅÇÏ ÏÔ ÐÏÄÄÅÌËÉ, É ÎÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ ÅÇÏ ÐÏÄÐÉÓÙ×ÁÔØ. ÷ ÄÅÊÓÔ×ÉÔÅÌØÎÏÓÔÉ, ÜÔÏ ÍÅÔÏÄ ÎÅ ÚÁÝÉÝÁÅÔ ÄÏËÕÍÅÎÔ ÏÔ ÐÏÄÄÅÌËÉ. úÁËÒÙÔÙÍ ËÌÀÞÏÍ ÏÔÐÒÁ×ÉÔÅÌÑ ÛÉÆÒÕÅÔÓÑ ÔÏÌØËÏ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ ÓÉÍÅÔÒÉ×ÎÏÇÏ ÁÌÇÏÒÉÔÍÁ. ìÀÂÏÊ, ÉÓÐÏÌØÚÕÑ ÏÔËÒÙÔÙÊ ËÌÀÞ ÏÐÒÁ×ÉÔÅÌÑ, ÍÏÖÅÔ ×ÏÓÓÔÁÎÏ×ÉÔØ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ. îÅÔÒÃÄÏÍ, ÚÁÔÅÍ, ÉÚÍÅÎÉÔØ ÄÏËÕÍÅÎÔ, ÚÁÛÉÆÒÏ×ÁÔØ ÅÇÏ ÏÂÒÁÔÎÏ, ÉÓÐÏÌØÚÕÑ ÐÏÕÞÅÎÎÙÊ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ, É ÐÅÒÅÓÌÁÔØ ÄÁÌØÛÅ ÏÔ ÉÍÅÎÉ ÏÐÒÁ×ÉÔÅÌÑ.

áÌÇÏÒÉÔÍ, ËÏÔÏÒÙÊ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÒÁÂÏÔÁÅÔ, ÉÓÐÏÌØÚÕÅÔ ÍÅÔÏÄ ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ ÔÏÌØËÏ ÚÁÞÅÎÉÑ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ. ðÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÍÖÅÔ ÂÙÔØ ÏÐÒÁ×ÌÅÎ Ó ÉÓÐÏÌØÚÏ×ÁÎÉÅÍ ÌÀÂÏÇÏ ÄÒÕÇÏÇÏ ÁÌÇÏÒÉÔÍÁ ÛÉÆÒÏ×ÁÎÉÑ, ÌÉÂÏ × ÞÉÓÔÍÍ ×ÉÄÅ, ÅÓÌÉ ÄÏËÕÍÅÎÔ ÎÅ ÓÏÄÅÒÖÉÔ ËÍÎÆÉÄÅÎÃÉÁÌØÎÙÈ Ó×ÅÄÅÎÉÊ. åÓÌÉ ÄÏËÕÍÅÎÔ ÉÚÍÅÎÅÎ ÐÒÏ×ÅÒÅÎ ÐÏÄÐÉÓÉ ÐÏÔÅÒÐÅÎ ÎÅÕÄÁÞÕ. óÔÁÎÄÁÒÔ ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓÉ DSA ÒÁÂÏÔÁÅÔ ÔÁË, ËÁË ÂÙÌÏ ÏÐÉÓÁÎÏ. DSA - ÏÓÎÏ×ÎÏÊ ÁÌÇÏÒÉÔÍ ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓÉ, ÉÓÐÏÌØÚÕÅÍÙÊ × GnuPG.

1. ûÉÆÒ ÄÏÌÖÅÎ ÏÂÌÁÄÁÔØ ÔÅÍ Ó×ÏÊÓÔ×ÏÍ, ÞÔÏ É ÎÁÓÔÏÑÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, É ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÍÇÕÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÙ ÁÌÇÏÒÉÔÍÍ ÛÉÆÒÏ×ÁÎÉÑ ËÁË ÏÔËÒÙÔÙÊ ËÌÀÞ. RSA - ÐÒÉÍÅÒ ÔÁËÏÇÏ ÁÌÇÏÒÉÔÍÁ, Á ElGamal ÎÅÔ.

3. õÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ

ðÏÄÄÅÌËÁ ËÌÀÞÁ - ÎÁÉÂÏÌÅÅ ÓÌÁÂÏÅ ÍÅÓÔÏ × ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÌÏÕÍÙÛÌÅÎÎÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÐÏÌØÚÏ×ÁÔÅÌØÓËÕÀ Ó×ÑÚËÕ ËÌÀÞÅÊ ÉÌÉ ÐÏÄÄÅÌÁÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ ÐÏÌØÚÏ×ÁÔÅÌÑ É ÐÏÓÙÁÔØ ÅÇÏ ÄÒÕÇÉÍ ÄÌÑ ÚÁÇÒÕÚËÉ É ÉÓÐÏÌØÚÏ×ÁÎÉÑ. îÁÐÒÉÍÅÒ, ÐÒÅÄÐÏÌÏÖÉÍ, ÞÔÏ èÌÏÊ ÈÏÞÅÔ ÏÔÓÌÅÖÉ×ÁÔØ ÓÏÎÂÝÅÎÉÑ, ËÏÔÒÙÅ üÌÉÓ ÐÏÓÙÁÅÔ âÌÜÊËÕ. ïÎÁ ÍÇÌÁ ÂÙ ÉÓÐÏÌØÚÏ×ÁÔØ ÁÔÁËÕ, ÎÁÚÙ×ÁÅÍÕÀ *ÞÅÌÏ×ÅË × ÓÅÒÅÄÉÎÅ (man in the middle)*. äÌÑ ÜÔÇÏ èÌÏÊ ÓÏÚÄÁÅÔ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ. ïÎÁ ÚÁÍÅÎÑÅÔ ËÏÐÉÀ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ âÌÜÊËÁ, ÐÒÉÎÄÌÅÖÝÕÀ üÌÉÓ, ÎÏ×ÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÁÔÅÍ ÏÎÁ ÐÅÒÅ×ÁÔÙ×ÁÅÔ ÓÏÏÂÝÅÎÉÑ, ËÏÔÏÒÙÅ üÌÉÓ ÐÏÓÙÁÅÔ âÌÜÊËÕ. ëÁÖÄÏÅ ÐÅÒÅ×ÁÞÅÎÎÅ ÓÏÏÂÝÅÎÉÅ ÏÎÁ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ, ÉÓÐÏÌØÚÕÑ ÎÏ×ÙÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÎÁÓÔÑÝÉÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ âÌÜÊËÁ É ÎÁÐÒÁ×ÌÑÅÔ ÉÈ ÅÍÕ. ÷ÓÅ ÓÏÏÂÝÅÎÉÑ, ÎÁÐÒÁ×ÌÅÎÎÙÅ üÌÉÓ âÌÜÊËÕ, ÔÅÐÅÒØ ÍÇÕÔ ÂÙÔØ ÐÒÏÞÉÔÁÎÙ èÌÏÊ.

ðÒÁ×ÉÌØÎÏÅ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ Ñ×ÌÑÅÔÓÑ ÒÅÛÁÀÝÉÍ ÆÁËÔÏÒÏÍ ÄÌÑ ÏÂÅÓÐÅÞÅÎÉÑ ÃÅÌÏÓÔÎÏÓÔÉ ÎÅ ÔÏÌØËÏ ÷ÁÛÉÈ Ó×ÑÚÉË ËÌÀÞÅÊ, ÎÏ É Ó×ÑÚÉË ËÌÀÞÅÊ ÄÒÕÇÉÈ ÐÌØÚÏ×ÁÔÅÌÅÊ. ïÓÎÏ×ÎÊ ÕÐÒÁ×ÌÅÎÉÑ ËÌÀÞÁÍÉ × GnuPG Ñ×ÌÑÅÔÓÑ ÐÏÄÐÉÓÁÎÉÅ ËÌÀÞÅÊ. ðÏÄÐÉÓÁÎÉÅ ËÌÀÞÅÊ ÉÍÅÅÔ Ä×Á ÏÓÎÏ×ÎÙÈ ÐÒÉÍÅÎÅÎÉÑ: ÜÔÏ ÐÏÚ×ÌÑÅÔ ÷ÁÍ ÏÂÎÁÒÕÖÉ×ÁÔØ ×ÍÅÛÁÔÅÌØÓÔ×Ï × ÷ÁÛÕ Ó×ÑÚËÕ ËÌÀÞÅÊ, Á ÔÁËÖÅ ÐÏÚ×ÌÑÅÔ ÕÄÏÓÔÏ×ÅÒÝÁÔØ ÞÔÏ ËÌÀÞ ÄÅÉÓ×ÉÔÅÌØÎÏ ÐÒÉÎÁÄÌÅÖÉÔ ÞÅÌÏ×ÅËÕ, ÞØÉÍ ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ÐÌØÚÏ×ÁÔÅÌÑ ÎÏ ÐÍÅÞÅÎ. ðÏÄÐÉÓÉ ÎÁ ËÌÀÞÁÈ ÔÁËÖÅ ÉÓÐÏÌØÚÕÀÔÓÑ × ÓÈÅÍÅ ÉÚ×ÅÓÔÎÏÊ ËÁË *ÓÅÔØ ÄÏ×ÅÒÉÑ (web of trust)*, ËÏÔÏÒÁÑ ÒÁÓÛÉÒÑÅÔ ÄÏÐÕÓÔÉÍÙÅ ËÌÀÞÉ ÎÅ ÔÏÌØËÏ ÐÏÄÐÉÓÁÎÎÙÍÉ ÌÉÞÎÏ ÷ÁÍÉ, ÎÏ É ÐÏÄÐÉÓÁÎÎÙÍÉ ÌÀÄØÍÉ, ËÏÔÏÒÙÍ ÷Ù ÄÏ×ÅÒÑÅÔÅ. áËËÕÒÁÔÎÙÅ ÐÌØÚÏ×ÁÔÅÌÉ, ÐÒÁ×ÉÌØÎÏ ÒÅÁÌÉÚÏ×Á×ÛÉÅ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ, ÍÇÕÔ ÉÓËÌÀÞÉÔØ ÐÏÄÍÅÎÕ ËÌÀÞÅÊ ËÁË ×ÉÄ ÁÔÁËÉ ÎÁ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏÓÔØ Ó×ÑÚÉ ÐÒÉ ÐÍÍÝÉ GnuPG.

3.1. õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÐÁÒÏÊ ËÌÀÞÅÊ

ðÁÒÁ ËÌÀÞÅÊ ÓÏÓÔÏÉÔ ÉÚ ÏÔËÒÙÔÏÇÏ É ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÅÊ. ïÔËÒÙÔÙÊ ËÌÀÞ ÓÏÓÔÏÉÔ ÉÚ ÏÔËÒÙÔÏÊ ÞÁÓÔÉ ÇÌÁ×ÎÏÇÏ ÐÏÄÐÉÓÙ×ÁÀÝÅÇÏ ËÌÀÞÁ, ÏÔËÒÙÔÙÈ ÞÁÓÔÅÊ ÐÏÄÞÉÌÅÎÙÈ ÐÏÄÐÉÓÙ×ÁÀÝÉÈ É ÛÉÆÒÏÀÝÉÈ ËÌÀÞÅÊ, ÎÁÂÏÓÁ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÎØÚÏ×ÁÔÅÌÑ, ÁÓÓÏÃÉÉÒÕÀÝÉÈ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó ÒÅÁÌØÎÙÍ ÞÅÌ×ÅËÍÍ. ëÁÖÁÑ ÞÁÓÔØ ÓÏÄÅÒÖÉÔ ÄÁÎÎÙÅ Ï ÓÅÂÅ. äÌÑ ËÌÀÞÁ ÜÔÏ ÅÇÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ, ÄÁÔÁ ÓÏÚÄÁÎÉÑ, ÓÒÏË ÄÅÊÓ×ÉÑ É Ô.Ä. äÌÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÎØÚÏ×ÁÔÅÌÑ ÜÔÏ ÉÍÑ ÞÅÌ×ÅËÁ, ÄÏÐÏÎÉÔÅÌØÎÙÊ ËÏÍÍÅÎÔÁÒÉÊ É ÁÄÒÅ email. óÔÒÕËÔÕÒÁ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÁÎÁÌÏÇÉÞÎÁ, ÎÏ ÓÏÄÅÒÖÉÔ ÓÅËÒÅÔÎÙÅ ÞÁÓÔÉ ËÌÀÞÅÊ É ÎÅ ÓÏÄÅÒÖÉÔ ÉÎÆÏÒÍÁÃÉÀ ÏÂ ÉÄÅÎÔÉÆÉËÁÔÏÒÅ ÐÎØÚÏ×ÁÔÅÌÑ.

äÌÑ ÐÒÏÓÍÏÔÒÁ ÐÁÒÙ ËÌÀÞÅÊ ÉÓÐÏØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--edit-key`. îÁÐÒÉÍÅÒ,

```
chloe% gpg --edit-key chloe@cyb.org
Secret key is available.

pub  1024D/26B6AAE1  created: 1999-06-15 expires: never      trust: -/u
sub  2048g/0CF8CB7A  created: 1999-06-15 expires: never
sub  1792G/08224617  created: 1999-06-15 expires: 2002-06-14
sub   960D/B1F423E7  created: 1999-06-15 expires: 2002-06-14
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>
Command>
```

ðÒÉ ÏÔÏÂÒÁÖÅÎÉÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ×Ù×ÏÄÉÔÓÑ ÉÎÆÏÒÍÁÃÉÑ Ï ÔÏÍ, ÄÏÓÔÒÁÎ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÉÌÉ ÎÅÔ. úÁÔÅÍ ×Ù×ÏÄÉÔÓÑ ÉÎÆÏÒÍÁÃÉÑ Ï ËÁÖÄÏÍ ËÏÍÐÏÎÅÎÔÅ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ðÅÒ×ÁÑ ËÏÌÏÎËÁ ÐÏËÁÚÙ×ÁÅÔ ÔÉÐ ËÌÀÞÁ. óÉÍ×ÏÌ `pub` ÕÊÁÚÙ×ÁÀÔ ÏÔËÒÙÔÏÇÏ ÇÌÁ×ÎÏÇÏ ÐÏÄÐÉÓÙ×ÁÀÝÅÇÏ ËÌÀÞÁ, Á ÓÉÍ×ÏÌ `sub` ÏÔËÒÙÔÕÀ ÞÁÓÔØ ÐÏÄÞÉÎÅÎÎÙÈ ËÌÀÞÅÊ. ÷ÔÏÒÁÑ ËÏÌÏÎËÁ ÐÏËÁÚÙ×ÁÅÔ ÄÌÉÎÕ ËÌÀÞÁ × ÂÉÔÁÈ, ÔÉÐ É ÉÄÅÎÔÉÆÉËÁÔÏÒ. ôÉÐ `D` ÜÔÏ ËÌÀÞ DSA, `g` - ËÌÀÞ ElGamal, ÐÒÉÇÏÄÎÙÊ ÔÏÌØËÏ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ, É `G` - ËÌÀÞ ElGamal, ËÏÔÏÒÙÊ ÍÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ É ÄÌÑ ÐÏÄÐÉÓÉ É ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. äÁÔÁ ÓÏÚÄÁÎÉÑ É ÏËÏÎÞÁÎÉÑ ÓÒÏËÁ ÄÅÊÓ×ÉÑ ÐÏËÁÚÁÎÁ × ËÏÌÏÎËÁÈ ÔÒÉ É ÞÅÔÙÒÅ. éÄÅÎÔÉÆÉËÁÔÏÒ ÐÎØÚÏ×ÁÔÅÌÑ ÐÒÅÄÓÔÁÎÙ ÐÏÓÌÅ ËÌÀÞÅÊ.

äÏÐÏÎÎÉÔÅÌØÎÁÑ ÉÎÆÏÒÍÁÃÉÑ Ï ËÌÀÞÅ ÍÏÖÅÔ ÂÙÔØ ÐÏÎÕÞÅÎÁ ÒÁÚÌÉÞÎÙÍÉ ËÏÍÁÎÄÁÍÉ. ëÏÍÁÎÄ **toggle** ÐÅÒÅËÌÀÞÁÅÔ ÍÅÖÄÕ ÏÔËÒÙÔÏÊ É ÚÁËÒÙÔÏÊ ËÏÍÐÏÎÅÎÔÁÍÉ ÐÁÒÙ ËÌÀÞÅÊ, ÅÓÌÉ ÏÎÅ ÉÚ ÎÉÈ ÄÏÓÔÕÐÎÙ.

```
Command> toggle

sec  1024D/26B6AAE1  created: 1999-06-15 expires: never
sbb  2048g/0CF8CB7A  created: 1999-06-15 expires: never
sbb  1792G/08224617  created: 1999-06-15 expires: 2002-06-14
sbb   960D/B1F423E7  created: 1999-06-15 expires: 2002-06-14
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>
```

ðÒÅÄÓÔÁ×ÌÅÎÎÁÑ ÉÎÆÏÒÍÁÃÉÑ ÐÏÄÏÂÎÁ ×Ù×ÏÄÉÍÏÊ ÄÌÑ ÎÔËÒÙÔÏÇÏ ËÌÀÞÁ. óÉÍ×ÏÌÙ `sec` ÕËÁÚÙ×ÁÀÔ ÓÅËÒÅÔÎÙÊ ÇÌÁ×ÎÙÊ ÐÏÄÐÉÓÙ×ÁÀÝÉÊ ËÌÀÞ, ÓÉÍ×ÏÌÙ `sbb` ÕËÁÚÙ×ÁÀÔ ÓÅËÒÅÔÎÙÅ ÐÏÄÞÉÎÅÎÎÙÅ ËÌÀÞÉ. ôÁËÖÅ ×Ù×ÏÄÑÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÌØÚÏ×ÁÔÅÌÑ ÉÚ ÎÔËÒÙÔÏÇÏ ËÌÀÞÁ.

3.1.1. ãÅÌÏÓÔÏÓÔØ ËÌÀÞÁ.

ðÒÉ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ÎÔËÒÙÔÏÇÏ ËÌÀÞÁ ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ ÎÔËÒÙÔÙÅ ËÏÍÐÏÎÅÎÔÙ ÷ÁÛÅÇÏ ÇÌÁ×ÎÏÇÏ É ÐÏÄÞÉÎÅÎÎÙÈ ËÌÀÞÅÊ É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÌØÚÏ×ÁÔÅÌÑ. òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ÜÔÏÇÏ ÍÁÔÅÒÉÁÌÁ, ÏÂÙÞÎÏ, ÒÉÓÕÅÔ ×ÁÛÅÊ ÓÏÂÓÔ×ÅÎÎÏ ÓÏÂÓÔ×ÅÎÎÏÊ ÐÏÄÐÉÓÉ, Ô.Ë. ÄÅÌÅÔ ×ÏÚÍÏÖÎÏÊ ÐÏÄÍÅÎÏ ËÌÀÞÁ. ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎ ÄÏÂÁ×ÌÅÎÁÍ ÉÌÉ ÚÁÍÅÝÅÎ ËÌÀÞÅÊ, ÉÌÉ ÄÏÂÁ×ÌÅÎÁÍ ÉÌÉ ÚÁÍÅÝÅÎ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÌØÚÏ×ÁÔÅÌÑ. ðÏÄÐÉÓÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÌØÚÏ×ÁÔÅÌÑ, ×ÚÌÍÝÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ email ÁÄÒÅÓ ÐÌØÚÏ×ÁÔÅÌÑ, ÞÔÏÂÙ ÐÌÕÞÁÔØ ÐÅÒÅÁÐÒÁ×ÌÅÎÎÕÀ ÅÍÕ ÐÏÞÔÕ. ðÒÉ ÉÚÍÅÎÅÎÉÉ ÏÄÎÏÇÏ ÉÚ ËÌÀÞÅÊ ÛÉÆÒÏ×ÁÎÑ, ×ÚÌÍÝÉË ÓÍÏÖÅÔ, ÔÁËÖÅ, ÒÁÓÛÉÆÒÏ×Ù×ÁÔØ ÐÅÒÅÁÐÒÁ×ÌÅÎÎÕÀ ÅÍÕ ÓÏÏÂÝÅÎÉÑ.

éÓÐÏÌØÚÏ×ÁÎÅ ÃÉÆÒÏ×ÙÈ ÐÏÄÐÉÓÅÊ ÒÅÛÁÅÔ ÜÔÕ ÐÒÏÂÌÅÍÕ. ëÏÇÄÁ ÄÁÎÎÙÅ ÐÏÄÐÉÓÁÎÙ ÓÅËÒÅÔÎÙÍ ËÌÀÞÏÍ, ÓÏÏÔ×ÅÔÓ×ÕÝÉÊ ÎÔËÒÙÔÙÊ ËÌÀÞ ÏÇÒÁÎÉÞÅÎ ÐÏÄÐÉÓÁÎÎÙÍÉ ÄÁÎÎÙÍÉ. äÒÕÇÉÍÉ ÓÏÏ×ÁÍ, ÔÏÌØËÏ ÓÏÏÔ×ÅÔÓÔ×ÕÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÅÊ É ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ ÄÁÎÎÙÅ ÎÅ ÂÙÌÉ ÉÚÍÅÎÅÎÙ.

ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÚÁÝÉÝÅÎ ÏÔ ÉÚÍÅÎÅÎÉÑ ÉÓÐÏØÚÏ×ÁÎÉÅÍ ÓÏÏÔ×ÅÔÓ×ÕÀÝÅÇÏ ÇÌÁ×ÎÏÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÄÌÑ ÐÏÄÐÉÓÉ ËÏÍÐÏÎÅÎÔÏ× ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ É ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÏØÚÏ×ÁÔÅÌÑ, ÐÒÉ×ÑÚÙ×ÁÑ, ÔÁËÉÍ ÏÂÒÁÚÏÍ, ËÏÍÐÏÎÅÎÔÙ ÇÌÁ×ÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ðÏÄÐÉÓÙ ËÏÍÐÏÎÅÎÔ× ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÓÏÏÔ×ÅÔÓ×ÕÀÝÉÍ ÇÌÁ×ÎÙÍ ÓÅËÒÅÔÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ ÎÁÚÙ×ÁÅÔÓÑ *ÓÁÍÏÐÏÄÐÉÓØÀ (self-signing)*, É ÏÔËÒÙÔÙÊ ËÌÀÞ, ÉÍÅÀÝÉÊ ÓÁÍÏÐÏÄÐÉÓÁÎÎÙÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏØÚÏ×ÁÔÅÌÑ, ÐÒÉ×ÑÚÁÎÎÙÅ Ë ÎÅÍÕ, ÎÁÚÙ×ÁÅÔÓÑ *ÓÅÒÔÉÆÉËÁÔÏÍ (certificate)*.

îÁÐÒÉÍÅÒ, Õ èÌÎÊ ÅÓÔØ Ä×Á ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏØÚÏ×ÁÔÅÌÑ É ÔÒÉ ÐÏÄÌÀÞÁ. ðÏÄÐÉÓÉ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁÈ ÐÏØÚÏ×ÁÔÅÌÑ ÍÏÇÕÔ ÂÙÔØ ÐÒÏ×ÅÒÅÎÙ ËÏÍÁÎÄÏÊ **check** ÉÚ ÍÅÎÀ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ ËÌÀÞÁ.

```
chloe% gpg --edit-key chloe
Secret key is available.

pub  1024D/26B6AAE1  created: 1999-06-15 expires: never      trust: -/u
sub  2048g/0CF8CB7A  created: 1999-06-15 expires: never
sub  1792G/08224617  created: 1999-06-15 expires: 2002-06-14
sub   960D/B1F423E7  created: 1999-06-15 expires: 2002-06-14
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>

Command> check
uid  Chloe (Jester) <chloe@cyb.org>
sig!       26B6AAE1 1999-06-15   [self-signature]
uid  Chloe (Plebian) <chloe@tel.net>
sig!       26B6AAE1 1999-06-15   [self-signature]
```

ëÁË É ÏÖÉÄÁÌÏÓØ, ×ÓÅ ÐÏÄÐÉÓÉ ÓÄÅÌÁÎÙ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ Ó ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ËÌÀÞÁ `0x26B6AAE1`. óÁÍÏÐÏÄÐÉÓÉ ÎÁ ÐÏÄÌÀÞÁÈ ÔÁËÖÅ ÐÒÅÄÓÔÁ×ÌÅÎÙ × ÏÔËÒÙÔÏÍ ËÌÀÞÅ, ÎÏ ÏÎÉ ÎÅ ÐÏËÁÚÙ×ÁÀÔÓÑ × GnuPG.

3.1.2. äÏÂÁ×ÌÅÎÉÅ É ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ

ëÁË ÎÏ×ÙÅ ÐÏÄËÌÀÞÉ, ÔÁË É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏØÚÏ×ÁÔÅÌÑ ÍÏÇÕÔ ÂÙÔØ ÄÏÂÁ×ÌÅÎÙ Ë ÷ÁÛÅÊ ÐÁÒÅ ËÌÀÞÅÊ ÐÏÓÌÅ ÅÅ ÓÏÚÄÁÎÉÑ.

éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÄÏÂÁ×ÌÑÅÔÓÑ ËÏÍÁÎÄÏÊ **adduid**. ÷Ù ÂÕÄÅÅ ÚÁÐÒÏÛÅÎÙ ÏÔÎÏÓÉÔÅÌØÎÏ ÷ÁÛÉÈ ÉÍÅÎÉ, ÁÄÒÓÁ email É ËÏÍÍÅÎÔÁÒÉÑ, ÔÁËÖÅ ËÁË ÐÒÉ ÓÏÚÄÁÎÉÉ ÐÁÒÙ ËÌÀÞÅÊ. ðÏÄËÌÀÞ ÄÏÂÁ×ÌÑÅÔÓÑ ËÏÍÁÎÄÏÊ **addkey**. ðÒÏÃÅÄÕÒÁ ÁÎÁÌÏÇÉÞÎÁ ÉÓÐÏÌØÚÕÅÍÏÊ ÐÒÉ ÐÅÒ×ÉÞÎÏÍ ÓÏÚÄÁÎÉÉ ÐÁÒÙ ËÌÀÞÅÊ. ðÏÄËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ DSA ËÌÀÞÍÍ, ElGamal ËÌÀÞÍÍ ÐÒÉÇÏÄÎÙÍ ÔÏÌØËÏ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ, ÉÌÉ ËÌÀÞÍÍ ElGamal ÐÒÉÇÏÄÎÙÍ É ÄÌÑ ÐÏÄÐÉÓÉ É ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ëÏÇÄÁ ÓÏÚÄÁÀÔÓÑ ÐÏÄËÌÀÞ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÏÎÉ ÐÏÄÐÉÓÙ×ÁÀÔÓÑ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÍÍ, ÄÌÑ ÞÅÇÏ ÷Ù ÄÎÏÖÎÙ ×ÓÅÔÉ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ ÐÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ.

äÏÐÏÎÉÔÅÌØÎÙÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÒÉÅÎÉÎÙ, ËÏÇÄÁ ÷Ù ×ÙÓÔÕÐÁÅÔÅ × ÎÅÓËÏÌØËÉÈ ËÁÞÅÓÔ×ÁÈ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ ÒÁÂÏÔÉËÏÍ ËÁËÏÊ-ÌÉÂÏ ÆÉÒÍÙ É, × ÔÏ ÖÅ ×ÒÅÍÑ, ÐÏÌÉÔÉÞÅÓËÉÍ ÄÅÑÔÅÌØÎÏÓÔÉ ÂÕÄÕÔ ÚÎÁÔØ ÷ÁÓ ÐÏ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÅÍÕ ×ÉÄÕ ÄÅÑÔÅÌØÎÏÓÔÉ ÂÕÄÕÔ ÚÁÐÒÅÝÅÎÙ ÎÅÚÁËÏÎÎÙÍÉ ÓÐÏÓÏÂÁÍÉ. ôÁË ËÁË ÜÔÉ ÇÒÕÐÐÙ ÌÀÄÅÊ ÎÅ ÐÒÅÄÓÔÁ×ÌÑÀÔ, ÔÏ ËÁÖÄÁÑ ÇÒÕÐÐÁ ÍÏÖÅÔ ÎÅ ÄÏ×ÅÒÑÔØ ÄÒÕÇÏÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ. óÌÅÄÏ×ÁÔÅÌØÎÏ, ÏÂÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÎÕÖÎÙ.

äÏÐÏÎÉÔÅÌØÎÙÅ ÐÏÄËÌÀÞÉ ÔÁËÖÅ ÍÏÇÕÔ ÂÙÔØ ÐÏÌÚÏÙ. éÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÁÓÓÏÃÉÉÒÏ×ÁÎÎÙÅ Ó ÷ÁÛÉÍ ÇÌÁ×ÎÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÚÁ×ÅÑÀÔÓÑ ÄÒÕÇÉÍÉ ÌÀÄØÍÉ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÁÅÔÅÓØ, É ÓÍÅÎÁ ÇÌÁ×ÎÏÇÏ ËÌÀÞÁ, ÓÌÅÄÏ×ÁÔÅÌØÎÏ, ÐÏÔÒÅÂÕÅÔ ÐÅÒÅÐÒÏÄÐÉÓÙ×ÁÎÉÑ ÄÒÕÇÉÈ ÌÀÄØÅÊ. üÔÏ ÍÏÖÅÔ ËÁÚÁÔØÓÑ ÓÌÏÖÎÙÍ É ÚÁÎÑÔÏÍ, ÐÏÜÔÏÍÕ ÐÒÅÄÐÏÞÔÅÎÉÅ ÌÀÄØÍÉ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÁÅÔÅ, ÓÏÚÄÁÀÔ ÓÅÔØ ÍÏÇÉÈ ÌÀÞÁ, ÓÌÅÄÏ×ÁÔÅÌØÎÏ, ÐÏÔÒÅÂÕÅÔ ÐÅÒÅÐÒÏÄÐÉÓÙ×ÁÎÉÑ ÄÒÕÇÉÈ ÌÀÄØÅÊ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÎÅÐÒÅÄÓÔÁ×ÌÅÎÎÏÓÔØ ÐÒÉ ÐÅÒÅÄÁÞÅ ÓÅÒÉÉ ×ÚÁÉÍÏÄÅÊÓÔ×ÉÊ ÍÅÖÄÕ ÐÏÌØÚÏ×ÁÔÅÌÑÍÉ ÍÏÖÅÔ ÐÒÉ×ÅÓÔÉ ×ÏÚÍÏÖÎÏÍÕ ÎÁÒÕÛÅÎÉÀ ÂÅÚÏÐÁÓÎÏÓÔÉ. ÷ ÔÁËÉÈ ÓÌÕÞÁÑÈ ÐÒÅÄÐÏÞÔÅÎÉÅ ÄÏÌÖÎÏ ÂÙÔØ ÄÁÎÏ ÐÏÌØÚÏ×ÁÔÅÌÀ, ÞÔÏÂÙ ÏÎ ÍÏÇ ÓÁÍ ÒÅÛÉÔØ, ÎÕÖÅÎ ÌÉ ÅÍÕ ÉÓÐÏÌØÚÏ×ÁÔØ ÓÉÌØÎÕÀ ÁÕÔÅÎÔÉÆÉËÁÃÉÀ.

ðÒÉÍÅÒ É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ ÍÏÇÕÔ ÂÙÔØ ÕÄÁÌÅÎÙ. äÌÑ ÕÄÁÌÅÎÉÑ ÐÒÉÍÅÒÁ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÷Ù ÄÏÌÖÎÙ ÓÎÁÞÁÌÁ ×ÙÂÒÁÔØ ÅÇÏ, ÉÓÐÏÌØÚÕÑ ËÏÍÁÎÄÕ **key** ÉÌÉ **uid**. üÔÏ ËÏÍÁÎÄÙ ÐÅÒÅËÌÀÞÁÔÅÌÉ. îÁÐÒÉÍÅÒ, ËÏÍÁÎÄÁ **key *2*** ×ÙÅÒÅÔ ×ÔÏÒÏÊ ÐÒÉÍÅÒ, ÐÏ×ÔÏÒÎÑ ËÏÍÁÎÄÁ **key *2*** ÏÎÉÅÔ ×ÙÅÛÅÎÎÙÊ ÁÒÇÕÍÅÎÔ, ×ÙÅÌ ×ÓÅ ÐÒÅÄÌÀÅÊ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÌØÚÏ×ÁÔÅÌÑ ÂÕÄÅÔ ÏÎÉÅÎÅÎ. åÓÌÉ

ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏØÚÏ×ÁÔÅÌÑ, ËÏÔÏÒÙÊ ÎÁÄÏ ÕÄÁÌÉÔØ, ×ÙÂÒÁÎ, ÔÏ ËÏÍÁÎÄÁ **deluid** ÕÄÁÌÉÔ ÅÇÏ ÉÚ ËÌÀÞÁ. áÎÁÌÏÇÉÞÎÏ, ËÏÍÁÎÄÁ **delkey** ÕÄÁÌÑÅÔ ×ÓÅ ×ÙÂÒÁÎÎÙÅ ÐÏÄËÌÀÞÉ ÉÚ ÏÂÏÉÈ, ÏÔËÒÙÔÏÇÏ É ÓÅËÒÅÔÎÏÇÏ, ËÌÀÞÅÊ.

