ïÐÉÓÁÎÉÅ GNU Privacy Guard

ïÐÉÓÁÎÉÅ GNU Privacy Guard

Copyright © 1999 The Free Software Foundation
Copyright © 2000-2002 ðÁ×ÅÌ ûÁÊÄÉ. ðÅÒÅ×ÏÄ. éÓÐÒÁ×ÌÅÎÉÑ É ÄÏÐÏÎÎÅÎÉÑ.

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

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

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

÷ËÌÁÄ × ÓÏÚÄÁÎÉÅ ÄÁÎÎÏÇÏ ÒÕËÏ×ÏÓÔÁ ×ÎÅÓÌÉ, ÔÁËÖÅ, ÍÜÔØÀ ëÏÕÐÌÜÄ (Matthew Copeland), êÏÒÇÅÎ çÒÜÎ (Joergen Grahn), äÜ×ÉÄ á. ÷ÉÌÅÒ (David A. Wheeler).

ðÏÌÎÏÅ ×ÅÒÓÉÀ ÄÁÎÎÏÇÏ ÄÏËÕÍÅÎÔÁ ÍÏÖÎÏ ÎÁÊÔÉ ÎÁ http://www.gnupg.org/docs.html.

1. âÙÓÔÒÙÊ ÓÔÁÒÔ 1
çÅÎÅÒÁÃÉÑ ÎÏ×ÏÊ ÐÁÒÙ ËÌÀÞÅÊ 1
óÏÚÄÁÎÉÅ ÏÔÚÙ×ÁÀÝÅÇÏ ÓÅÒÔÉÆÉËÁÔÁ 3
ïÂÍÅÎ ËÌÀÞÁÍÉ 4
üËÓÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ 4
éÍÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ 4
ûÉÆÒÏ×ÁÎÉÅ 6
çÅÎÅÒÁÃÉÑ ÐÏÄËÌÀÞÁ 6
úÁÛÉÆÒÏ×ÁÎÉÅ É ÒÁÓÛÉÆÒÏ×ÁÎÉÅ ÄÏËÕÍÅÎÔÏ× 7
ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ É ÉÈ ÐÒÏ×ÅÒËÁ 8
ðÒÏÚÒÁÞÎÏ ÐÏÄÐÉÓÁÎÎÙÅ(Clearsigned) ÄÏËÕÍÅÎÔÙ 9
ïÔÄÅÌ£ÎÎÁÑ ÐÏÄÐÉÓØ 9
2. ïÂÝÉÅ ÐÏÎÑÔÉÑ 11
óÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ 11
ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ 12
óÍÅÛÁÎÎÙÅ ÛÉÆÒÙ 13
ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ 13
3. õÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ 16
õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÐÁÒÏÊ ËÌÀÞÅÊ 16
ãÅÌÏÓÔÏÓØ ËÌÀÞÁ 17
äÏÂÁ×ÌÅÎÉÅ É ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ 18
ïÔÚÙ× ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ 19
éÚÍÅÎÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ 21
ðÒÏ×ÅÒËÁ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÅÊ 21
äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ 22
éÓÐÏØÚÏ×ÁÎÉÅ ÄÏ×ÅÒÉÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÏÓÔÉ ËÌÀÞÅÊ 23
òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÅÊ 25
4. åÖÅÄÎÅ×ÎÏÅ ÉÓÐÏØÚÏ×ÁÎÉÅ GnuPG 27
ïÐÒÅÄÅÌÅÎÉÅ ÷ÁÛÉÈ ÔÒÅÂÏ×ÁÎÉÊ Ë ÚÁÝÉÔÅ 27
÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ 28
úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÏÇÏ ËÌÀÞÁ 28
÷ÙÂÏÒ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ É ÉÓÐÏØÚÏ×ÁÎÉÅ ÄÐÏÌÎÉÔÅÌØÎÙÈ ËÌÀÞÅÊ 29
õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅ ÓÅØÀ ÄÏ×ÅÒÉÑ 30
ðÏÓÔÏÄÎÅÉ ÷ÁÛÅ ÓÅÔÉ ÄÏ×ÅÒÉÑ 31
úÁËÌÎÎÏÓÔØ ÉÓÐÏØÚÏ×ÁÎÉÑ GnuPG 32
5. òÁÚÌÉÞÎÙÅ ×ÐÒÏÓÙ 33
îÁÐÉÓÁÎÉÅ ÐÌØÚÏ×ÁÔÅÌØÓÖÄÅÎÉÊ ÉÎÔÅÒÆÅÊÓÁ 33
A. éÚÍÅÎÅÎÉÑ (History) 35
B. GNU Free Documentation License 36
0. PREAMBLE 36
1. APPLICABILITY AND DEFINITIONS 36
2. VERBATIM COPYING 37
3. COPYING IN QUANTITY 37
4. MODIFICATIONS 38
5. COMBINING DOCUMENTS 39
6. COLLECTIONS OF DOCUMENTS 39

7. AGGREGATION WITH INDEPENDENT WORKS....40
8. TRANSLATION....40
9. TERMINATION....40
10. FUTURE REVISIONS OF THIS LICENSE....40
How to use this License for your documents....41

3-1. ðÒÉÍÅÒ ÓÅÔÉ ÄÏ×ÅÒÉÑ.....25

1. âÙÓÔÒÙÊ ÓÔÁÒÔ

GnuPG - ÉÎÓÔÒÕÍÅÎÔ ÄÌÑ ÚÁÝÉÔÙ ËÏÍÍÕÎÉËÁÃÉÊ. ÷ ÜÔÏÊ ÇÌÁ×Å ËÒÁÔËÏ ÏÐÉÓÙ×ÁÀÔÓÑ ÏÓÎÏ×Ù ÒÁÂÏÔÙ Ó GnuPG, ×ËÌÀÐÁÑ ÓÏÚÄÁÎÉÅ ÐÁÒÙ ËÌÀÐÅÊ, ÏÂÍÅÎ ËÌÀÐÁÍÉ É ÉÈ ÐÒÏ×ÅÒËÕ, ÚÁÛÉÆÒÏ×ËÕ É ÒÁÓÛÉÆÒÏ×ËÕ ÄÏËÕÍÅÎÔÏ×, ÚÁ×ÅÒÅÎÉÅ ÄÏËÕÍÅÎÔÏ× ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓØÀ. úÄÅØØ ÎÅ ÏÐÉÓÙ×ÁÀÔÓÑ × ÄÅÔÁÌÑÈ ÐÒÉÎÃÉÐÙ ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÐÏÍ, ÛÉÆÒÏ×ÁÎÉÑ É ÃÉÆÒÏ×ÙÈ ÐÏÄÐÉÓÅÊ, ÜÔÉ ×ÏÐÒÏÓÙ ÒÁÓÍÁÔÒÉ×ÁÀÔÓÑ × ÇÌÁ×Å 2. úÄÅØ, ÔÁËÖÅ, ÎÅ ÒÁÓÍÁÔÒÉ×ÁÀÔÓÑ ÔÏÎËÏÓÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG, ÜÔÉ ×ÏÐÒÏÓÙ ÒÁÓÍÁÔÒÉ×ÁÀÔÓÑ × ÇÌÁ×ÁÈ 3 É 4.

GnuPG ÉÓÐÏÌØÚÕÅÔ ËÒÉÐÔÏÇÒÁÆÉÀ Ó ÏÔËÒÙÔÙÍ ËÌÀÐÏÍ. ëÁÖÄÙÊ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÅÅÔ ÐÁÒÕ ËÌÀÐÅÊ (keypair), ÓÏÓÔÏÑÝÕÀ ÉÚ *ÓÅËÒÅÔÎÏÇÏ (private)* É *ÏÔËÒÙÔÏÇÏ (public)* ËÌÀÐÅÊ. óÅËÒÅÔÎÙÊ ËÌÀÐ Ñ×ÌÑÅÔÑ ÓÅËÒÅÔÎÉ ÐÌØÚÏ×ÁÔÅÌÑ É ÎÅ ÍÏÖÅÔ ÂÙÔØ ÐÒÅÄÁÎ ÄÒÕÇÏÍÕ ÌÉÃÕ, ÎÉ ÐÒÉ ËÁËÉÈ ÏÂÓÔÏÑÔÅÌØÓÔ×ÁÈ. ïÔËÒÙÔÙÊ ËÌÀÐ ÐÒÅÄÁÅÔÓÑ ×ÓÅÍ ÌÀÄÑÍ, Ó ËÏÔÏÒÙÍÉ ÐÌØÚÏ×ÁÔÅÌØ ÂÕÄÅÔ ÏÂÍÅÎÉ×ÁÔØÓÑ ÓÏÂÝÅÎÉÑÍÉ. GnuPG ÉÓÐÏÌØÚÕÅÔ ÎÅÓÉÍÍÅËÌÅ ÂÎÅÅ ÈÉÔÒÏÎÕÀ ÓÈÅÍÕ, ÐÒÉ ËÏÔÒÏÊ ÐÌØÚÏ×ÁÔÅÌØ ÉÍÅÅÔ ÐÁÒÕ ÐÕÂÌÉÞÎÏÇÏ É ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÅÊ É, ×ÚÍÏÖÎ, ÄÏÐÏÌÎÉÔÅÌØÎÏÊ ÎÅÓÅÌØËÏ ÐÏÄÐÉÓÅÊ. ðÅÒ×ÉÞÎÁÑ É ÐÏÄÐÉÓÁÎÎÙÅ ÐÁÒÙ ÏÂßÄÉÎÅÎÙ, ÄÌÑ ÕÐÒÏÝÅÎÉÑ ÉÈ ÉÓÐÏÌØÚÏ×ÁÎÑ, É ÜÔÁ Ó×ÑÚÅÁ, ÚÁÞÁÓÔÒÀ, ÍÖÅÔ ÒÁÓÍÁÔÒÉ×ÁÔØÓÑ ÐÒÏÓÔÏ, ËÁË ÏÄÎÁ ÐÁÒÁ ËÌÀÞÅÊ.

çÅÎÅÒÁÃÉÑ ÎÏ×ÏÊ ÐÁÒÙ ËÌÀÞÅÊ

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

```
alice% gpg --gen-key
gpg (GnuPG) 1.2.0; Copyright (C) 2002 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)
   (5) RSA (sign only)
Your selection?
```

GnuPG ÍÏÖÅÔ ÓÏÚÄÁ×ÁÔØ ÎÅÓËÏÌØËÏ ÒÁÚÎÙÈ ÔÉÐÏ× ËÌÀÞÅÊ, ÎÏ ÐÅÒ×ÉÞÎÕÊ ËÌÀÞ ÄÏÌÖÅÎ ÂÙÔØ ÐÒÉÇÏÄÅÎ ÄÌÑ ÓÏÚÄÁÎÉÑ ÐÏÄÐÉÓÉ (signature). ðÏÜÔÏÍÕ ÅÓÔØ ÔÏÌØËÏ ÞÅÔÙÒÅ ×ÁÒÉÁÎÔÁ. ÷ÁÒÉÁÎÔ 1 ÓÏÚÄÁÅÔ Ä×Å ÐÁÒÙ ËÌÀÞÅÊ. DSA - ÐÅÒ×ÉÞÎÁÑ, ÉÓÐÏÌØÚÕÅÍÁÑ ÔÏÌØËÏ ÄÌÑ ÐÏÄÐÉÓÉ. ElGamal - ÐÏÄÞÉÎÎÁÑ, ÉÓÐÏÌØÚÕÅÍÁÑ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ÷ÁÒÉÁÎÔ 2 ÐÏÈÏÖ, ÎÏ ÓÏÚÄÁÅÔ ÔÏÌØËÏ ÐÁÒÕ DSA, ËÏÔÏÒÁÑ ÎÅ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ÷ÁÒÉÁÎÔ 5 ÓÏÚÄÁ£Ô ÐÁÒÕ RSA, ËÏÔÏÒÁÑ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÔÏÌØËÏ ÄÌÑ ÐÏÄÐÉÓÉ. ÷ ÌÀÂÏÍ ÓÌÕÞÁÅ, ÐÏÚÔÅ ÍÏÖÎÏ ÓÏÚÄÁÔØ ÄÐÏÌÎÉÔÅÌØÎÙÅ ÐÁÒÙ ËÌÀÞÅÊ ÄÌÑ ÐÏÄÐÉÓÉ É ÛÉÆÒÏ×ÁÎÉÑ. îÁÉÂÏÌÅÅ ÕÄÁÞÎÙÍ, ÐÏÓÁÌÕÊ, Ñ×ÌÑÅÔÓÑ ×ÁÒÉÁÎÔ 5.