äÌÑ ÕÐÒÁ×ÌÅÎÉÑ ÌÏËÁÌØÎÙÍÉ Ó×ÑÚËÁÍÉ ËÌÀÞÅÊ, ÕÄÁÌÅÎÅ ËÏÍÐÏÎÅÎÔ× ËÌÀÞÁ ÈÏÞÛÉÊ ÓÐÏÓÎÂ ÏÞÉÓÔÉÔØ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÄÒÕÇÉÈ ÌÀÄÅÊ ÏÂ ÎÅÎÕÖÎÏÇÏ ÍÁÔÅÒÉÁÌÁ. õÄÁÌÅÎÅ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÏÌØÚÏ×ÁÔÅÌÑ É ÐÏÄËÌÀÞÅÊ ÉÚ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ ËÌÀÞÁ, ÏÄÎÁËÏ, ÎÅ ×ÓÅÇÄÁ ÒÁÚÕÍÎÏ, Ô.Ë. ÕÓÌÏÖÎÅÔ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÁ. ðÏ ÕÍÍÏÞÁÎÉÀ, ËÏÇÄÁ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÐÏÒÔÉÒÕÅÔ ÷ÁÛ ÏÂÏ×ÌÅÎÎÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, ÔÏÔ ÏÂßÅÄÉÎÅÔÓÑ ÓÏ ÓÔÁÔÕÓÏÍ ÄÏÖÄÉÔÅÌØ ÷ÁÛÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÅÓÌÉ ÏÎÁ ÅÓÔØ × Ó×ÑÚËÅ. ëÏÍÐÏÎÅÎÔÙ ÏÂÏÉÈ ËÌÀÞÅÊ ÏÂßÅÄÉÎÑÀÔÓÑ, É ÜÔÏ - ÜÆÆÅËÔÉ×ÎÙÊ ÓÐÏÓÏÂ ×ÏÓÔÁÎÏ×ÉÔØ ÕÄÁÌÅÎÎÙÅ ÷ÁÍÉ ËÏÍÐÏÎÅÎÔÙ. þÔÏÂÙ ÐÒÁ×ÉÌØÎÏ ÏÂÎ×ÉÔØ ËÌÀÞ, ÐÏÌØÚÏ×ÁÔÅÌØ ÄÏÖÅÎ ÓÎÁÞÁÌÁ ÕÄÁÌÉÔØ ÓÔÁÒÕÀ ×ÅÒÓÉÀ ÷ÁÛÅÇÏ ËÌÀÞÁ É ÔÏÌØËÏ ÚÁÔÅÍ ÉÍÐÏÒÔÉÒÏ×ÁÔØ ÎÏ×ÕÀ. üÔÏ ÄÏÂÁ×ÌÑÅÔ ÍÏÒËÉ ÌÀÄÑÍ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÁÅÔÅÓØ. ëÒÏÍÅ ÔÏÇÏ, ÅÓÌÉ ÷Ù ÏÔÐÒÁ×ÌÑÅÔÅ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ, ÏÂßÅÄÉÎÅÎÉÅ ÐÒÏÉÚÏÊÄÅÔ ÎÅÍÉÎÕÅÍÏ, É ÎÉËÔÏ ÉÚ ÐÌÕÞÉ×ÛÉÈ ÷ÁÛ ËÌÀÞ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ ÎÉËÏÇÄÁ ÎÅ ÕÚÎÁÅÔ Ï ÔÏÍ, ÞÔÏ ÷Ù ÞÔÏ-ÔÏ ÔÁÍ ÕÄÁÌÉÌÉ. óÌÅÄÏ×ÁÔÅÌØÍÏ, ÄÌÑ ÏÂÍ×ÌÅÎÑ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ ËÌÀÞÁ ÌÕÞÛÅ ÏÔÚ×ÁÔØ ÓÏÏÔ×ÅÔÓÔ×ÕÝÉÅ ËÏÍÐÏÎÅÎÔÙ ËÌÀÞÁ, ÎÅÖÅÌÉ ÕÄÁÌÑÔØ ÉÈ.

3.1.3. ïÔÚÙ× ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ

äÌÑ ÏÔÚÙ×Á ÐÏÄËÌÀÞÁ ÏÎ ÄÏÖÅÎ ÂÙÔØ ×ÙÂÒÁÎ. âÕÄÕÞÉ ×ÙÂÒÁÎ, ÏÎ ÍÏÖÅÔ ÂÙÔØ ÏÔÏÚ×ÁÎ ËÏÍÁÎÄÏÊ **revkey**. ëÌÀÞ ÏÔÚÙ×ÁÅÔÓÑ ÄÏÂÁ×ÌÅÉÅÍ ÏÔÚÙ×ÁÀÝÅÊ ÓÁÍÏÐÏÄÐÉÓÉ Ë ËÌÀÞÕ. ÷ ÏÔÌÉÞÉÁ ÏÔ ÏÐÃÉÏ ËÏÍÁÎÄÏÊ ÓÔÒÏËÉ --gen-revoke, ÜÆÆÅËÔ ÎÁÓÔÕÐÁÅÔ ÎÁÍÅÄÌÅÎÎÏ.

```
Command> revkey
Do you really want to revoke this key? y

You need a passphrase to unlock the secret key for
user: "Chloe (Jester) <chloe@cyb.org>"
1024-bit DSA key, ID B87DBA93, created 1999-06-28
```

```
pub  1024D/B87DBA93  created: 1999-06-28 expires: never      trust: -/u
sub  2048g/B7934539  created: 1999-06-28 expires: never
sub  1792G/4E3160AD  created: 1999-06-29 expires: 2000-06-28
rev! subkey has been revoked: 1999-06-29
sub   960D/E1F56448  created: 1999-06-29 expires: 2000-06-28
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>
```

éÄÅÎÔÉÆÉËÁÔÏÒ ÐÎÌØÚÏ×ÁÔÅÌÑ ÏÔÍÅÎÑÅÔÓÑ ÉÎÁÞÅ. ëÁË ÐÒÁ×ÉÌÏ, ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÎÌØÚÏ×ÁÔÅÌÑ ÓÔÁ×ÑÔÓÑ ÐÏÄÐÉÓÅ, ÕÄÏÓÔÏ×ÅÒÑÀÝÅÅ ÌÉÞÎÏÓÔØ ÏÂÌÁÄÁÔÅÌÑ ËÌÀÞÁ. ôÅÏÒÅÉÞÅÓËÉ, ÉÄÅÎÔÉÆÉËÁÔÏÒ ×ÅÞÅÎ, Ô.Ë. ÞÅÌ×ÅË ×ÓÅÇÄÁ ÏÓÔÁÅÔÓÑ ÓÏÂÏÊ. îÁ ÐÒÁËÔÉËÅ, ÏÌÅÍÅÎÎ, ÜÌÅÍÅÎÔÙ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÎÌØÚÏ×ÁÔÅÌÑ, ÔÁËÉÅ, ËÁË ÁÄÒÅÓ email É ËÏÍÍÅÎÔÁÒÉÊ ÍÇÕÔ ÉÚÍÅÎÑÔØÓÑ, ÄÅÌÁÑ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÎÌØÚÏ×ÁÔÅÌÑ ÎÅÄÅÊÓÔ×ÉÔÅÌØÎÙÍ.

óÐÅÃÉÆÉËÁÃÉÑ OpenPGP

* *ðÅÒ×ÁÑ ÓÓÙÌËÁ ÎÁ OpenPGP*

ÎÅ ÐÏÄÄÅÒÖÉ×ÁÅÔ ÏÔÚÙ× ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÎÌØÚÏ×ÁÔÅÌÑ, ÎÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÍÖÅÔ ÂÙÔØ ÜÆÆÅËÔÉ×ÎÏ ÏÔÚÙ×ÍÍ ÓÁÍÏÐÏÄÐÉÓÉ ÎÁ ÎÅÍ. ðÏ ÐÒÉÞÉÎÅ ÂÅÚÐÁÓÏÓÔÉ ÏÐÉÓÁÎÙÍ ÒÁÎÅÅ, ËÏÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕÔ ÄÏ×ÅÒÑÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ ÐÎÌØÚÏ×ÁÔÅÌÑ ÎÅ ÉÍÅÀÝÅÍÕ ÓÁÍÏÐÏÄÐÉÓÉ.

ðÏÄÐÉÓØ ÏÔÚÙ×ÁÅÔÓÑ ËÏÍÁÎÄÏÊ **revsig**. ô.Ë. ÷Ù ÍÏÖÅÔÅ ÉÍÅÔØ ÌÀÂÏÅ ÞÉÓÌÏ ÐÏÄÐÉÓÁÎÎÙÈ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÎÌØÚÏ×ÁÔÅÌÑ, ÐÒÏÇÒÁÍÍÁ ÚÁÐÒÏÓÉÔ ÷ÁÓ Ï ËÁÖÄÏÊ ÐÏÄÐÉÓÉ.

```
Command> revsig
You have signed these user IDs:
     Chloe (Jester) <chloe@cyb.org>
   signed by B87DBA93 at 1999-06-28
     Chloe (Plebian) <chloe@tel.net>
   signed by B87DBA93 at 1999-06-28
user ID: "Chloe (Jester) <chloe@cyb.org>"
signed with your key B87DBA93 at 1999-06-28
Create a revocation certificate for this signature? (y/N)n
user ID: "Chloe (Plebian) <chloe@tel.net>"
signed with your key B87DBA93 at 1999-06-28
Create a revocation certificate for this signature? (y/N)y
You are about to revoke these signatures:
```

```
     Chloe (Plebian) <chloe@tel.net>
   signed by B87DBA93 at 1999-06-28
Really create the revocation certificates? (y/N)y

You need a passphrase to unlock the secret key for
user: "Chloe (Jester) <chloe@cyb.org>"
1024-bit DSA key, ID B87DBA93, created 1999-06-28


pub  1024D/B87DBA93  created: 1999-06-28 expires: never      trust: -/u
sub  2048g/B7934539  created: 1999-06-28 expires: never
sub  1792G/4E3160AD  created: 1999-06-29 expires: 2000-06-28
rev! subkey has been revoked: 1999-06-29
sub   960D/E1F56448  created: 1999-06-29 expires: 2000-06-28
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>
```

ïÔÏÚ×ÁÎÎÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏØÚÏ×ÁÔÅÌÑ ÕËÁÚÁÎ ÏÔÚÙ×ÁÀÝÅÊ ÐÏÄÐÉÓØÀ ÐÒÉ ÐÅÒÅÞÉÓÌÅÎÉÉ ÐÏÄÐÉÓÅÊ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁÈ ÐÏØÚÏ×ÁÔÅÌÑ.

```
Command> check
uid  Chloe (Jester) <chloe@cyb.org>
sig!       B87DBA93 1999-06-28   [self-signature]
uid  Chloe (Plebian) <chloe@tel.net>
rev!       B87DBA93 1999-06-29   [revocation]
sig!       B87DBA93 1999-06-28   [self-signature]
```

ïÔÚÙ× É ÐÏÄËÌÀÞÅÊ, É ÓÁÍÏÐÏÄÐÉÓÅÊ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÅ ÐÏØÚÏ×ÁÔÅÌÑ ÄÏÂÁ×ÌÑÅÔ ÏÔÚÙ×ÁÀÝÉÅ ÓÁÍÏÐÏÄÐÉÓÉ Ë ËÌÀÞÕ. ô.Ë. ÐÏÄÐÉÓÉ ÂÙÌÉ ÄÏÂÁ×ÌÅÎÙ, É ÎÉÞÅÇÏ ÎÅ ÕÄÁÌÑÌÏÓØ, ÔÏ ÏÔÚÙ× ×ÓÅÇÄÁ ÂÕÄÅÔ ×ÉÄÅÎ ÄÒÕÇÉÍ ÐÒÉ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ÷ÁÛÅÇÏ ÏÂÏ×ÌÅÎÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ É ÏÂßÄÉÎÅÎÉÉ ÅÇÏ Ó ÒÁÎÎÉÍÉ ËÏÐÉÑÍÉ. ïÔÚÙ×, ÔÁËÉÍ ÏÂÒÁÚÏÍ, ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ Õ ×ÓÅÈ ÂÕÄÅÔ ÎÅÐÒÏÔÉ×ÏÒÅÞÉ×ÁÑ ËÏÐÉÑ ÷ÁÛÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ.

3.1.4. éÚÍÅÎÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ

óÒÏË ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎ ËÏÍÁÎÄÏÊ **expire** ÉÚ ÍÅÎÀ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ ËÌÀÞÁ. åÓÌÉ ÎÅÔ ×ÙÂÒÁÎÎÙÈ ËÌÀÞÅÊ, ÔÏ ÂÕÄÅÔ

ÉÚÍÅÎÅÎ ÓÒÏË ÄÅÊÓÔ×ÉÑ ÐÅÒ×ÉÞÎÏÇÏ ËÌÀÞÁ. éÎÁÞÅ ÉÚÍÅÎÑÅÔÓÑ ÓÒÏË ÄÅÊÓÔ×ÉÑ ×ÙÂÒÁÎÎÏÇÏ ÐÏÄÞÉÎÅÎÎÏÇÏ ËÌÀÞÁ.

÷ÒÅÍÑ ÏËÏÎÞÁÎÉÑ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ Ó×ÑÚÁÎÏ Ó ÓÁÍÏÐÏÄÐÉÓØÀ ÎÁ ËÌÀÞÅ. ïËÏÎÞÁÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ÉÚÍÅÎÑÅÔÓÑ ÕÄÁÌÅÎÉÅÍ ÓÔÁÒÏÊ ÐÏÄÉÓÉ É ÄÏÂÁ×ÌÅÎÉÅÍ ÎÏ×ÏÊ. ôÁË ËÁË ÷ÁÛÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕÔ ÕÄÁÌÑÔØ ÓÔÁÒÕÀ ËÏÐÉÀ ËÌÀÞÁ, ÏÎÉ ÂÕÄÕÔ ×ÉÄÅÎÙ ÄÏÐÏÎÉÔÅÌØÎÕÀ ÓÁÍÏÐÏÄÐÉÓØ ÎÁ ËÌÀÞÅ ÐÏÓÌÅ ÅÇÏ ÏÂÎ×ÌÅÎÉÑ. ðÏÚÄÎÅÊÛÁÑ ÓÁÍÏÐÏÄÐÉÓØ ÉÍÅÅÔ ÐÒÉÏÉÔÅÔ, ÐÏÜÔÏÍÕ ×ÓÅ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÂÕÄÕÔ ÏÂÎÏÚÎÁÐÎÏ ÏÓ×ÅÄÏÍÌÅÎÙ Ï ×ÒÅÍÅÎÉ ÄÅÊÓÔ×ÉÑ ÷ÁÛÅÇÏ ËÌÀÞÁ.

3.2. ðÒÏ×ÅÒËÁ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ × ÷ÁÛÅÊ Ó×ÑÚËÅ

÷ çÌÁ×Å 1 ÂÙÌÁ ÏÐÉÓÁÎÁ ÐÒÏÃÅÄÕÒÁ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÷ÁÛÅÇÏ ËÏÒÒÅÓÐÏÎÄÅÎÔÁ: ËÏÒÒÅÓÐÏÎÄÅÎÔ ÌÉÞÎÏ ÐÒÏ×ÅÒÑÅÔ ÏÐÅÒÁÔÏÒÓÔÉ ÎÁ ÷ÁÛÅÊ ËÏÐÉÉ ËÌÀÞÁ, É ÚÁÔÅÍ ÷Ù ÐÏÄÉÓÙ×ÁÅÔÅ ÅÇÏ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó×ÏÉÍ ÓÅËÒÅÔÎÙÍ. ðÒÉ ÌÉÞÎÏÊ ÐÒÏ×ÅÒËÅ ÏÐÅÒÁÔÏÒ × ×ÌÁÄÅÌØÃÅÍ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ Õ×ÅÒÅÎÙ, ÞÔÏ ËÌÀÞ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÐÒÉÎÁÄÌÅÖÉÔ ÅÍÕ, É, ÐÏÄÉÓÁ× ÅÇÏ, ÷Ù ÓÍÏÖÅÔÅ ÏÂÎÁÕÖÉÔØ ÌÀÂÌÅ ÉÚÍÅÎÅÎÉÅ ËÌÀÞÁ × ÂÕÄÕÝÅÍ. ë ÓÏÖÁÌÅÉÀ, ÜÔÁ ÐÒÏÃÅÄÕÒÁ ÐÒÁËÔÉÞÅÓËÉ Î×ÏÚÍÏÖÎÁ ÅÓÌÉ ÷Ù ÌÉÂÏ ËÏÎÔÁËÔÉÒÕÅÔÅ Ó ÂÏÌØÛÉÍ ÞÉÓÌÏÍ ÌÀÄÅÊ, ÌÉÂÏ ÎÅ ÚÎÁËÏÍÙ ÓÏ ×ÓÅÍ ÉÚ ÎÉÈ ÌÉÞÎÏ.

GnuPG ÒÅÛÁÅÔ ÜÔÕ ÐÒÏÂÌÅÍÕ ÐÒÉ ÐÏÍÏÝÉ ÍÅÈÁÎÉÚÍÁ ÉÍÅÎÏÅÚÍÏÇÏ *ÓÅÔØ ÄÏ×ÅÒÉÑ (web of trust)*. ÷ ÍÏÄÅÌÉ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÏÔ×ÅÔÓÔ×ÅÎÎÏÓÔØ ÚÁ ÐÒÏ×ÅÒÕ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ×ÏÚÌÏÄÎÁ ÎÁ ÌÀÄÅÊ, ËÏÔÏÒÙÍ ÷Ù ÄÏ×ÅÒÑÅÔÅ. îÁÐÒÉÍÅÒ, ÐÒÅÄÐÏÌÏÖÉÍ

- üÌÉÓ ÐÏÄÐÉÓÁÌÁ ËÌÀÞ âÌÜÊËÁ, Á
- âÌÜÊË ÐÏÄÐÉÓÁÌ ËÌÀÞÉ èÏÎÊ É äÈÁÒÍÙ.

åÓÌÉ üÌÉÓ Õ×ÅÒÅÎÁ, ÞÔÏ âÌÜÊË ÐÒÏ×ÅÒÑÅÔ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÅÊ, ËÏÔÏÒÙÅ ÏÎ ÐÏÄÐÉÓÙ×ÁÅÔ, ÔÏ üÌÉÓ ÍÏÖÅÔ ÂÙÔØ Õ×ÅÒÅÎÁ, ÞÔÏ ËÌÀÞÉ èÌÏÊ É äÈÁÓÍÙ ÄÏÓÔÏ×ÅÒÎÙ ÎÅ ÐÒÏ×ÅÒÑÑ ÉÈ ÌÉÞÎÏ. ïÎÁ ÐÒÏÓÔÏ ÉÓÐÏÌØÚÕÅÔ Ó×ÏÀ ÄÏÓÔÏ×ÅÒÎÕÀ ËÏÐÉÀ ÎÔËÒÙÔÏÇÏ ËÌÀÞÁ âÌÜÊËÁ ÄÌÑ ÐÒÏ×ÅËÉ ÅÇÏ ÐÏÄÐÉÓÉ ÎÁ ËÌÀÞÁÈ èÌÏÊ É äÈÁÓÍÙ. ÷ÏÂÝÅ, ÐÒÅÄÐÌÁÇÁÑ, ÞÔÏ üÌÉÓ ÓÏ×ÅÒÛÅÎÎÏ Õ×ÅÒÅÎÁ, ÞÔÏ ×ÓÅ ÐÒÁ×ÉÌØÎÏ ÐÒÏ×ÅÑÀÔ ËÌÀÞÉ, ÐÅÒÅ ÔÅÍ ËÁË ÉÈ ÐÏÄÐÉÓÁÔØ, ÔÏ ÌÀÂÏÊ ËÌÀÞ, ÐÏÄÐÉÓÁÎÎÙÊ ÄÏÓÔÏ×ÅÒÎÙÍ ËÌÀÞÏÍ, ÂÕÄÅÔ ÄÏÓÔÏ×ÅÒÎÙÍ.

3.2.1. äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ

îÁ ÐÒÁËÔÉËÅ ÄÏ×ÅÒÉÅ ÓÕÂßÅËÔÉ×ÎÏ. îÁÐÒÉÍÅÒ, ËÌÀÞ âÌÜÊËÁ ÄÏÓÔÏ×ÅÒÅÎ, Ô.Ë. üÌÉÓ ÐÏÄÐÉÓÁÌÁ ÅÇÏ, ÎÏ ÎÅ ÍÏÖÅÔ ÎÅ ÂÙÔØ Õ×ÅÒÅÎÁ, ÞÔÏ âÌÜÊË ÐÓÁ×ÉØÎÏ ÐÒÏ×ÅÑÅÔ ËÌÀÞÉ, ËÏÔÏÒÙÅ ÏÎ ÐÏÄÐÉÓÙ×ÁÅÔ. ÷ ÜÔÏÍ ÓÌÕÞÁÅ, ÏÎÁ ÎÅ ÂÕÄÅÔ ÓÞÉÔÁÔØ ËÌÀÞÉ èÌÏÊ É äÈÁÓÍÙ ÄÏÓÔÏ×ÅÒÎÙÍÉ, ÏÓÎ×Ù×ÁÑÓØ ÎÁ ÐÏÄÐÉÓÉ âÌÜÊËÁ. íÏÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÒÅÛÁÅÔ ÜÕÕ ÚÁÄÁÞÕ Ó×ÑÚÙ×ÁÑ Ó ËÁÖÄÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ × ÷ÁÛÅÊ Ó×ÑÚËÅ ÚÎÁÞÅÎÉÅ ÕËÁÚÙ×ÁÀÝÅÅ ÕÒÏ×ÅÎØ ÷ÁÛÅÇÏ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ. éÍÅÅÔÓÑ ÞÅÔÙÒÅ ÕÒÏ×ÎÑ ÄÏ×ÅÒÉÑ.

unknown (ÎÅÉÚ×ÅÓÔÎÏÅ)

> îÉÞÅÇÏ ÎÅ ÉÚ×ÅÓÔÎÏ Ï ÐÏÌÉÔÉËÅ ÐÏÄÐÉÓÁÎÉÑ ËÌÀÞÅÊ ÄÁÎÎÙÍ ×ÌÁÄÅÌØÃÅÍ. ëÌÀÞÁÍ × ÷ÁÛÅÊ Ó×ÑÚËÅ, ËÒÏÍÅ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ, ÐÅÒ×ÏÁÞÁÌØÎÏ ÐÒÉÓ×ÁÉ×ÁÅÔÓÑ ÜÔÏÔ ÕÒÏ×ÅÎØ ÄÏ×ÅÒÉÑ.

none (ÎÅÔ)

> éÚ×ÅÓÔÎÁ ÎÅÄÏÂÒÏÓ×ÅÓÔÎÏÓÔØ ÜÔÏÇÏ ÌÉÃÁ ÐÒÉ ÐÏÄÐÉÓÉ ÞÕÖÉÈ ËÌÀÞÅÊ.

marginal (ÇÒÁÎÉÞÎÏÅ)

> ðÏÎÉÍÁÅÔ ÓÍÙÓÌ ÐÏÄÐÉÓÁÎÉÑ ËÌÀÞÅÊ É ÐÒÏ×ÅÒÑÅÔ ÉÈ

ÄÏÓÔÏ×ÅÒÎÏÓÔØ ÐÅÒÅÄ ÔÅÍ, ËÁË ÐÏÄÐÉÓÙ×ÁÔØ.

full (ÐÏÌÎÏÅ)

÷ÌÁÄÅÌÅÃ ÏÞÅÎØ ÒÁÚÂÏÒÞÉ× × ÐÏÄÐÉÓÉ ËÌÀÞÅÊ É ÅÇÏ ÐÏÄÐÉÓÉ ÎÁ ËÌÀÞÅ ÍÏÖÎÏ ×ÅÒÉÔØ ËÁË Ó×ÏÅÊ ÓÏÂÓÔ×ÅÎÎÏÊ.

õÒÏ×ÅÎØ ÄÏ×ÅÒÉÑ ËÌÀÞÕ ÜÔÏ ÔÏ, ÞÔÏ ÷Ù ÐÒÉÓ×ÁÉ×ÁÅÔÅ ÌÉÞÎÏ, É ÜÔÏ ÷ÁÛÁ ÞÁÓÔÎÁÑ ÉÎÆÏÒÍÁÃÉÑ. ïÎÁ ÎÅ ÜËÓÐÏÒÔÉÒÕÅÔÓÑ Ó ËÌÀÞÏÍ; ÏÎÁ ÄÁÖÅ ÈÒÁÎÉÔÓÑ ÏÔÄÅÌØÎÏ ÏÔ ËÌÀÞÅÊ × ÓÐÅÃÉÁÌØÎÏÊ ÂÁÚÅ ÄÁÎÎÙÈ.

äÌÑ ÐÒÉÓ×ÏÅÎÉÑ ÕÒÏ×ÎÑ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ ÉÓÐÏÌØÚÕÅÔÓÑ ÒÅÄÁËÔÏÒ ËÌÀÞÅÊ GnuPG. ëÏÍÁÎÄÁ **trust**. ÷ ÜÔÏÍ ÐÒÉÍÅÒÅ üÌÉÓ ÒÅÄÁËÔÉÒÕÅÔ ÕÒÏ×ÅÎØ Ó×ÏÅÇÏ ÄÏ×ÅÒÉÑ âÌÜËËÕ É ÚÁÔÅÍ ÏÂÎÏ×ÌÑÅÔ ÂÁÚÕ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ, ÞÔÏÂÙ ÐÅÒÅÓÉÁÔØ ÄÏÓÔÏ×ÅÒÏÓÔØ ËÌÀÞÅÊ ÏÓÎÏ×Ù×ÁÑÓØ ÎÁ ÎÏ×ÏÍ ÚÎÁÞÅÎÉÉ ÄÏ×ÅÒÉÑ âÌÜËËÕ.

```
alice% gpg --edit-key blake

pub  1024D/8B927C8A  created: 1999-07-02 expires: never      trust: q/f
sub  1024g/C19EA233  created: 1999-07-02 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Command> trust
pub  1024D/8B927C8A  created: 1999-07-02 expires: never      trust: q/f
sub  1024g/C19EA233  created: 1999-07-02 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Please decide how far you trust this user to correctly
verify other users' keys (by looking at passports,
checking fingerprints from different sources...)?

 1 = Don't know
 2 = I do NOT trust
 3 = I trust marginally
 4 = I trust fully
 s = please show me more information
 m = back to the main menu

Your decision? 3

pub  1024D/8B927C8A  created: 1999-07-02 expires: never      trust: m/f
sub  1024g/C19EA233  created: 1999-07-02 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Command> quit
[...]
```

äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ É ÄÏÓÔÏ×ÅÒÏÓÔØ ËÌÀÞÁ ×Ù×ÏÄÑÔÓÑ ÓÐÒÁ×Á ÏÔ ËÌÀÞÁ, ËÏÇÄÁ ×Ù×ÏÄÉÔÓÑ ËÌÀÞ. äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ×Ù×ÏÄÉÔÓÑ ÐÅÒ×ÙÍ, ÄÏÓÔÏ×ÅÒÏÓÔØ ËÌÀÞÁ ×ÔÏÒÏÊ[1]. þÅÔÙÒÅ ÕÒÏ×ÎÑ ÄÏ×ÅÒÉÑ/ÄÏÓÔÏ×ÅÒÏÓÔÉ ÏÂÏÚÎÁÞÁÀÔÓÑ ÓÉÍ×ÏÌÁÍÉ: ÎÅÉÚ×ÅÓÔÎÙÊ (q), ÎÅÔ (n), ÇÒÁÎÉÞÎÙÊ (m), É ÐÏÎÎÙÊ (f). ÷ ÜÔÏÍ ÓÌÕÞÁÅ, ËÌÀÞ âÌÜÊËÁ ÐÏÎÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎ, Ô.Ë. üÌÉÓ ÓÁÍÁ ÐÏÄÐÉÓÁÌÁ ÅÇÏ. éÚÎÁÞÁÌØÎÏ ÕÓÔÁÎÏ×ÌÅÎ ÎÅÉÚ×ÅÓÔÎÅ ÄÏ×ÅÒÅ ÏÔÎÏÓÉÔÅÌØÎÏ ÐÒÁ×ÉØÎÏÓÔÉ ÐÏÄÐÉÓÉ âÌÜÊËÏÍ ËÌÀÞÅÊ, ÎÏ üÌÉÓ ÒÅÛÁÅÔ ÕÓÔÁÎÏ×ÉÔØ ÇÒÁÎÉÞÎÙÊ ÕÒÏ×ÅÎØ ÄÏ×ÅÒÉÑ.

3.2.2. éÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏ×ÅÒÉÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÅÊ

óÅÔØ ÄÏ×ÅÒÉÑ ÐÏÚ×ÏÑÎÔ ÉÓÐÏÌØÚÏ×ÁÔØ ÂÏÌÅÅ ÇÉÂËÉÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÁ. åÓÌÉ ÐÒÅÖÄÅ ÄÏÓÔÏ×ÅÒÏÙÍÉ ÓÞÉÔÁÌÉÓØ ÔÏÌØËÏ ÔÅ ËÌÀÞÉ, ËÏÔÏÒÙÅ ÷Ù ÐÏÄÐÉÓÁÌÉ ÌÉÞÎÏ, ÔÏ ÔÅÐÅØ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÌÅÄÕÀÝÉÊ ÁÌÇÏÒÉÔÍ. ëÌÀÞ *K* ÓÞÉÔÁÅÔÓÑ ÄÏÓÔÏ×ÅÒÎÙÍ, ÅÓÌÉ ÏÎ ÕÄÏ×ÌÅÔ×ÏÒÑÅÔ ÓÌÅÄÕÀÝÉÍ Ä×ÕÍ ÓÓÌÏ×ÉÑÍ:

1. ÏÎ ÐÏÄÐÉÓÁÎ ÄÏÓÔÁÔÏÞÎÙÍ ËÏÌÉÞÅÓÔ×ÏÍ ÄÏÓÔÏ×ÅÒÎÙÈ ËÌÀÞÅÊ, Ô.Å.

   - ÷Ù ÐÏÄÐÉÓÁÌÉ ÅÇÏ ÌÉÞÎÏ,
   - ÏÎ ÂÙÌ ÐÏÄÐÉÓÁÎ ËÌÀÞÏÍ ×ÌÁÄÅÌØÃÕ ËÏÔÏÒÏÇÏ ÷Ù ÐÏÌÏÓÔØÀ ÄÏ×ÅÒÑÅÔÅ, ÉÌÉ
   - ÏÎ ÂÙÌ ÐÏÄÐÉÓÁÎ ÔÒÅÍÑ ËÌÀÞÁÍÉ Ó ÇÒÁÎÉÞÎÙÍ ÕÒÏ×ÎÅÍ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ; É

2. ÃÅÐÏÞËÁ ÐÏÄÐÉÓÁÎÎÙÈ ËÌÀÞÅÊ ÎÁÞÉÎÁÀÝÁÑÓÑ Ó *K* É ÚÁËÁÎÞÉ×ÁÀÝÁÑÓÑ ÷ÁÛÉÍ ËÌÀÞÏÍ ÎÅ ÄÌÉÎÎÅÅ ÐÑÔÉ ÉÌÉ ÂÏÌØÛÅ ÉÚÍÅÎÅÎÉÊ. ãÉÆÒÙ

ÐÒÉ×ÅÄÅÎÎÙÅ ×ÙÛÅ - ÚÎÁÞÅÎÉÑ ÉÓÐÏÌØÚÕÅÍÙÅ GnuPG ÐÏ ÕÍÌÞÁÎÉÀ.

. 3-1 ÒÁÓÓÍÎÔÒÉÍ ÓÅÔØ ÄÏ×ÅÒÉÑ ÎÁÞÉÎÁÀÝÕÀÓÑ Ó üÌÉÓ. çÒÁÆ ÉÌÌÀÓÔÒÉÒÕÅÔ ËÔÏ ÐÏÄÐÉÓÁÌ ÞÅÊ ËÌÀÞ. ôÁÂÌÉÃÁ ÐÏËÁÚÙ×ÁÅÔ ËÌÀÞÉ, ËÏÔÏÒÙÅ üÌÉÓ ÐÒÉÚÎÁÅÔ ÄÏÓÔÏ×ÅÒÎÙÍÉ ÏÓÎ×Ù×ÁÑÓØ ÎÁ ÄÏ×ÅÒÉÉ ÄÒÕÇÉÍ ÞÌÅÎÁÍ ÓÅÔÉ.

* *ðÏÔÅÎÃÉÁÌØÎÁÑ ÏÛÉÂËÁ: ÏÐÃÉÑ `--completes-needed` × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ ÂÕÄÕ ÐÒÏÉÇÎÏÒÉÒÏ×ÁÎÁ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ Ó ËÏÍÁÎÄÏÊ `--update-trustdb`. úÎÁÞÅÎÉÅ ×ÙÞÉÓÌÑÅÔÑ ËÏÒÒÅËÔÎÏ ÅÓÌÉ ÕËÁÚÁÔØ ÅÇÏ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.*

üÔÏ ÐÒÉÍÅÒ ÐÒÅÄÐÏÁÇÁÅÔ, ÞÔÏ ÄÌÑ ÐÒÉÚÎÁÎÉÑ ÄÒÕÇÏÇÏ ËÌÀÞÁ ÄÏÓÔÏ×ÅÒÎÙÍ ÔÒÅÂÕÅÔÓÑ Ä×Á ËÌÀÞÁ Ó ÇÒÁÎÉÞÎÙÍ ÄÏ×ÅÒÉÅÍ ÉÌÉ ÏÄÉÎ Ó ÐÏÎÎÙÍ. íÁËÓÉÍÁÌØÎÁÑ ÄÌÉÎÁ ÃÅÐÏÞËÉ ÒÁ×ÎÁ ÔÒÅÍ.

ðÒÉ ×ÙÞÉÓÌÅÎÉÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ, × ÜÔÏÍ ÐÒÉÍÅÒÅ, ËÌÀÞÉ âÌÜÊËÁ É äÈÁÒÍÙ ×ÓÅÇÄÁ ÓÞÉÔÁÀÔÓÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙÍÉ, Ô.Ë. ÏÎÉ ÐÏÄÐÉÓÁÎÙ üÌÉÓ. äÏÓÔÏ×ÅÒÎÏÓÔØ ÄÒÕÇÉÈ ËÌÀÞÅÊ ÚÁ×ÉÓÉÔ ÏÔ ÄÏ×ÅÒÉÑ. ÷ ÐÅÒ×ÏÍ ÓÌÕÞÁÅ, ÄÏ×ÅÒÑÅÔ ÐÏÌØÚÏ×ÁÔÅÌÀ ÐÏÌÎÏÓÔØÀ ËÌÀÞÅ è ÆÜÎÏÉÓÁ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÉÑ. ÷Ï ×ÔÏÒÏÍ ÓÌÕÞÁÅ, ÄÏ×ÅÒÅÔ âÌÜÊËÕ É äÈÁÒÍÅ ÇÒÁÎÉÞÎÏÅ. ô.Ë. Ä×Á ËÌÀÞÁ Ó ÇÒÁÎÉÞÎÙÍ ÄÏ×ÅÒÉÍ ÔÒÅÂÕÅÔÓÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÄÌÑ ÐÒÉÄ×ÅÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ, ËÌÀÞ èÌÏÊ ÂÕÄÅÔ ÐÒÉÚÎÁÎ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÅÎ, ÎÏ ÄÏÓÔÏ×ÅÒÏÓÔØ ËÌÀÞÁ æÒÜÎÓÉÓÁ ÂÕÄÅÔ ÔÏÌØËÏ ÞÁÓÔÉÞÎÏ ÐÏÄ×ÅÒÅÎÁ. ÷ ÓÌÕÞÁÅ ÇÒÁÎÉÞÎÏÇÏ ÄÏ×ÅÒÑ èÌÏÊ É äÈÁÒÍÅ, ËÌÀÞ èÌÏÊ ÂÕÄÅÔ ÞÁÓÔÉÞÎÏÅ ÄÏÓÔÏ×ÅÎ, Á ËÌÀÞ äÈÁÒÍÙ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÎ. ëÌÀÞ æÒÜÎÓÉÓÁ ÂÕÄÅÔ ÞÁÓÔÉÞÎÏ ÄÏÓÔÏ×ÅÎ, Ô.Ë. ÔÏÌØËÏ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÎÙÊ ËÌÀÞ ÍÏÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÒÄÔ×ÅÒÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÏÓÔÉ ÄÒÕÇÉÈ ËÌÀÞÅÊ, Á ÅÄÉÎÓÔ×ÅÎÎÙÊ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙ ËÌÀÞ, ËÏÔÏÒÙÍ ÐÒÄÐÉÓÁÎ ËÌÀÞ æÒÜÎËÁ, ÜÔÏ ËÌÀÞ äÈÁÒÍÙ. ðÏÓÌÅ ÄÏÂ×ÌÅÎÉÑ ÇÒÁÎÉÞÎÏÇÏ ÄÏ×ÅÒÑ âÌÜÊËÕ ËÌÀÞ èÌÏÊ ÓÔÁÎÏ×ÉÔÓÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙÍ É ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÏÌÎÏÇÏ ÐÏÄ×ÅÒÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÁ æÒÜÎÓÉÓÁ É ÞÁÓÔÉÞÎÏÇÏ ÐÏÄ×ÅÒÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÁ åÌÅÎÙ. îÁËÏÎÅÃ, ÅÓÌÉ ÄÏ×ÅÒÅÎ âÌÜÊËÕ, èÌÏÊ É åÌÅÎ ÐÏÌÎÅ, ÜÔÏÇÏ ×ÓÅ ÅÝÅ ÎÅ ÄÏÓÔÁÔÏÞÎÏ ÄÌÑ ÐÏÄ×ÅÒÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÁ äÖÅÁ, Ô.Ë. ÍÁËÓÉÍÁÌØÎÁÑ ÄÌÉÎÁ ÃÅÐÏÞËÉ ÐÏÄ×ÅÒÄÅÎÉÑ ÒÁ×ÎÁ ÔÒÅÍ, ÎÏ ÐÕÔØ ÏÔ äÖÅÁ Ë üÌÉÓ ÒÁ×ÅÎ

ÞÅÔÙÒÅÍ.

íÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÒÅÁÌÉÚÕÅÔ ÇÉÂÒÉÄÎÕÀ ËÏÍÂÉÎÁÃÉÀ ÂÅÚÏÐÁÓÏÎÇÏ ÏÂÍÅÎÁ ËÌÀÞÁÍÉ. ïÎÁ ÐÏÚ×ÏÑÑÅÔ ÎÁÓÔÒÁÉ×ÁÔØ GnuPG × ÓÏÏÔ×ÅÔÓÔ×ÉÉ Ó ÷ÁÛÉÍÉ ÐÏÒÒÅÂÎÏÓÔÑÍÉ. ÷Ù ÍÏÖÅÔÅ ÔÒÅÂÏ×ÁÔØ ÍÎÏÇÏ ËÏÏÐÕÉÈ ÃÅÐÏÞÅË ÏÔ ÷ÁÛÅÇÏ ËÌÀÞÁ ÄÏ ËÌÀÞÁ *K* ÄÌÑ ÐÒÉÚÎÁÎÉÑ ÅÇÏ ÄÏÓÔ×ÅÒÎÙÍ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ ÕÄÏ×ÌÅÔ×ÏÒÅÎÙ ÏÄÎÏÎÎÏÊ ÃÅÐÏÞËÏÊ. ôÒÅÂÏ×ÁÎÉÅ ÍÎÏÇÏÞÉÓÌÅÎÎÙÈ ËÏÒÏÔËÉÈ ÃÅÐÏÞÅË - ÓÉÌØÎÁÑ ÇÁÒÁÎÔÉÑ ÔÏÇÏ, ÞÔÏ ËÌÀÞ *K* ÐÒÉÁÄÌÅÖÉÔ ÔÏÍÕ, ÎÁ ËÏÇÏ ÕËÁÚÙ×ÁÅÔ ÅÇÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÌØÚÏ×ÁÔÅÌÑ. ãÅÎÁ ÚÁ ÔÁËÕÀ ÎÁÄÅÖÎÏÓÔØ, ËÏÎÅÞÎÏ, ×ÙÛÅ, Ô.Ë. ÷Ù ÌÉÞÎÏ ÄÎÏÔÙ ÐÒÏ×ÅÒÑÔ É ÐÏÄÐÉÓÁÔØ ÂÎÌØÛÅÅ ËÏÌÉÞÅÓÔ×Ï ËÌÀÞÅÊ, ÞÅÍ × ÓÌÕÞÁÅ ËÏÇÄÁ ÷ÁÓ ÕÓÔÒÁÉ×ÁÅÔ ÎÅÂÌØÛÏÅ ÞÉÓÌÏ ÄÌÉÎÎÙÈ ÃÅÐÏÞÅË.

3-1. ðÒÉÍÅÒ ÓÅÔÉ ÄÏ×ÅÒÉÑ

ÄÏ×ÅÒÉÅ		**ÄÏÓÔÏ×ÅÒÏÓÔØ**	
ÇÒÁÎÉÞÎÏÅ	**ÐÏÌÎÏÅ**	**ÇÒÁÎÉÞÎÁÑ**	**ÐÏÌÎÁÑ**
	äÈÁÒÍÁ		âÌÜÊË, èÏÎÊ, äÈÁÒÍÁ, æÒÜÎÓÉÓ
âÌÜÊË, äÈÁÒÍÁ		æÒÜÎÓÉÓ	âÌÜÊË, èÏÎÊ, äÈÁÒÍÁ
èÏÎÊ, äÈÁÒÍÁ		èÏÎÊ, æÒÜÎÓÉÓ	âÌÜÊË, äÈÁÒÍÁ
âÌÜÊË, èÏÎÊ, äÈÁÒÍÁ		åÌÅÎÁ	âÌÜÊË, èÏÎÊ, äÈÁÒÍÁ, æÒÜÎÓÉÓ
	âÌÜÊË, èÏÎÊ, åÌÅÎÁ		âÌÜÊË, èÏÎÊ, åÌÅÎÁ, æÒÜÎÓÉÓ

3.3. òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÅÊ

÷ ÉÄÅÁÌÅ, ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ ÷ÁÛÉ ËÌÀÞÉ ÐÅÒÓÏÎÁÌØÎÏ ÐÅÒÅÄÁ×ÁÑ ÅÇÏ ÷ÁÛÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ. îÁ ÐÒÁËÔÉËÅ, ÏÄÎÁËÏ, ËÌÀÞÉ ÞÁÓÔÏ ÒÁÓÐÒÏÓÔÒÁÎÑÀÔÓÑ ÐÏ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÅ ÉÌÉ ÄÒÕÇÉÍÉ ÓÐÏÓÏÂÁÍÉ ÜÌÅËÔÒÏÎÎÏÊ Ó×ÑÚÉ. òÁÓÐÒÏÓÔÒÁÎÅÎÅ ÐÏ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÅ ÈÏÒÏÛÏ ËÏÇÄÁ ÷Ù ÉÍÅÅÔÅ ÔÏÌØËÏ ÎÁÓËÌØËÉÈ ËÏÒÒÅÓÐÏÎÄÅÎÔÏ×, ÅÓÌÉ ËÏÒÒÅÓÐÏÎÄÅÎÔ ÍÏÇÅ, ÷Ù ÍÏÅÔÅ ÒÁÚÍÁÓÔÅÔØ Ó×ÏÊ ËÌÀÞ ÎÁ ÐÅÒÓÏÎÁØÎÏÊ ×ÅÂ-ÓÔÒÁÎÉÃÅ. üÔÏ ÎÅ ÐÒÉÎÅÓÉÔ, ÏÄÎÁËÏ, ÅÓÌÉ ÌÀÄÉ, ËÏÔÏÒÙÍ ÎÕÖÅÎ ÷ÁÛ ÏÔËÒÙÔÙÊ ËÌÀÞ, ÎÅ ÚÎÁÀÔ ÇÄÅ ÎÁÊÔÉ ÅÇÏ × ÓÅÔÉ.

äÌÑ ÒÅÛÅÎÉÑ ÜÔÏÊ ÐÒÏÂÌÅÍÙ ÉÓÐÏÌØÚÕÀÔÓÑ ÓÅÒ×ÅÒÙ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ, ËÏÔÏÒÙÅ ÓÏÂÉÒÁÀÔ É ÒÁÓÐÒÏÓÔÒÁÎÑÀÔ ÏÔËÒÙÔÙÅ ËÌÀÞÉ. ïÔËÒÙÔÙÊ ËÌÀÞ ÌÉÂÏ ÄÏÂ×ÌÑÅÔÓÑ Ë ÂÁÚÅ ÄÁÎÎÙÈ ÓÅÒ×ÅÒÁ, ÌÉÂÏ ÏÂßÅÄÉÎÑÅÔÓÑ Ó ÓÕÝÅÓÔ×ÕÀÝÉÍ ËÌÀÞÏÍ, ÅÓÌÉ ÔÁËÎÊ ÓÕÝÅÓÔ×ÕÅÔ. ëÏÇÄÁ ÎÁ ÓÅÒ×ÅÒ ÐÒÉÈÏÄÉÔ ÚÁÐÒÏÓ ËÌÀÞÁ, ÓÅÒ×ÅÒ ÐÒÏÓÍÁÔÒÉ×ÁÅÔ ÂÁÚÕ ÄÁÎÎÙÈ É, ÅÓÌÉ ÎÁÈÏÄÉÔ, ×ÏÚ×ÒÁÝÁÅÔ ÚÁÐÒÏÛÅÎÎÙÊ ËÌÀÞ.

óÅÒ×ÅÒÙ ËÌÀÞÅÊ ÔÁËÖÅ ÐÏÌÚÛÙ ËÏÇÄÁ ÍÏÇÉÅ ÌÀÄÉ ÞÁÓÔÏ ÐÏÄÐÉÓÙ×ÁÀÔ ËÌÀÞÉ ÄÒÕÇÉÈ ÌÀÄÅÊ. âÅÚ ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ, ËÏÇÄÁ âÌÜÊË ÐÏÄÐÉÓÙ×ÁÀÔ ËÌÀÞ üÌÉÓ, ÏÎ ÄÏÌÖÅÎ ÐÏÓÌÁØ ÅÊ ÐÏÄÐÉÓÁÎÎÕÀ ÉÍ ËÏÐÉÀ ÅÅ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ËÏÔÒÕÀ üÌÉÓ ÍÏÖÅÔ ÄÏÂ×ÉÔØ Ë Ó×ÏÅÊ Ó×ÑÚÅÅ É ÐÅÒÅÄÁ×ÁÔØ, ÚÁÔÅÍ, ×ÓÅÍ Ó×ÏÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ. ÷ÙÐÏÌÎÅÎÉÅ ÜÔÉÈ ÄÅÉÓÔ×ÉÊ ÓÐÏÓÏÂÓÔ×ÕÅÔ ÐÏÓÔÒÏÅÎÉÀ ÐÏÔÏÙÈ ÓÅÔÅÊ ÄÏ×ÅÒÉÑ É ÐÏ×ÙÛÅÎÉÀ ÂÅÚÏÐÁÓÎÏÓÔÉ PGP. ïÄÎÁËÏ ÏÎÉ ÓÔÁÎÏ×ÑÔÓÑ ÐÍÅÈÎÉÊ ËÏÇÄÁ ËÌÀÞÉ ÐÏÄÐÉÓÙ×ÁÀÔÓÑ ÞÁÓÔÏ.

éÓÐÏÌØÚÏ×ÁÎÉÅ ÓÅÒ×ÅÒÏ× ËÌÀÞÅÊ ÏÂÌÅÇÞÁÅÔ ÜÔÏ ÐÒÏÃÅÓÓ. ëÏÇÄÁ âÌÜÊË ÐÏÄÐÉÓÙ×ÁÀÔ ËÌÀÞ üÌÉÓ ÏÎ ÐÓÙÌÁÅÔ ÐÏÄÐÉÓÁÎÎÙÊ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ. óÅÒ×ÅÒ ËÌÀÞÅÊ ÄÏÂ×ÌÑÅÔ ÐÏÄÐÉÓØ âÌÜÊËÁ Ë Ó×ÏÅÊ ËÏÐÉÉ ËÌÀÞÁ üÌÉÓ. ôÅ ËÔÏ ÉÎÔÅÒÅÓÕÅÔÓÑ ÏÂÎ×ÌÅÉÁÍ ËÏÐÉÉ

ËÌÀÞÅÊ üÌÉÓ, ÐÏ Ó×ÏÅÊ ÉÎÉÃÉÁÌÉ×Å Ó×ÑÚÙ×ÁÀÔÓÑ Ó ÓÅÒ×ÅÒÏÍ ËÌÀÞÅÊ É ÐÏÌÕÞÁÀÔ ÏÔÕÄÁ ÏÂÎÏ×ÌÅÎÎÙÊ ËÌÀÞ üÌÉÓ. üÌÉÓ ÎÅ ÐÒÉÎÉÍÁÅÔ ÕÞÁÓÔÉÑ × ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ËÌÀÞÁ É ÍÏÖÅÔ ÐÏÌÕÞÉÔØ ÐÏÄÐÉÓÉ ÍÁ Ó×ÏÅÍ ËÌÀÞÅ ÐÒÏÓÔÏ ÚÁÐÒÏÓ× ÓÅÒ×ÅÒ.

* *`--keyserver` ÄÏÌÖÅÎ ÎÁÈÏÄÉÔØÓÑ ÐÅÒÅÄ `--send-key` ÉÌÉ `--recv-key`. üÔÏ ÍÏÖÅÔ ×ÙÚ×ÁÔØ ÏÛÉÂËÉ.*

ïÄÉÎ ÉÌÉ ÂÏÌÅÅ ËÌÀÞÅÊ ÍÏÇÕÔ ÂÙÔØ ÏÐÒÁ×ÌÅÎÙ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ ËÏÍÁÎÄÏÊ `--send-keys`. ÷ ËÁÞÅÓÔ×Å ÁÒÇÕÍÅÎÔÁ ÕËÁÚÙ×ÁÀÔÓÑ ÏÄÉÎ ÉÌÉ ÂÏÌÅÅ ÓÐÅÃÉÆÉËÁÔÏÒ× ËÌÀÞÅÊ. óÅÒ×ÅÒ ËÌÀÞÅÊ, ËÏÔÏÒÏÍÕ ÂÕÄÕÔ ÐÅÒÅÄÁÎÙ ËÌÀÞÉ ÚÁÄÁÅÔÓÑ ÏÐÃÉÑ `--keyserver`. áÎÁÌÏÇÉÞÎÏ, ËÏÍÁÎÄÁ `--recv-keys` ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÏÌÕÞÅÎÉÑ ËÌÀÞÅÊ Ó ÓÅÒ×ÅÒÁ, ÏÏ ËÏÍÁÎÄÅ `--recv-keys` ÔÒÅÂÕÅÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒ ËÌÀÞÁ. ÷ ÓÌÅÄÕÀÝÅÍ ÐÒÉÍÅÒÅ üÌÉÓ ÏÂÎÏ×ÌÑÅÔ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó ÎÏ×ÙÍ ÐÏÄÐÉÓÑÍÉ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ *certserver.pgp.com* É ÚÁÔÅÍ ÐÏÓÙÌÁÅÔ Ó×ÏÀ ËÏÐÉÀ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ âÌÜÊËÁ ÎÁ ÔÏÔ ÖÅ ÓÅÒ×ÅÒ ËÌÀÞÅÊ ÄÌÑ ÐÅÒÅÄÁÞÉ Ó×ÏÅÊ ÐÏÄÐÉÓÉ ÎÁ ÎÅÍ.

```
alice% gpg --keyserver certserver.pgp.com --recv-key 0xBB7576AC
gpg: requesting key BB7576AC from certserver.pgp.com ...
gpg: key BB7576AC: 1 new signature

gpg: Total number processed: 1
gpg:         new signatures: 1
alice% gpg --keyserver certserver.pgp.com --send-key blake@cyb.org
gpg: success sending to 'certserver.pgp.com' (status=200)
```

óÕÝÅÓÔ×ÕÀÔ ÎÅÓËÏÌØËÏ ÐÏÐÕÌÑÒÎÙÈ ÓÅÒ×ÅÒÏ× ËÌÀÞÅÊ. ïÓÎÏ×ÎÙÅ ÓÅÒ×ÅÒÙ ËÌÀÞÅÊ ÓÉÎÈÒÏÎÉÚÉÒÕÀÔÓÑ ÄÒÕÇ Ó ÄÒÕÇÏÍ, ÐÏÙÔÏÕ ÌÕÞÛÅÊ ×ÙÂÒÁÔØ ÂÌÉÖÁÉÛÉÊ Ë ÷ÁÍ É ÒÅÇÕÌÑÒÎÏ ÓÓÐÏÌØÚÏ×ÁÔØ ÅÇÏ ÄÌÑ ÏÔÐÒÁ×ËÉ É ÐÏÕÐÅÎÉÑ ËÌÀÞÅÊ.

1. GnuPG ÐÅÒÅÇÒÕÖÁÅÔ ÓÏÏ×Ï "ÄÏ×ÅÒÉÅ" ÉÓÐÏÌØÚÕÑ ÅÇÏ × ÓÍÙÓÌÅ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ É × ÓÍÙÓÌÅ ÄÏ×ÅÒÉÑ ËÌÀÞÕ. üÔÏ ÍÏÖÅÔ ×ÙÚ×ÁÔØ ÐÕÔÁÎÉÃÕ. éÎÏÇÄÁ ÄÏ×ÅÒÅ ×ÌÁÄÅÌØÃÕ ÕËÁÚÙ×ÁÅÔÓÑ ÐÒÑÍÏ. ÷ ÏÓÎÏ×ÎÏÍ, × ÜÔÏÍ ÒÕËÏ×ÏÄÓÔ×Å, ÔÅÒÍÉÎ "ÄÏ×ÅÒÉÅ"

ÉÓÐÏÌØÚÕÅÔÓÑ × ÓÍÙÓÌÅ ÄÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ É ÔÅÒÍÉÎ “ÄÏÓÔ×ÅÒÎÓÔØ” ÄÌÑ ÏÂÚÅÁÞÅÎÉÑ Õ×ÅÒÅÎÎÏÓÔÉ × ÔÏÍ, ÞÔÏ ËÌÀÞ ÐÒÉÎÁÄÌÅÖÉÔ ÞÅÌÏ×ÅËÕ ÕËÁÚÁÎÎÏÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ÐÏØÚÏ×ÁÔÅÌÑ.

4. åÖÅÄÎÅ×ÏÏÅ ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG

GnuPG ÓÌÏÖÎÙÊ ÉÎÓÔÒÕÍÅÎÔ Ó ÎÁÂÏÒÍ ÔÅÈÎÉÞÅÓËÉÈ, ÓÏÃÉÁÌØÎÙÈ É ÚÁËÏÎÏÄÁÔÅÌØÎÙÈ ÔÏÎËÏÓÔÅÊ, ×ÏÚÎÉËÁÀÝÉÈ ÐÒÉ ÅÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÉ. ôÅÈÎÉÞÅÓËÉ, ÏÎ ÂÙÌ ÒÁÚÒÁÂÏÔÁÎ ÄÌÑ ÕÄÏ×ÌÅÔ×ÏÒÅÎÑ ÏÞÅÌØ ÒÁÚÌÉÞÁÀÝÉÈÓÑ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ. üÔÏ ÕÓÌÏÖÎÑÅÔ ÕÐÒ×ÌÅÎÉÅ ËÌÁÞÁÍÉ. óÏÃÉÁÌØÎÏ, ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG ÎÅ Ñ×ÌÑÅÔÓÑ ÔÏÌØËÏ ÐÒÒÓÍÌØÎÙÍ ÒÅÛÅÎÉÅÍ. äÌÑ ÜÆÆÅËÔÉ×ÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG, ÅÇÏ ÄÏÌÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ ÏÂÅ ÓÔÒÏÎÙ. îÁËÏÅÃ, ÚÁËÏÎÏÄÁÔÅÌØÓÔ×Ï ÏÇÒÁÎÉÞÉ×ÁÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÃÉÆÒÏ×ÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ, É, × ÞÁÓÔÎÓÔÉ, ÏÔ×ÅÔ ÎÁ ×ÌÐÒÏÓ Ï ÚÁËÏÎÎÏÓÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG ÒÁÚÌÉÞÅÎ × ÒÁÚÎÙÈ ÇÏÓÕÄÁÒÓÔ×ÁÈ.

úÄÅÓØ ÒÁÓÍÁÔÒÉ×ÁÀÔÓÑ ÜÔÉ ×ÌÐÒÏÓÙ. ôÁËÖÅ ÄÁÀÔÓÑ ÐÒÁËÔÉÞÅÓËÉÅ ÓÏ×ÅÔÙ ËÁË ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ÄÌÑ ÕÄÏ×ÌÅÔ×ÏÒÅÎÑ Ó×ÏÉÈ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ. òÁÓÍÁÔÒÉ×ÁÀÔÓÑ ÐÕÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG ÄÌÑ ÚÁÝÉÝÅÎÎÏÇÏ ÏÂÍÅÎÁ ÉÎÆÏÒÍÁÃÉÅÊ ÍÅÖÄÕ ÷ÁÍÉ É ÷ÁÛÉÍÉ ËÏÌÌÅÇÁÍÉ ÅÓÌÉ ÎÉÉ ÅÝÅ ÎÅ ÉÓÐÏÌØÚÕÀÔ GnuPG. ÷ ÚÁËÌÀÞÅÎÉÅ, ×ÙÅÌÅÎ ÚÁËÎÎÏÄÁÔÅÌØÊ ÓÔÁÔÕÓ GnuPG, ÏÐÒÅÄÅÌÑÅÍÙÊ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÍÉ ÚÁËÏÎÁÍÉ × ÍÉÒÅ.

4.1. ïÐÒÅÄÅÌÅÎÉÅ ÷ÁÛÉÈ ÔÒÅÂ×ÁÎÉÊ Ë ÚÁÝÉÔÅ

GnuPG ÉÎÓÔÒÕÍÅÎÔ ÄÌÑ ÚÁÝÉÔÙ ÷ÁÛÉÈ ÓÅËÒÅÔÏ×. ÷ÁÛÉ ÓÅËÒÅÔÙ ÚÁÝÉÝÅÎÙ ÅÓÌÉ ÷ÁÛÉ ÓÏÏÂÝÅÎÉÑ ÎÅ ÄÏÓÔÕÐÎÙ ÐÏÓÔÏÒÏÎÎÅÍÕ ÇÌÁÚÕ.

ôÏ, ËÁË ÷ÁÍ ÓÌÅÄÕÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, ÚÁ×ÉÓÉÔ ÏÔ ÖÅÌÁÎÉÑ É ×ÏÚÍÏÖÎÏÓÔÅÊ ÔÅÈ, ËÔÏ ÍÏÖÅÔ ÚÁÈÏÔÅÔØ ÐÒÏÞÁÓÔØ ÷ÁÛÉ ÓÏÏÂÝÅÎÉÑ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÂÅÓÃÅÒÅÍÏÎÎÙÊ ÓÉÓÔÅÍÙÊ ÁÄÍÉÎÉÓÔÒÁÔÏÒ, ÎÅÂÅÖÎÏ ÐÒÏÍÁÔÒÉ×ÁÀÝÉÊ ÷ÁÛ ÐÏÞÔÓ, ÐÒÍÚÙÌÅÎÎÙÊ ÛÐÉÎ, ÐÙÔÁÝÉÊÓÑ ÐÏÉÓÔÉØ ÓÅËÒÅÔÙ ÷ÁÛÅÇÏ ÐÒÅÄÐÒÉÑÔÉÑ, ÉÌÉ ÇÏÓÕÄÁÒÓÔ×ÅÎÎÙÅ

ÓÐÅÃÓÌÕÖÂÙ, ÉÎÔÅÒÁÔÉÖÁÝÉÅÓÑ ÷ÁÍÉ. éÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG ÄÌÑ ÚÁÝÉÔÙ ÏÔ ÓÌÕÞÁÊÎÏÇÏ ÐÒÏÍÁÔÒ×ÁÎÉÑ ÏÔ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG × ÓÌÕÞÁÅ ÅÓÌÉ ËÔÏ-ÔÏ ÃÅÌÅÎÁÐÒÁ×ÌÅÎÎÏ ÐÙÔÁÅÔÓÑ ÐÒÏÞÉÓÔØ ÷ÁÛÕ ÐÏÞÔÕ. ÷ÁÛÁ ÃÅÌØ, × ËÏÎÅÞÎÏÍ ÓÞÅÔÅ, ÓÏÓÔÉÔ × ÔÏÍ, ÞÔÏÂÙ ÓÄÅÌÁÔØ ÒÁÓÛÉÆÒÏ×ËÕ ÄÁÎÎÙÈ ÂÏÌÅÅ ÄÏÒÇÏÊ ÞÅÍ ÉÈ ÓÔÏÉÍÏÓÔØ.

îÁÓÔÒÏÊËÁ GnuPG ×ËÌÀÞÁÅÔ ÒÅÛÅÎÉÅ ÞÅÔÙÒÅÈ ÚÁÄÁÞ:

- ×ÙÂÏÒ ÒÁÚÍÅÒÁ ÷ÁÛÅÊ ÐÁÒÙ ËÌÀÞÅÊ,
- ÚÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ,
- ×ÙÂÏÒ ÓÒÏËÏ× ÄÅÊÓÔ×ÉÑ ËÌÀÞÅÊ, É
- ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅØÀ ÄÏ×ÅÒÉÑ.

ðÒÁ×ÉÌØÎÏ ×ÙÂÒÁÎÎÙÊ ÒÁÚÍÅÒ ËÌÀÞÁ ÚÁÝÉÝÁÅÔ ÷ÁÓ ÏÔ ÌÏÂÏ×ÙÈ ÁÔÁË ÎÁ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÓÏÏÂÝÅÎÉÑ. úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÐÒÅÄÏÔ×ÒÁÝÁÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÅÇÏ ËÅÍ-ÔÏ ÄÒÕÇÉÍ ÄÌÑ ÒÁÚÛÉÆÒÏ×ËÉ ÎÁÐÒÁ×ÌÅÎÎÙÈ ÷ÁÍ ÓÏÏÂÝÅÎÉÊ É ÐÏÄÐÉÓ�Ó×ÏÉÈ ÓÏÏÂÝÅÎÉÊ ÷ÁÛÅÊ ÐÏÄÐÉÓØÀ. ðÒÁ×ÉÌØÎÏÅ ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ ÐÒÅÄÐÒÉÎÉÍÁÔÅÌÑ ÚÁÝÉÔÙ ÐÒÉ ÞÌÏ×ÅËÅ Ó ËÌÏÏÒÍ ÷Ù ÐÅÒÅÐÉÓÙ×ÁÅÔÅÓØ. ÷ ËÏÎÅÃÎÏÍ ÓÞÅÔÅ, ÏÔ ÔÏÇÏ ËÁË ÷Ù ÓÏÏÔÎÓÉÔÅ ÒÅÛÅÎÉÅ ÜÔÉÈ ÐÒÏÀÌÍ Ó ÐÏÔÒÅÂÎÏÓÔÉ ÚÁÝÉÔÙ, ÚÁ×ÉÓÉÔ ÂÁÌÁÎÓ ÍÅÖÄÕ ÄÏÎÎÉÔÅÌØÎÏÊ ÒÁÂÏÔÏÊ, Ó×ÑÚÁÎÎÏÊ Ó ÉÓÐÏÌØÚÏ×ÁÎÉÅÍ GnuPG, É ÚÁÝÉÔÏÊ, ËÏÔÏÒÀ ÷ÁÍ ÜÔÏ ÄÁÅÔ.

4.1.1. ÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ

÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ ÚÁ×ÉÓÉÔ ÏÔ ÔÉÐÁ ËÌÀÞÁ. ÷ OpenPGP, ÐÁÒÁ ÏÔËÒÙÔÏÇÏ/ÚÁËÒÙÔÏÇÏ ËÌÀÞÅÊ ÏÂÙÞÎÏ ÓÏÓÔÉÔ ÉÚ ÎÁÓÉÌØËÉÈ ËÌÀÞÅÊ. ëÁË ÍÉÎÉÍÕÍ × ÎÅÅ ×ÈÏÄÉÔ ÇÌÁ×ÎÙÊ ËÌÀÞ ÄÌÑ ÐÏÄÐÉÓÉ, ËÒÏÍÅ ÔÏÇÏ, ÏÂÙÞÎÏ ÏÎÁ ÓÏÄÅÒÖÉÔ ÏÄÎÏ ÉÌÉ ÎÁÓÉÌØËÏ ÄÏÐÏÌÎÉÔÅÌØÎÏÙÈ ËÌÀÞÅÊ ÄÌÑ ÛÉÆÒÏ×ÁÎÑ. ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÐÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÐÁÒÁÍÅÔÒÏ× ÐÏ ÕÍÏÌÞÁÎÉÀ, ÇÌÁ×ÎÙÊ ËÌÀÞ ÂÕÄÅÔ DSA ËÌÀÞÏÍ, Á ÐÏÄËÌÀÞÉ ÂÕÄÕÔ ElGamal ËÌÀÞÁÍÉ.

DSA ÄÏÐÕÓËÁÅÔ ËÌÀÞÉ ÄÌÉÎÎÊ ÄÏ 1024 ÂÉÔ. üÔÏ ÎÅ ÓÌÉÛËÏÍ ÍÎÏÇÏ, ÕÞÉÔÙ×ÁÑ ÓÅÇÏÄÎÑÛÎÅÅ ÒÁÚ×ÉÔÉÅ ÔÅÈÎÏÌÏÇÉÉ, ÎÏ ÜÔÏ ÔÏ, ÞÔÏ ÏÐÉÓÙ×ÁÅÔ ÓÔÁÎÄÁÒÔ. âÅÚ ×ÏÐÒÏÓ×, ÷Ù ÄÎÌÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ 1024 ÂÉÔ DSA ËÌÀÞÉ.

ElGamal ËÌÀÞÉ ÍÏÇÕÔ ÂÙÔØ ÌÀÂÏÇÏ ÒÁÚÍÅÒÁ. ô.Ë. GnuPG ÓÍÅÛÁÎÎÁÑ ÓÉÓÔÅÍÁ, ÏÔËÒÙÔÙÊ ËÌÀÞ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÚÁÛÉÆÒÏ×ÁÎÉÑ 128-ÂÉÔÎÏÇÏ ÓÅÁÎÓÏ×ÏÇÏ ËÌÀÞÁ, Á ÚÁËÒÙÔÙÊ ËÌÀÞ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÅÇÏ ÒÁÓÛÉÆÒÏ×ÁÎÉÑ. òÁÚÍÅÒ ËÌÀÞÁ ×ÌÉÑÅÔ ÎÁ ÓËÏÒÏÓÔØ ÚÁÛÉÆÒÏ×ÁÎÉÑ É ÒÁÓÛÉÆÒÏ×ÁÎÉÑ, Ô.Ë. ÓÔÏÉÍÓÔØ ÜÔÉÈ ÁÌÇÏÒÉÔÍÏ× ÜËÓÐÏÎÅÎÃÉÁÌØÎÁ ÏÔÎÓÉÔÅÌØÎÏ ÒÁÚÍÅÒÁ ËÌÀÞÁ. âÏÌØÛÉÅ ËÌÀÞÉ ÔÁËÖÅ ÔÒÅÂÕÔ ÂÏÌØÛÅ ×ÒÅÍÅÎÉ ÄÌÑ ÇÅÎÅÒÁÃÉÉ É ÂÏÌØÛÅ ÍÁÓÔÁ ÄÌÑ ÈÒÁÎÅÎÉÑ. îÁËÏÎÅÃ, ÅÓÌÉ ËÌÀÞ ÓÌÉÛËÏÍ ×ÅÌÉË ÄÌÑ ÁÔÁËÉ × ÏÏÂ, ÐÏÈÉÔÉÔÅÌØ ÐÒÏÓÏ ÐÒÉÂÅÇÎÅÔ Ë ÄÒÕÇÉÍ ÍÅÔÏÄÁÍ, ÞÔÏÂÙ ÐÏÔÒÅÓÏÔØ ÉÎÔÅÒÅÓÙ ÅÇÏ ÄÁÎÎÙÅ. ðÒÉÍÅÒÁÍÉ ÄÒÕÇÉÈ ÍÅÔÏÄÏ× Ñ×ÌÑÀÔÓÑ ÏÇÒÁÂÌÅÎÉÅ ÷ÁÛÅÇÏ ÄÏÍÁ ÉÌÉ ÏÆÉÓÁ, ÌÉÂÏ ÎÁÐÁÄÅÎÉÅ ÌÉÞÎÏ ÎÁ ÷ÁÓ. 1024 ÂÉÔ - ÒÅËÏÍÅÎÄÕÅÍÙÊ ÒÁÚÍÅÒ ËÌÀÞÁ. åÓÌÉ ÷Ù ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÎÕÖÄÁÅÔÅÓØ × ËÌÀÞÅ ÂÏÌØÛÅÇÏ ÒÁÚÍÅÒÁ, ÔÏ ÓËÏÒÅÅ ×ÓÅÇÏ ÕÖÅ ÚÎÁÂÅ ÏÂ ÜÔÏÍ É ÄÏÌÖÎÙ ÐÒÏËÏÍÍÅÎÔÉÒÏ×ÁÔØ Ó ÜËÓÐÅÒÔÏÍ ÐÏ ÚÁÝÉÔÅ ÄÁÎÎÙÈ.