ôÁËÖÅ ÷Ù ÄÏÌÖÎÙ ×ÙÂÒÁÔØ ÒÁÚÍÅÒ ËÌÀÞÁ. òÁÚÍÅÒ ËÌÀÞÁ DSA ÄÏÌÖÅÎ ÂÙÔØ ÍÅÖÄÕ 512 É 1024 ÂÉÔ. ëÌÀÞÉ ElGamal É RSA ÍÏÇÕÔ ÉÍÅØ ÌÀÂÏÊ ÒÁÚÍÅÒ. GnuPG ÎÅ ÄÐÕÓËÁÅÔ ÄÌÉÎÕ ËÌÀÞÅÊ ÍÅÎÅÅ 768 ÂÉÔ. åÓÌÉ ÷Ù ×ÛÒÁÌÉ ×ÁÒÉÁÎÔ 1, ÔÏ ÒÁÚÍÅÒ DSA ËÌÀÞÁ ÐÏÌÕÞÁÅÔÓÑ ÒÁ×ÎÙÍ 1024 ÂÉÔÁÍ É ÚÁÐÒÁÛÉ×ÁÅÔÓÑ ÔÏÌØËÏ ÒÁÚÍÅÒ ËÌÀÞÁ ElGamal.

```
Your selection? 1
DSA keypair will have 1024 bits.
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 ÂÏÌØÛÕÀ ÚÁÝÉÔÕ ÏÔ ×ÚÌÍÁ, ÎÏ ÒÁÚÍÅÒ ÐÏ ÕÍÍÌÞÁÎÉÀ ÄÏÓÔÁÔÏÞÅÎ ÐÒÁËÔÉÞÅÓËÉ ÄÌÑ ÌÀÂÙÈ ÃÅÌÅÊ. âÏÌØÛÁÑ ÄÌÉÎÁ ËÌÀÞÁ ÚÁÍÅÄÌÑÅÔ ÚÁÛÉÆÒÏ×ËÕ É ÒÁÓÛÉÆÒÏ×ËÕ É ÍÏÖÅÔ ÏÔÒÁÚÉÔØÓÑ ÎÁ ÄÌÉÎÅ ÐÏÄÐÉÓÅÊ. òÁÚÍÅÒ ËÌÀÞÁ ÎÅÌØÚÑ ÂÕÄÅÔ ×ÐÏÓÌÄÓÔ×ÉÉ ÉÚÍÅÎÉÔØ.

îÁËÏÎÅÃ, ÷Ù ÄÏÖÎÙ ÕËÁÚÁÔØ ÓÒÏË ÄÅÉÓ×ÉÑ ËÌÀÞÁ. ÷ ÓÌÕÞÁÅ ×ÁÒÉÁÎÔÁ 1, ÕËÁÚÁÎÎÙÊ ÓÒÏË ÉÓÐÌØÚÕÅÔÓÑ 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×ÁÔÅÌÅ ÐÏÄÏËÄÅÔ ÂÅÓÓÒÏÞÎÙÊ ËÌÀÞ. óÒÏË ÄÅÊÓÔ×ÉÑ ÓÌÅÄÕÅÔ ×ÙÂÉÒÁÔØ Ó ÏÓÕÝÅÓÔÌÑÅÔÓØÀ; ÈÏÔÑ ÍÏÖÎÏ ÉÚÍÅÎÉÔØ ÓÒÏË ÄÅÊÓÔ×ÉÑ ÐÏÓÌÅ ÓÏÚÄÁÎÉÑ ËÌÀÞÁ, ÎÅ ÉÓËÌÀÞÅÎÙ ÐÒÏÂÌÅÍÙ Ó ÐÅÒÄÁÐÅÊ ÉÚÍÅÎÅÎÉÊ ÔÅÍ ÐÏØÚÏ×ÁÔÅÌÑÍ, Õ ËÏÔÏÒÙÈ ÕÖÅ ÉÍÅÅÔÓÑ ÷ÁÛ ÏÔËÒÙÔÙÊ ËÌÀÞ.

÷ ÄÏÐÏÎÅÎÉÅ Ë ÐÁÒÁÍÅÔÒÁÍ ËÌÀÞÁ, ÷Ù ÄÏÖÎÙ ÕËÁÚÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏØÚÏ×ÁÔÅÌÑ. éÄÅÎÔÉÆÉËÁÔÏÒ ÎÕÖÅÎ, ÞÔÏÂÙ Ó×ÑÚÁÔØ ÓÏÚÄÁÎÎÙÊ ËÌÀÞ Ó ËÏÎËÒÅÔÎÙÍ ÌÉÃÎÍ.

```
You need a User-ID to identify your key; the software constructs the user id
from Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Alice
Email address: alice@wonderland.uk
Comment: test key
You selected this USER-ID:
    "Alice (test key) <alice@wonderland.uk>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
```

ðÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÓÏÚÄÁÅÔÓÑ ÔÏÌØËÏ ÏÄÎÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÎÏ ×ÏÚÍÏÖÎÏ ÓÏÚÄÁÎÅÅ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ×, ÅÓÌÉ ÷Ù ÈÏÔÉÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ ËÌÀÞ × ÎÁÓËÏÌØËÉÈ ËÏÎÔÅËÓÔÁÈ; ÎÁÐÒÉÍÅÒ, ËÁË ÉÎÔÅÎÅÒ Î× ÒÁÂÏÔÅ É ËÁË ÐÏÌÉÔÉÞÅÓËÉÊ ÄÅÑÔÅÌØ ÐÏÓÌÅ ÎÅÅ. éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏØÚÏ×ÁÔÅÌÑ ÎÅ ÍÏÖÅÔ ÂÙÔØ ÏÔÒÅÄÁÊÔÉÒÏ×ÁÎ ÐÏÓÌÅ ÓÏÚÄÁÎÉÑ.

GnuPG ÚÁÐÒÏÓÉÔ ÐÁÒÏÌØ ÄÌÑ ÚÁÝÉÔÙ ÐÅ×ÉÞÎÏÇÏ É ÐÏÄÐÉÓÅÎÎÏÇÏ ÓÅËÒÅÔÎÙÈ ËÌÀÞÅÊ, ËÏÔÏÒÙÅ ÷Ù ÂÕÄÅÔÅ ÄÅÒÖÁÔØ × ÎÅÄÏÓÕÐÎÏÍ 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 ÏÐÅÒÁÔÏÒÁ GnuPG (É ÄÒÕÇÉÈ ÓÉÓÔÅÍÁÈ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ), Ô.Ë. ÜÔÏ ÷ÁÛÁ ÅÄÉÎÓ×ÅÎÎÁÑ ÚÁÝÉÔÁ × ÓÌÕÞÁÅ, ÅÓÌÉ ÷ÁÛ ÓÅËÒÅÔÙÊ ËÌÀÞ ÐÏÐÁÄÅÔ × ÞÕÖÉÅ ÒÕËÉ. îÅ ÓÌÅÄÕÅÔ ÂÒÁÔØ ÓÏÏ×Á ÉÚ âóü, ÞÅÒÅÄÕÊÔÅ ÒÅÇÉÓÔ ÂÕË× É ÉÓÐÏÌØÚÕÊÔÅ ÎÅÁÌÆÁ×ÉÔÎÅ ÓÉÍ×ÏÌÙ. èÏÒÏÛÉÊ ÐÁÒÏÌØ ËÒÉÔÉÞÅÎ ÄÌÑ ÎÁÄÅÖÎÏÓÔÉ GnuPG.

ðÏÓÌÅ ÜÔÏÇÏ GnuPG ÇÅÎÅÒÉÒÕÅÔ ËÌÀÞ. ÷ ÓÌÕÞÁÅ ÅÓÌÉ × ÷ÁÛÅÊ ÓÉÓÔÅÍÅ ÎÅ ÏÐÅÎØ ÈÏÒÏÛÉÊ ÇÅÎÅÒÁÔÏÒ ÓÌÕÞÁÊÎÙÈ ÞÉÓÅÌ, ÐÒÏÃÅÄÕÒÁ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÍÏÅÔ ÚÁÎÑÔØ ÄÏ×ÌØÎÏ ÍÍÏÇÏ ×ÒÅÍÅÎÉ. ÷ ÎÅËÏÔÏÒÙÈ ÓÌÕÞÁÑÈ ÐÏÍÇÁÅÔ ÛÅ×ÅÌÎÉÅ ÍÙÛËÏÊ, × ÎÅËÏÔÏÒÙÈ ÎÁÓÔÒÏÊËÁ ÓÉÓÔÅÍÙ.

óÏÚÄÁÎÉÅ ÏÔÚÙ×ÁÝÅÇÏ ÓÅÒÔÉÆÉËÁÔÁ

ðÏÓÌÅ ÓÏÚÄÁÎÉÑ ÐÁÒÙ ËÌÀÞÅÊ, ÷ÁÍ ÓÌÅÄÕÅÔ ÓÏÚÄÁÔØ ÏÔÚÙ×ÁÝÉÊ 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×ÅÄÏÌÅÎÉÑ Ï ÔÏÍ, ÞÔÏ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÅÌØÚÑ ÂÏÌØÛÅ ÉÓÐÏÌØÚÏ×ÁÔØ. ïÔÚ×ÁÎÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÓÄÅÌÁÎÎÙÈ ÷ÁÍÉ ÐÏÄÐÉÓÅÊ É ÄÁÌØÛÅ, ÎÏ ÎÅ ÎÏÓÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÓÏÏÂÝÅÎÉÊ ÄÌÑ ÷ÁÓ. ðÒÉ ÜÔÏÍ, ÷Ù ÓÏÈÒÁÎÑÅÅ ×ÏÚÍÏÖÎÏÓÔØ ÒÁÓÛÉÆÒÏ×ÁÔØ ÷ÁÍ ÓÏÏÂÝÅÎÉÊ, ÐÒÉ ÎÁÌÉÞÉÉ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ.

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

áÒÇÕÍÅÎÔ **`mykey`** - ÉÄÅÎÔÉÆÉËÁÔÏÒ ÷ÁÛÅÊ ÐÒ×ÉÞÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ ÉÌÉ ÌÀÂÁÑ ÞÁÓÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÌØÚÏ×ÁÔÅÌÑ ÷ÁÛÅÊ ÐÁÒÙ ËÌÀÞÅÊ. óÇÅÎÅÒÉÒ×ÁÎÎÙÊ ÓÅÒÔÉÆÉËÁÔ ÂÕÄÅÔ ÓÏÈÒÁÎÅÎ × ÆÁÊÌÅ *`revoke.asc`*. åÓÌÉ ÏÐÃÉÑ `--output` ÏÐÕÝÅÎÁ, ÒÅÚÕÌØÔÁÔ ÐÏÍÝÅÝÅÔÓÑ × ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ. ëÒÏÍÅ ÔÏÇÏ, GnuPG ÚÁÐÒÁÛÉ×ÁÅÔ ÐÒÉÞÉÎÕ ÇÅÎÅÒÁÃÉÉ ÏÔÚÙ×ÁÝÅÇÏ ÓÅÒÔÉÆÉËÁÔÁ.

```
alice% gpg --output revoke.asc --gen-revoke alice@wonderland.uk

sec  1024R/B115BDB6 2002-05-01   Alice (test key) <alice@wonderland.uk>

Create a revocation certificate for this key? y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 1
Enter an optional description; end it with an empty line:
>
Reason for revocation: Key has been compromised
(No description given)
Is this okay? y
```

÷Ù ÍÏÖÅÔÅ ×Ù×ÅÓÔÉ ÓÅÒÔÉÆÉËÁÔ ÎÁ ÐÒÉÎÔÅÒ É ÈÒÁÎÉÔØ ÅÇÏ ÇÄÅ-ÎÉÂÕÄØ × ÎÁÄÅÖÎÏÍ ÍÅÓÔÅ (ÂÁÎËÏ×ÓËÉÊ ÓÂÏÒ). åÓÌÉ ÓÅÒÔÉÆÉËÁÔ ÐÏÐÁÄÅÔ × ÞÕÖÉÅ ÒÕËÉ É ÂÕÄÅÔ ÏÐÕÂÌÉËÏ×ÁÎ, ÔÏ ÏÔËÒÙÔÙÊ ËÌÀÞ ÕÔÒÁÔÉÔ Ó×ÏÅ ÄÅÉÓ×ÉÌ.

ïÂÍÅÎ ËÌÀÞÁÍÉ

äÌÑ ÏÂÝÅÂÍÉÑ Ó ËÅÍ-ÌÉÂÏ, ×Ù ÄÏÌÖÎÙ ÏÂÍÅÎÑÔØÓÑ ËÌÀÞÁÍÉ. ðÒÏÓÍÏÔÒÅÔØ ÓÐÉÓÏË ÉÍÅÀÝÉÈÓÑ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ, ÍÏÖÎÏ ÉÓÐÏÌØÚÕÑ ËÏÍÁÎÄÕ `--list-keys`.