4.1.2. úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ

úÁÝÉÔÁ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÏÄÎÁ ÉÚ ÎÁÉÂÏÌÅÅ ×ÁÖÎÙÈ ÚÁÄÁÞ ÄÌÑ ÐÒÁ×ÉÌØÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG. åÓÌÉ ËÔÏ-ÌÉÂÏ ÐÏÌÕÞÉÔ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÔÏ ÏÎ ÓÍÏÖÅÔ ÒÁÓÛÉÆÒÏ×Ù×ÁÔØ ×ÓÅ ÎÁÐÒÁ×ÌÅÎÎÙÅ ÷ÁÍ ÓÏÂÝÅÎÉÑ É ÓÍÏÖÅÔ ÐÏÄÐÉÓÙ×ÁÔØ ÷ÁÛÅÊ ÐÏÄÐÉÓØÀ. åÓÌÉ ÷Ù ÐÔÅÒÑÅÔÅ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÔÏ ÎÅ ÓÍÏÖÅÔÅ ÂÏÌØÛÅ ÒÁÓÛÉÆÒÏ×Ù×ÁÔØ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÌÑ ÷ÁÓ É ÎÅ ÓÍÏÖÅÔÅ ÐÏÄÐÉÓÙ×ÁÔØ Ó×ÏÉ ÓÏÂÝÅÎÉÑ. ðÏÅÔÑ ÅÄÉÎÓÔ×ÅÎÎÏÊ ËÏÐÉÉ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ËÁÔÁÓÔÒÏÆÉÞÅÎ.

îÅÚ×ÉÓÉÍÏ ÏÔ ÔÏÇÏ, ËÁË ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG ÷Ù ÄÏÌÖÎÙ ÓÏÈÒÁÎÉÔØ ÓÅÒÅÆÉËÁÔ ÏÔÚÙ×Á ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ É ÒÅÚÅÒ×ÎÕÀ ËÏÐÉÀ ÷ÁÛÅÇÏ

ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÎÁ ÚÁÝÉÝÅÎÎÙÊ ÏÔ ÚÁÐÉÓÉ ÎÏÓÉÔÅÌØ É ÈÒÁÎÉÔØ ÅÇÏ × ÎÁÄÅÖÎÏÍ ÍÅÓÔÅ. îÁÐÒÉÍÅ, ÷Ù ÍÏÖÅÔÅ ÚÁÐÉÓÁÔØ ËÏÐÉÀ ËÌÍÐÁËÔ-ÄÉÓË É ÈÒÁÎÉÔØ ÅÇÏ × ÂÁÎËÏ×ÓËÍÍ ÓÂÊÆÅ. íÖÎÏ, ÔÁËÖÅ, ÚÁÐÉÓÁÔØ ÉÈ ÎÁ ÄÉÓËÅÔÕ É ÓÐÒÑÔÁÔØ ÅÅ ÄÍÍÁ. þÔÏÂÙ ÷Ù ÎÉ ÄÅÌÁÌÉ, ËÏÐÉÉ ÄÎÖÎÙ ÂÙÔØ ÓËÏÐÉÓÒ×ÁÎÙ ÎÁ ÎÏÓÉÔÅÌØ, ÎÁ ËÏÔÒÏÍÍ ÏÎÉ ÓÍÇÕÔ ÎÁÄÅÖÎÏ ÈÒÁÎÉÔØÓÑ ÎÁ ÐÒÏÑÖÅÎÉÉ ×ÓÅÇÏ ÓÒÏËÁ ÉÓÐÏÌØÚÏ×ÁÎÉÑ ËÌÀÞÁ, É ÉÈ ÓÌÅÄÕÂ ÓÐÒÑÔÁÔØ ÂÏÌÅ ÔÝÁÔÅÌØÎÏ, ÞÅÍ ËÏÐÉÀ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÄÌÑ ÅÖÄÎÅ×ÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ.

þÔÏÂÙ ÚÁÝÉÔÉÔØ ÷ÁÛ ËÌÀÞ, GnuPG ÎÅ ÓÏÈÒÁÎÑÅÔ ÅÇÏ ÎÁ ÄÉÓË × ÞÉÓÔÍÍ ×ÉÄÅ. ÷ÍÅÓÔÏ ÜÔÏÇÏ ÍÎ ÛÉÆÒÕÅÔÓÑ ÓÉÍÅÔÒÉÞÎÙÍ ÁÌÇÏÒÉÔÍÍÍ. ÷ÏÔ ÚÁÞÅÍ ÎÕÖÎÁ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÄÌÑ ÄÏÓÕÕÐÁ Ë ËÌÀÞÕ. ðÏÜÔÍÕ ×ÚÌÍÝÉË ÄÏÌÖÅÎ ÒÅÛÉÔØ Ä×Å ÐÒÏÂÌÅÍÙ, ÞÔÏÂÙ ÐÎÌÕÞÉÔØ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ: (1) ÍÎ ÄÎÖÅÎ ÐÎÌÕÞÉÔØ ËÌÀÞ, (2) ÍÎ ÄÎÖÅÎ ÒÁÓÛÉÆÒÏ×ÁÔØ ËÌÀÞ.

îÁÄÅÖÎÏÅ ÈÒÁÎÅÎÉÅ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ - ÓÌÏÖÎÁÑ ÚÁÄÁÞÁ. ÷ ÉÄÅÁÌÅ, ÷Ù ÄÎÖÎÙ ÈÒÁÎÉÔØ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÎÁ ÓÍÅÎÎÍÍ, ÚÁÝÉÝÅÎÎÍÍ ÏÔ ÚÁÐÉÓÉ ÄÉÓË ÉÓÐÏÌØÚÏ×ÁÔØ ÅÇÏ ÔÎÌØËÏ ÎÁ ÎÁÎÐÒÌØÚÏ×ÁÔÅÌÅ ÍÁÛÉÎÅ ÎÅ ÐÏÄËÌÀÞÅÎÎÎÊ Ë ÓÅÔÉ. üÔÏ ÍÏÖÅÔ ÏËÁÚÁÔØÓÑ ÎÅÕÄÏÂÎÙÍ ÉÌÉ ÎÅ×ÏÚÍÏÖÎÙÍ ÄÌÑ ÷ÁÓ. îÁÐÒÉÍÅÒ, Õ ÷ÁÓ ÍÏÖÅÔ ÎÅ ÂÙÔØ Ó×ÏÅÇÏ ËÏÍÐØÀÔÅÒÁ É ÷Ù ÉÓÐÏÌØÚÕÅÔÅ ËÏÍÐØÀÔÅÒ ÎÁ ÒÁÂÏÔÅ, ÉÌÉ ÜÔÏ ÍÏÖÅÔ ÏÚÎÁÞÁÔØ, ÞÔÏ ÷ÁÍ ÐÒÉÊÄÅÔÓÑ ÏÔËÌÀÞÁÔØ ËÏÍÐØÀÔÅÒ ÏÔ ÓÅÔÉ ËÁÖÄÙÊ ÒÁÚ ËÏÇÄÁ ÷Ù ÚÁÐÕÓËÁÅÔÅ GnuPG

üÔÏ ÎÅ ÏÚÎÁÞÁÅÔ, ÞÔÏ ÷Ù ÎÅ ÍÏÖÅÔÅ ÉÌÉ ÎÅ ÄÏÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG. üÔÏ ÏÚÎÁÞÁÅÔ ÔÏÌØËÏ, ÞÔÏ ÷Ù ÓÞÉÔÁÅÔÅ Ó×ÏÉ ÄÁÎÎÙÅ ÄÏÓÔÁÔÏÞÎÏ ×ÁÖÎÙÍÉ, ÞÔÏÂÙ ÛÉÆÒÏ×ÁÔØ, ÎÏ ÎÅ ÎÁÓÔÏÌØËÏ ×ÁÖÎÙÍÉ, ÞÔÏÂÙ ÐÒÉÎÉÁÔØ ÏÓÏÂÙÅ ÍÅÒÙ ÐÒÄÐÒÉÎÉÍÁÔØ ÄÌÑ ÕÓÉÌÅÎÉÑ ÐÅÒ×ÏÇÏ ÂÁÒØÅÒÁ ÚÁÝÉÔÙ. üÔÏ ÷ÁÛ ×ÙÂÏÒ.

èÏÒÏÛÁÑ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÏÞÅÎØ ËÒÉÔÉÞÎÁ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ GnuPG. ìÀÂÏÊ ×ÚÌÍÝÉË, ÐÏÕÞÉ×ÛÉÊ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÄÏÖÅÎ ×ÚÌÍÁÔØ ÛÉÆÒ ÎÁ ÓÅËÒÅÔÎÏÍ ËÌÀÞÅ. ÷ÍÅÓÔ ÁÔÄË × ÏÂ, ×ÚÌÍÝÉË, ÎÁ×ÅÒÎÑÁ, ÐÏÐÒÏÂÕÊ ÕÇÁÄÁÔØ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ.

íÏÉ×ÁÃÉÅÊ ÄÌÑ ÐÏÄÂÏÒÁ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ Ñ×ÌÑÅÔÓÑ ÔÏ, ÞÔÏ

ÂÏÌØÛÉÎÓÔ×Ï ÌÀÄÅÊ ×ÙÂÉÒÁÀÔ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ, ËÏÔÏÒÕÀ ÐÒÏÝÅ ÐÏÄÏÂÒÁÔØ, ÞÅÍ ÐÒÏÉÚ×ÎÌØÎÙÊ 128 ÂÉÔÎÙÊ ËÌÀÞ. åÓÌÉ × ËÁÞÅÓÔ×Å ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÌÏ×Ï, ÔÏ ÇÏÒÁÚÄÏ ÐÒÏÝÅ ÐÅÒÅÐÒÏÂÏ×ÁÔØ ×ÓÅ ÓÌÏ×Á × ÓÌÏ×ÁÒÑÈ ÍÉÒÏ×ÙÈ ÑÚÙËÏ×. äÁÖÅ ÅÓÌÉ ÓÌÏ×Ï ÉÓËÁÖÅÎÏ, ÎÁÐÒÉÍÅÒ, k3wldood, ÇÏÒÁÚÄÏ ÐÒÏÝÅ ÐÏÐÒÏÂÏ×ÁÔØ ÓÌÏ×Á ÉÚ ÓÌÏ×ÁÒÑ Ó ËÁÔÁÌÏÇÏÍ ÐÅÒÅÓÁÎÏ×ÏË. ôÁÖÅ ÐÒÏÂÌÅÍÁ Ó ÃÉÔÉÒÏ×ÁÎÉÅÍ. ÷ ÏÂÝÅÍ ÓÌÕÞÁÅ, ËÌÀÞÅ×ÙÅ ÆÒÁÚÙ ÏÓÎÏ×ÁÎÙÅ ÎÁ ÅÓÔÅÓÔ×ÅÎÎÍ ÑÚÙËÅ ÎÅÄÏÓÔÁÔÏÞÎÙ, Ô.Ë. × ÅÓÔÅÓÔ×ÅÎÎÙÈ ÑÚÙËÁÈ ÎÅ È×ÁÔÁÅÔ ÓÌÕÞÁÊÎÏÓÔÉ É ÉÚÂÙÔÏÞÎÏÓÔÉ. ÷Ù ÄÏÌÖÎÙ ÉÚÂÅÇÁÔØ ÉÓÐÏÌØÚÏ×ÁÎÉÑ ÅÓÔÅÓÔ×ÅÎÎÙÈ ÑÚÙËÏ× × ËÌÀÞÅ×ÙÈ ÆÒÁÚÁÈ, ÅÓÌÉ ÍÏÖÅÔÅ.

èÏÒÏÛÁÑ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÔÁËÏ×Á, ÞÔÏ ÷Ù ÍÏÖÅÔÅ ÅÅ ÚÁÐÏÍÍÉÔØ, ÎÏ ÅÅ ÔÒÕÄÎÏ ÐÏÄÏÂÒÁÔØ. ïÎÁ ÄÏÌÖÎÁ ×ËÌÀÞÁÔØ ÓÉÍ×ÏÌÙ ÉÚ ×ÓÅÇÏ ÄÉÁÐÁÚÏÎÁ ÐÅÞÁÔÎÙÈ ÓÉÍ×ÏÌÏ× ÎÁ ×ÁÛÅÊ ËÌÁ×ÉÁÔÕÒÅ. óÀÄÁ ×ÈÏÄÑÔ ÁÌÆÁ×ÉÔÎÙÅ ÓÉÍ×ÏÌÙ, × ÒÁÚÎÙÈ ÒÅÇÉÓÔÒÁÈ, ÃÉÆÒÙ É ÓÐÅÃÉÁÌØÎÙÅ ÓÉÍ×ÏÌÙ, ÔÁËÉÅ ËÁË } É |. ðÒÏÑ×ÉÔÅ Ô×ÏÒÞÅÓËÉÊ ÐÏÄÈÏÄ É ÚÁÔÒÁÔØÔÅ ÎÅÍÎÏÇÏ ×ÒÅÍÅÎÉ ÏÂÄÕÍÙ×ÁÑ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ, ÈÏÒÛÉÊ ×ÙÂÏÒ ×ÁÖÅÎ ÄÌÑ ÏÂÅÓÐÅÞÅÎÉÑ ÷ÁÛÅÊ ÓÅËÒÅÔÎÏÓÔÉ.

4.1.3. ÷ÙÂÏÒ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ É ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏÐÏÎÉÔÅÌØÎÙÈ ËÌÀÞÅÊ

ðÏ ÕÍÏÌÞÁÎÉÀ, ËÏÇÄÁ ÷Ù ÓÏÚÄÁÅÔÅ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ, ÇÅÎÅÒÉÒÕÅÔÓÑ ÇÌÁ×ÎÙÊ ËÌÀÞ DSA ÄÌÑ ÐÏÄÐÉÓÉ É ÐÏÄÞÉÎÅÎÎÙÊ ËÌÀÞ ElGamal ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. üÔÏ ÕÄÏÂÎÏ, Ô.Ë. ÒÏÌÉ Ä×ÕÈ ËÌÀÞÅÊ ÒÁÚÌÉÞÎÙ, É ÷Ù ÍÏÖÅÔÅ ÐÏÖÅÌÁÔØ, ÞÔÏÂÙ ÏÎÉ ÉÍÅÌÉ ÒÁÚÌÉÞÎÙÅ ÓÒÏËÉ ÄÅÊÓÔ×ÉÑ. çÌÁ×ÎÙÊ ËÌÀÞ ÄÌÑ ÐÏÄÐÉÓÉ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÓÏÚÄÁÎÉÑ ÃÉÆÒÏ×ÙÈ ÐÏÄÐÉÓÅÊ, ÎÁ ÎÅÍ, ÔÁËÖÅ, ÓÏÂÉÒÀÔÓÑ ÐÏÄÐÉÓÉ ÔÅÈ, ËÔÏ ÐÏÄÔ×ÅÒÖÄÁÅÔ ÐÒÁÄÌÅÎÎÏÓÔØ ËÌÀÞÁ ÷ÁÍ. ëÌÀÞ ÛÉÆÒÏ×ÁÎÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÚÁÛÉÆÒÏ×ÁÎÎÙÈ ÄÏËÕÍÅÎÔÏ×, ÏÔÐÒÁ×ÌÅÎÎÙÈ ÷ÁÍ. ïÂÙÞÎÏ, ÃÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÉÍÅÅÔ ÐÒÏÄÏÌØÎÙÊ ÓÒÏË ÄÅÊÓÔ×ÉÑ, ÎÁÐÒÉÍÅÒ, ÎÅÏÇÒÁÎÉÞÅÎÎÙÊ, É ÷Ù, ÔÁËÖÅ, ÎÅ ÈÏÉÓÅ ÕÔÒÁÔÉÔØ

ÐÏÄÐÉÓÉ ÎÁ ÷ÁÛÅÍ ËÌÀÞÅ, ÓÏÂÀÁÎÎÙÅ Ó ÂÎÌØÛÉÍ ÔÀÕÄÏÍ. ó ÄÀÕÇÏÊ ÓÔÏÀÏÎÙ, ÐÏÄËÌÀÞ ÛÉÆÀÏ×ÁÎÉÑ ÍÏÖÅÔ ÐÅÀÉÏÄÉÞÅÓËÉ ÉÚÍÅÎÑÔØÓÑ, ÞÔÏ ÐÏ×ÙÓÉÔ ÂÅÚÏÐÁÓÎÏÓÔØ, Ô.Ë. ×ÚÌÍÁÎÎÙÊ ËÌÀÞ ÛÉÆÀÏ×ÁÎÉÑ ÐÚ×ÌÍÉÔ ×ÚÌÍÝÉËÕ ÐÀÏÞÅÓÔØ ×ÓÅ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÀÏ×ÁÎÎÙÅ ÄÌÑ ÜÔÏÇÏ ËÌÀÞÁ, ËÁË × ÂÕÄÕÝÅÍ, ÔÁË É × ÐÀÏÛÌÍÍ.

ðÏÜÔÍÕ ÷Ù ÐÏÞÔÉ ×ÓÅÇÄÁ ÚÁÈÏÉÔÅ ÏÓÔÁ×ÉÔØ ÇÌÁ×ÎÙÊ ËÌÀÞ Ó ÎÅÏÇÀÁÉÞÅÎÎÙÍ ÓÀÏËÍÍ ÄÅÊÓ×ÉÑ. åÓÔØ Ä×Å ÐÀÉÞÉÎÙ ÐÏ ËÏÔÏÀÙÍ ÷Ù ÍÏÖÅÔÅ ÏÇÀÁÉÞÉÔØ ÓÀÏËÍÍ ÄÅÊÓ×ÉÑ ËÌÀÞÁ. ÷Ï-ÐÅÀ×ÙÈ, ÷ÁÍ ÍÏÖÅÔ ÐÏÎÁÄÏÂÉÔØÓÑ ËÌÀÞ ÎÁ ÏÐÀÅÄÅÌÅÎÙÊ ÐÅÀÉÏÄ. îÁÐÀÉÅÀÒ, ËÌÀÞ ÂÕÄÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ×Ï ×ÀÅÑ ÉÚÂÉÀÁÔÅÌØÎÏÎÊ ËÁÍÐÁÎÉÉ É ÎÅ ÐÏÎÁÄÏÂÉÔÓÑ ÐÏÓÌÅ ÅÄ ÏËÍÍÞÁÎÉÑ. äÀÕÇÁÑ ÐÀÉÞÉÎÁ ÓÏÓÔÉÔ × ÔÏÍ, ÞÔÏ ÅÓÌÉ ÷Ù ÔÅÀÑÅÔÅ ËÏÎÔÀÏØ ÎÁÄ ËÌÀÞÏÍ É, ÐÀÉ ÜÔÏÍ, ÎÅ ÉÍÅÅÔÅ ÓÅÀÔÉÆÉËÁÔÁ ÏÔÚÙ×Á, ÎÁÌÉÞÉÅ ÓÀÏËÁ ÄÅÊÓ×ÉÑ ÇÁÀÁÎÔÉÀÕÅÔ, ÞÔÏ × ËÏÎÅÞÎÍÍ ÓÞÅÔÅ ËÌÀÞ ÓÔÁÎÅÔ ÎÅÄÅÊÓ×ÉÔÅÌÅÎ.

óÍÅÎÁ ÐÏÄËÌÀÞÅÊ ÛÉÆÀÏ×ÁÎÉÑ ÐÀÏÓÔÁ, ÎÏ ÍÏÖÅÔ ×ÙÚ×ÁÔØ ÎÅÕÄÏÂÓÔ×Á. åÓÌÉ ÷Ù ÓÏÚÄÁÅÔÅ ÎÏ×ÕÀ ÐÁÀÕ ËÌÀÞÅÊ ÓÏ ÓÀÏËÍÍ ÄÅÊÓ×ÉÑ ÐÏÄËÌÀÞÅÊ, ÜÔÏÔ ÓÀÏË ÒÁÎÏ ÉÌÉ ÐÏÚÄÎÏ ÉÓÔÅÞÅÔ ÉÓÔÏÞÎÉË ÐÏÄÐÉÓÉ ÄÅÊÓ×ÉÑ ÓÀÏËÁ, ÷ÁÍ ÓÌÅÄÕÅÔ ÄÏÂÁ×ÉÔØ ÎÏ×ÙÊ ÐÏÄËÌÀÞ É ÏÐÕÂÌÉËÏ×ÁÔØ ÌÅÎÎÙÊ ÏÔËÙÔÙÊ ËÌÀÞ. ðÏÓÌÅ ÉÓÔÅÞÅÎÉÑ ÓÀÏËÁ ÄÅÊÓ×ÉÑ, ÔÅ, ËÔÏ ÈÏÑÔ ÏÔÐÒÁ×ÉÔØ ÷ÁÍ ËÏÒÒÅÓÐÏÎÄÅÎÃÉÀ, ÄÏÌÖÎÙ ÎÁÊÔÉ ÷ÁÛ ÏÂÎÏ×ÌÅÎÎÙÊ ËÌÀÞ, Ô.Ë. ÎÅ ÓÍÏÇÕÔ ÂÏÌÅÅ ÛÉÆÀÏ×ÁØ ËÌÀÞÏÍ Ó ÐÒÏÓÏÞÅÎÎÙÍ ÓÀÏËÍÍ ÄÅÊÓ×ÉÑ. üÔÏ ÍÏÖÅÔ ÎÅÑÄÏÂÎÙÍ, × ÚÁ×ÉÓÉÍÓÔÉ ÏÔ ÔÏÇÏ, ËÁË ÷Ù ÒÁÓÐÒÏÓÔÁÎÑÅÔÅ Ó×ÏÊ ÏÔËÙÛÙÊ ËÌÀÞ. ïÄÎÁËÏ ÎÅ ÔÒÅÂÕÅÔÓÑ ÎÉËÁËÉÈ ÄÏÐÏÎÉÔÅÌØÎÙÈ ÐÏÄÐÉÓÅÊ, Ô.Ë. ÐÏÄËÌÀÞ ÐÏÄÐÉÓÁÎ ÷ÁÛÉÍ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÙ×ÁÀÝÉÍ ËÌÀÞÏÍ, ËÏÔÏÒÙÊ, ×ÅÒÑÔÎÏÍ, ÕÖÅ ÂÙÌ ÐÏÂ×ÅÒÖÄÅÎ ÷ÁÛÉÍÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍÉ.

üÔÉ ÎÅÕÄÏÂÓ×Á ÍÏÇÕÔ ÏÐÒÁ×ÄÙ×ÁÔØ, Á ÍÏÇÕÔ É ÎÅ ÏÐÒÁ×ÄÙ×ÁÔØ ÐÏÎÕÞÁÅÍÕÀ ÄÏÐÏÎÍÉÔÅÌØÎÕÀ ÚÁÝÉÔÕ. ôÁË ÖÅ ËÁË É ÷Ù, ×ÚÌÍÝÉËÕ ÍÏÖÅÔ ÞÉÔÁÔØ ×ÓÅ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÀÏ×ÁÎÎÙÅ ÉÓÔÅËÛÉÍ ËÌÀÞÍÍ. óÍÅÎÁ ÐÏÄËÌÀÞÁ ÚÁÝÉÝÁÅÔ ÔÏÌØËÏ ÎÏ×ÙÅ ÄÏËÕÍÅÎÔÙ. äÌÑ ÞÔÅÎÉÑ ÄÏËÕÍÅÎÔÏ×, ÚÁÛÉÆÀÏ×ÁÎÎÙÈ ÎÏ×ÙÍ ÐÏÄËÌÀÞÍÍ, ×ÚÌÍÝÉËÕ ÐÀÉÊÄÅÔÅ ×ÚÌÁÍÙ×ÁÔØ ÎÏ×ÙÊ ËÌÀÞ, ÉÓÐÏÌØÚÕÑ ÔÅ ÖÅ ÍÅÔÏÄÙ, ÞÔÏ É × ÐÀÒ×ÙÊ ÒÁÚ.

îÁËÏÎÅÃ, ×ÓÅ ÜÔÏ ÉÍÅÅÔ ÓÍÙÓÌ, ÅÓÌÉ × Ó×ÑÚËÅ ÉÍÅÅÔÓÑ ÔÏÌØËÏ ÏÄÎÁ ÄÅÊÓÔ×ÕÀÝÉÊ ÐÏÄÄÉÌÀÞ. ÷Ù ÎÅ ÐÏÕÞÉÔÅ ÎÉËÁËÏÊ ÄÏÐÏÌÎÉÔÅÌØÎÏÊ ÚÁÝÉÔÙ ÐÒÉ ÎÁÌÉÞÉÉ Ä×ÕÈ É ÂÎÌÅÅ ÁËÔÉ×ÎÙÊ ËÌÀÞÅÊ. ÷Ù, ËÏÎÅÞÎÏ, ÍÏÖÅÔÅ ÉÍÅÔØ ÌÀÂÏÅ ÞÉÓÌÏ ÉÓÔÅËÛÉÈ ËÌÀÞÅÊ × Ó×ÑÚËÅ, ÞÔÏÂÙ ÞÉÔÁØ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÙÅ ÒÁÎÎÅÅ, ÎÏ ÔÏÌØËÏ ÏÄÎÏ ÐÏÄÐÉÓÁÎÎÙÊ ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÄÏÌÖÅÎ ÓÏÄÅÒÖÁÔØ ÔÏÌØËÏ ÏÄÎÕ ÐÏÄÐÉÓØ × ÄÁÎÎÏÍ ÓÌÕÞÁÅ.

4.1.4. õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÒÒÉÑ.

ëÁË É ÚÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÕÐÒÁ×ÌÅÎÉÅ ÓÅÔØÀ ÄÏ×ÒÒÉÑ Ñ×ÌÑÅÔÓÑ ÔÅÍ ÁÓÐÅÈÎÍ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG, ËÏÔÒÙÊ ÔÒÅÂÕÅÔ ÓÏÂÌÀÄÅÎÉÑ ÂÁÌÁÎÓÁ ÍÅÖÄÕ ÚÁÝÉÔÏÊ É ÌÅÇËÏÓÔØÀ ÉÓÐÏÌØÚÏ×ÁÎÉÑ. åÓÌÉ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG ÄÌÑ ÚÁÝÉÔÙ ÏÔ ÓÌÕÞÁÊÎÏÇÏ ÐÏÄÓÌÕÛÉ×ÁÎÉÑ É ÐÏÄÄÅÌÏË, ÔÏ ÍÏÖÅÔÅ ÐÏÚ×ÌÉÔØ ÓÅÂÅ ÏÔÎÏÓÉÔÅÌØÎÕÀ ÌÅÇËÏÓÔØ × ÄÏ×ÅÒÉÉ ÞÕÖÉÍ ÐÏÄÐÉÓÑÍ ÎÁ ËÌÀÞÁÈ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÅÓÌÉ ÷Ù ÓÞÉÔÁÅÔÅ, ÞÔÏ ËÔÏ-ÌÉÂÏ ÚÁÉÎÔÅÒÅÓÏ×ÁÎ × ÐÏÌÕÞÅÎÉÉ ÄÏÓÕÐÁ Ë ÷ÁÛÉÍ ÓÅËÒÅÔÁÍ, ÔÏ ÷ÁÍ ÓÌÅÄÕÅÔ ÐÒÏÑ×ÌÑÔØ ÍÅÎØÛÅÅ ÄÏ×ÒÉÅ × ÏÔÎÏÛÅÎÉÉ ÞÕÖÉÈ ÐÏÄÐÉÓÅÊ É ÔÒÁÔÉÔØ ÂÏÌØÛÅ ×ÒÅÍÅÎÉ ÎÁ ÐÒÏ×ÅÒËÕ ËÌÀÞÅÊ.

îÅÚÁ×ÉÓÉÍÏ ÏÔ ÷ÁÛÉÈ ÌÉÞÎÙÈ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ, ÷Ù ×*ÓÅÇÄÁ ÄÏÌÖÎÙ ÂÙÔØ ×ÎÉÍÁÔÅÌØÎÙ* ÐÏÄÐÉÓÙ×ÁÑ ÞÕÖÉÅ ËÌÀÞÉ. ðÏÄÐÉÓÙ×ÁÔØ ËÌÀÞ ÏÐÉÒÁÑÓØ ÎÁ ÓÏÂÓÔ×ÅÎÎÙÅ ÐÏÔÒÅÂÎÏÓÔÉ × ÚÁÝÉÔÅ ÜÇÏÉÓÔÉÞÎÏ. îÁ ÷ÁÛÕ ÐÏÄÐÉÓØ ÍÇÕÔ ÐÌÁÇÁÔØÓÑ ÄÕÇÉÅ, ÞØÉ ÔÒÅÂ×ÁÎÉÑ, ×ÏÚÍÏÖÎÏ, ÂÏÌÅÅ ×ÙÓÏËÉ. åÓÌÉ ÏÎÉ ÎÅ ÓÍÇÕÔ ÐÌÁÇÁÔØÓÑ ÎÁ ÷ÁÓ, ÜÔÏ ÏÓÌÁÂÉÔ ÓÅÔØ ÄÏ×ÅÒÉ É ÚÁÔÒÕÄÎÉÔ ×ÓÅÇÏ ÓÏÎÁÝÅÔÔ×Á ÐÌØÚÏ×ÁÔÅÌÅÊ GnuPG. éÓÐÌØÚÕÊÔÅ ÔÅ ÖÅ ÍÅÒÙ ÐÒÅÄÏÔÒÏÎÏÓÔÉ, ÐÏÄÐÉÓÙ×ÁÑ ËÌÀÞÉ, ËÁËÉÅ ÷Ù ÈÏÔÉÔÅ ÂÙ, ÞÔÏÂÙ ÐÒÉÎÉÍÁÌÉ ÔÅ, ÎÁ ÞØÉ ÐÏÄÐÉÓÉ ÐÌÏÇÁÅÔÅÓØ ÷Ù.

îÁ ÐÒÁËÔÉËÅ, ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ Ó×ÅÄÅÎÏ Ë ÐÒÉÓ×ÏÅÎÉÀ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ ÎÅËÏÔÏÒÏÍÕ ÍÉÎÉÍÁÌØÎÏÍÕ ÞÉÓÌÕ ÄÕÇÉÈ ÌÉÃ É ÎÁÓÔÒÏÊËÅ ÐÁÒÁÍÅÔÒÏ× `--marginals-needed` É `--completes-needed`. ìÀÂÏÊ ËÌÀÞ, ÐÏÄÐÉÓÁÎÎÙÊ ÷ÁÍÉ ÌÉÞÎÏ, ÓÞÉÔÁÅÔÓÑ

ÐÏÄÔ×ÅÒÖÄÅÎÎÙÍ, ÎÏ, ËÒÏÍÅ ËÁË ÄÌÑ ÍÁÌÅÎØËÉÈ ÇÒÕÐÐ, ÎÅ Ñ×ÌÑÅÔÓÑ ÐÒÁËÔÉÞÎÙÍ ÐÏÄÐÉÓÙ×ÁÔØ ËÌÀÞ ËÁÖÄÏÇÏ, Ó ËÅÍ ÷Ù ÐÅÒÅÐÉÓÙ×ÁÅÔÅÓØ. ÷Ù ÂÕÄÅÔÅ, ÓÌÅÄÏ×ÁÔÅÌØÎÏ, ÄÎÏÔÙ ÐÎÌÁÇÁÔØÓÑ ÎÁ ÄÒÕÇÉÈ.

îÁÉÂÏÌÅÅ ÒÁÚÕÍÎÏ, ÐÒÏÑ×ÉÔØ ÁËËÕÒÁÔÎÏÓÔØ ÐÒÉÓ×ÁÉ×ÁÑ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ É ÚÁÔÅÍ ÎÁÓÔÒÏÉÔØ ÏÐÃÉÉ, ÕËÁÚÙ×ÁÀÝÉÅ GnuPG ÓÔÒÏÇÏÓÔØ ÐÒÏ×ÅÒËÉ ËÌÀÞÅÊ. îÁÐÒÍÅÒ, ÷Ù ÍÏÖÅÅ ÐÌÍÏÓÔØÀ ÄÏ×ÅÒÑÔØ ÕÚËÍÍÕ ËÒÕÇÕ ÄÒÕÚÅÊ, ËÏÔÏÒÙÅ, ËÁË ÷Ù ÚÎÁÅÔÅ, ÏÓÔÏÒÏÖÎÙ ÐÒÉ ÐÏÄÐÉÓÉ ËÌÀÞÅÊ, É ÎÅÚÎÁÞÉÔÅÌØÎÏ ÄÏ×ÅÒÑÔØ ×ÓÅÍ ÏÓÔÁÌØÎÙÍ, ÞØÉ ËÌÀÞÉ ÉÍÅÀÔÓÑ × ÷ÁÛÅÊ Ó×ÑÚËÅ. ôÏÇÄÁ, ÷Ù ÍÏÖÅÔÅ ÕÓÔÁÎÏ×ÉÔØ ÚÎÁÞÅÎÉÑ `--completes-needed` ÒÁ×ÎÙÍ `1` É `--marginals-needed` ÒÁ×ÎÙÍ `2`. åÓÌÉ ÷Ù ÂÏÌÅÅ ÏÓÔÏÒÏÖÎÙ, ÔÏ ÍÏÖÅÔÅ ×ÙÂÒÁÔØ ÚÎÁÞÅÎÉÑ `1` É `3` ÉÌÉ `2` É `3` ÓÏÏÔ×ÅÔÓÔ×ÅÎÎÏ. åÓÌÉ ÷Ù ÍÅÎØÛÅ ÏÚÁÂÏÞÅÎÙ ÓÅËÒÅÔÎÏÓÔØÀ É ÐÒÏÓÔÏ ÚÁÉÎÔÅÒÅÓÏ×ÁÎÙ × ÎÅËÏÔÏÒÏÍ ÐÒÉÅÎÌÅÍÍ ÐÏÄÔ×ÅÒÖÄÅÎÉÅ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ, ÕÓÔÁÎÏ×ÉÔÅ ÚÎÁÞÅÎÉÑ `1` É `1`. ÷ ÃÅÌÏÍ, ÂÏÌÅÅ ×ÙÓÏËÉÅ ÚÎÁÞÅÎÉÑ ÜÔÉÈ ÐÁÒÁÍÅÔÒÏ× ÏÚÎÁÞÁÀÔ, ÞÔÏ ÂÏØÛÅÅ ÞÉÓÌÏ ÌÀÄÅÊ ÄÏÖÎÏ ÓÇÏ×ÏÒÉÔÓÑ ÐÒÏÔÉ× ÷ÁÓ, ÞÔÏÂÙ ÐÏÎÑÞÉÔØ ÐÏÄÔ×ÅÒÖÄÅÎÉÅ ËÌÀÞ, ÎÅ ÐÒÉÎÄÌÅÖÁÝÉÊ ÔÏÍÕ, ËÏÍÕ ÷Ù ÄÕÍÁÅÔÅ.

4.2. ðÏÓÔÒÏÅÎÉÅ ÷ÁÛÅÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ

ïÄÎÏÇÏ ÖÅÌÁÀÝÅÇÏ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ÎÅÄÏÓÔÁÔÏÞÎÏ. äÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÓÏÏÂÝÁÔØÓÑ ÚÁÝÉÝÅÎÎÏ Ó ÄÒÕÇÉÍÉ, ÷Ù ÄÏÌÖÎÙ ÉÍÅÔØ ÓÅÔØ ÄÏ×ÅÒÉÑ. ðÏÓÔÒÏÅÎÉÅ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÐÏÈÏÖÅ ÎÁ ÕËÒÏÝÅÎÉÅ. ìÀÄÉ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÁÅÔÅÓØ, ÄÏÌÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG[1], É ÄÏÌÖÎÏ ÉÍÅÔØÓÑ ÄÏÓÔÁÔÏÞÎÅ ËÏÌÉÞÅÓÔ×Ï ÐÏÄÐÉÓÁÎÎÙÈ ËÌÀÞÅÊ, ÞÔÏÂÙ ËÌÀÞÉ ÍÇÌÉ ÐÏÄÔ×ÅÒÖÄÅÎÙ. üÔÏ ÎÅ ÓÔÒÏØËÏ ÔÀÈÎÉÞÅÓËÉÅ, ÓËÏÌØËÏ ÓÏÃÉÁÌØÎÙÅ ÐÒÏÂÌÅÍ. ïÄÎÁËÏ, ÷Ù ÄÏÌÖÎÙ ÐÒÅÄÐÒÉÎÉÍÁÔØ ÜÔÉ ÐÒÏÂÌÅÍÙ, ÅÓÌÉ ÈÏÔÉÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG.

ëÏÇÄÁ ÷Ù ÎÁÞÉÎÁÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, ×ÁÖÎÏ ÐÏÎÎÔØ, ÞÔÏ ÎÅÔ ÎÁÏÂÈÄÉÍÏÔÉ × ÚÁÝÉÔÅ ÐÒÅÐÒÉËÉ Ó ËÁÖÄÙÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÏÍ.

îÁÞÎÉÔÅ Ó ÎÅÂÏÌØÛÏÇÏ ËÒÕÇÁ ÌÀÄÅÊ, ×ÏÚÍÏÖÎÏ ÔÏÌØËÏ ÷Ù É ÏÄÉÎ ÉÌÉ Ä×Á ÷ÁÛÉÈ ÔÏ×ÁÒÉÝÁ, ÔÏÖÅ ÖÅÌÁÀÝÉÈ ÒÅÁÌÉÚÏ×ÁÔØ Ó×ÏÅ ÐÒÁ×Ï ÎÁ ÔÁÊÎÕ ÐÅÒÅÐÉÓËÉ. óÏÚÄÁÊÔÅ ÷ÁÛÉ ËÌÀÞÉ É ÐÏÄÐÉÛÉÔÅ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÄÒÕÇ ÄÒÕÇÁ. üÔÏ ÷ÁÛÁ ÎÁÞÁÌØÎÁÑ ÓÅÔØ ÄÏ×ÅÒÉÑ. äÅÌÁÑ ÔÁË, ÷Ù ÏÃÅÎÉÔÅ ÚÎÁÞÅÎÉÅ ÍÁÌÅÎØËÏÊ, ÎÁÄÅÖÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ É ÂÕÄÅÔÅ ÂÏÌÅÅ ÏÓÔÏÖÏÔÙ × ÂÕÄÕÝÅÍ, ËÏÇÄÁ ÷ÁÛÁ ÓÅÔØ ÓÔÁÎÅÔ ÒÁÓÔÉ.

÷ ÄÏÐÏÎÅÎÉÅ Ë ÜÔÏÊ ÎÁÞÁÌØÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ, ÷Ù ÍÏÖÅÔÅ ÚÁÈÏÔÅÔØ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏ ÐÅÒÅÐÉÓÙ×ÁÔØÓÑ Ó ÄÒÕÇÉÍÉ ÌÀÄØÍÉ, ÔÁËÖÅ ÉÓÐÏÌØÚÕÀÝÉÍÉ GnuPG. òÅÁÌÉÚÁÃÉÑ ÜÔÏÇÏ ÖÅÌÁÎÉÑ, ÏÄÎÁËÏ, ÍÏÖÅÔ ÏËÁÚÁÔØÓÑ ÎÅÕÄÏÂÎÏÅ ÐÏ Ä×ÕÍ ÐÒÉÞÉÎÁÍ: (1) ÷Ù ÎÅ ×ÓÅÇÄÁ ÚÎÁÅÔÅ, ÞÔÏ ÞÅÌÏ×ÅË ÉÓÐÏÌØÚÕÅÔ ÉÌÉ ÖÅÌÁÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, É (2) ÅÓÌÉ ÷Ù É ÚÎÁÅÔÅ, ÞÔÏ ÞÅÌÏ×ÅË ÉÓÐÏÌØÚÕÅÔ ÅÇÏ, ÍÏÇÕÔ ×ÏÚÎÉËÎÕÔØ ÓÌÏÖÎÏÓÔÉ Ó ÐÏÄÔ×ÅÒÖÄÅÎÉÅÍ ËÌÀÞÅÊ. ðÅÒ×ÁÑ ÐÒÉÞÉÎÁ Ñ×ÌÑÅÔÓÑ ÓÌÅÄÓÔ×ÉÍ ÔÏÇÏ, ÞÔÏ ÌÀÄÉ ÎÅ ×ÓÅÇÄÁ ÏÂßÑ×ÌÑÀÔ Ï ÔÏÍ, ÞÔÏ ÉÓÐÏÌØÚÕÀÔ GnuPG. ÷ÏÚÍÏÖÎÙÊ ×ÁÒÉÁÎÔ ÒÅÛÅÎÉÑ ÜÔÏÊ ÐÒÏÂÌÅÍÙ, ÐÏÄÁÔØ ÐÒÉÍÅÒ É ÏÂßÑ×ÉÔØ, ÞÔÏ ÷Ù ÉÓÐÏÌØÚÕÅÅ GnuPG. åÓÔØ ËÁË ÍÉÎÉÍÕÍ ÔÒÉ ÓÐÏÓÏÂÁ ÓÄÅÌÁÔØ ÜÔÏ: ÷Ù ÍÏÖÅÅ ÐÏÄÐÉÓÙ×ÁÔØ Ó×ÏÉ ÓÏÎÝÅÎÉÑ, ÷Ù ÍÏÖÅÅ ÐÏÎÏÖÉÔØ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÁ Ó×ÏÅÊ ×ÅÂ-ÓÔÒÁÎÉÃÅ, ÷Ù ÍÏÖÅÅ ÕËÁÚÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÷ÁÛÅÇÏ ËÌÀÞÁ × ÐÏÄÐÉÓÉ ÐÏÞÔÏ×ÏÇÏ ÓÏÎÝÅÎÉÑ. åÓÌÉ ÷Ù ÓÏÎÝÅÅÔÅ Ï Ó×ÏÅÍ ËÌÀÞÅ, ÔÏ ÄÅÌÅÔÅ ÂÎÅÅ ÕÍÅÎØÛÉÔÅ ÄÌÑ ÄÒÕÇÉÈ ÓÏÎÝÉÈ ÐÏÄÐÉÓÅÊ, ÎÁÞÉÎÁÑ Ó ËÌÀÞÁ ÐÏÄ ×ÏÐÒÏÓÏÍ É ÚÁËÁÎÞÉ×ÁÑ ÷ÁÛÉÍ. äÌÑ ÎÁÈÏÄÅÎÉÑ ÃÅÐÏÞËÉ, ÷Ù ÄÎÌÖÎÙ ÐÒÏÑ×ÉÔØ ÉÎÉÃÉÁÔÉ×Õ É ÐÎÕÞÉÔØ ÷ÁÛ ËÌÀÞ ÐÏÄÐÉÁÎÎÙÊ ËÅÍ-ÌÉÂÏ ÚÁ ÐÒÅÄÅÌÁÍÉ ÷ÁÛÅÊ ÎÁÞÁÌØÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ.

éÍÅÊÔÅ ÏÄÎÁËÏ × ×ÉÄÕ, ÞÔÏ ×ÓÅ ÜÔÏ × ÚÁ×ÉÓÉÍÏÓÔÉ ÏÔ ÐÏÔÒÅÂÎÏÓÔÅÊ. ÷Ù ÎÅ ÏÂÑÚÁÔÅÌØÎÏ ÄÎÖÎÙ ÚÁÑ×ÌÑÔØ Ï Ó×ÏÅÍ ËÌÀÞÅ ÉÌÉ ÐÏÄÐÉÓÙ×ÁÔØ

ÞÕÖÉÅ ËÌÀÞÉ. óÉÌÁ GnuPG ÓÏÓÔÉÊ × ÔÏÍ, ÞÔÏ ÏÎ ÄÏÓÔÁÔÏÞÎÏ ÇÉÂÏË É ÍÏÖÅÔ ÂÙÔØ ÁÄÁÐÔÉÒ×ÁÎ Ë ÷ÁÛÉÍ ÐÏÔÒÅÂÎÏÓÔÑÍ, ËÁËÉÍÉ ÂÙ ÏÎÉ ÎÅ ÂÙÌÉ. ðÒÉ ÜÔÏÍ ÄÅÊÓÔ×ÉÔÅÌØÎÏÓÔØ ÔÁËÏ×Á, ÞÔÏ ÷Ù ÄÏÌÖÎÙ ÐÒÏÑ×ÌÑÔØ ÉÎÉÃÉÁÔÉ×Õ, ÅÓÌÉ ÈÏÔÉÔÅ ÒÁÓÛÉÒÉÔØ Ó×ÏÀ ÓÅÔØ ÄÏ×ÅÒÉÑ É ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ËÁË ÍÏÖÎÏ ÂÏÌØÛÅ.

4.3. úÁËÏÍÍÏÓÔØ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG

úÁËÏÎÎÙÊ ÓÔÁÔÕÓ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÐÒÏÇÒÁÍÍ ÒÁÚÌÉÞÅÎ × ÒÁÚÎÙÈ ÓÔÒÁÎÁÈ, ËÒÏÍÅ ÔÏÇÏ, ÚÁËÏÎÙ, ÒÅÇÕÌÉÒÕÀÝÉÅ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÓÒÅÄÓÔ×, ÂÙÓÔÒ ÍÅÎÑÀÔÓÑ. Bert-Japp Koops (http://cwis.kub.nl/~frw/people/koops/bertjaap.htm) ÓÄÅÌÁÌ ÎÅÐÌÈÕÀ ÓÔÒÁÎÉÞËÕ Crypto Law Survey (http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm), Ë ËÏÔÒÏÊ ÷Ù ÍÏÖÅÔ ÏÂÒÁÔÉÔØÓÑ, ÞÔÏÂÙ ÕÚÎÁÔØ ÚÁËÏÎÏÄÁÔÅÌØÎÙÊ ÓÔÁÔÕÓ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÐÒÏÇÒÁÍÍ × ÷ÁÛÅÊ ÓÔÒÁÎÅ.

1. ÷ ÜÔÏÍ ÒÁÚÄÅÌÅ, GnuPG ÏÔÎÏÓÉÔÓÑ Ë GnuPG ÒÅÁÌÉÚÁÃÉÉ OpenPGP ÔÁËÖÅ, ËÁË Ë ÄÒÕÇÉÍ ÒÅÁÌÉÚÁÃÉÑÍ, ÔÉÐÁ PGP ÐÒÏÉÚÉÄÉÍÏÍÕ NAI.

5. òÁÚÌÉÞÎÙÅ ×ÏÐÒÏÓÙ

üÔÁ ÇÌÁ×Á ÒÁÓÓÍÁÔÒÉ×ÁÅÔ ÒÁÚÌÉÞÎÙÅ ×ÏÐÒÏÓÙ ËÏÔÏÒÙÍ ÎÅ ÎÁÛÌÏÓØ ÍÅÓÔÁ × ÄÒÕÇÉÍ ÍÅÓÔÅ ÒÕËÏ×ÏÄÓÔ×Á. äÏÂÁ×ÌÅÎÎÙÅ ×ÏÐÒÏÓÙ ÍÏÇÕÔ ÓÏÂÉÒÁÔØÓÑ É ÒÁÓÐÒÅÄÅÌÑÔØÓÑ ÐÏ ÇÌÁ×ÁÍ. åÓÌÉ ÷Ù ÈÏÔÅÌÉ ÂÙ Õ×ÉÄÅÔØ ÏÓ×ÅÝÅÎÎÙÍ ÎÅËÏÔÏÒÙÊ ×ÏÐÒÏÓ, ÐÏÖÁÌÕÊÓÔÁ ÓÏÏÂÝÉÔÅ ÏÂ ÜÔÏÍ. á ÅÝÅ ÌÕÞÛÅ, ÎÁÐÉÛÉÔÅ ÞÅÒÎÏ×ÕÀ ×ÅÒÓÉÀ, ÏÐÉÓÙ×ÁÀÝÕÀ ÉÎÔÅÒÅÓÕÀÝÉÊ ÷ÁÓ ×ÏÐÒÏÓ!

5.1. îÁÐÉÓÁÎÉÅ ÐÎØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ

Alma Whitten (http://www.cs.cmu.edu/~alma) É Doug Tygar (http://www.cs.berkeley.edu/~tygar) ÐÒÏ×ÅÌÉ ÁÎÁÌÉÚ (http://reports-archive.adm.cs.cmu.edu/anon/1998/abstracts/98-155.html) ÐÎØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ PGP 5.0 É ÐÒÉÛÌÉ Ë ÚÁËÌÀÞÅÎÉÀ, ÞÔÏ ÎÁÞÉÎÁÀÝÉÅ ÐÎØÚÏ×ÁÔÅÌÉ ÎÁÈÏÄÑÔ PGP ÓÏÏÔÎÙÍ É ÎÅÐÏÑÔÎÙÍ. ðÏ ÒÅÚÕÌØÔÁÔÁÍ ÉÈ ÔÅÓÔÏ×, ÔÏÌØËÏ ÞÅÔ×ÅÒÏ ÉÚ Ä×ÅÎÁÄÃÁÔÉ ÔÅÓÔÉÒÕÅÍÙÈ ÐÒÁ×ÉÌØÎÏ ÏÐÒÁ×ÉÌÉ ÚÁÛÉÆÈÏ×ÁÎÎÙÅ ÓÏÏÂÝÅÎÉÑ ÞÌÅÎÁÍ ÉÈ ËÏÍÁÎÄÙ, É ÔÒÏÅ ÉÚ Ä×ÅÎÁÄÃÁÔÉ ÏÐÒÁ×ÉÌ ÓÅËÒÅ ÎÅÚÁÛÉÆÈÏ×ÁÎÎÙÍ. ðÒÉ ÜÔÏÍ ÐÏÌÌ×ÉÎÁ ÔÅÓÔÉÒÕÅÍÙÈ ÐÒÏÛÌÉ ÔÅÈÎÉÞÅÓËÕÀ ÐÏÄÇÏÔÏ×ËÕ.

üÔÉ ÒÅÚÕÌØÔÁÔÙ ÎÅ ÕÄÉ×ÌÑÀÔ. PGP 5.0 ÉÍÅÅÔ ÈÏÒÏÛÉÊ ÐÎØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ, ËÏÔÏÒÙÊ ÐÒÅ×ÏÓÈÏÄÅÎ ÅÓÌÉ ÷Ù ÕÖÅ ÐÎÉÍÅÅÔÅ ÛÉÆÒÏ×ÁÎÉÅ ÎÅËÒÛÔÙÍ ËÌÀÞÎÍ É ÄÒÕÖÉÔÅ Ó ÍÏÄÅÌØÀ ÐÏÄÔ×ÅÒÖÄÅÎÑ ËÌÀÞÅÊ ÓÐÅÃÉÆÉÃÉÏ×ÁÎÎÏÊ OpenPGP. ë ÓÏÖÁÌÅÎÀ, ÎÁÞÉÎÁÀÝÉÅ ÐÎØÚÏ×ÁÔÅÌÉ, ÎÅ ÐÎÉÍÁÀÔ ÎÉ ÛÉÆÒÏ×ÁÎÑ Ó ÏÔËÒÙÛÙÍ ËÌÀÞÎÍ, ÎÉ ÐÒÁ×ÉÌ ÕÐÒÁ×ÌÅÎÑ ËÌÀÞÁÍÉ, É ÐÎØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ ÍÁÌÏ ÐÎÎÏÇÁÅÔ ÉÍ.

÷ÁÍ ÓÌÅÄÕÅÔ ×ÎÉÍÁÔÅÌØÎÏ ÏÚÎÁËÎÍÉÔØÓÑ Ó ×Ù×ÏÄÁÍÉ Whitten'Á É Tygar'Á

ÅÓÌÉ ÷Ù ÐÉÛÅÔÅ ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ. ïÎÉ ÄÁÀÔ ËÏÍÍÅÎÔÁÒÉÉ ÐÏ ËÁÖÄÏÍÕ ÉÚ ÔÅÓÔÉÒÕÅÍÙÈ. îÁÐÒÉÍÅÒ, ÏËÁÚÁÌÏÓØ, ÞÔÏ ÍÏÇÉÅ ×ÅÒÑÔ, ÞÔÏ ÓÏÎÂÝÅÎÉÅ ÐÏÓÙÌÁÅÍÏÅ ÄÒÕÇÉÍ ÌÀÄÑÍ ÎÁÄÏ ÚÁÛÉÆÒÏ×Ù×ÁÔØ Ó×ÏÉÍ ÓÏÂÓÔ×ÅÎÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ. úÁÄÕÍÁÊÔÅÓØ ÎÁÄ ÜÔÉÍ, É ÷Ù ÐÏÊÍÅÔÅ, ÞÔÏ ÌÅÇËÏ ÄÏÐÕÓÔÉÔØ ÔÁËÕÀ ÏÛÉÂËÕ. ëÁË ÐÒÁ×ÉÌÏ, ÎÁÞÉÎÁÀÝÉÅ ÐÏÌØÚÏ×ÁÔÅÌÉ ÉÓÐÙÔÙ×ÁÀÔ ÔÒÕÄÎÏÓÔÉ × ÐÎÉÍÁÎÉÉ ÒÁÚÌÉÞÉÊ ÍÅÖÄÕ ÏËÒÙÔÙÍ É ÚÁËÒÙÔÙÍ ËÌÀÞÁÍÉ ËÏÇÄÁ ÉÓÐÏÌØÚÕÀÔ GnuPG. ëÁË ÄÉÚÁÊÎÅÒ ÐÏÌØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ, ÷Ù ÄÏÖÎÙ ÐÏÔÔÁÒÁÔØÓÑ ÓÄÅÌÁÔØ ×ÙÂÏÒ ÔÏÇÏ ÉÌÉ ËÌÀÞÁ ÐÒÏÚÒÁÞÎÙÍ. ÷Ù ÍÏÖÅÔÅ, ÔÁËÖÅ, ÉÓÐÏÌØÚÏ×ÁÔØ ÍÁÓÔÅÒ É ÄÒÕÇÉÅ ÏÂÝÅÐÒÉÎÑÔÙÅ ÐÒÉÁÍÙ GUI ÄÌÑ ÐÒÏ×ÅÄÅÎÉÑ ÐÏÌØÚÏ×ÁÔÅÌÑ ÓË×ÏÚØ ÏÓÎÏ×ÎÙÅ ÚÁÄÁÞÉ, ÔÁËÉÅ ËÁË ÇÅÎÅÒÁÃÉÑ ËÌÀÞÁ, ÄÏÐÏÎÎÉÎÁÑ ÇÅÎÅÒÁÃÉÅÊ ÓÅÒÔÉÆÉËÁÔÁ ÏÔÚÙ×Á ËÌÀÞÁ, É Ô.Ð. Other comments from the paper include the following.

- âÅÚÏÐÁÓÎÏÓÔØ, ÏÂÙÞÎÏ Ñ×ÌÑÅÔÓÑ ×ÔÏÒÏÓÔÅÐÅÎÎÏÊ ÚÁÄÁÞÅÊ; ÌÀÄÉ ÈÏÑÔ ÏÔÐÒÁ×ÌÑÔØ ÐÏÞÔÕ, ÐÒÏÓÍÁÔÒÉ×ÁÔØ É Ô.Ä. îÅ ÄÕÍÁÊÔÅ ÞÔÏ ÐÏÌØÚÏ×ÁÔÅÌÉ ÓÔÁÎÕÔ ÞÉÔÁÔØ ÔÏÓÔÙÅ ÒÕËÏ×ÏÄÓÔ×Á ÉÌÉ ÒÁÚÂÉÒÁÔØÓÑ × ÎÁÓÔÒÏÊËÁÈ ÛÉÆÒÏ×ÁÎÉÑ.
- úÁÝÉÔÁ ÓÅÔÅ×ÏÇÏ ËÏÍÐØÀÔÅÒÁ ÎÅ ÓÉÌØÎÅÅ ÓÁÍÏÇÏ ÓÌÁÂÏÇÏ ÉÚ ÅÅ ËÏÍÐÏÎÅÎÔÏ×. ðÏÌØÚÏ×ÁÔÅÌÉ ÄÏÖÎÙ ÂÙÔØ ÏÓ×ÅÄÏÍÌÅÎÙ ÏÂ ×ÓÅÈ ÁÓÐÅËÁÈ Ó×ÏÅÊ ÂÅÚÏÐÁÓÏÏÓÔÉ, ÎÅ ÏÇÒÁÍÉÞÉ×ÁÑØ ÞÁÓÔÉÞÎÙÍÉ Ó×ÅÄÅÎÉÑÍÉ, ËÁË ÜÔÏ ÍÏÖÅÔ ÂÙÔØ Ó ÔÅËÓÔÏ×ÙÍÉ ÐÒÏÃÅÓÓÏÒÁÍÉ ÉÌÉ ÜÌÅËÔÒÏÎÎÙÍÉ ÔÁÂÌÉÃÁÍÉ.
- ÷ÓÅÇÄÁ ÉÓÐÏÌØÚÕÊÔÅ ÏÄÉÎÁËÏ×ÙÅ ÔÅÒÍÉÎÙ ÄÌÑ ÏÄÉÎÁËÏ×ÙÈ ÄÅÊÓÔ×ÉÊ. éÚÂÅÇÁÊÔÅ ÕÐÏÒÒÅÌÅÎÑ ÓÉÎÏÎÉÍ×, ÔÉÐÁ “encrypt” É “encipher”.
- äÌÑ ÎÅÉÓËÕÛÅÎÙÈ ÐÏÌØÚÏ×ÁÔÅÌÅÊ ÕÐÒÏÓÔÉÔÅ ×Ù×ÏÄ ÉÎÆÏÒÍÁÃÉÉ. óÌÉÛËÏÍ ÂÏÌØÛÏÅ ËÏÌÉÞÅÓÔ×Ï ÉÎÆÏÒÍÁÃÉÉ ÓËÒÙ×ÁÅÔ ÕÕ, ËÏÔÏÒÁÑ ×ÁÖÎÁ. îÁÞÁÌØÎÁÑ ËÏÎÆÉÇÕÒÁÃÉÑ ÉÎÔÅÒÆÅÊÓÁ ÄÏÌÖÁ ÏÂÅÓÐÅÞÉÔØ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÒÁ×ÉÌØÎÙÊ ÍÉÄÅÌØÀ ÏÔÏÛÅÉÊ ÍÅÖÄÕ ÏÔËÒÙÔÙÍ É ÚÁËÒÙÔÙÍ ËÌÀÞÁÍÉ É ÐÒÏÚÒÁÞÎÙÍ ÐÎÉÍÁÎÉÅÍ ÆÕÎËÃÉÊ ÐÏÕÞÅÎÉÑ É

ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÑ ËÌÀÞÅÊ.

òÁÚÒÁÂÏÔËÁ ÜÆÆÅËÔÉ×ÎÏÇÏ ÐÏÌØÚÏ×ÁÔÀÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ ÄÌÑ ÕÐÒÁ×ÌÅÎÉÑ ËÌÀÞÁÍÉ ÅÝÅ ÂÏÌÅÅ ÓÌÏÖÎÁ. íÏÅÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ OpenPGP, Ë ÓÏÖÁÌÅÎÉÀ, ÄÏ×ÏÌØÎÏ ÔÒÕÄÎÁ ÄÌÑ ÐÏÎÉÍÁÎÉÑ. îÁÐÒÉÍÅÒ, ÓÐÅÃÉÆÉËÁÃÉÑ ÏÐÅÒÅÄÅÌÑÅÔ ÔÒÉ ÓÔÅÐÅÎÉ ÄÏ×ÅÒÉÑ ÐÏÌØÚÏ×ÁÔÅÌÀ: ÎÅÔ (none), ÏÔÏÍÉÔÅÌØÎÏÅ (marginal), É ÐÏÌÎÏÅ (Óomplete). ÷ÓÅ ÇÒÁÎÉ ÄÏ×ÅÒÉÑ, ÉÓÐÙÔÙ×ÁÅÍÇÏ ÐÏÌØÚÏ×ÁÔÅÌÁ, ÄÏÌÖÎÙ ÕÍÅÔØÓÑ × ÜÔÉ ÔÒÉ ÑÞÅËÉ. áÌÇÏÒÉÔÍ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ËÌÀÞÅÊ ÔÁËÖÅ ÓÌÏÖÅÎ ÄÌÑ ÐÏÎÉÍÁÎÉÑ ÎÅ ÓÐÅÃÉÁÌÉÓÔÏ×, ÏÓÏÂÅÎÎÏ ÐÁÒÁÍÅÔÒÙ "marginals needed" É "completes needed". ôÁË ËÁË ÍÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÞÅÔËÏ ÏÐÒÅÄÅÌÅÎÁ É ÎÅ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎÁ, ÷ÁÍ ÐÒÉÊÄÅÔÓÑ ÐÏÓÔÁÒÁÔØÓÑ É ÒÁÚÒÁÂÏÔÁØ ÉÎÔÅÒÆÅÊ, ËÏÔÏÙÊ ÐÍÍÖÅÔ ÐÏÎÑÔØ ÅÅ ÐÌØÚÏ×ÁÔÅÌÀ. ïÐÒÅÄÅÌÅÎÎÁÑ ÆÕÎËÃÉÑ, Ë ÐÒÉÍÅÒÕ, ÍÇÌÁ ÂÙ ÏÔÂÒÁÖÁÔØ ÄÉÁÇÒÁÍÍÕ ÔÏÇÏ, ËÁË ÂÙÌ ÐÏÔ×ÒÄÅÎ ËÌÀÞ, ÐÏ ÚÁÐÒÏÓÕ ÐÌØÚÏ×ÁÔÅÌÑ. ïÓÎÏ×ÎÙÅ ×Ù×ÏÄÙ ÓÌÅÄÕÀÝÉÅ.

- ðÏÌØÚÏ×ÁÔÅÌÉ ÍÏÇÕÔ ÏÓÔÁ×ÁÔØÓÑ × ÎÅ×ÅÄÅÎÉÉ ÏÔÎÓÉÔÅÌØÎÏ ÔÏÇÏ, ËÁË É ËÏÇÄÁ ÐÒÅÄÏÓÔÁ×ÉÔØ ÄÏÓÕÐ.
- ðÒÉÄÁÊÔÅ ×ÙÓÏËÉÊ ÐÒÉÏÉÔÅÔ ÔÏÍÕ, ÞÔÂÙ ÚÁÝÉÔÉÔØ ÐÏÌØÚÏ×ÁÔÅÌÅ ÏÔ ÓÏ×ÅÒÛÅÎÑ ÄÏÏÇÓÓÔÑÝÉÈ ÏÛÉÂÏË, ÔÁËÉÈ ËÁË ÏÛÉÂÏÞÎÅ ÕÄÁÌÅÎÉÅ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÐÕÂÌÉËÁÃÉÑ ËÌÀÞÁ, ÏÛÚ×ËÌÀÞÁ, ÐÏÔÅÒÑ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ, ÎÅÐÒÁ×ÉÌØÎÁÑ ÁÒÈÉ×ÁÃÉÑ ËÌÀÞÁ.