```
alice% gpg --list-keys
/home/alice/.gnupg/pubring.gpg
------------------------------------
pub  1024R/B115BDB6 2002-05-01 Alice (test key) <alice@wonderland.uk>
```

üËÓÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ

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

```
alice% gpg --output alice.gpg --export alice@wonderland.uk
```

ëÌÀÞ ÜËÓÐÏÒÔÉÒÕÅÔÓÑ × Ä×ÏÉÞÎÍÍ ÆÏÒÍÁÔÅ, ÞÔÏ ÂÙ×ÁÅÔ ÎÅÕÄÏÂÎÏ. GnuPG ÉÍÅÅÔ ÏÐÃÉÀ ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÉ ÕËÁÚÙ×ÁÅÔ ÎÁ ÎÅÏÂÈÏÄÉÍÏÓÔØ ×Ù×ÏÄÁ × ÆÏÒÍÁÔÅ ASCII. ðÒÁËÔÉÞÅÓËÉ ÌÀÂÏÊ ×Ù×ÏÄ GnuPG, Ô.Å. ËÌÀÞÉ, ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÏËÕÍÅÎÔÙ, ÐÏÄÐÉÓÉ, ÍÏÖÅÔ ÐÒÏÉÓÈÏÄÉÔØ × ÆÏÒÍÁÔÅ ASCII.[1]

```
alice% gpg --armor --export alice@wonderland.uk
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.0 (FreeBSD)

mIsEPNAu8wEEALf1zGv9/bkEKL1fTpkr0lvsmtK5Frgymlk7uInWfFdoucjAci9t
wyU8HXNdFNCx1utWT5GNDD1aDhiFukc7UrFVuVbAjtOikFrZ939RrLKqOEoVd8XI
ZXbgiSjs2ZqG32PpB+9X+3Z4OM64tna0NTvyqYP9LtOPHZpYGHwd5McfAAYptCZB
bGljZSAodGVzdCBrZXkpIDxhbGljZUB3b25kZXJsYW5kLnVrPoiyBBMBAgAcBQI8
0C7zAhsDBAsHAwIDFQIDAxYCAQIeAQIXgAAKCRDHOpmHsRW9tvsYBACmRyUoCnj5
Awh/bFTcmsZi687ec4EzCby8OF586FAQSj4HX4LvAUc/u+4NHVbQRkKW2RJVnaHv
YHUmjgteywMN3YqKd80/fbWIjyIgKNY+vgSEPMwiNMo6hR1frtfTMBnmwIWADMn0
3I1kxP2GfreSCHgy+FA3k5lrxvFnZwkXcA==
=RowZ
-----END PGP PUBLIC KEY BLOCK-----
```

éíÐÏÒÔ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ

ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÄÏÂÁ×ÌÅÎ Ë Ó×ÑÚÅÁ ÷ÁÛÉÈ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÐÒÉ ÐÏÍÝÉ ËÏÍÁÎÄÙ `--import`.

```
alice% gpg --import blake.asc
gpg: key 01A1FE63: public key "Blake (dumb) <blake@anywhere.ru" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
alice% gpg --list-keys
/home/alice/.gnupg/pubring.gpg
------------------------------------
pub  1024R/B115BDB6 2002-05-01 Alice (test key) <alice@wonderland.uk>

pub  1024R/01A1FE63 2002-05-01 Blake (dumb) <blake@anywhere.ru>
sub  1024R/526C7F7F 2002-05-01 [expires: 2003-05-01]
```

äÏÓÔÏ×ÅÒÎÏÓÔØ ÉÍÐÏÒÔÉÒÏ×ÁÎÎÏÇÏ ËÌÀÞÁ ÄÎÌÖÎÁ ÂÙÔØ ÐÏÄÔ×ÅÒÖÄÅÎÁ. GnuPG ÉÓÐÏÌØÚÕÅÔ ÇÉÂËÕÀ É ÍÏÝÎÕÀ ÍÏÄÅÌØ ÐÒÏ×ÅÒËÉ ÐÏÀÍÉÎÎÏÓÔÉ, ÎÅ ÔÒÅÂÕÀÝÕÀ, ÞÔÏÂÙ ÷Ù ÌÉÞÎÏ ÐÒÏ×ÅÒÑÌÉ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÁÖÄÏÇÏ ÉÍÐÏÒÔÉÒÏ×ÁÎÎÏÇÏ ËÌÀÞÁ. ôÅÍ ÎÅ ÍÅÎÅÅ, ÄÏÓÔÏ×ÅÒÎÏÓÔØ ÎÅËÏÔÏÒÙÈ ËÌÀÞÅÊ ÷ÁÍ ÐÒÉÄÅÔÅÓÑ ÐÒÏ×ÅÒÎÔØ ÓÁÍÏÍÕ. óÎÁÞÁÌÁ ÐÒÏ×ÅÒÑÅÔÅ ÎÏÐÅÐÁÔÏË (fingerprint) ËÌÀÞÁ, ÚÁÔÅÍ ËÌÀÞ ÚÁ×ÅÒÑÅÔÅ ÐÏÄÐÉÓØÀ, ÄÌÑ ÐÏÄ×ÅÒÖÄÅÎÉÑ ÔÏÇÏ, ÞÔÏ ÏÎ ÄÏÓÔÏ×ÅÒÅÎ. ïÔÐÅÞÁÔÏË ËÌÀÞÁ ÍÏÖÏ ÂÙÓÔÒ ÐÒÏÓÍÏÔÒÅÔ ËÏÍÁÎÄÏÊ `--fingerprint`.

```
alice% gpg --fingerprint alice@wonderland.uk
pub  1024R/B115BDB6 2002-05-01 Alice (test key) <alice@wonderland.uk>
     Key fingerprint = DE49 CDEF 12A3 8B7B 272B  A572 C73A 9987 B115 BDB6

alice% gpg --fingerprint
/home/test/.gnupg/pubring.gpg
------------------------------
pub  1024R/B115BDB6 2002-05-01 Alice (test key) <alice@wonderland.uk>
     Key fingerprint = DE49 CDEF 12A3 8B7B 272B  A572 C73A 9987 B115 BDB6

pub  1024R/01A1FE63 2002-05-01 Blake (dumb) <blake@anywhere.ru>
     Key fingerprint = 80B8 1955 7D68 FE4F D882  DAD1 D85C 124A 01A1 FE63
sub  1024R/526C7F7F 2002-05-01 [expires: 2003-05-01]
```

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

ðÏÓÌÅ ÐÒÏ×ÅÒËÉ ÎÔÐÅÞÁÔËÏ× ÷Ù ÍÏÖÅÔÅ ÐÏÄÐÉÓÁÔØ ËÌÀÞ. ôÁË ËÁË ÐÒÏ×ÅÒËÁ ÓÌÁÂÏÅ Ú×ÅÎÏ × ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÔÏ ÷Ù ÄÎÌÖÎÙ ÂÙÔØ ÓÏ×ÅÒÛÅÎÎÏ Õ×ÅÒÅÎÙ × ËÌÀÞÅ ÐÅÒÅÄ ÔÅÍ, ËÁË ÅÇÏ ÐÏÄÐÉÓÙ×ÁÔØ, É ×*ÓÅÇÄÁ* ÐÒÏ×ÅÑÊÔÅ ÏÔÐÅÞÁÔËÉ.

äÌÑ ÐÏÄÐÉÓÉ ËÌÀÞÁ ÎÅÏÂÈÏÄÉÍÏ ÐÅÒÅÊÔÉ × ÒÅÖÉÍ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ ËÌÀÞÁ ÐÒÉ ÐÏÍÏÝÉ ËÏÍÁÎÄÙ `--edit-key`.

```
alice% gpg --edit-key blake@anywhere.ru

pub  1024R/01A1FE63  created: 2002-05-01 expires: never      trust: -/-
sub  1024R/526C7F7F  created: 2002-05-01 expires: 2003-05-01
(1). Blake (dumb) <blake@anywhere.ru>

Command> sign

pub  1024R/01A1FE63  created: 2002-05-01 expires: never      trust: -/-
 Primary key fingerprint: 80B8 1955 7D68 FE4F D882  DAD1 D85C 124A 01A1 FE63

     Blake (dumb) <blake@anywhere.ru>

How carefully have you verified the key you are about to sign actually belongs
to the person named above?  If you don't know what to answer, enter "0".

   (0) I will not answer. (default)
   (1) I have not checked at all.
   (2) I have done casual checking.
   (3) I have done very careful checking.

Your selection? 3
Are you really sure that you want to sign this key
```

```
with your key: "Alice (test key) <alice@wonderland.uk>"

Really sign? y
```

GnuPG ÐÏÉÎÔÅÒÅÓÕÅÔÓÑ ÎÁÓËÏÌØËÏ ÔÝÁÔÅÌØÎÏ ÷Ù ÐÒÏ×ÅÒÉÌÉ ÄÏÓÔ×ÅÒÎÓÔØ ËÌÀÞÁ É ÐÏÐÒÏÓÉÔ ÐÏÄ×ÅÒÄÉÔØ ÷ÁÛÅ ÖÅÌÁÎÉÅ ÐÏÄÐÉÓÁÔØ ËÌÀÞ. ðÏÄÉÓÁ× ËÌÀÞ, ÷Ù ÍÏÖÅÔÅ ÐÒÏÍÏÔÒÅÔØ ÓÐÉÓÏË ÐÏÄÐÉÓÅÊ ÎÁ ËÌÀÞÅ É Õ×ÉÄÅÔØ ÔÁÍ ÄÏÂÁ×ÌÅÎÎÕÀ ÷ÁÍÉ. ëÁÖÄÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ËÌÀÞÁ ÐÏÄÐÉÓÁÎ ÓÁÍÉÍ ËÌÀÞÏÍ É ËÌÀÞÏÍ ËÁÖÄÏÇÏ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÚÁ×ÅÒÉ×ÛÅÇÏ ÜÔÏÔ ËÌÀÞ.

```
Command> check
uid  Blake (dumb) <blake@anywhere.ru>
sig!3       01A1FE63 2002-05-01   [self-signature]
sig!        B115BDB6 2002-05-01   Alice (test key) <alice@wonderland.uk>
```

ûÉÆÒÏ×ÁÎÉÅ

çÅÎÅÒÁÃÉÑ ÐÏÄËÌÀÞÁ.

åÓÌÉ ÷Ù ÐÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ×ÙÂÒÁÌÉ ×ÁÒÉÁÎÔ 2 (DSA) ÉÌÉ 5 (RSA), ÔÏ ÉÍÅÀÝÉÊÓÑ Õ ÷ÁÓ ËÌÀÞ ÍÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÔÏÌØËÏ ÄÌÑ ÐÏÄÐÉÓÉ. äÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÷ÁÛÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÍÏÇÌÉ ÚÁÛÉÆÒÏ×Ù×ÁÔØ ÎÁÐÒÁ×ÌÑÅÍÙÅ ÷ÁÍ ÓÏÏÂÝÅÎÉÑ, ÎÅÏÂÈÏÄÉÍÏ ÓÏÚÄÁÔØ ÄÐÐÏÎÉÔÅÌØÎÙÊ ËÌÀÞ, ËÏÔÏÒÙÊ ÍÏÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. çÅÎÅÒÁÃÉÑ ÄÐÐÏÎÉÔÅÌØÎÏÇÏ ËÌÀÞÁ ÏÓÕÝÅÓÔ×ÌÑÅÔÓÑ × ÒÅÖÉÍÅ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ.

```
alice%gpg --edit-key alice@wonderland.uk
Secret key is available.

pub  1024R/B115BDB6  created: 2002-05-01 expires: never      trust: u/u
(1). Alice (test key) <alice@wonderland.uk>

Command> addkey
Key is protected.

You need a passphrase to unlock the secret key for
user: "Alice (test key) <alice@wonderland.uk>"
1024-bit RSA key, ID B115BDB6, created 2002-05-01

Please select what kind of key you want:
   (2) DSA (sign only)
   (3) ElGamal (encrypt only)
   (5) RSA (sign only)
   (6) RSA (encrypt only)
Your selection?
```

åÓÌÉ ÷Ù ÎÁÍÅÒÅÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ ÐÏÄËÌÀÞ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ, ÔÏ ÓÌÅÄÕÅÔ ×ÙÂÒÁÔØ ×ÁÒÉÁÎÔ 3 ÉÌÉ 6.