I. óÐÉÓÏË ËÏÍÁÎÄ

1. óÐÅÃÉÆÉËÁÔÏÒÙ ËÌÀÞÅÉ

íÎÏÇÉÅ ËÏÍÁÎÄÙ É ÏÐÃÉÉ ÔÒÅÂÕÀÔ *ÓÐÅÃÉÆÉËÁÔÏÒ ËÌÀÞÁ* (key specifier). óÐÅÃÉÆÉËÁÔÏÒ ËÌÀÞÁ ÜÔÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ËÌÀÞÁ ÉÌÉ ÌÀÂÁÑ ÞÁÓÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ ËÌÀÞÁ. ÒÁÓÍÏÔÒÉÍ ÓÌÅÄÕÀÝÉÊ ÐÒÉÍÅÒ:

```
alice% gpg --list-keys chloe
pub  1024D/B87DBA93 1999-06-28 Chloe (Jester) <chloe@cyb.org>
uid                            Chloe (Plebian) <chloe@tel.net>
sub  2048g/B7934539 1999-06-28
```

äÌÑ ÜÔÏÇÏ ËÌÀÞÁ, `0xB87DBA93`, `Chloe`, `Plebian`, É `oe@tel` ÐÒÉÍÅÒÙ ÓÐÅÃÉÆÉËÁÔÏÒ× ËÌÀÞÁ.

sign

Name

`sign` — ÐÏÄÐÉÓÁÔØ ÄÏËÕÍÅÎÔ

Synopsis

`sign` *filename*

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ ÐÏÄÐÉÓÙ×ÁÅÔ ÄÏËÕÍÅÎÔ *filename*. åÓÌÉ ÐÁÒÁÍÅÔÒ *filename* ÏÐÕÝÅÎ, ÔÏ ÄÏËÕÍÅÎÔ ÄÌÑ ÐÏÄÐÉÓÉ ÂÅÒÅÔÓÑ ÉÚ ÓÔÁÎÄÁÒÔÎÏÇÏ ××ÏÄÁ. åÓÌÉ ÉÓÐÏÌØÚÕÅÔÓÑ ÏÐÃÉÑ `output`, gpg ÐÏÍÅÝÁÅÔ ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ × ÕËÁÚÁÎÎÙÊ ÆÁÊÌ.

detach-signature

Name

`detach-signature` — ÓÏÚÄÁÔØ ÏÔÄÅÌÅÎÎÕÀ ÐÏÄÐÉÓØ

Synopsis

```
detach-signature filename
```

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÓÏÚÄÁÅÔ ÆÁÊÌ ÐÏÄÐÉÓÉ, ËÏÔÏÒÙÊ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÒÏ×ÅÒËÉ ÔÏÇÏ, ÞÔÏ ÉÓÈÏÄÎÙÊ ÆÁÊÌ *filename* ÎÅ ÂÙÌ ÉÚÍÅÎÅÎ. ðÒÏ×ÅÒÁ ÆÁÊÌÁ Ó ÉÓÐÏÌØÚÏ×ÁÎÉÅÍ ÏÔÄÅÌØÎÏÇÏ ÐÏÄÐÉÓÉ ×ÙÐÏÎÑÅÔÓÑ ËÏÍÁÎÄÏÊ `verify`.

encrypt

Name

`encrypt` — ÚÁÛÉÆÒÏ×ÁÔØ ÄÏËÕÍÅÎÔ

Synopsis

```
encrypt filename
```

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÄÏËÕÍÅÎÔ *filename* ÄÌÑ ÐÏÌÕÞÁÔÅÌÅÊ ÕËÁÚÁÎÎÙÈ ÏÐÃÉÅÊ `recipient`. åÓÌÉ ÐÁÒÁÍÅÔÒ *filename* ÏÐÕÝÅÎ, ÛÉÆÒÕÅÍÙÊ ÄÏËÕÍÅÎÔ ÂÅÒÅÔÓÑ ÓÏ ÓÔÁÎÄÁÒÔÎÏÇÏ ××ÏÄÁ. åÓÌÉ ÏÐÃÉÑ

recipient ÏÐÕÝÅÎÁ, gpg ÚÁÐÒÏÓÉÔ ÐÏÌÕÞÁÔÅÌÑ. åÓÌÉ ÉÓÐÏÌØÚÕÅÔÓÑ ÏÐÃÉÑ output, gpg ÐÏÍÅÓÔÉÔ ÚÁÛÉÆÒÏ×ÁÎÎÕÀ ÉÎÆÏÒÍÁÃÉÀ × ÕËÁÚÁÎÙÊ ÆÁÊÌ.

symmetric

Name

symmetric — ÚÁÛÉÆÒÏ×ÁÔØ ÄÏËÕÍÅÎ ÉÓÐÏÌØÚÕÑ ÔÏÌØËÏ ÁÌÇÏÒÉÔÍ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ

Synopsis

symmetric *filename*

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÄÏËÕÍÅÎÔ ÉÓÐÏÌØÚÕÑ ÓÉÍÍÅÔÒÉÞÎÙÊ ÁÌÇÏÒÉÔÍ Ó ËÌÀÞÏÍ ÏÂÒÁÚÏ×ÁÎÎÙÍ ÉÚ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ, ÐÏÕÞÅÎÎÏÊ ÐÒÉ ×ÙÐÏÌÎÅÉÉ. ëÌÀÞ ÓÌÅÄÕÅÔ ×ÙÂÉÒÁÔØ ÔÁË, ÞÔÏÂÙ ÅÇÏ ÎÅÌØÚÑ ÂÙÌÏ ÕÇÁÄÁÔØ. äÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÐÏÌÕÞÅÎÎÏÇÏ × ÒÅÚÕÌØÔÁÔÅ ÄÏËÕÍÅÎÔÁ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ decrypt.

decrypt

Name

decrypt — ÒÁÓÛÉÆÒÏ×ÁÎØ ÄÏËÕÍÅÎÔ

Synopsis

decrypt *filename*

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ *filename* É ÐÏÍÅÝÁÅÔ ÒÅÚÕÌØÔÁÔ × ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ. åÓÌÉ ÐÁÒÁÍÅÔÒ *filename* ÏÐÕÝÅÎ, ÔÏ ÄÏËÕÍÅÎÔ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÂÅÒÅÔÓÑ ÉÚ ÓÔÁÎÄÁÒÔÎÏÇÏ ××ÏÄÁ. éÓÐÏÌØÚÕÊÔÅ ÏÐÃÉÀ output ÄÌÑ ×Ù×ÏÄÁ ÒÁÓÛÉÆÒÏ×ÁÎÎÏÇÏ ÄÏËÕÍÅÎÔÁ × ÆÁÊÌ.

clearsign

Name

clearsign — ÓÏÚÄÁÔØ ÐÒÏÚÒÁÞÎÕÀ ÐÏÄÐÉÓØ

Synopsis

```
clearsign filename
```

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ ÐÏÄÐÉÓÙ×ÁÅÔ ÓÏÏÂÝÅÎÉÅ. ðÒÉ ÜÔÏÍ ÏÎÁ ÏÓÔÁ×ÌÑÅÔ ÓÏÏÂÝÅÎÉÅ × ÞÉÔÁÅÍÏÍ ×ÉÄÅ. ðÒÏ×ÅÒËÁ ÓÏÏÂÝÅÎÉÑ ÐÒÏÉÚ×ÏÄÉÔÓÑ ËÏÍÁÎÄÏÊ `verify`.

verify

Name

`verify` — ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ

Synopsis

```
verify signature document
```

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ Ó×ÅÒÑÅÔ ÐÏÄÐÉÓØ Ó ÄÏËÕÍÅÎÔÏÍ, ÞÔÏÂÙ ÕÄÏÓÔÏ×ÅÒÉÔØÓÑ, ÞÔÏ ÄÏËÕÍÅÎÔ ÅÝÅ ÂÙÌ ÉÚÍÅÎÅÎ Ó ÍÏÍÅÎÔÁ ÓÏÚÄÁÎÉÑ ÐÏÄÐÉÓÉ. åÓÌÉ *`signature`* ÏÐÕÝÅÎÁ, gpg ÐÒÏ×ÅÒÑÅÔ ÎÁÌÉÞÉÅ ÐÒÏÚÒÁÞÎÏÊ ÐÏÄÐÉÓÉ × *`document`*.

gen-key

Name

gen-key — ÇÅÎÅÒÉÒÏ×ÁÔØ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ

Synopsis

```
gen-key
```

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÇÅÎÅÒÉÒÕÅÔ ÐÁÒÕ ÏÔËÒÙÔÙÊ/ÚÁËÒÙÔÙÊ ËÌÀÞ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ, ÒÁÓÛÉÆÒÏ×ËÉ É ÐÏÄÐÉÓÉ ÓÏÎÁÝÅÎÉÊ. ÷Ù ÂÕÄÅÔÅ ÚÁÐÒÏÛÅÎÙ Ï ÔÉÐÅ ËÌÀÞÁ, ÅÇÏ ÒÁÚÍÅÒÅ É ÓÒÏËÅ ÄÅÊÓÔ×ÉÑ.

gen-revoke

Name

gen-revoke — ÇÅÎÅÒÉÒÏ×ÁÔØ ÓÅÒÔÉÆÉËÁÔ ÏÔÚÙ×Á ÄÌÑ ÐÁÒÙ ËÌÀÞÅÊ

Synopsis

`gen-revoke` *key*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÇÅÎÅÒÉÒÕÅÔ ÓÅÒÔÉÆÉËÁÔ ÏÔÚÙ×Á ÄÌÑ ÐÁÒÙ ËÌÀÞÅÊ. ðÁÒÁÍÅÔÒ *key* - ÓÐÅÃÉÆÉËÁÔÏÒ ËÌÀÞÁ.

send-keys

Name

`send-keys` — ÐÏÓÌÁÔØ ËÌÀÞÉ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ

Synopsis

`send-keys` *key*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÐÏÓÙÌÁÅÔ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ. ðÁÒÁÍÅÔÒ *key* ÚÁÄÁÅÔ ÐÏÓÙÌÁÅÍÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ. ëÏÍÁÎÄÁ ÔÒÅÂÕÅÔ ÏÐÃÉÀ `keyserver` ÄÌÑ ÕËÁÚÁÎÉÑ ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ, ÎÁ ËÏÔÏÒÙÊ gpg ÏÔÐÒÁ×ÉÔ ËÌÀÞ.

recv-keys

Name

recv-keys — ÚÁÐÒÏÓÉÔØ ËÌÀÞ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ

Synopsis

recv-keys *key-id key-id ...*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÚÁÇÒÕÖÁÅÔ ÏÄÉÎ ÉÌÉ ÎÅÓËÏÌØËÏ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ. ëÁÖÄÙÊ *key-id* - ÉÄÅÎÔÉÆÉËÁÔÏÒ ËÌÀÞÁ. ëÏÍÁÎÄÁ ÔÒÅÂÕÅÔ ÏÐÒÅÄÅÌÅÎÎÏÇÏ keyserver ÄÌÑ ÕËÁÚÁÎÉÑ ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ, Ó ËÏÔÏÒÏÇÏ gpg ÂÕÄÅÔ ÚÁÇÒÕÖÁÔØ ËÌÀÞÉ.

list-keys

Name

list-keys — ×Ù×ÅÓÔÉ ÉÎÆÏÒÍÁÃÉÀ Ï ËÌÀÞÁÈ

Synopsis

```
list-keys key ...
```

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ×Ù×ÏÄÉÔ ÓÐÉÓÏË ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÚÁÄÁÎÙÈ ÓÐÅÃÉÆÉËÁÔÏÒÁÍÉ ÕËÁÚÁÎÎÙÍÉ × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ. åÓÌÉ ÓÐÅÃÉÆÉËÁÔÏÒ ËÌÀÞÅÊ ÎÅ ÚÁÄÁÎ, gpg ÐÒÏÐÅÓÙÉÔ ×ÓÅ ÏÔËÒÙÔÙÅ ËÌÀÞÉ.

list-public-keys

Name

list-public-keys — ÐÒÏÐÅÓÙÉÔØ ËÌÀÞÉ ÉÚ ÏÔËÒÙÔÙÈ Ó×ÑÚÉ

Synopsis

```
list-public-keys name ...
```

ïÐÉÓÁÎÉÅ

óÐÉÓÏË ×ÓÅÈ ËÌÀÞÅÊ ÉÚ ÏÔËÒÙÔÙÈ Ó×ÑÚÉ ÉÌÉ ÔÏÌØËÏ ËÌÀÞÉ ÚÁÄÁÎÎÙÅ ÐÁÒÁÍÅÔÒÏÍ *name ...*.

list-secret-keys

Name

`list-secret-keys` — ÐÅÒÅÞÉÓÌÉÔØ ËÌÀÞÉ × ÚÁËÒÙÔÙÈ Ó×ÑÚËÁÈ

Synopsis

`list-secret-keys` *`name ...`*

ïÐÉÓÁÎÉÅ

óÐÉÓÏË ×ÓÅÈ ËÌÀÞÅÊ ÉÚ ÚÁËÒÙÔÙÈ Ó×ÑÚÏË ÉÌÉ ÔÏÌØËÏ ËÌÀÞÉ ÚÁÄÁÎÎÙÅ ÐÁÒÁÍÅÔÒÏÍ *`name ...`*.

list-sigs

Name

`list-sigs` — ×Ù×ÅÓÔÉ ÉÎÆÏÒÍÁÃÉÀ Ï ËÌÀÞÁÈ, ×ËÌÀÞÁÑ ÐÏÄÐÉÓÉ

Synopsis

```
list-sigs name ...
```

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ×Ù×ÏÄÉÔ ÓÐÉÓÏË ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÚÁÄÁÎÙÈ ÓÐÅÃÉÆÉËÁÔÏÁÍÉ ÕËÁÚÁÎÎÙÍÉ × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ. ôÁËÖÅ ×Ù×ÏÄÉÔÓÑ ÉÎÆÏÒÍÁÃÉÑ Ï ÐÏÄÐÉÓÑÈ ÎÁ ËÌÀÞÁÈ. åÓÌÉ ÓÐÅÃÉÆÉËÁÔÏÒÙ ËÌÀÞÅÊ ÎÅ ÚÁÄÁÎÙ, gpg ÐÅÒÅÞÉÓÌÉÔ ×ÓÅ ÏÔËÒÙÔÙÅ ËÌÀÞÉ.

check-sigs

Name

check-sigs — ×Ù×ÅÓÔÉ ÉÎÆÏÒÍÁÃÉÀ Ï ËÌÀÞÁÈ, ×ËÌÀÞÁÑ ÚÁ×ÅÒÅÎÎÙÅ ÐÏÄÐÉÓÉ

Synopsis

```
check-sigs name ...
```

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ×Ù×ÏÄÉÔ ÓÐÉÓÏË ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÚÁÄÁÎÙÈ ÓÐÅÃÉÆÉËÁÔÏÁÍÉ ÕËÁÚÁÎÎÙÍÉ × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ. ôÁËÖÅ

×Ù×ÏÄÉÔÓÑ ÉÎÆÏÒÍÁÃÉÑ Ï ÐÏÄÐÉÓÑÈ ÎÁ ËÌÀÞÁÈ É Ï ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÁÖÄÏÊ ÐÏÄÐÉÓÉ. åÓÌÉ ÓÐÅÃÉÆÉËÁÔÏÒÙ ËÌÀÞÅÊ ÎÅ ÚÁÄÁÎÙ, gpg ÐÅÒÅÞÉÓÌÉÔ ×ÓÅ ÎÔËÒÙÔÙÅ ËÌÀÞÉ.

fingerprint

Name

`fingerprint` — ×Ù×ÅÓÔÉ ÏÔÐÅÞÁÔËÉ ËÌÀÞÅÊ

Synopsis

`fingerprint` *`name ...`*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ×Ù×ÏÄÉÔ ÏÔÐÅÞÁÔËÉ ÕËÁÚÁÎÎÙÈ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ. ðÁÒÁÍÅÔÒ *`name`* - ÓÐÅÃÉÆÉËÁÔÏÒ ËÌÀÞÁ. åÓÌÉ ÐÁÒÁÍÅÔÒ *`name`* ÎÅ ÚÁÄÁÎ, gpg ×Ù×ÅÄÅÔ ÏÔÐÅÞÁÔËÉ ×ÓÅÈ ËÌÀÞÅÊ ÉÚ ÏÔËÒÙÔÏÊ Ó×ÑÚËÉ.

import

Name

`import` — ÉÍÐÏÒÔÉÒÏ×ÁÔØ ËÌÀÞ × ÌÏËÁÌØÎÕÀ Ó×ÑÚËÕ

Synopsis

`import` *filename*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÉÍÐÏÒÔÉÒÕÅÔ ÏÄÉÎ ÉÌÉ ÂÏÌØÛÅ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ × ÏÔËÒÙÔÕÀ Ó×ÑÚËÕ ÐÏÌØÚÏ×ÁÔÅÌÑ ÉÚ *ÆÁÊÌÁ filename*.

fast-import

Name

`fast-import` — ÉÍÐÏÒÔ/ÏÂßÅÄÉÎÅÎÉÅ ËÌÀÞÅÊ

Synopsis

`fast-import` *file ...*

ïÐÉÓÁÎÉÅ

ôÏ ÖÅ, ÞÔÏ É import, ÎÏ ËÌÀÞÉ ÎÅ ÄÏÂÁ×ÌÑÀÔÓÑ × ÂÁÚÕ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ. äÏÂÁ×ÌÅÎÉÅ ËÌÀÞÅÊ × ÂÁÚÕ ÍÏÖÎÏ ×ÙÐÏÎÉÔØ ÐÚÖÅ ËÏÍÁÎÄÏÊ update-trustdb,

export

Name

`export` — ÜËÓÐÏÒÔÉÒÏ×ÁÔØ ËÌÀÞÉ ÉÚ ÌÏËÁÌØÎÏÊ Ó×ÑÚËÉ

Synopsis

`export` *`key ...`*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÜËÓÐÏÒÔÉÒÕÅÔ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÓÐÅÃÉÆÉÃÉÒÏ×ÁÎÎÙÅ ÐÁÒÁÍÅÔÒÏÍ *`key ...`*. òÅÚÕÌØÔÁÔ ÐÏ ÕÍÏÌÞÁÎÉÀ ÎÁÐÒÁ×ÌÑÅÔÓÑ ÎÁ ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ. ëÌÀÞ, × ÄÁÌØÎÅÊÛÅÍ, ÍÏÖÅÔ ÂÙÔØ ÉÍÐÏÒÔÉÒÏ×ÁÎ × ÄÒÕÇÕÀ Ó×ÑÚËÕ ËÏÍÁÎÄÏÊ `import`.

export-all

Name

`export-all` — ÜËÓÐÏÒÔÉÒÏ×ÁÔØ ×ÓÅ ÏÔËÒÙÔÙÅ ËÌÀÞÉ

Synopsis

`export-all` *`name ...`*

ïÐÉÓÁÎÉÅ

ôÏ ÖÅ, ÞÔÏ É ËÏÍÁÎÄÁ export, ÎÏ ÍÏÖÅÔ ÜËÓÐÏÒÔÉÒÏ×ÁÔØ ËÌÀÞÉ ÎÅ Ñ×ÌÑÀÝÉÅÓÑ OpenPGP-ÓÏ×ÍÅÓÔÉÍÙÍÉ.

export-secret-keys

Name

`export-secret-keys` — ÜËÓÐÏÒÔÉÒÏ×ÁÔØ ÚÁËÒÙÔÙÊ ËÌÀÞ

Synopsis

`export-secret-keys` *`name ...`*

ïÐÉÓÁÎÉÅ

ðÏÄÏÂÎÁ ËÏÍÁÎÄÅ export, ÎÏ ÜËÓÐÏÒÔÉÒÕÅÔ ÚÁËÒÙÔÙÊ ËÌÀÞ. ïÂÙÞÎÏ ÎÅ ÉÓÐÏÌØÚÕÅÔÓÑ É Ñ×ÌÑÅÔÓÑ ÒÉÓËÏ×ÁÎÎÊ, Ô.Ë. ÚÁËÒÙÔÙÊ ËÌÀÞ ÓÔÁÎÏ×ÉÔÓÑ ÎÅÚÁÝÉÝÅÎÎÙÍ.

edit-key

Name

`edit-key` — ×ÙÄÁÅÔ ÍÅÎÀ ÄÌÑ ÒÁÂÏÔÙ Ó ËÌÀÞÁÍÉ

Synopsis

`edit-key` *`key`*

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÐÏÚ×ÏÑÑÅÔ ÏÓÕÝÅÓÔ×ÌÑÔØ ÒÁÂÏÔÕ Ó ËÌÀÞÁÍÉ. óÐÅÃÉÆÉËÁÔÏÒ ËÌÀÞÁ *`key`* ÏÐÒÅÄÅÌÑÅÔ ÒÅÄÁËÔÉÒÕÅÍÕÀ ÐÁÒÕ ËÌÀÞÅÊ. åÓÌÉ ÓÐÅÃÉÆÉËÁÔÏÒ ÏÐÒÅÄÅÌÑÅÔ ÂÏÌÅ ÏÄÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ, gpg ×ÙÄÁÅÔ ÓÏÎÂÝÅÎÉÅ ÏÂ ÏÛÉÂËÅ É ÚÁ×ÅÒÛÁÅÔÓÑ.

ìÉÓÔÉÎÇ ËÌÀÞÁ ×Ù×ÏÄÉÍÙÊ ×Ï ×ÒÅÑ ÒÅÄÁËÔÉÒ×ÁÎÉÑ ÐÏËÁÚÙ×ÁÅÔ ËÌÀÞ Ó ÅÇÏ ×ÔÏÉÞÎÙÍ ËÌÀÞÁÍÉ É ×ÓÅÍ ÉÄÅÎÔÉÆÉËÁÔÏÒÁÍÉ ÐÏØÚÏ×ÁÔÅÌÑ. ÷ÙÂÒÁÎÎÙÅ ËÌÀÞÉ É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏØÚÏ×ÁÔÅÌÅÊ ÐÏÍÅÐÅÎÙ ÁÓÔÅÒÉÓËÍ. äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ É ÅÇÏ

ÄÏÓÔÏ×ÅÒÎÏÓÔØ ×Ù×ÏÄÑÔÓÑ Ó ÐÅÒ×ÉÞÎÙÍ ËÌÀÞÏÍ: ÐÅÒ×ÏÅ - ÐÒÉÓ×ÏÅÎÎÅ ÄÏ×ÅÒÉÅ É ×ÔÏÒÏÅ ×ÙÞÉÓÌÅÎÎÁÑ ÄÏÓÔÏ×ÅÒÎÏÓÔØ. úÎÁÞÅÎÉÑ ÏÂÏÚÎÁÞÅÎÙ ÓÉÍ×ÌÁÍÉ:

óÉÍ×ÌÌ	**úÎÁÞÅÎÉÅ**
-	îÅ ÐÒÉÓ×ÏÅÎÏ ÚÎÁÞÅÎÉÅ ÄÏ×ÅÒÉÑ / ÅÝÅ ÎÅ ×ÙÞÉÓÌÅÎÁ.
e	÷ÙÞÉÓÌÅÎÉÅ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÐÏÔÅÒÐÅÌÏ ÎÅÕÄÁÞÕ.
q	îÅÔ ÄÏÓÔÁÔÏÞÎÏÊ ÉÎÆÏÒÍÁÃÉÉ ÄÌÑ ×ÙÞÉÓÌÅÎÉÑ.
n	îÅ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ.
m	çÒÁÎÉÞÎÏÅ ÄÏ×ÅÒÅ.
f	ðÏÌÎÏÅ ÄÏ×ÅÒÅ.
u	âÅÚÕÓÌÏ×ÎÏ ÄÏÓÔÏ×ÅÒÅÎ.

äÁÌÅÅ ÐÒÉ×ÏÄÉÔÓÑ ÓÐÉÓÏË ×ÓÅÈ ËÏÍÁÎÄ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ ËÌÀÞÁ É ÉÈ ÏÐÉÓÁÎÉÅ.

sign

ðÏÄÐÉÓÁÔØ ÔÅËÕÝÉÊ ËÌÀÞ. åÓÌÉ ËÌÀÞ ÎÅ ÂÙÌ ÅÝÅ ÐÏÄÐÉÓÁÎ ÌÏËÁÌØÎÙÍ ÐÌØÚÏ×ÁÔÅÌÅÍ ÉÌÉ ÐÏØÚÏ×ÁÔÅÌÅÍ, ÚÁÄÁÎÎÙÍ ÏÐÃÉÅÊ `local-user`, ÐÒÏÇÒÁÍÍÁ ×Ù×ÏÄÉÔ ÉÎÆÏÒÍÁÃÉÀ Ï ËÌÀÞÅ, ×ËÌÀÞÁÑ ÏÔÐÅÞÁÔËÉ, É ÚÁÐÒÁÛÉ×ÁÅÔ ÐÏÄ×ÅÒÖÄÅÎÉÅ ÐÏÄÐÉÓÉ ËÌÀÞÁ. üÔÏ ×ÏÐÒÏÓ ÐÏ×ÔÏÑÅÔÓÑ ÄÌÑ ×ÓÅÈ ÐÌØÚÏ×ÁÔÅÌÅÊ ÚÁÄÁÎÎÙÈ ÏÐÃÉÅÊ `local-user`.

lsign

ðÏÄÏÂÎÁ sign, ÎÏ ÐÏÄÐÉÓØ ÐÏÍÅÐÁÅÔÓÑ ËÁË ÎÅ ÜËÓÐÏÔÉÔÕÅÍÑ É

ÎÉËÏÇÄÁ ÎÅ ÂÕÄÅÔ ÉÓÐÏÌØÚÏ×ÁÎÁ ÄÒÕÇÉÍÉ. éÓÐÏÌØÚÕÅÔÓÑ ÞÔÏÂÙ ÓÄÅÌÁÔØ ËÌÀÞÉ ÄÏÓÔÕ×ÅÒÎÙÍÉ ÔÏÌØËÏ ÌÏËÁÌØÎÏ.

revsig

ïÔÏÚ×ÁÔØ ÐÏÄÐÉÓØ. úÁÐÒÁÛÉ×ÁÅÔ ÄÏÌÖÅÎ ÌÉ ÂÙÔØ ÓÇÅÎÅÒÉÒÏ×ÁÎ ÓÅÒÔÉÆÉËÁÔ ÏÔÚÙ×Á, ÄÌÑ ËÁÖÄÏÊ ÐÏÄÐÉÓÉ ÓÄÅÌÁÎÎÏÊ ÏÄÎÉÍ ÉÚ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ.

trust

éÚÍÅÎÉÔØ ÚÎÁÞÅÎÉÅ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ. îÅÍÅÄÌÅÎÎÏ ÏÂÎÏ×ÌÑÅÔ ÂÁÚÕ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ É ÎÅ ÔÒÅÂÕÅÔ ÓÏÈÒÁÎÅÎÉÑ.

disable

úÁÂÌÏËÉÒÏ×ÁÔØ ËÌÀÞ. úÁÂÌÏËÉÒÏ×ÁÎÎÙÊ ËÌÀÞ ÎÅ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÛÉÆÒ×ÁÎÉÑ.

enable

òÁÚÂÌÏËÉÒÏ×ÁÔØ ËÌÀÞ ËÏÔÏÒÙÊ ÂÙÌ ÒÁÎÅÅ disabled.

adduid

äÏÂÁ×ÉÔØ ÎÏ×ÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ Ë ËÌÀÞÕ.

deluid

õÄÁÌÉÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÉÚ ËÌÀÞÁ.

addkey

äÏÂÁ×ÉÔØ ÎÏ×ÙÊ ÐÏÄËÌÀÞ Ë ÔÅËÕÝÅÍÕ ËÌÀÞÕ.

delkey

õÄÁÌÉÔØ ÐÏÄËÌÀÞ ÉÚ ÔÅËÕÝÅÇÏ ËÌÀÞÁ.

revkey

ïÔÏÚ×ÁÔØ ÐÏÄËÌÀÞ ÉÚ ÔÅËÕÝÅÇÏ ËÌÀÞÁ.

expire

éÚÍÅÎÉÔØ ÓÒÏË ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ. åÓÌÉ ×ÙÂÒÁÎ ÐÏÄËÌÀÞ, ÔÏ ÂÕÄÅÔ ÉÚÍÅÎÅÎ ÓÒÏË ÅÇÏ ÄÅÊÓÔ×ÉÑ. åÓÌÉ ÎÅÔ ×ÙÂÒÁÎÙÈ ËÌÀÞÅÊ, ÂÕÄÅÔ ÉÚÍÅÎÅÎ ÓÒÏË ÄÅÊÓÔ×ÉÑ ÔÅËÕÝÅÇÏ ÐÅÒ×ÉÞÎÏÇÏ ËÌÀÞÁ.

key n

÷ÙÂÒÁÔØ ÐÏÄËÌÀÞ Ó ÉÎÄÅËÓÏÍ n. éÓÐÏÌØÚÕÅÔÓÑ 0, ÞÔÏÂÙ ÏÔÍÅÎÉÔØ ×ÙÂÏÒ ×ÓÅÈ.

uid n

÷ÙÂÒÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ Ó ÉÎÄÅËÓÏÍ n. éÓÐÏÌØÚÕÅÔÓÑ 0, ÞÔÏÂÙ ÏÔÍÅÎÉÔØ ×ÙÂÏÒ ×ÓÅÈ.

passwd

éÚÍÅÎÉÔØ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÄÌÑ ×ÙÂÒÁÎÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ.

toggle

ðÅÒÅËÌÀÞÁÎÉÅ ÍÅÖÄÕ ÓÐÉÓËÏÍ ÏÔËÒÙÔÙÈ É ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ.

check

ðÒÏ×ÅÒÉÔØ ×ÓÅ ×ÙÂÒÁÎÎÙÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏØÚÏ×ÁÔÅÌÑ.

pref

÷Ù×ÅÓÔÉ ÓÐÉÓÏË ÐÒÅÄÐÏÞÔÅÎÉÊ.

save

óÏÈÒÁÎÉÔØ ÉÚÍÅÎÅÎÉÑ É ×ÙÊÔÉ.

quit

÷ÙÊÔÉ ÂÅÚ ÓÏÈÒÁÎÅÎÉÑ ÉÚÍÅÎÅÎÉÊ.

sign-key

Name

`sign-key` — ðÏÄÐÉÓÁÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ ÓÅËÒÅÔÎÙÍ

Synopsis

`sign-key` *name*

ïÐÉÓÁÎÉÅ

áÎÁÌÏÇÉÞÎÁ ÐÏÄÐÉÓÁÎÁÅ sign. ËÏÍÁÎÄÙ edit-key.

lsign-key

Name

`lsign-key` — ÐÏÄÐÉÓÁÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ ÌÏËÁÌØÎÏ

Synopsis

`lsign-key` *name*

ïÐÉÓÁÎÉÅ

áÎÁÌÏÇÉÞÎÁ ÐÏÄËÏÍÁÎÄÅ lsign. ËÏÍÁÎÄÙ edit-key.

delete-key

Name

`delete-key` — ÕÄÁÌÉÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ

Synopsis

`delete-key` *`name`*

ïÐÉÓÁÎÉÅ

õÄÁÌÉÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ ÏÐÒÅÄÅÌÅÎÎÙÊ ÐÁÒÁÍÅÔÒÏÍ *`name`*.

delete-secret-key

Name

`delete-secret-key` — ÕÄÁÌÉÔØ ÏÔËÒÙÔÙÊ É ÚÁËÒÙÔÙÊ ËÌÀÞ

Synopsis

`delete-secret-key` *name*

ïÐÉÓÁÎÉÅ

õÄÁÌÉÔØ ÐÁÒÕ ËÌÀÞÅÊ (ÏÂÁ, ÏÔËÒÙÔÙÊ É ÚÁËÒÙÔÙÊ, ËÌÀÞÁ) ÚÁÄÁÎÎÏÀ ÐÁÒÁÍÅÔÒÏÍ *name*.

store

Name

`store` — ÓÏÚÄÁ×ÁÔØ ÐÁËÅÔÙ rfc1991

Synopsis

`help`

ïÐÉÓÁÎÉÅ

óÌÏÖÎÏ.

export-ownertrust

Name

`export-ownertrust` — ÜËÓÐÏÒÔÉÒÏ×ÁÔØ ÐÒÉÓ×ÏÅÎÎÙÅ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ

Synopsis

`export-ownertrust` *`file ...`*

ïÐÉÓÁÎÉÅ

úÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ ÜËÓÐÏÒÔÉÒÕÀÔÓÑ × ÆÏÒÍÁÔÅ ASCII. ðÒÉÍÅÎÉÍÏ ÄÌÑ ÓÏÚÄÁÎÉÑ ÒÅÚÅÒ×ÎÙÈ ËÏÐÉÊ ÚÎÁÞÅÎÉÊ ÄÏ×ÅÒÉÑ, ÐÒÉÓ×ÏÅÎÎÙÈ ×ÌÁÄÅÌØÃÁÍ ËÌÀÞÅÊ.

import-ownertrust

Name

`import-ownertrust` — ÉÍÐÏÒÔÉÒÏ×ÁÔØ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ

Synopsis

`import-ownertrust` *`file ...`*

ïÐÉÓÁÎÉÅ

âÁÚÁ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ ÏÂÎÏ×ÌÑÅÔÓÑ ÚÎÁÞÅÎÉÑÍÉ ÄÏ×ÅÒÉÑ ÉÚ *`file ...`*. åÓÌÉ ÆÁÊÌÙ ÎÅ ÕËÁÚÁÎÙ, ÚÎÁÞÅÎÉÑ ÂÅÒÕÔÓÑ ÉÚ ÓÔÁÎÄÁÒÔÎÏÇÏ ××ÏÄÁ.

update-trustdb

Name

`update-trustdb` — ÏÂÎÏ×ÉÔØ ÂÁÚÕ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ

Synopsis

```
update-trustdb
```

ïÐÉÓÁÎÉÅ

÷ÓÅ ÓËÁÚÁÎÏ.

print-md

Name

print-md — ×Ù×ÅÓÔÉ ÄÁÊÄÖÅÓÔ ÓÏÏÂÝÅÎÉÑ

Synopsis

print-md *algo file ...*

ïÐÉÓÁÎÉÅ

÷Ù×ÏÄÉÔ ÄÁÊÄÖÅÓÔ ÓÏÏÂÝÅÎÉÑ ÉÓÐÏÌØÚÕÑ ÁÌÇÏÒÉÔÍ *algo* ÄÌÑ ËÁÖÄÏÇÏ ÉÚ *ÆÁÊÌ× file ...*. åÓÌÉ ÆÁÊÌÙ ÎÅ ÕËÁÚÁÎÙ, ÉÓÐÏÌØÚÕÅÔÓÑ ÓÔÁÎÄÁÒÔÎÙÊ ××ÏÄ. åÓÌÉ ÁÌÇÏÒÉÔÍ ÚÁÄÁÎ ËÁË "*", ÔÏ ×Ù×ÏÄÉÔÓÑ ÄÁÊÄÖÅÓÔ ×ÙÁ×ÁÅÍÙÊ ×ÓÅÍÉ ÄÏÓÔÕÐÎÙÍÉ ÁÌÇÏÒÉÔÍÁÍÉ.

gen-random

Name

gen-random — ÇÅÎÅÒÉÒÏ×ÁÎØ ÓÌÕÞÁÊÎÙÅ ÄÁÎÎÙÅ

Synopsis

gen-random *level n*

ïÐÉÓÁÎÉÅ

üÔÁ ËÏÍÁÎÄÁ ÇÅÎÅÒÉÒÕÅÔ *n* ÂÁÊÔ ÓÌÕÞÁÊÎÙÈ ÄÁÎÎÙÈ Ó ËÁÞÅÓÔ×ÏÍ *level*. åÓÌÉ ÐÁÒÁÍÅÔÒ *n* ÏÐÕÝÅÎ, ÔÏ ÂÕÄÅÔ ÓÇÅÎÅÒÉÒÏ×ÁÎÁ ÂÅÓËÏÎÅÞÎÁÑ ÐÏÓÌÅÄÏ×ÁÔÅÌØÎÏÓÔØ ÓÌÕÞÁÊÎÙÈ ÄÁÎÎÙÈ. This command should not be frivolously since it takes entropy from the system.

gen-prime

Name

gen-prime — ?

Synopsis

```
gen-prime mode bits qbits
```

ïÐÉÓÁÎÉÅ

ëÏÍÁÎÄÁ ÇÅÎÅÒÉÒÕÅÔ ÓÌÕÞÁÊÎÏÅ ÞÉÓÌÏ. éÝÉÔÅ ÐÏÄÒÏÂÎÏÓÔÉ × ÉÓÈÏÄÎÏÍ ÔÅËÓÔÅ, ÅÓÌÉ ÉÎÔÅÒÅÓÕÅÔÅÓØ.

version

Name

version — ×Ù×ÅÓÔÉ ÉÎÆÏÒÍÁÃÉÀ Ï ×ÅÒÓÉÉ

Synopsis

```
version
```

ïÐÉÓÁÎÉÅ

ðÅÞÁÔÁÅÔ ÉÎÆÏÒÍÁÃÉÀ Ï ×ÅÒÓÉÉ É ÓÐÉÓÏË ÐÏÄÄÅÒÖÉ×ÁÅÍÙÈ ÁÌÇÏÒÉÔÍ×.

warranty

Name

warranty — ×Ù×ÅÓÔÉ ÉÎÆÏÒÍÁÃÉÀ Ï ÇÁÒÁÎÔÉÑÈ

Synopsis

```
warranty
```

ïÐÉÓÁÎÉÅ

÷ÓÅ ÓËÁÚÁÎÏ.

help

Name

help — ×Ù×ÅÓÔÉ ÓÐÒÁ×ËÕ ÏÂ ÉÓÐÏÌØÚÏ×ÁÎÉÉ

Synopsis

```
help
```

ïÐÉÓÁÎÉÅ

÷Ù×ÏÄÉÔ ÓÐÉÓÏË ËÏÍÁÎÄ É ÏÐÃÉÉ. óÐÉÓÏË ÏÐÃÉÉ ÍÏÖÅÔ ÂÙÔØ ÎÅ ÐÏÌÎÙÍ.

II. óÐÉÓÏË ÏÐÃÉÊ

1. õÓÔÁÎÏ×ËÁ ÏÐÃÉÊ

ïÐÃÉÉ ÍÏÇÕÔ ÂÙÔØ ÕËÁÚÁÎÙ × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ ÉÌÉ × ËÏÎÆÉÇÕÒÁÃÉÏÎÎÏÍ ÆÁÊÌÅ. ïÂÙÞÎÏÅ ÒÁÓÐÏÌÏÖÅÎÅ ËÏÎÆÉÇÕÒÁÃÉÏÎÎÏÇÏ ÆÁÊÌÁ `~/.gnupg/options`. ðÒÉ ÕËÁÚÁÎÉÉ ÏÐÃÉÉ × ÆÁÊÌÅ ÏÐÕÓËÁÀÔÓÑ Ä×Á ÐÒÅÄÛÅÓÔ×ÕÀÝÉÈ ÏÐÃÉÉ ÚÎÁËÁ "ÍÉÎÕ" É ÉÓÐÏÌØÚÕÅÔÓÑ ÐÒÏÓÔ ÎÁÚ×ÁÎÉÅ ÏÐÃÉÉ Ó ÐÏÓÌÅÄÕÀÝÉÍÉ ÁÒÇÕÍÅÎÔÁÍÉ. óÔÒÏËÉ ÐÅÒ×ÙÊ ÎÅ ÐÒÏÂÅÌØÎÙÊ ÓÉÍ×ÏÌ × ËÏÔÒÙÈ "#" ÉÇÎÏÒÉÒÕÀÔÓÑ.

keyserver

Name

`keyserver` — ÕËÁÚÙ×ÁÅÂ ÓÅÒ×ÅÒ ËÌÀÞÅÊ

Synopsis

`keyserver` *server-name*

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ × ÓÏÞÅÔÁÎÉÉ ÌÉÂÏ Ó `recv-keys`, ÌÉÂÏ Ó `send-keys` ÄÌÑ ÕËÁÚÁÎÉÑ ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ, ÕÐÒÁ×ÌÑÀÝÅÇÏ ÎÁÂÏÒÏÍ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ.

output

Name

`output` — ïÐÒÅÄÅÌÑÅÔ ÆÁÊÌ, × ËÏÔÏÒÙÊ ÂÕÄÅÔ ÐÏÍÅÝÅÎ ÒÅÚÕÌØÔÁÔ

Synopsis

`output` *file-name*

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÐÅÒÅÎÁÐÒÁ×ÌÑÅÔ ×Ù×ÏÄ ËÏÍÁÎÄÙ × ÆÁÊÌ ÕËÁÚÁÎÎÙÊ ÐÁÒÁÍÅÔÒÏÍ.

recipient

Name

`recipient` — ÕËÁÚÙ×ÁÅÔ ÐÌÎÕÞÁÔÅÌÑ ÛÉÆÒÏÂÁÎÎÏÇÏ ÄÏËÕÍÅÎÔÁ

Synopsis

`recipient` *name*

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÏ×ÍÅÓÔÎÏ Ó ËÏÍÁÎÄÏÊ `encrypt`. ïÎÁ ÄÏÌÖÎÁ ÎÁÈÏÄÉÔØÓÑ ÐÅÒÅÄ `encrypt` × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ. ðÁÒÁÍÅÔÒ *name* ÌÉÂÏ ÉÍÑ ÉÎÄÉ×ÉÄÕÕÍÁ, ËÏÔÏÒÏÍÕ ÏÔÐÒÁ×ÌÑÅÔÓÑ ÓÏÏÂÝÅÎÉÅ, ÌÉÂÏ ÅÇÏ e-mail.

default-recipient

Name

`default-recipient` — ÕËÁÚÙ×ÁÅÔ ÐÏÌÕÞÁÔÅÌÑ ÛÉÆÒÕÅÍÏÇÏ ÄÏËÕÍÅÎÔÁ ÐÏ ÕÍÏÌÞÁÎÉÀ

Synopsis

`default-recipient` *`name`*

ïÐÉÓÁÎÉÅ

ID ÐÏÌØÚÏ×ÁÔÅÌÑ *`name`* ÉÓÐÏÌØÚÕÅÔÓÑ × ËÁÞÅÓÔ×Å ÚÎÁÞÅÎÉÑ recipient ÐÏ ÕÍÏÌÞÁÎÉÀ, ÅÓÌÉ ÚÎÁÞÅÎÉÅ recipient ÎÅ ÕËÁÚÁÎÏ ÄÒÕÇÉÍ ÏÂÒÁÚÏÍ.

default-recipient-self

Name

`default-recipient-self` — ÉÓÐÏÌØÚÏ×ÁÔØ ID ÐÏÌØÚÏ×ÁÔÅÌÑ ËÌÀÞÁ ÐÏ ÕÍÏÌÞÁÎÉÀ, ËÁË ÐÏÌÕÞÁÔÅÌÑ ÚÁÛÉÆÒÏ×ÁÎÎÏÇÏ ÄÏËÕÍÅÎÔÁ ÐÏ ÕÍÏÌÞÁÎÉÀ

Synopsis

```
default-recipient-self
```

ïÐÉÓÁÎÉÅ

ID ÐÏÌØÚÏ×ÁÔÅÌÑ ËÌÀÞÁ ÐÏ ÕÍÏÌÞÁÎÉÀ ÉÓÐÏÌØÚÏ×ÁÔØ ËÁË ÐÏÌÕÞÁÔÅÌÑ ÐÏ ÕÍÏÌÞÁÎÉÀ. gpg ÎÅ ÔÒÅÂÕÅÔ ×ÏÄÁ ÐÏÌÕÞÁÔÅÌÑ ÅÓÌÉ ÜÔÁ ÏÐÃÉÑ ÉÄÅÎÔÉÆÉÃÉÒÕÅÔ ÄÅÊÓÔ×ÉÔÅÌØÎÙÊ ËÌÀÞ. ëÌÀÞ ÐÏ ÕÍÏÌÞÁÎÉÀ ÜÔÏ ÐÅÒ×ÙÊ ËÌÀÞ × ÎÁÂÏÒÅ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ ÉÌÉ ËÌÀÞ ÕËÁÚÁÎÎÙÊ ÏÐÃÉÅÊ `default-key`.

no-default-recipient

Name

`no-default-recipient` — ÉÇÎÏÒÉÒÏ×ÁÔØ ÚÎÁÞÅÎÉÑ ÏÐÃÉÉ `default-recipient` É `default-recipient-self`

Synopsis

```
no-default-recipient
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÒÉÍÁÎÑÅÔÓÑ, ÏÂÙÞÎÏ, ÅÓÌÉ ÐÏÌÕÞÁÔÅÌØ ÐÏ ÕÍÏÌÞÁÎÉÀ ÕÓÔÁÎÏ×ÌÅÎ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ, ÎÏ ÄÏÌÖÅÎ ÂÙÔØ ÐÒÏÇÎÏÒÉÒÏ×ÁÎ ÐÒÉ ÄÁÎÎÏÍ ÚÁÐÕÓËÅ gpg.

encrypt-to

Name

`encrypt-to` — ÕËÁÚÁÔØ ÄÏÐÏÎÉÔÅÌØÎÏÇÏ ÐÏÌÕÞÁÔÅÌÑ ÛÉÆÒÕÅÍÏÇÏ ÄÏËÕÍÅÎÔÁ

Synopsis

`encrypt-to` *name*

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÓÈÏÖÁ Ó ÏÐÃÉÅÊ `recipient`, ÎÏ ÐÒÅÄÎÁÚÎÁÞÅÎÁ ÄÌÑ ÉÓÐÏÌØÚÏ×ÁÎÉÑ × ËÏÎÆÉÇÕÒÁÃÉÏÎÎÏÍ ÆÁÊÌÅ. íÖÎÏ ÅÅ ÉÓÐÏÌØÚÏ×ÁÔØ Ó ÏÄÎÏÉ ÉÚ Ó×ÏÉÈ ID ÐÏÌØÚÏ×ÁÔÅÌÑ ÄÌÑ ÒÅÁÌÉÚÁÃÉÉ ÏÐÃÉÉ “encrypt-to-self”. ëÌÀÞ, ÕËÁÚÁÎÎÙÊ *name*, ÉÓÐÏÌØÚÕÅÔÓÑ ÔÏÌØËÏ ÔÏÇÄÁ, ËÏÇÄÁ ÚÁÄÁÎÙ ÄÒÕÇÉÅ ÐÏÌÕÞÁÔÅÌÉ, ÐÏÌØÚÏ×ÁÔÅÌÁÍ, ÌÉÂÏ ÏÐÃÉÉ `recipient`. ðÒÉ ÜÔÏÍ ÎÅ ÐÒÏ×ÅÒÑÅÔÓÑ ÃÅÐÏÞËÁ ÄÏ×ÅÒÉÑ ËÌÀÞÁ *name*, É ÄÁÖÅ ÂÅÚÄÅÊÓÔ×ÕÀÝÉÅ ËÌÀÞÉ ÍÏÇÕÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÙ.

no-encrypt-to

Name

no-encrypt-to — ÉÇÎÏÒÉÒÏ×ÁÔØ ÏÐÃÉÀ encrypt-to

Synopsis

```
no-encrypt-to
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÒÉÍÅÎÉÍÁ ÅÓÌÉ ÓÏÏÂÝÅÎÉÑ, ÏÂÙÞÎÏ, ÚÁÛÉÆÒÏ×Ù×ÁÀÔÓÑ ÏÄÎÉÍ ÉÌÉ ÎÅÓËÏÌØËÉÍÉ ËÌÀÞÁÍÉ ÐÏ ÕÍÏÌÞÁÎÉÀ, ÎÏ ÎÅ ÄÏÌÖÎÙ ÉÍÉ ÚÁÛÉÆÒÏ×Ù×ÁÔØÓÑ ÐÒÉ ÄÁÎÎÏÍ ÚÁÐÕÓËÅ gpg.

armor

Name

armor — ASCII-ÆÏÒÍÁÔÉÒÏ×ÁÎÎÙÊ ×Ù×ÏÄ

Synopsis

```
armor
```

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÐÒÅÏÂÒÁÚÕÅÔ ×Ù×ÏÄ ËÏÍÁÎÄÙ × ASCII ÆÏÒÍÁÔ, ËÏÔÏÒÙÊ ÍÏÖÅÔ ÂÙÔØ ÂÅÚ ÐÒÏÂÌÅÍ ÐÅÒÅÄÁÎ ÐÏ e-mail.

no-armor

Name

no-armor — ÐÒÅÄÐÌÁÇÁÔØ ×ÈÏÄÑÝÉÅ ÄÁÎÎÙÅ ÎÅ ASCII ÆÏÒÍÁÔÉÒÏ×ÁÎÎÙÍÉ

Synopsis

```
no-armor
```

ïÐÉÓÁÎÉÅ

îÅÞÅÇÏ ÄÏÂÁ×ÉÔØ.

no-greeting

Name

no-greeting — ÐÏÄÁ×ÉÔØ ×Ù×ÏÄ ÌÉÃÅÎÚÉÏÎÎÏÊ ÉÎÆÏÒÍÁÃÉÉ, ÎÉ ÎÅ ×ÈÏÄÉÔØ × ÐÁËÅÔÎÙÊ ÒÅÖÉÍ

Synopsis

```
no-greeting
```

ïÐÉÓÁÎÉÅ

îÅÞÅÇÏ ÄÏÂÁ×ÉÔØ.

no-secmem-warning

Name

no-secmem-warning — ÐÏÄÁ×ÉÔØ ÐÒÅÄÕÐÒÅÖÄÅÎÉÅ ÏÂ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÎÅÚÁÝÉÝÅÎÎÏÊ ÐÁÍÑÔÉ

Synopsis

```
no-secmem-warning
```

ïÐÉÓÁÎÉÅ

îÅÞÅÇÏ ÄÏÂÁ×ÉÔØ.

batch

Name

batch — ÒÁÂÏÔÁ × ÐÁËÅÔÎÏÍ ÒÅÖÉÍÅ

Synopsis

```
batch
```

ïÐÉÓÁÎÉÅ

gpg ÎÅ ÂÕÄÅÔ ÚÁÄÁ×ÁÔØ ×ÏÐÒÏÓ× É ÎÅ ÄÏÐÕÓÔÉÔ ÉÎÔÅÒÁËÔÉ×ÎÙÈ ËÏÍÁÎÄ.

no-batch

Name

no-batch — ÏÔËÌÀÞÉÔØ ÐÁËÅÔÎÙÊ ÒÅÖÉÍ

Synopsis

```
no-batch
```

ïÐÉÓÁÎÉÅ

ðÒÉÍÅÎÉÍÁ ÅÓÌÉ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ ÕÓÔÁÎÏ×ÌÅÎ ÏÐÃÉÑ batch.

local-user

Name

local-user — ÓÐÅÃÉÆÉÃÉÒÕÅÔ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÌØÚÏ×ÁÔÅÌÑ ÉÓÐÏÌØÚÕÅÍÙÊ ÄÌÑ ÐÏÄÐÉÓÉ

Synopsis

```
local-user name
```

ïÐÉÓÁÎÉÅ

éÓÐÏÌØÚÏ×ÁÔØ *name* ËÁË ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÒÉ ÐÏÄÐÉÓÉ. íÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.

default-key

Name

`default-key` — ÚÁÄÁÅÔ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ËÁË ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏ ÕÍÏÌÞÁÎÉÀ ÄÌÑ ÐÏÄÐÉÓÅÊ

Synopsis

`default-user` *name*

ïÐÉÓÁÎÉÅ

éÓÐÏÌØÚÏ×ÁÔØ *name* × ËÁÞÅÓÔ×Å ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÒÉ ÐÏÄÐÉÓÉ. åÓÌÉ ÏÐÃÉÑ ÎÅ ÚÁÄÁÎÁ, ÐÏ ÕÍÏÌÞÁÎÉÀ ÉÓÐÏÌØÚÕÅÔÓÑ ÐÅÒ×ÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÎÁÊÄÅÎÎÙÊ × Ó×ÑÚËÅ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ.

completes-needed

Name

`completes-needed` — ÚÁÄÁÅÔ ÞÉÓÌÏ ÐÏÌÎÏÓÔØÀ ÄÏ×ÅÒØÈ ÌÉÃ, ÎÅÏÂÈÏÄÉÍÅ ÄÌÑ ÐÏÂ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÓÔÉ ÎÏ×ÏÇÏ ËÌÀÞÁ

Synopsis

`completes-needed` *n*

ïÐÉÓÁÎÉÅ

äÏÓÔÏ×ÅÒÎÓÔØ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ × ÷ÁÛÅÊ Ó×ÑÚËÅ ÐÏÄÔ×ÅÒÖÄÁÅÔÓÑ ÎÁ ÏÓÎ×Å ÐÏÄÐÉÓÅÊ ÎÁ ÜÔÏÍ ËÌÀÞÅ, ÓÄÅÌÁÎÎÙÈ ÄÒÕÇÉÍ ËÌÀÞÁÍÉ ÉÚ ÷ÁÛÅÊ Ó×ÑÚËÉ, ÄÏÓÔ×ÅÒÎÓÔØ ËÏÔÏÒÙÈ ÕÖÅ ÐÒÏ×ÅÒÅÎ. ïÐÃÉÑ ÕËÁÚÙ×ÁÅÔ ÞÉÓÌÏ ÎÅÏÂÈÏÄÉÍÙÈ ÐÏÄÐÉÓÅÊ, ÓÄÅÌÁÎÎÙÈ ×ÌÁÄÅÌØÃÁÍÉ ËÌÀÞÅÊ ËÏÔÏÒÙÍ ÷Ù ÐÏÌÎÏÓÔØÀ ÄÏ×ÅÒÑÅÔÅ. ÷ÁÛÅ ÄÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ ÕÓÔÁÎÁ×ÌÉ×ÁÅÔÓÑ ÐÒÉ ÐÏÍÏÝÉ ËÏÍÁÎÄÙ `edit-key`.

marginals-needed

Name

`marginals-needed` — ÚÁÄÁÅÔ ÞÉÓÌÏ ÏÔÎÏÓÉÔÅÌØÎÏ ÎÁÄÅÖÎÙÈ ÌÉÃ, ÎÅÏÂÈÏÄÉÍÏÅ ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔ×ÅÒÎÓÔÉ ÎÏ×ÏÇÏ ËÌÁÞÁ

Synopsis

`marginals-needed` *n*

ïÐÉÓÁÎÉÅ

äÏÓÔ×ÅÒÎÓØ ÏÔËÒÙÔÏÇÏ ËÌÁÞÁ × ÷ÁÛÅÊ Ó×ÑÚËÅ ÐÏÄÔ×ÅÒÖÄÁÅÔÓÑ ÎÁ ÏÓÎ×Å ÐÏÄÐÉÓÅÊ ÎÁ ÜÔÏÍ ËÌÁÞÅ, ÓÄÅÌÁÎÎÙÈ ÄÒÕÇÉÍ ËÌÁÞÁÍÉ ÉÚ ÷ÁÛÅÊ Ó×ÑÚËÉ, ÄÏÓÔ×ÅÒÎÏÓÔØ ËÏÎÏÙÈ ÕÖÅ ÐÒÏ×ÅÒÅÎ. ïÐÃÉÑ ÕËÁÚÙ×ÁÅÔ ÞÉÓÌÏ ÎÅÏÂÈÏÄÉÍÙÈ ÐÏÄÐÉÓÅÊ, ÓÄÅÌÁÎÎÙÈ ×ÌÁÄÅÌØÃÁÍÉ ËÌÁÞÅÊ ËÏÎÏÒÙÍ ÷Ù ÎÅ ÄÏ ËÏÎÃÁ ÄÏ×ÅÒÑÅÔÅ. ÷ÁÛÅ ÄÏ×ÅÉÅ ×ÌÁÄÅÌØÃÕ ËÌÁÞÁ ÕÓÔÁÎÁ×ÌÉ×ÁÅÔÓÑ ÐÒÉ ÐÏÍÝÉ ËÏÍÁÎÄÙ `edit-key`.

load-extension

Name

`load-extension` — ÕËÁÚÙ×ÁÅÔ ÒÁÓÛÉÒÅÎÉÅ ÄÌÑ ÚÁÇÒÕÚËÉ.

Synopsis

```
load-extension object-file
```

ïÐÉÓÁÎÉÅ

âÅÚ ËÏÍÅÎÔÁÒÉÅ×.

rfc1991

Name

rfc1991 — ÂÙÔØ ÂÏÌØ ÓÏ×ÍÅÓÔÉÍÙÍ Ó RFC1991 (PGP 2.x)

Synopsis

```
rfc1991
```

ïÐÉÓÁÎÉÅ

âÅÚ ËÏÍÅÎÔÁÒÉÅ×.

allow-non-selfsigned-uid

Name

`allow-non-selfsigned-uid` — ÐÏÚ×ÏÑÅÔ ÉÍÐÏÒÔ ËÌÀÞÅÊ Ó ÉÄÅÎÔÉÆÉËÁÔÏÒÁÍÉ ÐÎØÚÏ×ÁÔÅÌÑ ÎÅ ÐÏÄÐÉÓÁÎÎÙÍÉ ÜÔÉÍ ËÌÀÞÏÍ

Synopsis

```
allow-non-selfsigned-uid
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÏÚ×ÏÑÅÔ ÔÏÎØËÏ ÉÍÐÏÒÔ - ÐÏÄÔ×ÅÒÖÄÅÎÉÅ ËÌÀÞÁ ÎÅ ÐÒÏÊÄÅÔ. üÔÁ ÏÐÃÉÑ ÎÕÖÎÁ ÄÌÑ ÎÅËÏÔÏÙÈ ÎÅÍÅÃËÉÈ ËÌÀÞÅÊ ÓÇÅÎÅÒÉÒÏ×ÁÎÎÙÈ pgp 2.6.3in. ÷ÁÍ ÓÌÅÄÕÅÔ ÉÚÂÅÇÁÔØ ÉÓÐÏØÚÏ×ÁÎÉÑ ÜÔÏÊ ÏÐÃÉÉ.

cipher-algo

Name

`cipher-algo` — ÉÓÐÏØÚÏ×ÁÔØ ÕËÁÚÁÎÎÙÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ

Synopsis

```
cipher-algo name
```

ïÐÉÓÁÎÉÅ

éÓÐÏÌØÚÏ×ÁÎØ ÁÌÇÏÒÉÔÍ *name* ÄÌÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ. úÁÐÕÓË gpg Ó ÏÐÃÉÅÊ `version` ×ÙÄÁÅÔ ÓÐÉÓÏË ÐÏÄÄÅÒÖÉ×ÁÅÍÙÈ ÁÌÇÏÒÉÔÍÏ×. åÓÌÉ ÏÐÃÉÑ ÎÅ ÕËÁÚÁÎÁ, ÁÌÇÏÒÉÔÍ ÛÉÆÒÏ×ÁÎÉÑ ×ÙÂÉÒÁÅÔÓÑ ÉÚ Ó×ÏÊÓÔ×ÀÐÅ×ÏÊ ÐÁÒÙ ÐÏ ÕÍÏÌÞÁÎÉÀ. äÌÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ, ÜÔÏ Blowfish.

compress-algo

Name

`compress-algo` — ÉÓÐÏÌØÚÏ×ÁÔØ ÕËÁÚÁÎÎÙÊ ÁÌÇÏÒÉÔÍ ÓÖÁÔÉÑ

Synopsis

```
compress-algo n
```

ïÐÉÓÁÎÉÅ

ðÏ ÕÍÏÌÞÁÎÉÀ 2, ËÏÔÏÒÙÊ ÏÐÒÅÄÅÌÅÎ × RFC1950. ÷Ù ÍÏÖÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ 1 ÄÌÑ ÓÔÁÒÏÊ ×ÅÒÓÉÉ zlib, ËÏÔÏÒÁ ÉÓÐÏÌØÚÕÅÔ PGP. áÌÇÏÒÉÔÍ ÐÏ ÕÍÏÌÞÁÎÉÀ ÍÖÅÔ ÄÁ×ÁÔØ ÌÕÞÛÉÅ ÒÅÚÕÌØÔÁÔÙ, Ô.Ë. ÒÁÚÍÅÒ ÏËÎÁ ÎÅ

ÏÇÒÁÎÉÞÅÎ 8K. åÓÌÉ ÏÐÃÉÑ ÎÅ ÕËÁÚÁÎÁ, ÉÓÐÏÌØÚÕÀÔÓÑ ÎÁÓÔÒÏËÉ ÐÒÉÎÑÔÙÅ × OpenPGP, Ô.Å., ×ÙÂÉÒÁÅÔÓÑ ÐÒÅÄÐÏÞÔÉÔÅÌØÎÙÊ ÁÌÇÏÒÉÔÍ ÓÖÁÔÉÑ.

z

Name

z — ÕÓÔÁÎÏ×ÉÔØ ÓÔÅÐÅÎØ ÓÖÁÔÉÑ

Synopsis

z *n*

ïÐÉÓÁÎÉÅ

õÓÔÁÎÏ×ËÁ *n* × 0 ÏÔËÌÀÞÁÅÔ ÓÖÁÔÉÅ. ðÏ ÕÍÏÌÞÁÎÉÀ ÉÓÐÏÌØÚÕÅÔÓÑ ÏÂÙÞÎÙÊ ÕÒÏ×ÅÎØ ÓÖÁÔÉÑ ÄÌÑ zlib (6). ÷ ÏÔÌÉÞÉÅ ÏÔ ×ÓÅÈ ÏÓÔÁÌØÎÙÈ ÏÐÃÉÊ, ÜÔÁ ÍÏÄÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÁ ÔÏÌØËÏ × ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÅ, É ÅÊ ÐÒÅÄÛÅÓÔ×ÕÅÔ ÔÏÌØËÏ ÏÄÉÎ ÚÎÁË ÍÉÎÕÓ Á ÎÅ Ä×Á.

verbose

Name

verbose — ×ÙÄÁ×ÁÔØ ÄÏÐÏÎÎÉÔÅÌØÎÕÀ ÉÎÆÏÒÍÁÃÉÀ ×Ï ×ÒÅÍÑ ÒÁÂÏÔÙ

Synopsis

```
verbose
```

ïÐÉÓÁÎÉÅ

ðÒÉ ÏÄÎÏËÒÁÔÎÏÍ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ×ÙÄÁÅÔ ÄÏÐÏÎÎÉÔÅÌØÎÕÀ ÉÎÆÏÒÍÁÃÉÀ Ï ÈÏÄÅ ÒÁÂÏÔÙ. åÓÌÉ ÕËÁÚÁÎÁ Ä×ÁÖÄÙ, ÄÅÔÁÌØÎÏ ×Ù×ÏÄÑÔÓÑ ×ÈÏÄÑÝÅÅ ÄÁÎÎÙÅ.

no-verbose

Name

no-verbose — ÏÔËÌÀÞÁÅÔ ×Ù×ÏÄ ÄÏÐÏÎÎÉÔÅÌØÎÏÊ ÉÎÆÏÒÍÁÃÉÉ

Synopsis

```
no-verbose
```

ïÐÉÓÁÎÉÅ

éÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÏÔÌÀÞÅÎÉÑ ÐÒÅÄÙÄÕÝÅÊ ÏÐÃÉÉ `verbose`.

quiet

Name

`quiet` — ÐÏÄÁ×ÌÑÅÔ ×Ù×ÏÄ ÉÎÆÏÒÍÁÃÉÉ

Synopsis

```
quiet
```

ïÐÉÓÁÎÉÅ

÷Ù×ÏÄÉÔÓÑ ÍÉÎÉÍÕÍ ÉÎÆÏÒÍÁÃÉÉ.

textmode

Name

`textmode` — ÉÓÐÏÌØÚÏ×ÁÔØ ÔÅËÓÔÏ×ÙÊ ÒÅÖÉÍ

Synopsis

```
textmode
```

ïÐÉÓÁÎÉÅ

What good is this option?

dry-run

Name

`dry-run` — ÎÉÞÅÇÏ ÎÅ ÍÅÎÑÔØ

Synopsis

```
dry-run
```

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÎÅ ÒÅÁÌÉÚÏ×ÁÎÁ ÐÏÌÎÏÓÔØÀ. éÓÐÏÌØÚÕÊÔÅ Ó ÏÓÔÏÒÏÖÎÏÓÔØÀ.

interactive

Name

`interactive` — ÚÁÐÒÏÓ ÐÅÒÅÄ ÐÅÒÅÚÁÐÉÓØÀ ÆÁÊÌÏ×

Synopsis

```
interactive
```

ïÐÉÓÁÎÉÅ

÷ÓÅ ÓËÁÚÁÎÏ.

yes

Name

yes — ÏÔ×ÅÞÁÔØ “yes” ÎÁ ÂÎÌØÛÉÎÓÔ×Ï ×ÏÐÒÏÓÏ×

Synopsis

```
yes
```

ïÐÉÓÁÎÉÅ

÷ÓÅ ÓËÁÚÁÎÏ.

no

Name

no — ÏÔ×ÅÞÁÔØ “no” ÎÁ ÂÎÌØÛÉÎÓÔ×Ï ×ÏÐÒÏÓÏ×

Synopsis

```
no
```

ïÐÉÓÁÎÉÅ

îÅÞÅÇÏ ÄÏÂÁ×ÉÔØ.

always-trust

Name

always-trust — ÐÒÏÐÕÓÔÉÔØ ÐÒÏ×ÅÒËÕ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ

Synopsis

```
always-trust
```

ïÐÉÓÁÎÉÅ

üÔÉÍ ÐÒÅÄÐÌÁÇÁÅÔÓÑ, ÞÔÏ ÉÓÐÏÌØÚÕÅÍÙÊ ËÌÀÞ ÄÏÓÔÏ×ÅÒÅÎ. ïÐÃÉÑ ÎÅ ÄÌÖÎÁ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÉÎÁÞÅ, ËÁË × ÓÌÕÞÁÑÈ ËÏÇÄÁ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ ÉÓÐÏÌØÚÕÅÔÓÑ ÎÅËÏÔÏÒÁÑ ×ÎÅÛÎÑÑ ÐÒÏÃÅÄÕÒÁ.

skip-verify

Name

skip-verify — ÐÒÏÐÕÓÔÉÔØ ÐÒÏ×ÅÒËÕ ÐÏÄÐÉÓÉ

Synopsis

```
skip-verify
```

ïÐÉÓÁÎÉÅ

ðÒÏÐÕÓÔÉÔØ ÐÒÏ×ÅÒËÕ ÐÏÄÐÉÓÉ. üÔÏ ÕÓËÏÒÎÅÔ ÒÁÓÛÉÆÒÏ×ËÕ ÓÏÎÂÝÅÎÉÑ.

keyring

Name

keyring — ÄÏÂÁ×ÉÔØ Ó×ÑÚËÕ ËÌÀÞÅÊ Ë ÓÐÉÓËÕ Ó×ÑÚÏË ËÌÀÞÅÊ

Synopsis

```
keyring file
```

ïÐÉÓÁÎÉÅ

äÏÂÁ×ÌÑÅÔ ÆÁÊÌ *file* Ë ÓÐÉÓËÕ Ó×ÑÚÏË ËÌÀÞÅÊ ÉÓÐÏÌØÚÕÅÍÙÈ ×Ï ×ÒÅÍÑ ÒÁÂÏÔÙ. åÓÌÉ *file* ÎÁÞÉÎÁÅÔÓÑ Ó ÔÉÌØÄÙ É ÓÌÜÛÁ, ÏÎÉ ÚÁÍÅÎÑÀÔÓÑ ÎÁ ÄÏÍÁÛÎÉÊ ËÁÔÁÌÏÇ. åÓÌÉ ÉÍÑ ÆÁÊÌÁ ÎÅ ÓÏÄÅÒÖÉÔ ÓÌÜÛÁ, ÐÒÅÄÐÏÁÇÁÅÔÓÑ, ÞÔÏ ÆÁÊÌ ÎÁÈÏÄÉÔÓÑ × ÄÏÍÁÛÎÅÍ ËÁÔÁÌÏÇÅ. äÏÍÁÛÎÉÊ ËÁÔÁÌÏÇ - “~/.gnupg” ÅÓÌÉ ÎÅ ÉÓÐÏÌØÚÏ×ÁÎ ÏÐÃÉÑ `homedir`.

éÍÅÎÉ ÆÁÊÌÁ *file* ÍÏÖÅÔ ÐÒÅÄÛÅÓÔ×Ï×ÁÔØ ÐÒÅÆÉËÓ. ðÒÅÆÉËÓ “gnupg-ring:” ÄÅÌÁÅÔ ÕËÁÚÁÎÎÙÊ ÆÁÊÌ Ó×ÑÚÉÎÊ ÐÏ ÕÍÏÌÞÁÎÉÀ. ðÒÅÆÉËÓ “gnupg-gdbm:” ÄÅÌÁÅÔ ÕËÁÚÁÎÎÙÊ ÆÁÊÌ GDBM ÂÁÚÉÊ ËÌÀÞÅÊ. íÏÖÅÔ ÂÙÔØ ÐÏÌÅÚÎÏ ÉÓÐÏÌØÚÏ×ÁÔØ ÜÔÉ ÓÈÅÍÙ ÓÏ×ÍÅÓÔÎÏ Ó ÏÐÃÉÅÊ `no-default-keyring`.

secret-keyring

Name

`secret-keyring` — ÄÏÂÁ×ÉÔØ ÓÅËÒÅÔÎÕÀ Ó×ÑÚËÕ

Synopsis

`secret-keyring` *file*

ïÐÉÓÁÎÉÅ

ôÏ ÖÅ, ÞÔÏ É `keyring` ÎÏ ÄÌÑ ÓÅËÒÅÔÎÙÈ Ó×ÑÚÉË.

no-default-keyring

Name

no-default-keyring — ÎÅ ÄÏÂÁ×ÌÑÔØ Ó×ÑÚËÉ ÐÏ ÕÍÌÞÁÎÉÀ Ë ÓÐÉÓËÕ Ó×ÑÚÏË

Synopsis

```
no-default-keyring
```

ïÐÉÓÁÎÉÅ

ó×ÑÚËÉ ËÌÀÞÅÊ ÐÏ ÕÍÌÞÁÎÉÀ, ÎÁÈÏÄÑÝÉÅÓÑ × ÄÏÍÁÛÎÅÍ ËÁÔÁÌÏÇÅ, ÎÅ ÉÓÐÏÌØÚÕÀÔÓÑ ÐÒÉ ×ÙÐÏÌÎÅÎÉÉ ÐÒÏÇÒÁÍÍÙ.

homedir

Name

homedir — ÕÓÔÁÎÏ×ÉÔØ ÄÏÍÁÛÎÉÊ ËÁÔÁÌÏÇ

Synopsis

homedir *directory*

ïÐÉÓÁÎÉÅ

åÓÌÉ ÏÐÃÉÑ ÎÅ ÕËÁÚÁÎÁ, ÐÏ ÕÍÏÌÞÁÎÉÀ ÉÓÐÏÌØÚÕÅÔÓÑ ËÁÔÁÌÏÇ "~/.gnupg". ïÐÃÉÑ ÚÁÍÅÎÑÅÔ ÐÅÒÅÍÅÎÎÕÀ ÏËÒÕÖÅÎÉÑ GNUPGHOME. îÅÔ ÓÍÙÓÌÁ ÉÓÐÏÌØÚÏ×ÁÔØ ÅÅ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.

charset

Name

charset — ÕÓÔÁÎÏ×ÉÔØ ÉÍÑ ÒÏÄÎÏÇÏ ÎÁÂÏÒÁ ÓÉÍ×ÏÌ×.

Synopsis

charset *name*

ïÐÉÓÁÎÉÅ

éÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÒÅÏÂÒÁÚÏ×ÁÎÉÑ ÎÅËÏÔÏÒÙÈ ÓÔÒÏË × ËÏÄÉÒÏ×ËÕ UTF-8. äÏÐÕÓÔÉÍÙÅ ÚÎÁÞÅÎÉÑ *name*:

Name	Character set
iso-8859-1	îÁÂÏÒ Latin 1 (ÐÏ ÕÍÌÞÁÎÉÀ)
iso-8859-2	îÁÂÏÒ Latin 2
koi8-r	KOI8-R (rfc1489)

no-literal

Name

`no-literal` — ?

Synopsis

```
no-literal
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÎÅ ÄÌÑ ÎÏÒÍÁÌØÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ. óÍ. ÐÏÄÒÏÂÎÏÓÔÉ × ÉÓÈÏÄÎÏÍ ËÏÄÅ.

set-filesize

Name

`set-filesize` — ?