```
Your selection? 6
What keysize do you want? (1024)
Requested keysize is 1024 bits
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)
Key does not expire at all
Is this correct (y/n)? y
Really create? y
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++
..+++++

pub  1024R/B115BDB6  created: 2002-05-01 expires: never      trust: u/u
sub  1024R/89D3ED33  created: 2002-05-03 expires: never
(1). Alice (test key) <alice@wonderland.uk>

Command> save
```

îÅÔÒÕÄÎÏ ÚÁÍÅÔÉÔØ, ÞÔÏ × ÓÐÉÓËÅ ËÌÀÞÅÊ ÐÏÑ×ÉÌÓÑ ×ÔÏÒÏÊ ËÌÀÞ. äÌÑ ÔÏÇÏ, ÞÔÏÂÙ ×ÙÊÔÉ ÉÚ ÒÅÖÍÁ ÒÅÄÁÉÔÏÒ×ÁÎÉÑ, ÓÏÈÒÁÎÉ× ÉÚÍÅÎÅÎÉÑ, ×ÏÓÐÌÏØÚÕÊÔÅÓØ ËÏÍÁÎÄÏÊ save.

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 ÐÒÅÄÓÔÁ×ÉÔØ ËÁË ÏÔËÒÙÔÙÊ ÓÅÊÆ. ëÏÇÄÁ ËÏÒÒÅÓÐÏÎÄÅÎÔ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÎÂÝÅÎÉÅ ÐÒÉ ÐÏÍÝÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÜÔÏ ÓÏÎÂÝÅÎÉÅ ÐÍÅÝÁÅÔÓÑ × ÓÅÆÆ É ÓÅÆÆ ÚÁÉÒÙ×ÁÅÔÓÑ. óÏÎÔ×ÅÔÓ×ÕÀÝÉÊ ÚÁËÒÙÔÙÊ ËÌÀÞ - ËÏÍÂÉÎÁÃÉÑ, ÎÅÏÂÈÏÄÉÍÁÑ ÄÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÏÔËÒÙÔØ ÓÅÆÆ É ÐÏÎÕÞÉÔØ ÄÏËÕÍÅÎÔ. äÒÕÇÉÍÉ ÓÌ×ÁÍÉ, ÔÏÌØËÏ ÏÂÌÁÄÁÔÅÌØ ÚÁËÒÙÔÏÇÏ ËÌÀÞÁ ÍÏÖÅÔ ×ÍÓÓÔÁÎÏ×ÉÔØ ÄÏËÕÍÅÎÔ, ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÓÏÎÔ×ÅÔÓ×ÕÀÝÉÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ.

åÓÌÉ ÷Ù ÈÏÔÉÔÅ ÐÏÓÁÔØ ÓÏÎÂÝÅÎÉÅ ÄÒÕÇÕ, ÔÏ ÚÁÛÉÆÒÏ×Ù×ÁÅÔÅ ÅÇÏ ÐÒÉ ÐÏÍÝÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÄÒÕÇÁ, Á ÔÏÔ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ ÅÇÏ ÐÒÉ ÐÏÍÝÉ Ó×ÏÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ. åÓÌÉ ÄÒÕÇ ÚÁÈÏÞÅÔ ÷ÁÍ ÏÔ×ÅÔÔØ, ÔÏ ÏÎ ÚÁÛÉÆÒÕÅÔ ÏÔ×ÅÔ ÐÒÉ ÐÏÍÝÉ Ó×ÏÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, Á ÷Ù ÒÁÓÛÉÆÒÕÅÔÅ ÅÇÏ Ó×ÏÉÍ ÓÅËÒÅÔÎÙÍ.

äÌÑ ÚÁÛÉÆÒÏ×ÁÎÉÑ ÄÏËÕÍÅÎÔÁ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--encrypt`. ÷Ù ÄÏÌÖÎÙ ÉÍÅÔØ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÐÒÄÐÏÌÁÇÁÅÍÙÈ ÐÏÔÐ�previous ÐÒÅÄÁÔÅÌÅÊ. ðÒÏÇÒÁÍÍÁ ÏÓÉÄÁÅÔ × ËÁÞÁÓÔ×Å ÐÁÒÁÍÅÔÒÁ ÉÍÑ ÛÉÆÒÕÅÍÏÇÏ ÄÏËÕÍÅÎÔÁ ÉÌÉ, × ÓÌÕÞÁÅ ÅÇÏ ÏÓÕÔÓÔÓ×ÉÑ, ÛÉÆÒÕÅÔ ÓÔÁÎÄÁÒÔÙÊ ××ÏÄ. úÁÛÉÆÒÏ×ÁÎÎÙÊ ÒÅÚÙÌØÔÁÔ ÐÏÍÝÁÅÔÓÑ × ÓÔÁÎÄÁÒÔÙÊ ×Ù×ÏÄ, ÅÓÌÉ ÎÅ ÕËÁÚÁÎ ÏÐÃÍÑ `--output`. äÌÑ ÐÏ×ÙÛÅÎÑ ÚÁÝÉÛÙ ÄÏËÕÍÅÎÔ ÄÐÏÎÍÉÔÅÌØÎÏ ÓÖÉÍÁÅÔÓÑ.

```
alice% gpg --output message.gpg --encrypt --recipient blake@anywhere.ru message.txt
```

ïÐÃÍÑ `--recipient` ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ËÁÖÄÏÇÏ ÐÏÌÕÞÁÔÅÌÑ É ÉÍÅÅÔ ÁÒÇÕÍÅÎÔ, ÉÄÅÎÔÉÆÉÃÉÒÕÀÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, ËÏÔÏÒÙÍ ÄÏÌÖÅÎ ÂÙÛØ ÚÁÛÉÆÒÏ×ÁÎ ÄÏËÕÍÅÎÔ. úÁÛÉÆÒÏ×ÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÍÖÅÔ ÂÙÛØ ÒÁÓÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÔÅÍ, ÞÅÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÓÏÎÔ×ÅÔÓ×ÕÅÔ ÏÄÎÏÍÕ ÉÚ ÕËÁÚÁÎÎÙÈ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ. ÷ ÞÁÓÔÎÏÓÔÉ, ÷Ù ÎÅ

ÍÏÖÅÔÅ ÒÁÓÛÉÆÒÏ×ÁÔØ ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÷ÁÍÉ ÄÏËÕÍÅÎÔ, ÅÓÌÉ ÎÅ ×ËÌÀÞÉÌÉ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ × ÓÐÉÓÏË ÐÏÕÞÁÔÅÌÅÊ.

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

```
blake% gpg --output message.txt --decrypt message.gpg

You need a passphrase to unlock the secret key for
user: "Blake (dumb) <blake@anywhere.ru>"
1024-bit RSA key, ID 526C7F7F, created 2002-05-01 (main key ID 01A1FE63)

Enter passphrase:
```

äÏËÕÍÅÎÔÙ, ÔÁËÖÅ, ÍÏÖÎÏ ÚÁÛÉÆÒÏÙ×ÁÔØ ÂÅÚ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ÷ÍÅÓÔ ÜÔÏÇÏ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÉÍÅÔÒÉ×ÎÙÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÄÏËÕÍÅÎÔÁ. ëÌÀÞ, ÉÓÐÏÌØÚÕÅÍÙÊ ÐÒÉ ÚÁÛÉÆÒÏ×ÁÎÉÉ, ÏÂÓÕÖÄÁÅÔÓÑ ÉÚ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ. äÌÑ ÂÏÌØÛÅÊ ÂÅÚÏÐÁÓÏÔÓÉ ÜÔÁ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÎÅ ÄÏÌÖÎÁ ÓÏ×ÐÁÄÁÔØ Ó ÔÏÊ, ËÏÔÒÏÒÕÀ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ ÄÌÑ ÚÁÝÉÔÙ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ. óÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ ÐÒÉÍÅÎÉÍ, ËÏÇÄÁ ÎÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ ÏÂÍÅÎ×ÁÔØÓÑ ËÌÀÞÅ×ÏÊ ÆÒÁÚÏÊ. äÌÑ ÉÓÐÏÌØÚÏ×ÁÎÑ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ ÐÒÉÍÅÎÑÅÔÓÑ ËÏÍÁÎÄÁ `--symmetric`.

```
alice% gpg --output message.gpg --symmetric message.txt
Enter passphrase:
```

ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ É ÉÈ ÐÒÏ×ÅÒËÁ

ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÕÄÏÓÔÏ×ÅÒÑÅÔ ÓÏÚÄÁÔÅÌÑ É ÄÁÎÕ ÓÏÚÄÁÎÉÑ ÄÏËÕÍÅÎÔÁ. åÓÌÉ ÄÏËÕÍÅÎÔ ÂÕÄÅÔ ËÁËÉÍ-ÌÉÂÏ ÏÂÒÁÚÏÍ ÉÚÍÅÎÅÎ, ÔÏ ÐÒÏ×ÅÒËÁ ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓÉ ÂÕÄÅÔ ÎÅÕÄÁÞÎÏÊ. ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ × ÔÅÈ ÖÅ ÃÅÌÑÈ, ÞÔÏ É ÏÂÙÞÎÁÑ ÐÏÄÐÉÓØ. éÓÐÏÌÙÚÕÅ ÔÅËÓÔÙ GnuPG, ÎÁÐÒÉÍÅÒ, ÐÏÄÐÉÓÁÎÙ, É ÷Ù ÍÏÖÅÔÅ ÕÂÅÄÉÔØÓÑ, ÞÔÏ ÏÎÉ ÄÏÛÌÉ ÄÏ ÷ÁÓ ÎÅÉÚÍÅÎ£ÎÎÙÍÉ.

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

äÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÏ× ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--sign`.

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

You need a passphrase to unlock the secret key for
user: "Alice (test key) <alice@wonderland.uk>"
1024-bit RSA key, ID B115BDB6, created 2002-05-01

Enter passphrase:
```

åÓÌÉ ÎÅ ÕËÁÚÁÔØ ÐÏÄÐÉÓÙ×ÁÅÍÙÊ ÄÏËÕÍÅÎÔ, ÔÏ ÄÁÎÎÙÅ ÓÞÉÔÙ×ÁÀÔÓÑ ÓÏ ÓÔÁÎÄÁÒÔÎÏÇÏ ×××ÏÄÁ. ðÒÏÅ ÐÏÄÐÉÓØÀ ÄÏËÕÍÅÎÔ ÓÖÉÍÁÅÔÓÑ. ðÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ×Ù×ÏÄÉÔÓÑ × Ä×ÏÉÞÎÍ ÆÏÔÁÔÅ.

éÍÅÑ ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ, ÷Ù ÍÏÖÅÅ ÌÉÂÏ ÔÏÌØËÏ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ÌÉÂÏ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ É ×ÍÓÓÔÁÎ×ÉÔØ ÉÓÈÏÄÎÙÊ ÄÏËÕÍÅÎÔ. äÌÑ ÐÒÏ×ÅÒËÉ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--verify`. äÌÑ ÐÒÏ×ÅÒËÉ É ÉÚ×ÌÅÞÅÎÉÑ ÄÏËÕÍÅÎÔÁ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--decrypt`.

```
blake% gpg --output doc --decrypt doc.sig
gpg: Signature made Sat May  4 19:04:21 2002 MSD using RSA key ID B115BDB6
gpg: Good signature from "Alice (test key) <alice@wonderland.uk>"
```

ðÒÏÚÒÁÞÎÏ ÐÏÄÐÉÓÁÎÎÙÅ(Clearsigned) ÄÏËÕÍÅÎÔÙ

ïÂÙÞÎÏ ÃÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ ÐÒÉÍÅÎÑÀÔÓÑ ÐÒÉ ÐÏÄÐÉÓÉ ÓÏÎÁÝÅÎÉÊ usenet É e-mail. ðÒÉ ÜÔÏÍ ÎÅÖÅÌÅÂÅÌØÎÏ ÓÖÉÍÁÔÓÑ ÐÏÄÐÉÓÙ×ÁÅÍÙÅ ÄÏËÕÍÅÎÔÙ. ëÏÍÁÎÄÁ `--clearsign` ÄÏÂÁ×ÌÑÅÔ Ë ÄÏËÕÍÅÎÔÕ ÃÉÆÒÏ×ÕÀ ÐÏÄÐÉÓØ × ÆÏÒÍÁÔÅ ASCII, ÎÅ ÉÚÍÅÎÑÑ ÐÒÉ ÜÔÏÍ ÓÁÍ ÄÏËÕÍÅÎÔ.

```
alice% gpg --output doc.asc --clearsign doc

You need a passphrase to unlock the secret key for
user: "Alice (test key) <alice@wonderland.uk>"
1024-bit RSA key, ID B115BDB6, created 2002-05-01

Enter passphrase:
alice% cat doc.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

GnuPG - ÉÎÔÅÒÆÅÊÓ ÄÌÑ ÚÁÝÉÔÙ ËÏÍÍÕÎÉËÁÃÉÉ. üÔÁ ÇÌÁ×Á ËÏÒÏÔËÏ ÏÐÉÓÙ×ÁÅÔ ÏÓÎÏ×Ù
ÒÁÂÏÔÙ Ó GnuPG, ×ËÌÀÞÁÑ ÓÏÚÄÁÎÉÅ ÐÁÒ ËÌÀÞÅÊ, ÏÂÍÅÎ ËÌÀÞÁÍÉ É ÉÈ ÐÒÏ×ÅÒÏ,
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 ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ × ÇÌÁ×Å 2. úÄÅÓØ, ÔÅËÕÅ, ÎÅ
ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ ÔÏÎËÏÓÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG. üÔÉ ×ÏÐÒÏÓÙ ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ ×
ÇÌÁ×ÁÈ 3 É 4.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.0 (FreeBSD)

iQCVAwUBPNP8VMc6mYexFb22AQLdAAP/SXHINHglH00hLlscGoVE1FCiFX7qTSO3
qwUFQi29WhqCXCq4DFTfZGTs4XQzb7592KpDy9swwNZ2sB7vaxQjqukffBdWrksZ
ERSZsz+xxKLWPiiBURg958Nym/eIRFY7nislv9Kc4V0UFDD9CjuE0rA7eWCg1XEX
0RcI2Zxiiv4=
=UV8s
-----END PGP SIGNATURE-----
```