Synopsis

`set-filesize` *size*

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÎÅ ÄÌÑ ÎÏÒÍÁÌØÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ. óÍ. ÐÏÄÒÏÂÎÏÓÔÉ × ÉÓÈÏÄÎÏÍ ËÏÄÅ.

with-fingerprint

Name

`with-fingerprint` — ÍÏÄÉÆÉÃÉÒÕÅÔ ×Ù×ÏÄ ÓÐÉÓËÁ ËÌÀÞÅÊ

Synopsis

`with-fingerprint`

ïÐÉÓÁÎÉÅ

óÈÏÖÁ Ó ËÏÍÁÎÄÏÊ `fingerprint` ÎÏ ÜÔÏ ÏÐÃÉÑ. éÓÐÏÌØÚÕÅÔÓÑ ×ÍÅÓÔÅ Ó ËÏÍÁÎÄÏÊ `list-keys`.

with-colons

Name

`with-colons` — ÍÏÄÉÆÉÃÉÒÕÅÔ ×Ù×ÏÄ ÓÐÉÓËÁ ËÌÀÞÅÊ

Synopsis

```
with-colons
```

ïÐÉÓÁÎÉÅ

ëÌÀÞÉ ×Ù×ÏÄÉÍÙÅ ËÏÍÁÎÄÏÊ `list-keys` ÒÁÚÇÒÁÎÉÞÉ×ÁÀÔÓÑ Ä×ÏÅÔÏÞÉÑÍÉ.

with-key-data

Name

with-key-data — ÍÏÄÉÆÉÃÉÒÕÅÔ ×Ù×ÏÄ ÓÐÉÓËÁ ËÌÀÞÅÊ

Synopsis

```
with-key-data
```

ïÐÉÓÁÎÉÅ

õËÁÚÙ×ÁÅÔ ËÏÍÁÎÄÅ list-keys ÐÅÞÁÔÁÔØ ËÌÀÞÉ É ÄÁÎÎÙÅ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ.

lock-once

Name

lock-once — ÂÌÏËÉÒÏ×ÁÔØ ÂÁÚÕ ÏÄÉÎ ÒÁÚ

Synopsis

```
lock-once
```

ïÐÉÓÁÎÉÅ

ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÏÐÃÉÉ ÂÁÚÁ ÄÁÎÎÙÈ ÂÌÏËÉÒÕÅÔÓÑ ÐÒÉ ÐÅÒ×ÏÍ ÚÁÐÒÏÓÅ É ÎÅ ÏÓ×ÏÂÏÄÄÅÎÎÏÍ ÄÏ ÚÁ×ÅÒÛÅÎÉÑ ÐÒÏÃÅÓÓÁ.

lock-multiple

Name

`lock-multiple` — ÂÌÏËÉÒÏ×ÁÔØ ÂÁÚÙ ÐÒÉ ËÁÖÄÏÍ ÚÁÐÒÏÓÅ

Synopsis

```
lock-multiple
```

ïÐÉÓÁÎÉÅ

ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÏÐÃÉÉ ÂÁÚÁ ÂÌÏËÉÒÕÅÔÓÑ ÐÒÉ ËÁÖÄÏÍ ÚÁÐÒÏÓÅ É ÏÓ×ÏÂÏÄÄÅÎÎÏÍ ÓÒÁÚÕ ÐÏÓÌÅ ÅÇÏ ×ÙÐÏÌÎÅÎÉÑ. ïÐÃÉÑ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÁ ÄÌÑ ÐÅÒÅÐÒÏÓÁ ÏÐÃÉÉ `lock-once` × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.

passphrase-fd

Name

passphrase-fd — ÓÞÉÔÙ×ÁÔØ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ ÎÅ ÉÚ ÓÔÁÎÄÁÒÔÎÏÇÏ ×ÈÏÄÁ

Synopsis

passphrase-fd *n*

ïÐÉÓÁÎÉÅ

åÓÌÉ *n* ÒÁ×ÅÎ 0, ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÂÕÄÅÔ ÓÞÉÔÁÎÁ ÓÏ ÓÔÁÎÄÁÒÔÎÏÇÏ ××ÏÄÁ. íÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÅÓÌÉ ÔÒÅÂÕÅÔÓÑ ××ÏÄ ÔÏÌØËÏ ÏÄÎÏÊ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ. îÅ ÉÓÐÏÌØÚÕÊÔÅ ÜÔÕ ÏÐÃÉÀ ÂÅÚ ÎÅÏÂÈÏÄÉÍÏÓÔÉ.

force-mdc

Name

force-mdc — ÆÏÒÓÉÒÕÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÛÉÆÒÏ×ÁÎÉÑ Ó ÄÏÐÏÎÉÔÅÌØÎÙÍ ËÏÄÏÍ ÍÁÎÉÐÕÌÑÃÉÉ

Synopsis

```
force-mdc
```

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ×ÓÅÇÄÁ ÉÓÐÏÌØÚÕÅÔÓÑ Ó ÎÏ×ÙÍÉ ÛÉÆÒÁÍÉ Ó ÒÁÚÍÅÒÏÍ ÂÌÏËÁ ÂÏÌÅÅ 64 ÂÉÔ. ïÐÃÉÑ ÐÏËÁ ÎÅ ÒÅÁÌÉÚÏ×ÁÎÁ.

force-v3-sigs

Name

`force-v3-sigs` — ÆÏÒÓÉÒÕÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÐÏÄÐÉÓÅÊ v3 ÎÁ ÄÁÎÎÙÈ

Synopsis

```
force-v3-sigs
```

ïÐÉÓÁÎÉÅ

OpenPGP ÕÓÔÁÎÁ×ÌÉ×ÁÅÔ, ÞÔÏ ÒÅÁÌÉÚÁÃÉÑ ÄÏÖÎÁ ÇÅÎÅÒÉÒÏ×ÁÔØ ÐÏÄÐÉÓÉ v4, ÎÏ PGP 5.x ÐÒÉÚÎÁÅÔ ÐÏÄÐÉÓÉ v4 ÔÏÌØËÏ ÎÁ ËÌÀÞÁÈ. üÔÁ ÏÐÃÉÑ ÆÏÒÓÉÒÕÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÐÏÄÐÉÓÅÊ v3 ÎÁ ÄÁÎÎÙÈ.

openpgp

Name

openpgp — ÐÒÉ×ÏÄÉÔ ×ÓÅ ÏÐÃÉÉ × ÓÏÏÔ×ÅÔÓÔ×ÉÅ ÓÐÅÃÉÆÉËÁÃÉÉ OpenPGP

Synopsis

```
openpgp
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÓÂÒÁÓÙ×ÁÅÔ ÚÎÁÞÅÎÉÑ ×ÓÅÈ ÐÒÅÄÙÄÕÝÉÈ ÏÐÃÉÊ, ÔÁËÉÈ ËÁË `lock-once`, `lock-once`, `cipher-algo`, `digest-algo`, `compress-algo`, `s2k-cipher-algo`, `s2k-digest-algo`, É `s2k-mode`, Ë ÚÎÁÞÅÎÉÑÍ ÓÏ×ÍÅÓÔÉÍÙÍ Ó OpenPGP.

utf8-strings

Name

utf8-strings — ÐÒÅÄÐÏÌÁÇÁÔØ ÁÒÇÕÍÅÎÔÙ ÓÔÒÏËÁÍÉ UTF8

Synopsis

```
utf8-strings
```

ïÐÉÓÁÎÉÅ

áÒÇÕÍÅÎÔÙ ÏÐÃÉÊ ÓÌÅÄÕÀÝÉÈ ÚÁ ÜÔÏÊ ÏÐÃÉÅÊ ÐÒÅÄÐÏÌÁÇÁÀÔÓÑ ÓÔÒÏËÁÍÉ × ÆÏÒÍÁÔÅ UTF8.

no-utf8-strings

Name

no-utf8-strings — ÎÅ ÐÒÅÄÐÏÌÁÇÁÔØ ÁÒÇÕÍÅÎÔÙ ÓÔÒÏËÁÍÉ UTF8

Synopsis

```
no-utf8-strings
```

ïÐÉÓÁÎÉÅ

áÒÇÕÍÅÎÔÙ ÏÐÃÉÊ ÓÌÅÄÕÀÝÉÈ ÚÁ ÜÔÏÊ ÏÐÃÉÅÊ ÐÒÅÄÐÌÁÇÁÀÔÓÑ ÓÔÒÏËÁÍÉ × ËÏÄÉÒÏ×ËÅ `charset`. üÔÏ ÐÒÅÄÐÌÁÇÁÅÔÓÑ É ÐÏ ÕÍÏÌÞÁÎÉÀ × gpg.

no-options

Name

`no-options` — ÎÅ ÉÓÐÏÌØÚÏ×ÁÔØ ÆÁÊÌ ËÏÎÆÉÇÕÒÁÃÉÉ

Synopsis

```
no-options
```

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÏÂÒÁÂÁÔÙ×ÁÅÔÓÑ ÄÏ ÔÏÇÏ, ËÁË ÂÕÄÅÔ ÎÔËÒÙÔ ÆÁÊÌ ËÏÎÆÉÇÕÒÁÃÉÉ.

debug

Name

debug — ÕÓÔÁÎÏ×ÉÔØ ÆÌÁÇÉ ÏÔÌÁÄËÉ

Synopsis

debug *flags*

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *flags* ÐÏÌÕÞÁÅÔÓÑ ÐÒÉÍÅÎÅÎÉÅÍ ÏÐÅÒÁÔÏÒÁ OR Ë ÎÏÄÅÌØÎÙÍ ÆÌÁÇÁÍ. ðÁÒÁÍÅÔÒ ÍÏÖÅÔ ÂÙÔØ ÚÁÄÁÎ × ÆÏÒÍÁÔÅ C, ÎÁÐÒÉÍÅÒ, 0x0042. æÌÁÇÉ:

æÌÁÇ	úÎÁÞÅÎÉÅ
1	äÅÔÁÌÉ ÞÔÅÎÉÑ É ÚÁÐÉÓÉ ÐÁËÅÔÁ
2	ÄÅÔÁÌÉ MPI
4	äÅÔÁÌÉ ÛÉÆÒÁ É ÐÒÏÔÏÔÙÈ ÞÉÓÅÌ (ÍÏÖÅÔ ÏÔËÒÙÔØ ÞÕ×ÓÔ×ÉÔÅÌØÎÙÅ ÄÁÎÎÙÅ)
8	æÕÎËÃÉÉ ÆÉÌØÔÒÁ iobuf
16	äÅÔÁÌÉ iobuf
32	äÅÔÁÌÉ ×ÙÄÅÌÅÎÑ ÐÁÍßÔÉ
64	ëÜÛÉÒÏ×ÁÎÉÅ
128	ðÏËÁÚÁÔØ ÓÔÁÔÉÓÔÉËÕ ÐÁÍßÔÉ ÐÒÉ ×ÙÈÏÄÅ

æÌÁÇ	úÎÁÞÅÎÉÅ
256	äÅÔÁÌÉ ÐÒÏ×ÅÒËÉ ÄÏ×ÅÒÉÑ

debug-all

Name

`debug-all` — ÕÓÔÁÎÏ×ÉÔØ ×ÓÅ ÏÔÌÁÄÏÞÎÙÅ ÆÌÁÇÉ

Synopsis

```
debug-all
```

ïÐÉÓÁÎÉÅ

óÍÏÔÒÉÔ ÏÐÃÉÀ `debug`.

status-fd

Name

`status-fd` — ×Ù×ÏÄÉÔØ ÓÏÏÂÝÅÎÉÑ Ï ÓÏÓÔÏÑÎÉÉ × ÁÌØÔÅÒÎÁÔÉ×ÎÙÊ ÐÏÔÏË

Synopsis

`status-fd` *n*

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÅÒÅÎÁÐÒÁ×ÌÑÅÔ ÓÏÏÂÝÅÎÉÑ Ï ÓÏÓÔÏÑÎÉÉ × ÐÏÔÏË Ó ÄÅÓËÒÉÐÔÏÒÏÍ *n*. óÐÉÓÏË ÓÏÏÂÝÅÎÉÊ ÓÍÏÔÒÉ × ÆÁÊÌÅ `DETAILS` ÉÚ ÐÁËÅÔÁ.

logger-fd

Name

`logger-fd` — ×Ù×ÏÄ ÓÏÏÂÝÅÎÉÊ ÏÂ ÏÛÉÂËÁÈ × ÁÌØÔÅÒÎÁÔÉ×ÎÙÊ ÆÁÊÌ

Synopsis

```
logger-fd n
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÅÒÅÎÁÐÒÁ×ÌÑÅÔ ÓÏÏÂÝÅÎÉÑ ÏÂ ÏÛÉÂËÁÈ × ÆÁÊÌ Ó ÄÅÓËÒÉÐÔÏÒÏÍ *n* ×ÍÅÓÔÏ ÓÔÁÎÄÁÒÔÎÏÇÏ ÐÏÔÏËÁ ÏÛÉÂÏË.

no-comment

Name

`no-comment` — do not write comment packets

Synopsis

```
no-comment
```

ïÐÉÓÁÎÉÅ

This option affects only the generation of secret keys Output of option (comment?) packets is disabled since version 0.4.2 of GnuPG.

comment

Name

comment — ÕÓÔÁÎÏ×ÉÔØ ÓÔÒÏËÕ ËÏÍÍÅÎÔÁÒÉÑ ÄÌÑ ÉÓÐÏÌØÚÏ×ÁÎÉÑ × ÔÅËÓÔÏ×ÙÈ ÐÏÄÐÉÓÑÈ

Synopsis

comment *string*

ïÐÉÓÁÎÉÅ

÷ÓÅ ÓËÁÚÁÎÏ.

default-comment

Name

default-comment — ÉÓÐÏÌØÚÏ×ÁÔØ ÓÔÁÎÄÁÒÔÎÕÀ ÓÔÒÏËÕ ËÏÍÍÅÎÔÁÒÉÑ × ÔÅËÓÔÏ×ÙÈ ÐÏÄÐÉÓÑÈ

Synopsis

```
default-comment
```

ïÐÉÓÁÎÉÅ

üÔÁ ÏÐÃÉÑ ÐÅÒÅËÒÙ×ÁÅÔ ÒÁÎÅÅ ÉÓÐÏÌØÚÏ×ÁÎÎÕÀ ÏÐÃÉÀ `comment`.

no-version

Name

`no-version` — ÏÐÕÓÔÉÔØ ÓÔÒÏËÕ ×ÀÓÉÉ × ÔÅËÓÔÏ×ÙÈ ÐÏÄÐÉÓÑÈ

Synopsis

```
no-version
```

ïÐÉÓÁÎÉÅ

÷ÓÅ ÓËÁÚÁÎÏ.

emit-version

Name

emit-version — ×ËÌÀÞÁÔØ ÓÔÒÏËÕ ×ÀÓÓÉÉ × ÔÅËÓÔÏ×ÙÅ ÐÏÄÐÉÓÉ

Synopsis

```
emit-version
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÅÒÅËÒÙ×ÁÅÔ ÒÁÎÅÅ ÉÓÐÏÌØÚÏ×ÁÎÎÕÀ ÏÐÃÉÀ no-version.

notation-data

Name

notation-data — ÄÏÂÁ×ÉÔØ Ë ÐÏÄÐÉÓÉ ÐÒÉÍÅÞÁÎÉÅ

Synopsis

notation-data *name=value*

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÄÏÂÁ×ÌÑÅÔ Ë ÐÏÄÐÉÓÉ ÐÁÒÕ *name*/*value*. ðÁÒÁÍÅÔÒ *name* ÄÏÌÖÅÎ ÎÁÞÉÎÁÔØÓÑ Ó ÁÌÆÁ×ÉÔÎÏÇÏ ÓÉÍ×ÏÌÁ, ÐÏÓÌÅÄÕÀÝÉÅ ÓÉÍ×ÏÌÙ ÍÏÇÕÔ ÂÙÔØ ÔÁËÖÅ ÃÉÆÒÁÍÉ É ÚÎÁËÁÍÉ ÐÏÄÞÅÒËÉ×ÁÎÉÑ. ðÁÒÁÍÅÔÒ *value* ÍÏÖÅÔ ÂÙÔØ ÌÀÂÏÊ ÐÅÞÁÔÎÏÊ ÓÔÒÏËÏÊ. ïÎÁ ÂÕÄÅÔ ÐÅÒÅÄÁÎÁ × UTF8, ÐÏÜÔÏÍÕ ×ÁÖÎÏ, ÞÔÏÂÙ ÏÐÃÉÑ `charset` ÕÓÔÁÎÁ×ÌÅ×ÁÌÁ ÐÒÁ×ÉÌØÎÕÀ ËÏÄÉÒÏ×ËÕ. åÓÌÉ ÐÁÒÁÍÅÔÒ *name* ÎÁÞÉÎÁÅÔÓÑ ×ÏÓËÌÉÃÁÔÅÌØÎÙÍ ÚÎÁËÏÍ, ÐÒÉÍÅÞÁÎÉÅ ÂÕÄÅÔ ÐÏÍÅÞÅÎÏ ËÁË ËÒÉÔÉÞÅÓËÏÅ (ÓÍ. rfc2440:5.2.3.15).

set-policy-url

Name

`set-policy-url` — set the policy URL for signatures

Synopsis

`set-policy-url` *string*

ïÐÉÓÁÎÉÅ

The parameter *string* is used as the policy URL for signatures (ÓÍ. rfc2440:5.2.3.19). If the string is prefixed with an exclamation mark, the policy URL packet will be flagged as critical.

set-filename

Name

`set-filename` — ÕÓÔÁÎÏ×ÉÔØ ÉÍÑ ÆÁÊÌÁ × ÚÁÛÉ×ÏÏ×ÁÎÎÏÍ ÉÌÉ ÐÏÄÐÉÓÁÎÎÏÍ ÓÏÎÂÝÅÎÉÉ

Synopsis

`set-filename` *`string`*

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *`string`* ÉÓÐÏÌØÚÕÅÔÓÑ ËÁË ÉÍÑ ÆÁÊÌÁ, ÓÏÈÒÁÎÑÅÍÏÅ × ÓÏÎÂÝÅÎÉÉ. õËÁÚÙ×ÁÅÔ ÌÉ ÜÔÏ ÉÍÑ ÆÁÊÌÁ ÐÒÉ ÒÁÓÛÉÆÒÏ×ËÅ ÉÌÉ ÐÒÏ×ÅÒËÅ ÓÏÎÂÝÅÎÉÑ?

use-embedded-filename

Name

`use-embedded-filename` — ÉÓÐÏÌØÚÏ×ÁÔØ ÉÍÑ ÆÁÊÌÁ ÓÏÄÅÒÖÁÝÅÅÓÑ

× ÓÏÏÂÝÅÎÉÉ ÄÌÑ ÓÏÈÒÁÎÅÎÉÑ ÅÇÏ ÔÅËÓÔÏ×ÏÊ ÉÌÉ ÐÒÏ×ÅÒÅÎÎÏÊ ×ÀÓÉÉ

Synopsis

```
use-embedded-filename
```

ïÐÉÓÁÎÉÅ

üÔÕ ÏÐÃÉÀ ÓÌÅÄÕÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ Ó ÏÓÔÏÒÏÖÎÏÓÔØÀ, Ô.Ë. ÏÎÁ ÍÏÖÅÔ ÐÅÒÅÚÁÐÉÓÁÔØ ÓÕÝÅÓÔ×ÕÀÝÉÅ ÆÁÊÌÙ.

max-cert-depth

Name

`max-cert-depth` — ÕÓÔÁÎÏ×ÉÔØ ÍÁËÓÉÍÁÌØÎÕÀ ÄÌÉÎÕ ÓÅÒÔÉÆÉËÁÃÉÏÎÎÏÊ ÃÅÐÏÞËÉ

Synopsis

`max-cert-depth` *n*

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *n* ÕÓÔÁÎÁ×ÌÉ×ÁÅÔ ÍÁËÓÉÍÁÌØÎÕÀ ÄÌÉÎÕ ÃÅÐÏ ÐÒÏ×ÅÒÅÎÎÙÈ ËÌÀÞÅÊ, ÎÁÞÉÎÁÑ Ó ÂÅÚÕÓÌÏ×ÎÏ ÄÏÓÔÁ×ÌÑÅÔ ËÌÀÞÁ, ÄÏ ËÌÀÞÁ, ÄÏÓÔÁ×ÌÑÅÔÓÑ ËÏÔÏÒÏÇÏ ÎÁÄÏ ÐÒÏ×ÅÒÉÔØ. ðÏ ÕÍÏÌÞÁÎÉÀ 5.

digest-algo

Name

`digest-algo` — ÕÓÔÁÎÏ×ÉÔØ ÁÌÇÏÒÉÔÍ ÄÁÊÄÖÅÓÔÁ ÓÏÏÂÝÅÎÉÑ

Synopsis

`digest-algo` *name*

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *name* ÕËÁÚÙ×ÁÅÔ ÁÌÇÏÒÉÔÍ ÄÁÊÄÖÅÓÔÁ ÓÏÏÂÝÅÎÉÑ, ËÏÔÏÒÙÊ ÂÕÄÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ. úÁÐÕÓË gpg Ó ËÏÍÁÎÄÏÊ `version` ×Ù×ÏÄÉÔ ÓÐÉÓÏË ÐÏÄÄÅÒÖÉ×ÁÅÍÙÈ ÁÌÇÏÒÉÔÍ×. úÁÍÅÔÉÍ, ÞÔÏ ÜÔÁ ÏÐÃÉÑ ÍÏÖÅÔ ÐÒÏÉ×ÏÊÔÉ ÔÒÅÂÏ×ÁÎÉÀ OpenPGP ÏÂ ÉÓÐÏÌØÚÏ×ÁÎÉÉ 160-ÂÉÔÎÏÇÏ ÁÌÇÏÒÉÔÍÁ ÄÁÊÄÖÅÓÔÁ ÄÌÑ DSA. äÌÑ ÓÉÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ ÐÏ ÕÍÏÌÞÁÎÉÀ ÉÓÐÏÌØÚÕÅÔÓÑ RIPEMD-160

s2k-cipher-algo

Name

`s2k-cipher-algo` — ÉÓÐÏÌØÚÏ×ÁÔØ ÕËÁÚÁÎÎÙÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ

Synopsis

`s2k-cipher-algo` *name*

ïÐÉÓÁÎÉÅ

éÓÐÏÌØÚÏ×ÁÔØ *name* ËÁË ÁÌÇÏÒÉÔÍ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ ÄÌÑ ÚÁÝÉÔÙ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ. úÁÐÕÓË gpg Ó ËÏÍÁÎÄÏÊ `version` ×Ù×ÏÄÉÔ ÓÐÉÓÏË ÐÏÄÄÅÒÖÉ×ÁÅÍÙÈ ÁÌÇÏÒÉÔÍÏ×. ðÏ ÕÍÏÌÞÁÎÉÀ Blowfish.

s2k-digest-algo

Name

`s2k-digest-algo` — ÕÓÔÁÎÏ×ÉÔØ ÁÌÇÏÒÉÔÍ ÄÁÊÄÖÅÓÔÁ ÓÏÏÂÝÅÎÉÑ ÄÌÑ ÍÁÎÉÐÕÌÑÃÉÉ Ó ËÌÀÞÅ×ÏÊ ÆÒÁÚÏÊ ÚÁÝÉÝÁÀÝÅÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ

Synopsis

```
s2k-digest-algo name
```

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *name* ÚÁÄÁÅÔ ÁÌÇÏÒÉÔÍ ÄÁÊÄÖÅÓÔÁ ÐÒÉÍÅÎÑÅÍÙÊ ÄÌÑ ÍÁÎÉÐÕÌÑÃÉÉ Ó ËÌÀÞÅ×ÏÊ ÆÒÁÚÏÊ. ðÏ ÕÍÏÌÞÁÎÉÀ RIPEMD-160.

s2k-mode

Name

`s2k-mode` — ÕÓÔÁÎ×ÌÉ×ÁÅÔ ÍÅÔÄ ÏÂÒÁÂÏÔËÉ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ

Synopsis

```
s2k-mode n
```

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *n* ÚÁÄÁÅÔ ÞÉÓÌÏ ÏÂÒÁÂÏÔÏË ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ. åÓÌÉ *n* ÒÁ×ÎÏ 0, ÉÓÐÏÌØÚÕÅÔÓÑ ÞÉÓÔÁÑ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ. ðÏ ÕÍÏÌÞÁÎÉÀ ÒÁ×ÅÎ ÏÄÎÏÍÕ. åÓÌÉ ÎÅ ÉÓÐÏÌØÚÏ×ÁÎÁ ÏÐÃÉÑ `rfc1991`, ÜÔÏ ÒÅÖÉÍ ÉÓÐÏÌØÚÕÅÔÓÑ ÔÁËÖÅ ÄÌÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ.

disable-cipher-algo

Name

disable-cipher-algo — ÐÒÅÄÏÔ×ÒÁÔÉÔØ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÓÉÍÍÅÔÒÉ×ÎÏÇÏ ÛÉÆÒÁ

Synopsis

disable-cipher-algo *name*

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *name* ÕËÁÚÙ×ÁÅÔ ÉÍÑ ÓÉÍÍÅÔÒÉ×ÎÏÇÏ ÁÌÇÏÒÉÔÍÁ, ËÏÔÏÒÙÊ ÂÕÄÅÔ ÏÔËÌÀÞÅÎ. åÓÌÉ ÕËÁÚÁÎÎÙÊ ÁÌÇÏÒÉÔÍ ÛÉÆÒÏ×ÁÎÉÑ ÚÁÇÒÕÖÁÅÔÓÑ ÐÏÌØÚÏ×ÁÔÅÌÅÍ, ÏÎ ÎÅ ÂÕÄÅÔ ÏÔËÌÀÞÅÎ.

disable-pubkey-algo

Name

disable-pubkey-algo — ÐÒÅÄÏÔ×ÒÁÔÉÔØ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÛÉÆÒÁ Ó

ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ

Synopsis

```
disable-pubkey-algo name
```

ïÐÉÓÁÎÉÅ

ðÁÒÁÍÅÔÒ *name* ÚÁÄÁÅÔ ÁÌÇÏÒÉÔÍ ÛÉÆÒÏ×ÁÎÉÑ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ËÏÏÐÒÛÊ ÂÕÄÅÔ ÏÔËÌÀÞÅÎ. åÓÌÉ ÕËÁÚÁÎÎÙÊ ÛÉÆÒ ÚÁÇÒÕÖÁÅÔÓÑ ÐÏÓÌÅ ÕËÁÚÁÎÉÑ ÄÁÎÎÏÊ ÏÐÃÉÉ, ÏÎ ÎÅ ÂÕÄÅÔ ÏÔËÌÀÞÅÎ.

throw-keyid

Name

`throw-keyid` — ÎÅ ÐÏÍÅÝÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ËÌÀÞÁ × ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÐÁËÅÔÙ

Synopsis

```
throw-keyid
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÓËÒÙ×ÁÅÔ ÐÌÎÕÞÁÔÅÌÑ ÚÁÛÉÆÒÏ×ÁÎÎÙÈ ÄÁÎÎÙÈ, × ËÁÞÅÓÔ×Å ËÏÎÔÒÏÌÅÒÁ ÐÒÏÔÏÉ× ÁÎÁÌÉÚÁ ÓÅÔÅ×ÏÇÏ ÔÒÁÆÆÉËÁ. ïÎÁ ÚÁÍÅÄÌÑÅÔ ÒÁÓÛÉÆÒÏ×ËÕ, ÏÂÙÞÎÏ, ÔÁË ËÁË × ÈÕÄÛÅÍ ÓÌÕÞÁÅ ÐÒÉÈÏÄÉÔÓÑ ÉÓÐÙÔÙ×ÁÔØ ×ÓÅ ËÌÀÞÉ × ÓÅËÒÅÔÎÏÊ Ó×ÑÚËÅ ÐÎÕÞÁÔÅÌÑ, ÞÔÂÙ ÎÁÊÔÉ ËÌÀÞ ÒÁÓÛÉÆÒÏ×ËÉ.

not-dash-escaped

Name

not-dash-escaped — ÉÚÍÅÎÑÅÔ ÆÏÒÍÁÔ ÐÒÏÚÒÁÞÎÙÈ ÐÏÄÐÉÓÅÊ

Synopsis

```
not-dash-escaped
```

ïÐÉÓÁÎÉÅ

ïÐÃÉÑ ÐÎÅÚÎÁ ÄÌÑ ÐÒÏÚÒÁÞÎÙÈ ÐÏÄÐÉÓÅÊ ÎÁ ÐÁÔÞ ÆÁÊÌÁÈ. óÏÎÂÝÅÎÉÑ ÐÏÄÐÉÓÁÎÎÙÅ ÜÔÉÍ ÓÐÏÓÏÂÏÍ ÎÅ ÍÏÇÕÔ ÂÙÔØ ÏÐÒÁ×ÌÅÎÙ ÜÌÅËÔÒÏÎÎÙÊ ÐÏÞÔÏÊ, Ô.Ë. ÏÀÓÂÁÔÙ×ÁÀÓÑ ×ÓÅ ÐÒÏÂÌÅÍÙ É ËÏÎÃÙ ÓÔÒÏË. ïÐÃÉÑ ÎÅ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÁ ÄÌÑ ÄÁÎÎÙÈ ËÏÔÒÙÅ ÓÏÄÅÒÖÁÔ ÐÑÔÉ ÍÉÎÕÏ× × ÎÁÞÁÌÅ ÓÔÒÏËÉ. éÓÐÏÌØÚÕÅÔÓÑ ÓÐÅÃÉÁÌØÎÁÑ ÓÔÒÏËÁ ÚÁÇÏÌÏ×ËÁ, ÞÔÏÂÙ ÓÏÎÂÝÉÔØ GnuPG, ÞÔÏ ÂÙÌÁ ÉÓÐÏÌØÚÏ×ÁÎÁ ÜÔÁ ÏÐÃÉÑ.

escape-from-lines

Name

`escape-from-lines` — ÉÚÍÅÎÑÅÔ ÓÏÏÂÝÅÎÉÑ ÎÁÞÉÎÁÀÝÉÅÓÑ Ó “From” ÐÒÉ ÐÒÏÚÒÁÞÎÏÊ ÐÏÄÐÉÓÉ

Synopsis

```
escape-from-lines
```

ïÐÉÓÁÎÉÅ

ôÁË ËÁË ÎÅËÏÔÏÒÙÅ ÐÏÞÔÏ×ÙÅ ÐÒÏÇÒÁÍÍÙ ÚÁÍÅÎÑÀÔ “From” × ÎÁÞÁÌÅ ÓÔÒÏËÉ ÍÁ “<From”, ÐÒÉÍÅÎÑÅÔÓÑ ÜÔÁ ÏÐÃÉÑ ÄÌÑ ÕËÁÚÁÎÉÑ gpg ÏÂÒÁÂÁÔÙ×ÁÔØ ÔÁËÉÅ ÓÔÒÏËÉ ÏÔÄÅÌØÎÏ ÐÒÉ ÓÏÚÄÁÎÉÉ ÐÒÏÚÒÁÞÎÙÈ ÐÏÄÐÉÓÅÊ. ÷ÓÅ ÄÒÕÇÉÅ ×ÅÒÓÉÉ PGP ÄÅÌÁÀÔ ÜÔÏ ÔÁËÉÍ ÖÅ ÏÂÒÁÚÏÍ. üÔÁ ÏÐÃÉÑ ÎÅ ×ËÌÀÞÅÎÁ ÐÏ ÕÍÏÌÞÁÎÉÀ, ÐÏÓËÏÌØËÕ ÐÒÏÔÏ×ÏÌÅÞÉÔ rfc2440.

A. GNU Free Documentation License

Version 1.1, March 2000

Copyright (C) 2000 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The

"Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human

modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the

full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any,

be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly

provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have no Invariant Sections, write "with no Invariant Sections" instead of saying which ones are invariant. If you have no Front-Cover Texts, write "no Front-Cover Texts" instead of "Front-Cover Texts being LIST"; likewise for Back-Cover Texts.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.