ïÔÄÅÌ£ÎÙÁÑ ÐÏÄÐÉÓØ

ðÒÉÍÅÎÅÎÉÅ ÐÏÄÐÉÓÁÎÎÙÈ ÄÏËÕÍÅÎÔÏ× ÏÇÒÁÎÉÞÅÎÎÏ. ðÏÌÕÞÁÔÅÌØ ÄÏÌÖÅÎ ×ÏÓÓÔÁÎ×ÉÔ ×ÓÅ ÁÕÄ ÄÏËÕÍÅÎÔ ÉÚ ÐÏÄÐÉÓÁÎÎÏÊ ×ÅÒÓÉÉ, É ÄÁÖÅ × ÓÌÕÞÁÅ ÐÏÌÕÞÅÎÉÑ ÐÏÄÐÉÓÉ, ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÄÏÌÖÅÎ ÂÙÔØ ÔÒÅÄÓÔÏÑÝÉÍ ÄÏËÕÍÅÎÔÏ×, ËÏÔÏÒÙÅ ÓÏÚÄÁÅÔ

ÏÔÄÅÌ£ÎÎÕÀ ÐÏÄÐÉÓØ (detached signature). ïÔÄÅÌ£ÎÎÁÑ ÐÏÄÐÉÓØ ÓÏÚÄÁÅÔÓÑ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ËÏÍÁÎÄÙ `--detach-sign`.

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

You need a passphrase to unlock the secret key for
user: "Alice (test key) <alice@wonderland.uk>"
1024-bit RSA key, ID B115BDB6, created 2002-05-01

Enter passphrase:
```

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

```
blake% gpg --verify doc.sig doc
gpg: Signature made Sat May  4 19:34:08 2002 MSD using RSA key ID B115BDB6
gpg: Good signature from "Alice (test key) <alice@wonderland.uk>"
```

1. íÎÏÇÉÅ, ÞÁÓÔÉ ÉÓÐÏÌØÚÕÅÍÙÅ, ÏÐÃÉÉ ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÉ ÍÏÇÕÔ ÂÙÔØ ÕÓÔÁÎÏ×ÌÅÎÙ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.

2. ïÂÝÉÅ ÐÏÎÑÔÉÑ

GnuPG ÉÓÐÏÌØÚÕÅÔ ÎÅÓËÌÌØËÏ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÍÅÔÏÄÏ×, ×ËÌÀÞÁÑ *ÓÉÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ*, *ÛÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ*, É *ÏÄÎÏÁÐÒÁ×ÌÅÎÎÅ ÈÜÛÉÓÌ×ÁÎÉÅ*. ÷Ù ÍÏÖÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ ÏÓÏÍ×ÎÙÅ ÆÕÎËÃÉÉ GnuPG ÂÅÚ ÉÚÕÞÅÎÉÑ ÜÔÉÈ ÍÅÔÏÄÏ×, ÎÏ ÄÌÑ ÂÏÌØÅ ÒÁÚÑÍÍÏÇÏ ÐÒÉÍÅÎÅÎÉÑ ÖÅÌÁÔÅÌØÎÏ, ×ÓÅ ÖÅ, ËÏÅ-ÞÔÏ ÚÎÁÔØ.

üÔÁ ÇÌÁ×Á - ××ÅÄÅÎÉÅ × ÏÓÎ×ÎÙÅ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÅ ÍÅÔÏÄÙ, ÉÓÐÏÌØÚÕÅÍÙÅ × GnuPG. âÏÌÅÅ ÐÏÄÒÏÂÎÏ ÜÔÉ ×ÏÐÒÏÓÙ ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ × ÄÕÕÇÉÈ ÉÓÔÏÞÎÉËÁÈ. èÏÒÏÛÁÑ ËÎÉÇÁ, ÄÌÑ ÄÁÌØÎÅÊÛÅÇÏ ÉÚÕÞÅÎÉÑ: Bruce Schneier (http://www.counterpane.com/schneier.html) “Applied Cryptography” (http://www.counterpane.com/applied.html). (éÍÅÅÔÓÑ ÐÅÒÅ×ÏÄ ÎÁ ÒÕÓÓëÉÊ ÑÚÙË: â.ûÎÁÊÅÒ. ðÒÉËÌÁÄÎÁÑ ËÒÉÐÔÏÇÒÁÆÉÑ. ðÒÏÔÏËÏÌÙ, ÁÌÇÏÒÉÔÍÙ, ÉÓÈÏÄÎÙÅ ÔÅËÓÔÙ ÎÁ ÑÚÙËÅ óÉ.-í.:éÚÄÁÔÅÌØÓÔ×Ï ôòéõíæ, 2002 - 816Ó.:ÉÌ.)

óÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ

óÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ ÜÔÏ ÛÉÆÒ ÉÓÐÏÌØÚÕÀÝÉÊ ÏÄÉÎ ËÌÀÞ ÄÌÑ ÚÁÛÉÆÒÏ×ÁÎÉÑ É ÒÁÓÛÉÆÒÏ×ÁÎÉÑ. óÔÏÒÏÎÙ, ÏÂÝÁÀÝÉÅÓÑ ÐÒÉ ÐÏÍÝÉ ÓÉÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ, ÄÏÌÖÎÙ ÄÏÇÏ×ÏÒÉÌÉÓØ Ï ËÌÀÞÅ ÄÏ ÎÁÞÁÌÁ ÏÂÍÅÎÁ ÓÏÂÝÅÎÉÑÍÉ. ðÏÓÌÅ ÔÏÇÏ ËÁË ÏÎÉ ÄÏÇÏ×ÏÉÌÉÓØ, ÏÔÐÒÁ×ÉÔÅÌØ ÚÁÛÉÆÒÙ×Ù×ÁÅÔ ÓÏÂÝÅÎÉÅ, ÉÓÐÏÌØÚÕÑ ËÌÀÞ, ÏÐÒÁ×ÌÑÅÔ ÐÏÌÕÞÁÔÅÌÀ, É ÐÏÌÕÞÁÔÅÌØ ÒÁÓÛÉÆÒÙ×Ù×ÁÅÔÅ ÓÏÂÝÅÎÉÅ, ÉÓÐÏÌØÚÕÑ ÔÏÔ ÖÅ ÓÁÍÙÊ ËÌÀÞ. îÁÐÒÉÍÅÒ, ÎÅÍÃËÁÑ Enigma - ÓÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ, ÅÖÅÄÎÅ×ÎÙÅ ËÌÀÞÉ ÒÁÓÐÒÏÓÒÁÎÑÌÉÓØ ËÁË ËÎÉÇÉ ËÌÄÌ×. ëÁÖÄÙÊ ÄÅÎØ ÐÏÓÙÌÁÀÝÉÊ ÉÌÉ ÐÒÉÎÉÁÀÝÉÊ ÒÁÄÉÓÔ ÄÎÌÖÅÎ ÂÙÌ ÎÁÊÔÉ × Ó×ÏÅÊ ËÏÐÉÉ ËÎÉÇÉ ËÌÄÌ× ËÌÀÞ ÎÁ ÔÅËÕÝÉÊ ÄÅÎØ. òÁÄÉÇÒÁÍÙ × ÜÔÏ ÄÅÎØ ÚÁÛÉÆÒÏ×Ù×ÁÌÉÓØ É ÒÁÓÛÉÆÒÏ×Ù×ÁÌÉÓØ ÜÔÉÍ ËÌÀÞÍÍ. óÏ×ÒÅÍÅÎÎÙÅ ÐÒÉÍÅÒÙ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ×: 3DES, Blowfish, IDEA É çïóô.

èÏÒÏÛÉÊ ÛÉÆÒ ÚÁËÌÀÞÁÅÔ ×ÓÀ ÚÁÝÉÔÕ × ËÌÀÞÅ, ÎÏ ÎÅ × ÁÌÇÏÒÉÔÍÅ. äÒÕÇÉÉ ÓÌÏ×ÁÍÉ, ÚÎÁÎÉÅ ÉÓÐÒÁÎÎÏÇÏ ÁÌÇÏÒÉÔÍÁ ÎÅ ÄÎÌÖÎÏ ÐÍÍÞØ ×ÚÌÍÝÉËÕ. úÎÁÎÉÅ ÁÌÇÏÒÉÔÍÁ ÐÎÁÄÌÂÉÔÓÑ ÅÍÕ, ÔÎÌØËÏ ËÏÇÄÁ ÎÎ ÐÎÕÞÉÔ ËÌÀÞ. ûÉÆÒÙ, ÉÓÐÏÌØÚÕÅÍÙÅ × GnuPG, ÏÂÌÁÄÁÀÔ ÜÔÉÍ Ó×ÎÉÓÔ×ÍÍ.

ôÁË ËÁË ×ÓÑ ÚÁÝÉÔÁ ÚÁËÌÀÞÅÎÁ × ËÌÀÞÅ, ÔÏ ÏÞÅÎØ ×ÁÖÎÏ, ÞÔÏÂÙ ÅÇÏ ÂÙÌÌ ÔÒÕÄÎÏ ÐÏÄÌÂÒÁÔØ. äÒÕÇÉÉ ÓÌÏ×ÁÍÉ, ÍÍÖÅÓÔ×Ï ×ÍÚÍÏÖÎÙÈ ËÌÀÞÅÊ, Ô.Å. *ÐÒÏÓÒÀÎÓÔ×Ï ËÌÀÞÅÊ*, ÄÎÌÖÎÏ ÂÙÔØ ÄÏÓÁÓÏÞÎÏ ×ÅÍËÏ. âÕÄÕÞÉ × ìÏÓ áÌÁÍÏÓÅ, òÉÞÁÖÄ æÅÊÍÁÎ ÐÒÏÌÁ×ÉÌÓÑ ÕÍÅÎÅÅÍ ×ÓËÒÙ×ÁÔØ ÓÅÆÙ. äÌÑ ÐÏÄÅÅÒÖÁÍÉÑ ÍÉÓÔÉÆÉËÁÃÉÉ ÏÎ ÄÁÖÅ ÐÒÉÍÏÉÌ Ó ÓÍÎÎÊ ÎÁÂÌÒ ÉÍÓÒÕÕÕÑÅÎÏ×, ×ËÌÀÞÁÑ ÓÓÁÒÙÊ ÓÕÅÔÓÍÏÐ. ÷ ÄÅÉÓÔ×ÉÔÅÌØÎÏÓÔÉ, ÎÍ ÉÓÐÒÌØÚÏ×ÁÌ ÎÁÂÌÒ ÕÑ ×ÏË ÄÌÑ ÕÑÅÎØÛÅÍÑ ÞÉÓÌÁ ËÌÍÁÉÍÁÃÉÊ, Á ÚÁÔÅÍ ÐÒÌÓÓÍ ÐÏÄÂÉÒÁÀÔ ÐÒ×ÉÌØÎÕÀ ÐÁÒÕ ÓÌÕÞÁÊÎÙÈ ÞÉÓÅÌ, ÎÍ ÕÌÉ ÉÈ ÐÒÅÄÛÅÓÔ×ÅÎÎÉÁÍÉ.

óÏ×ÒÅÍÅÎÎÙÅ ËÏÍÐØÀÔÅÒÙ ÍÏÇÕÔ ÐÅÒÅÂÉÒÁÔØ Ë ÏÇÒÏÍÍÎÊ ÓËÏÒÏÓÔØÀ, ÐÏÜÔÍÕ ÒÁÚÍÅÒ ËÌÀÞÁ ÔÁË ×ÁÖÅÎ × ÓÏ×ÒÅÍÅÎÎÙÈ ËÒÉÐÔÏÓÉÓÔÅÍÁÈ. ûÉÆÒ DES ÉÓÐÏÌØÚÕÅÔ ËÌÀÞ ÄÌÉÎÎÊ 56 ÂÉÔ, Ô.Å. ÓÕÝÅÓÔ×ÕÅÔ 2^{56} ×ÏÚÍÏÖÎÙÈ ËÌÀÞÅÊ. 2^{56} ÜÔÏ 72,057,594,037,927,936 ËÌÀÞÅÊ. íÎÏÇÏ, ÎÏ ÏÂÙÞÎÙÊ ËÏÍÐØÀÔÅÒ ÍÏÖÅÔ ÐÅÒÅÂÒÁÔÙ ÉÈ ÚÁ ÓÞÉÔÁÎÙÅ ÄÎÉ, Á ÓÐÅÃÉÁÌÉÚÉÒÏ×ÁÎÎÙÊ ÚÁ ÞÁÓÙ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÂÏÌÅÅ ÐÏÚÄÎÉÅ ÁÌÇÏÒÉÔÙ - 3DES, Blowfish É IDEA ÉÓÐÏÌØÚÕÀÔ ËÌÀÞÉ ÄÌÉÎÎÊ 128 ÂÉÔ, ÞÔÏ ÏÚÎÁÞÁÅÔ 2^{128} ×ÏÚÍÏÖÎÙÈ ËÌÀÞÅÊ. üÔÏ ÎÁÍÎÏÇÏ ÂÏÌØÛÅ, É, ÄÁÖÅ, ÅÓÌÉ ×ÓÅ ËÍÍÐØÀÔÅÒÙ ÎÁ ÎÁÛÅÊ ÐÌÁÎÅÔÅ ÏßÅÄÉÎÉÔØ, ÉÍ ÐÏÔÒÅÂÕÅÔÓÑ ×ÒÅÍÅÉ ÂÏÌØÛÅ, ÞÅÍ ×ÏÚÒÁÓÔ ×ÓÅÌÅÎÎÏÊ, ÄÌÑ ÎÁÈÏÄÅÎÑ ËÌÀÞÁ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ

ïÓÎÏ×ÎÁÑ ÐÒÏÂÌÅÍÁ ÓÉÍÅÔÒÉ×ÎÙÈ ÛÉÆÒÏ× - ÏÂÍÅÎ ËÌÀÞÁÍÉ. ïÔÐÒÁ×ÉÔÅÌØ É ÐÏÌÕÞÁÔÅÌØ ÄÏÌÖÎÙ ÏÂÍÅÎÑÔØÓÑ ËÌÀÞÁÍÉ, ËÏÔÒÙÅ ÂÕÄÕÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÚÁÝÉÝÅÎÎÏÇÏ ÏÂÍÅÎÁ ÉÎÆÏÒÍÁÃÉÅÊ, ÎÏ ËÁËÉÍ ÚÁÝÉÝÅÎÎÙÍ ËÁÎÁÌÏÍ ÎÉ ÍÇÕÔ ×ÏÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÏÂÍÅÎÁ ÓÁÍÉÍÉ ËÌÀÞÁÍÉ? ÷ ÞÁÓÔÏÓÔÉ, ×ÚÌÍÝËËÕ ÍÏÅÔ ÂÙÔØ ÌÅÇÞÅ ÐÅÒÅÈ×ÁÔÉÔØ ËÌÀÞ, ÎÅÖÅ ÄÌÑ ÂÏÌØÛÉÈ ÅÇÏ ÐÏÄÂÉÒÁÔØ. äÒÕÇÁÑ ÐÒÏÂÌÅÍÁ - ËÏÌÉÞÅÓÔ×Ï ÎÅÏÂÈÏÄÉÍÙÈ ËÌÀÞÅÊ. åÓÌÉ *n* ÞÅÌÏ×ÅË ÈÏÑÔ ÏÂÍÅÎ×ÁÔØÓÑ ÍÅÖÄÕ ÓÏÂÏÊ ÓÍÏÂÝÅÎÉÑÍÉ, ÔÏ ÎÅÏÂÈÏÄÉÍÏ *n(n-1)/2* ËÌÀÞÅÊ, ÐÏ ÏÄÎÍÕ ÄÌÑ ËÁÖÄÏÊ ÐÁÒÙ, ÕÞÁ×ÓÔ×ÕÝÅÊ × ÐÅÒÅÐÉÓËÅ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÐÒÉÎÎÁÍ ÄÌÑ ÎÅÂÏØÛÏÊ ÇÒÕÐÐÙ ÌÀÄÅÊ, ÎÏ ÓÔÁÍÅÔ ÎÅÕÄÏÂÎÙÍ ÐÒÉ ÅÅ Õ×ÅÍÉÞÅÎÉÉ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÂÙÍ ÐÒÉÄÕÍÁÎÙ, ÞÔÏÂÙ ÒÅÛÉÔØ ÐÒÏÂÌÅÍÕ Ó ÏÍÅÎÎÍ ËÌÀÞÁÍÉ. ûÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÉÓÐÏÌØÚÕÅÔ ÐÁÒÕ ËÌÀÞÅÊ ÄÌÑ ÏÔÐÒÁ×ËÉ ÓÏÏÂÝÅÎÉÊ. ïÄÉÎ ËÌÀÞ *ÏÔËÒÙÔÙÊ (public key)* É ÍÏÖÅÔ ÂÙÔØ ÐÅÒÅÄÁÎ ÌÀÂÍÏÕ. äÒÕÇÏÊ ËÌÀÞ *ÓÅËÒÅÔÎÙÊ (private key)* É ÈÒÁÎÉÔÓÑ ÔÏÌØËÏ Õ ×ÌÁÄÅÌØÃÁ. ïÐÒÁ×ÉÔÅÌØ ÚÁÛÉÆÒÏ×Ù×ÅÐ ÓÏÏÂÝÅÎÉÅ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÐÏÓÐÁÔÅÌÑ, É ,ÂÕÄÞÉ ÚÁÛÉÆÒÏ×ÁÎÏ, ÓÏÏÂÝÅÎÉÅ ÍÏÖÅÔ ÒÁÓÛÉÆÒÏ×ÁÎÏ ÚÁËÒÙÔÙÍ ËÌÀÞÏÍ ÐÏÓÐÁÔÅÌÑ.

üÔÏÔ ÍÅÔÏÄ ÒÅÛÁÅÔ ÐÒÏÂÌÅÍÕ ÏÂÍÅÎÁ ËÌÀÞÁÍÉ, ÐÒÉÓÕÝÀ ÓÉÍÍÅÔÒÉ×ÎÙÍ ÛÉÆÒÏÍ. ïÔÐÁÄÁÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ Ï ËÌÀÞÅ ÍÅÖÄÕ ÏÔÐÒÁ×ÉÔÅÌÅÍ É ÐÏÌÕÞÁÔÅÌÅÍ. ÷ÓÅ ÞÔÏ ÔÒÅÂÕÅÔÓÑ, ÜÔÏ ÞÔÏÂÙ ÏÔÐÒÁ×ÉÔÅÌØ ÄÏ ÎÁÞÁÌÁ ÓÅÒÅÎÓÁ ÓÏÏÂÝÅÎÉÊ ×ÚÑÌ ËÏÐÉÀ ÏÔÐÒÁ×ÉÔÅÌÑ. ëÒÏÍÅ ÔÏÇÏ, ÏÄÉÎ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ×ÓÅÍ ËÌÒÞÁÔÅÌÑÍ. ôÁËÉÍ ÏÂÒÁÚÏÍ, ÔÏÌØËÏ *n* ÐÁÒ ËÌÀÞÅÊ ÎÅÏÂÈÏÄÉÍÏ ÄÌÑ *n* ÞÅÌÏ×ÅË, ÐÒÅÐÉÓÙ×ÁÀÝÉÈÓÑ ÄÒÕÇ Ó ÄÒÕÇÏÍ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÏÓÎÏ×ÁÎÙ ÎÁ ÏÄÎÏÓÔÒÏÏÎÎÉÈ ÆÕÎËÃÉÑÈ "c ÌÁÚÅËËÏÊ". ïÄÎÏÓÔÒÏÏÎÎÑ ÆÕÎËÃÉÑ ÜÔÏ ÆÕÎËÃÉÑ, ËÏÔÒÕÔÀ ÌÅÇËÏ ×ÙÞÉÓÌÉÔØ, ÎÏ ÔÒÕÄÎÏ ×ÙÞÉÓÌÉÔØ ÅÅ ÏÂÒÁÔÎÕÀ ÆÕÎËÃÉÀ, Ô.Å. ÐÏ ÚÎÁÞÅÎÉÀ ÆÕÎËÃÉÉ ÎÁÊÔÉ ÎÁËÏÔÒÁÑ ÓÅËÅÎÉÅ ÁÒÇÕÍÅÎÔÁ. îÁÐÒÉÍÅÒ, ÌÅÇËÏ ×ÙÞÉÓÌÉÔØ ÐÒÏÉÚ×ÅÄÅÎÉÅ Ä×ÕÈ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, ÎÏ ÔÒÕÄÎÏ ×ÙÞÉÓÌÉÔØ ÉÈ ÍÎÏÖÉÔÅÌØ, ÚÎÁÑ ÐÒÏÉÚ×ÅÄÅÎÉÅ. ïÄÎÏÓÔÒÏÏÎÎÉÊ ÆÕÎËÃÉÉ "Ó ÌÁÚÅËËÏÊ" ÐÏÈÏÖÉ, ÎÏ ÉÍÅÀÔ ÌÁÚÅËÕ. ïÎÁ ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏ ÅÓÌÉ ÎÅÏÔÒÙÁÑ ÞÁÓÔØ ÉÎÆÒÏÍÁÃÉÉ ÉÚ×ÅÓÔÎÁ, ÔÏ ×ÙÞÉÓÌÉÔØ ÏÂÁÔÎÕÀ ÆÕÎËÃÉÉ ÓÔÁÎÏ×ÉÔÓÑ ÌÅÇËÉÍ. îÁÐÒÉÍÅÒ, ÅÓÌÉ ÷ÁÍ ÉÚ×ÅÓÔÎÏ ÏÂÏ ÉÚ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, × ÐÒÉÍÅÒ ×ÙÛÅ, ÔÏ, ÚÎÁÑ ÐÒÏÉÚ×ÅÄÅÎÉÅ, ÷Ù ÌÅÇËÏ ÎÁÊÄÅÔÅ ×ÔÏÒÏÅ ÞÉÓÌÏ. äÁÎÎÙÊ ÛÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÏÓÎÏ×ÁÎ ÎÁ ÐÒÏÓÔÙÈ ÍÎÏÖÉÔÅÌØÑÈ, ÏÔËÒÙÔÙÊ ËÌÀÞ ÓÏ×ÒÅÍÅÎÎÙÅ Ä×ÕÈ

ÂÏÌØÛÉÈ ÐÒÏÓÔÙÈ ÞÉÓÀÌ, ÁÌÇÏÒÉÔÍÍ ÛÉÆÒÏ×ÁÎÉÑ ÉÓÐÏÌØÚÕÅÔ ÜÔÏ ÞÉÓÌÏ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÓÏÏÂÝÅÎÉÑ. áÌÇÏÒÉÔÍ ÒÁÓÛÉÆÒÏ×ËÉ ÔÒÅÂÕÅÔ ÚÎÁÎÉÑ ÐÒÏÓÔÙÈ ÍÎÏÖÉÔÅÌÅÊ, ÔÁË, ÒÁÓÛÉÆÒÏ×ËÁ ÓÔÁÎÏ×ÉÔÓÑ ÌÇËÏÊ, ÅÓÌÉ Õ ÷ÁÓ ÅÓÔØ ÓÅËÒÅÔÎÛÊ ËÌÀÞ, ÓÏÄÅÒÖÁÝÉÊ ÏÄÉÎ ÉÚ ÍÏÖÉÔÅÌÅÊ, ÏÏ ÞÒÅÚ×ÙÞÁÉÎÏ ÚÁÔÒÕÄÎÅÎÁ ÅÓÌÉ ÅÇÏ Õ ÷ÁÓ ÎÅÔ.

ëÁË É × ÓÌÕÞÁÅ ÓÉÍÅÔÒÉ×ÎÙÈ ÛÉÆÒÏ×, ×ÓÑ ÚÁÝÉÔÁ ÈÏÒÏÛÅÇÏ ÛÉÆÒÁ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÚÁËÌÀÞÅÎÁ × ËÌÀÞÅ. îÁÄÅÖÎÏÓÔØ ÚÁ×ÉÓÉÔ ÏÔ ÒÁÚÍÅÒÁ ËÌÀÞÁ, ÎÏ ÎÅÌØÚÑ ÓÒÁ×ÎÉ×ÁÔØ ÄÌÑ ÞÅÔÙÒÅØÚÎÁÞÎÙÈ ÛÉÆÒÏ×. É ÛÉÆÒÏ× Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ËÁË ÍÅÒÕ ÉÈ ÏÔÎÏÓÉÔÅÌØÎÏÊ ÎÁÄÅÖÎÏÓÔÉ. ðÒÉ ÇÒÃÅÄ ×ÚÌÏÍÅ ÓÉÍÅÔÒÉ×ÎÙÅ ÛÉÆÒÏ×Á Ó ÄÌÉÎÏÊ ËÌÀÞÁ 512 ÂÉÔ, ×ÚÌÏÍÝÉË ÄÏÌÅÎ ÒÁÚÌÏÖÉÔØ ÎÁ ÍÎÏÖÉÔÅÌÉ ÞÉÓÌ ÚÁËÌÄÉÒÏ×ÁÎÎÅ × 512 ÂÉÔÁÈ (ÄÏ 155 ÄÅÑÔÉÞÎÙÈ ÚÎÁËÏ×). äÅÊÔ×ÉÑ ×ÙÌÍÝÉËÁ ÓÉÌØÎÏ ÒÁÚÌÉÞÁÀÔÓÑ × ÚÁ×ÉÓÉÍÓÔÉ ÏÔ ÛÉÆÒÏ×, ÎÁ ÓÅÇÏÄÑÑÛÎÉÊ ÄÅÎØ, ÄÏÓÔÁÔÏÞÎÁ ÄÌÉÎÁ ËÌÀÞÁ 128 ÂÉÔ, ÔÏ ÄÌÑ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÒÅËÍÅÎÄÕÅÔÓÑ ÄÌÉÎÁ 1024 ÂÉÔÁ.

óÍÅÛÁÎÎÙÅ ÛÉÆÒÙ

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ ÎÅ ÐÁÎÁÃÅÑ. íÎÏÇÉÅ ÓÉÍÅÔÒÉ×ÙÅ ÛÉÆÒÙ ÂÏÌÅÅ ÕÓÔÏÊÞÉ×Ù ÐÒÏÔÉ× ×ÚÌÍÍÁ, É, ËÒÍÍÅ ÔÏÇÏ ÚÁÛÉÆÒÏ×ÁÎÉÅ/ÒÁÓÛÉÆÒÏ×ÁÎÉÅ ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ ÔÒÅÂÕÅÔ ÚÁÔÒÁÔ ÂÏØÛÉÈ ÚÁÔÒÁÔ, ÞÅÍ ÁÎÁÏÇÉÞÎÙÅ ÏÐÅÒÁÃÉÉ × ÓÉÍÅÔÒÉ×ÎÙÈ ÓÉÓÔÅÍÁÈ. ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ, ÔÅÍ ÎÅ ÍÅÎÅÅ, ÜÆÆÅËÔÉ×ÎÙ ÐÒÉ ÒÁÓÛÉÆÒÏ×ÁÎÎÉÉ ËÌÀÞÅÊ ÓÉÍÅÔÒÉ×ÎÙÈ ÛÉÆÒÏ× É ÉÍÅÎÎÏ ÔÁË ÏÐÒÏØÚÑÅÔ × ÓÉÓÔÅÍÁÈ ÓÏ ÓÍÅÛÁÎÎÙÍ ÛÉÆÒÏÍ.

óÍÅÛÁÎÎÙÊ ÛÉÆÒ ÉÓÐÏØÚÕÅÔ ÓÉÍÅÔÒÉ×ÎÙÊ ÛÉÆÒ É ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ. ïÎ ÒÁÂÏÔÁÅÔ ÉÓÐÏØÚÕÑ ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ ÄÌÑ ÐÅÒÅÄÁÞÉ ËÌÀÞÁ ÓÉÍÅÔÒÉ×ÎÏÇÏ ÛÉÆÒÁ. óÏÎÂÝÅÎÉÅ, ÚÁÔÅÍ, ÚÁÛÉÆÒÏ×Ù×ÁÅÔÓÑ ÜÔÉÍ ËÌÀÞÍÍ É ÐÏÓÙÌÁÅÔÓÑ ÁÄÒÅÓÁÔÕ. ôÁË ËÁË ÐÅÒÅÄÁÞÁ ÓÉÍÅÔÒÉÇÏ ËÌÀÞÁ ÚÁÝÉÝÅÎÁ, ÔÏ ÄÌÑ ËÁÖÄÏÇÏ ÓÏÎÂÝÅÎÉÑ ÉÓÐÏØÚÅÓÑ Ó×ÏÊ ÓÉÍÅÔÒÉ×ÎÙÊ ËÌÀÞ, ÎÁÚÙ×ÁÅÍÙÊ *ÓÅÁÎÓÏ×ÙÍ ËÌÀÞÏÍ*.

é PGP É GnuPG ÉÓÐÏØÚÕÀÔ ÉÍÅÎÎÏ ÓÍÅÛÁÎÎÙÅ ÛÉÆÒÙ. óÅÁÎÓÏ×ÙÊ ËÌÀÞ, ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÛÉÆÒÏÍ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ, É ÓÏÏÂÝÅÎÅ, ÚÁÛÉÆÒÏ×ÁÎÎÅ ÓÉÍÅÔÒÉ×ÎÙÍ ÛÉÆÒÏÍ, Á×ÔÏÍÁÔÉÞÅÓËÉ ÏÂßÅÄÉÑÀÔÓÑ ×ÍÅÓÅ. ðÏÔÒÁÂÌØ ÉÓÐÏØÚÓÅÔ Ó×ÏÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÄÌÑ ÒÁÓÛÉÆÒÏ×ÙÉ ÓÅÁÎÓÏ×ÇÏ ËÌÀÞÁ É, ÚÁÔÅÍ, ÉÓÐÏØÚÕÅÔ ÐÏÔÒÅÂÎÏÛÊ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ ÄÌÑ ÒÁÓÛÉÆÒÏ×ÙÉ ÓÅÁÎÓÏ×ÙÅ ÓÏÏÂÝÅÎÉÑ.

óÍÅÛÁÎÎÙÊ ÛÉÆÒ ÎÅ ÕÓÔÏÊÞÉ×ÅÅ ÞÅÍ ÓÌÁÂÅÊÛÉÊ ÉÚ ÉÓÐÏØÚÕÅÍÙÈ ÉÍ ÛÉÆÒÏ×. ÷ PGP É GnuPG, ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÍÍ, ×ÅÒÏÑÔÎÏ, ÓÌÁÂÅÅ. ë ÓÞÁÓÔØÀ, ÅÓÌÉ ×ÚÌÍÝÉËÕ ÕÄÁÂÔÓÑ ÒÁÓÛÉÆÒÏ×ÁÔØ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ, ÏÎ ÍÖÅÔ ÅÇÏ ÉÓÐÏØÚÏ×ÁÔØ ÄÌÑ ÒÁÓÛÉÆÒÏ×ÙÉ ÓÏÏÂÝÅÎÉÑ, ÚÁÛÉÆÒÏ×ÁÎÎÇÏ ÜÔÉÍ ËÌÀÞÍÍ. äÌÑ ÐÒÏÞÔÅÎÑ ÄÒÕÇÏÇÏ ÓÏÏÂÝÅÎÉÑ, ÅÍÕ ÐÒÉÄÅÔÓÑ ÎÁÞÁÔØ ×ÓÅ ÚÁÎÏ×Ï.

ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ

èÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ ÜÔÏ ÆÕÎËÃÉÑ "ÍÎÇÉÅ-Ë-ÏÄÎÍÕ", ÏÔÎÂÒÁÖÁÀÝÁÑ Ó×ÉÉ

ÁÒÇÕÍÅÎÔÙ ÎÁ ÏÇÒÁÎÉÞÅÎÎÏÅ ÍÎÏÖÅÓÓ×Ï ÚÎÁÞÅÎÉÊ. ïÂÙÞÎÏ ÜÔÏ ÍÎÏÖÅÓÔ×Ï - ÄÉÁÐÁÚÏÎ ÎÁÔÕÒÁÌØÎÙÈ ÞÉÓÅÌ. ðÒÏÔÁÑ ÈÅÛÉÒÒÀÝÁÑ ÆÕÎÊÃÉÑ - $f(x) = 0$ ÄÌÑ ×ÓÅÈ ÃÅÌÙÈ x. âÏÌÅÅ ÉÎÔÅÒÅÓÎÁ ÆÕÎÊÃÉÑ $f(x) = x \bmod 37$, ËÏÔÏÒÁÑ ÏÔÂÒÁÇÁÅÔ $x \times$ ÍÓÂÁÏÏË ÏÔ ÄÅÌÅÎÉÑ x ÎÁ 37.

ãÉÆÒÏ×ÁÑ ÐÏÄÐÉØ ÄÏËÕÍÅÎÔÁ - ÒÅÚÕÌØÔÁÔ ÐÒÉÍÅÎÅÎÉÑ ÈÅÛÉÒÒÀÝÅÊ ÆÕÎËÃÉÉ Ë ÄÏËÕÍÅÎÔÕ. äÌÑ ÔÏÇÏ ÞÔÏÂÙ ÂÙÔØ ÐÒÉÍÅÎÉÍÏÊ × ËÒÉÐÔÏÇÒÁÆÉÉ, ÈÅÛÉÒÒÀÝÁÑ ÆÕÎËÃÉÑ ÄÏÌÖÁ ÕÄÏ×ÌÅÔ×ÏÑÕÔØ Ä×ÕÍ ×ÁÖÎÙÍ ÕÓÌÏ×ÉÑÍ. ÷Ï-ÐÅÒ×ÙÈ, ÎÁÈÏÖÄÅÎÉÅ Ä×ÕÈ ÄÏËÕÍÅÎÔÏ× Ó ÏÄÉÎÁËÏ×ÙÍ ÚÍÁÞÅÎÉÅÍ ÆÕÎËÃÉÉ ÄÎÌÖÎÏ ÂÙÔØ ÐÒÁÉÐÅÐÅÓËÉ ÎÅ×ÏÚÍÏÖÎÙÍ. ÷Ï-×ÔÏÒÙÈ, ×ÏÓÓÔÁÎÏ×ÌÅÎÉÅ ÄÏËÕÍÅÎÔÁ ÐÏ ÉÍÅÀÝÅÊÓÑ ÐÏÄÐÉÓÉ ÄÎÌÖÎÏ ÂÙÔØ ÎÅ×ÏÚÍÏÖÎÙÍ.

îÅËÏÔÒÙÅ ÛÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ [1] ÍÏÇÕÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÙ ÄÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÏ×. ðÏÄÐÉÓÙ×ÁÀÝÉÊ ÚÁÛÉÆÒÏ×Ù×ÅÂÕ ÄÏËÕÍÅÎÔ Ó×ÏÉÍ *ÓÅËÒÅÔÎÙÍ* ËÌÀÞÏÍ. öÅÌÁÀÝÉÊ ÐÒÏ×ÅÒÉÔ ÐÏÄÐÉÓØ É Õ×ÉÄÅÔØ ÄÏËÕÍÅÎÔ, ÐÒÏÓÏ ÉÓÐÏÌØÚÕÅÔ ÏÔËÙÔÙÊ ËÌÀÞ ÐÏÄÐÉÓÁ×ÛÅÇÏ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÄÏËÕÍÅÎÔÁ. üÔÏ ÁÌÇÏÒÉÔÍ ÕÄÏ×ÌÅÔ×ÏÑÅÔ Ä×ÕÍ ÕÓÌÏ×ÉÑÍ, ÎÁÌÁÇÁÅÍÙÍ ÎÁ ÈÏÒÏÛÕÀ ÈÅÛÉÒÒÀÝÕÀ ÆÕÎËÃÉÀ, ÎÏ ÎÁ ÐÒÁËÔÉËÅ ÏÎ ÓÌÉÛËÏÍ ÍÅÄÌÅÎÎÙÊ.

÷ ËÁÞÅÓ×Å ÁÌØÔÅÒÎÁÔÉ×Ù ÉÓÐÏÌØÚÕÀÔÓÑ ÈÅÛÉÒÒÀÝÉÅ ÆÕÎËÃÉÉ, ÕÄÏ×ÌÅÔ×ÏÑÑÀÝÉÅ Ä×ÕÍ ×ÙÛÅÕËÁÚÁÎÎÙÍ ÕÓÌÏ×ÉÑÍ. SHA É MD5 ÐÒÉÍÅÀÒ ÔÁËÉÈ ÆÕÎËÃÉÊ. ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÄÁÎÎÏÇÏ ÁÌÇÏÒÉÔÍÁ ÄÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÁ, ÓÎÁÞÁÌÁ ×ÙÞÉÓÌÑÅÔÓÑ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÒÀÝÅÊ ÆÕÎËÃÉÉ, Á ÚÁÔÅÍ ÜÔÏ ÚÎÁÞÅÎÉÅ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ É ÕÄÏ×ÌÅÔ×ÏÒÅÔ ÄÏËÕÍÅÎÔÁ. ðÏÌÕÞÁÔÅÌØ ÍÖÅÔ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ×ÙÞÉÓÌÉ× ÚÎÁÞÅÎÉÅ ÆÕÎËÃÉÉ ÄÌÑ ÄÏËÕÍÅÎÔÁ É ÓÒÁ×ÎÉ× ÅÇÏ ÓÏ ÚÎÁÞÅÎÉÅÍ, ×ÙÞÉÓÌÅÎÎÙÍ ÏÐÒÁ×ÉÄÌÉ ÄÌÑ ÎÁÓÏÑÝÅÇÏ ÄÏËÕÍÅÎÔÁ. åÓÌÉ ÍÍÉ ÓÏ×ÐÁÄÕÔ, ÔÏ ÐÏÞÔÉ ÎÁ×ÅÒÎÑÁ ÄÏËÕÍÅÎÔÙ ÉÄÅÎÔÉÞÎÙ.

ôÅÐÅÒØ ÐÒÏÂÌÅÍÁ ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏÂÙ ÐÒÅÄÏ×ÒÁÔÉÔØ ÚÚÍÅÎÅÎÉÅ ÐÏÄÐÉÓÉ ÚÎÁÞÉÍÙÈ ÄÏËÕÍÅÎÔÏ×. åÓÌÉ ÄÏËÕÍÅÎÔ É ÐÏÄÐÉÓØ ÐÏÓÙÌÁÀÔÓÑ ÎÅÚÁÛÉÆÒÏ×ÁÎÙÍ, ×ÙÌÍÍÝÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÄÏËÕÍÅÎÔ É ×ÙÞÉÓÌÉÔØ ÓÏÎÔ×ÅÓÔ×ÕÀÝÅÅ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÒÀÝÅÊ ÆÕÎËÃÉÉ, ÂÅÚ ×ÅÄÏÍÁ ÐÌÕÐÁÔÅÌÑ. åÓÌÉ ÚÁÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÄÏËÕÍÅÎÔ, ×ÚÌÍÝÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÒÀÝÅÊ ÆÕÎËÃÉÉ É ÐÒÏ×ÁÍÉÔØ ÅÅ ÐÒÏ×ÅÒÕ. ôÒÅÉÊ ÐÕÔØ - ÉÓÐÏÌØÚÏ×ÁÔØ ÓÍÅÛÁÎÎÙÊ ÍÅÔÏÄ ÛÉÆÒÏ×ÁÎÉÑ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÐÏÄÐÉÓÉ É ÓÒÁ×ÎÉ× ÅÇÏ ÓÏ ÚÎÁÞÅÎÉÅÍ, ÔÁË ËÁË ÔÏÌØËÏ ÐÏÄÐÉÓØ ÍÏÖÅÔ ÓÇÅÎÅÒÉÒÏ×ÁÔØ ÔÏÌØËÏ ÏÎ, ÉÓÐÏÌØÚÕÑ ÓÅËÒÅÔÎÙÊ ËÌÀÞ. úÁÍÅÔÉÍ, ÞÔÏ ÐÒÉ ÜÔÏÍ ÐÏÄÐÉÓØ ÂÕÄÅÔ ÚÁÖÉÔÁ ÏÔ ÐÏÄÄÅÌÏË, Á ÐÏÌØÚÏ×ÁÔÅÌØ ÍÏÖÅÔ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ÉÓÐÏÌØÚÕÑ ÏÔËÒÙÔÙÊ ËÌÀÞ.

÷ ÜÔÏÍ ÒÁÚÄÅÌÅ ÍÙ ÒÁÓÓÍÏÔÒÉÍ ÐÒÏÔÏËÏÌÙ ÐÅÒÅÄÁŢ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÐÏÚ×ÏÌÑÀÝÉÅ ÄÁÎÎÙÍ ÂÙÔØ ÚÁÛÉÆÒÏ×ÁÎÙ ÐÏ ÏÔËÒÙÔÏÍÕ ËÁÎÁÌÕ. ÷ ÜÔÏÍ ÒÁÚÄÅÌÅ ÍÙ ÒÁÓÓÍÏÔÒÉÍ ÐÒÏÔÏËÏÌ ÄÌÑ ÏÂÍÅÎÁ ÓÅËÒÅÔÎÙÍ ËÌÀÞÏÍ ÍÅÖÄÕ ÄÁÎÎÙÍÉ ÏÄÎÏÇÏ ÐÏÌØÚÏ×ÁÔÅÌÑ.

14

ÐÏÄÐÉÓÉ, ÉÓÐÏÌØÚÕÅÍÙÊ × GnuPG.

1. ûÉÆÒ ÄÏÌÖÅÎ ÏÂÌÁÄÁÔØ ÔÅÍ Ó×ÏÊÓÔ×ÏÍ, ÞÔÏ É ÎÁÓÔÏÑÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, É ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÍÇÕÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎÙ ÁÌÇÏÒÉÔÍÉ ÛÉÆÒÏ×ÁÎÉÑ ËÁË ÏÔËÒÙÔÙÊ ËÌÀÞ. RSA - Ñ×ÌÑÅÔÓÑ ÔÁËÉÍ ÁÌÇÏÒÉÔÍÏÍ, Á ElGamal ÎÅÔ.

3. õÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ

ðÏÄÄÅÒÖË ËÌÀÞÁ - ÎÁÉÂÏÌÅÅ ÓÌÁÂÏÅ ÍÅÓÔÏ × ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÌÏÕÍÙÛÌÅÎÎÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÐÏÌØÚÏ×ÁÔÅÌØÓËÕÀ Ó×ÑÚËÕ ËÌÀÞÅÊ ÉÌÉ ÐÏÄÄÅÒÖÁÔØ ÏÔËÒÙÔÙÛ ËÌÀÞ ÐÏÌØÚÏ×ÁÔÅÌÑ É ÐÏÓÌÁÔØ ÅÇÏ ÄÒÕÇÉÍ ÄÌÑ ÚÁÇÒÕÚËÉ É ÉÓÐÏÌØÚÏ×ÁÎÉÑ. îÁÐÒÉÍÅÒ, ÐÒÅÄÐÏÌÏÖÉÍ, ÞÔÏ èÌÏÊ ËÏÞÅÔ ÏÓÓÌÅÖÉ×ÁÔØ ÓÏÂÝÅÎÉÑ, ËÏÔÏÒÙÅ üÌÉÓ ÐÏÓÙÌÁÅÔ âÌÜÊËÕ. ïÎÁ ÍÏÇÌÁ ÂÙ ÉÓÐÏÌØÚÏ×ÁÔØ ÁÔÁËÕ, ÎÁÚÙ×ÁÅÍÕÀ *ÞÅÌÏ×ÅË × ÓÅÒÅÄÉÎÅ (man in the middle)*. äÌÑ ÜÔÏÇÏ èÌÏÊ ÓÏÚÄÁÅÔ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ. ïÎÁ ÚÁÍÅÎÑÅÔ ËÏÐÉÀ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ âÌÜÊËÁ, ÐÒÉÎÄÌÅÖÁÝÕÀ üÌÉÓ, ÎÏ×ÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÁÔÅÍ ÏÎÁ ÐÀÒÅ×ÁÔÙ×ÁÅÔ ÓÏÏÂÝÅÎÉÑ, ËÏÔÏÒÙÅ üÌÉÓ ÐÏÓÙÌÁÅÔ âÌÜÊËÕ. ëÁÖÄÏÅ ÐÀÒÅ×ÁÞÅÎÎÅ ÓÏÏÂÝÅÎÉ ÏÎÁ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ, ÉÓÐÏÌØÚÕÑ ÎÏ×ÙÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÎÁÓÔÑÝÉÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ âÌÜÊËÁ É ÎÁÐÒÁ×ÌÑÅÔ ÉÈ ÅÍÕ. ÷ÓÅ ÓÏÏÂÝÅÎÑ, ÎÁÐÒÁ×ÌÅÎÎÙÅ üÌÉÓ âÌÜÊËÕ, ÔÅÐÅØ ÍÇÕÔ ÂÙÔØ ÐÒÏÞÉÔÁÎÙ èÌÏÊ.

ðÒÁ×ÉÌØÎÏÅ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ Ñ×ÌÑÅÔÓÑ ÒÅÛÁÀÝÉÍ ÆÁËÔÏÒÏÍ ÄÌÑ ÏÂßÅÐÅÞÅÎÑ ÃÅÌÏÓÔÎÏÓÔÉ ÎÅ ÔÏÌØËÏ ÷ÁÛÉÈ Ó×ÑÚÏË ËÌÀÞÅÊ, ÎÏ É Ó×ÑÚÏË ËÌÀÞÅÊ ÄÒÕÇÉÈ ÐÌØÚÏ×ÁÔÅÌÅÊ. ïÓÎÏ×ÎÊ ÕÐÒÁ×ÌÅÎÑ ËÌÀÞÁÍÉ × GnuPG Ñ×ÌÑÅÔÓÑ ÐÏÄÐÉÓÁÎÉÅ ËÌÀÞÅÊ. ðÏÄÐÉÓÁÎÉÅ ËÌÀÞÅÊ ÉÍÅÅÔ Ä×Á ÏÓÎ×ÎÙÈ ÐÒÉÎÎÁÎÉÑ: ÜÔÏ ÐÏÚ×ÌÑÅÔ ÷ÁÍ ÏÂÎÁÒÕÖÉ×ÁÔØ ×ÍÅÛÁÔÅÌØØÓÔ×Ï × ÷ÁÛÕ Ó×ÑÚËÕ ËÌÀÞÅÊ, Á ÔÁËÖÅ ÐÏÚ×ÌÑÅÔ ÕÄÏÓÔÏ×ÅÒÑÔØ, ÞÔÏ ËÌÀÞ ÄÅÉÓÔ×ÉÔÅÌØÎÏ ÐÒÉÎÁÄÌÅÖÉÔ ÞÅÌÏ×ÅËÕ, ÞØÉÍ ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ÐÌØÚÏ×ÁÔÅÌÑ ÎÏ ÐÍÅÞÅÎ. ðÏÄÉÓÉ ÎÁ ËÌÀÞÁÈ ÔÁËÖÅ ÉÓÐÏÌØÚÕÀÔÓÑ × ÓÈÅÍÅ ÉÚ×ÅÓÔÎÏÊ ËÁË *ÓÅÔØ ÄÏ×ÅÒÉÑ (web of trust)*, ËÏÔÏÒÁÑ ÐÏÚ×ÌÑÅÔ ÓÞÉÔÁØ ÄÏÕÖÄÅÎÎÙÍÉ ÎÅ ÔÏÌØËÏ ËÌÀÞÉ ÐÏÄÐÉÓÁÎÎÙÅ ÌÉÞÎÏ ÷ÁÍÉ, ÎÏ É ÐÏÄÐÉÓÁÎÎÙÅ ÌÀÄØÍÉ, ËÏÔÏÒÙÍ ÷Ù ÄÏ×ÅÒÑÅÔÅ. áËËÕÓÁÔÎÙÅ ÐÌØÚÏ×ÁÔÅÌÉ, ÐÓ×ÉØÎÏ ÒÅÁÌÉÚÏ×Á×ÛÉÅ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ, ÍÇÕÔ ÉÓËÌÀÞÉÔØ ÐÏÄÍÅÎÎÏÇÏ ËÌÀÞÅÊ ËÁË ×ÉÄ ÁÔÁËÉ ÎÁ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏÓÔØ Ó×ÑÚÉ ÐÒÉ ÐÍÍÝÉ GnuPG.

õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÐÁÒÏÊ ËÌÀÞÅÊ

ðÁÒÁ ËÌÀÞÅÊ ÓÏÓÔÉÔ ÉÚ ÏÔËÒÙÔÏÇÏ É ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÅÊ. ïÔËÒÙÔÙÊ ËÌÀÞ ÓÏÓÔÏÉÔ ÉÚ ÏÔËÒÙÔÏÊ ÞÁÓÔÉ ÇÌÁ×ÎÏÇÏ ÐÏÄÐÉÓÙ×ÁÀÝÅÇÏ ËÌÀÞÁ, ÏÔËÒÙÔÙÈ ÞÁÓÔÅÊ ÐÏÄÐÉÅÎÎÙÈ ÐÏÄÐÉÓÙ×ÁÀÝÉÈ É ÛÉÆÒÕÀÝÉÈ ËÌÀÞÅÊ, ÎÁÂÏÀ ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ×ÐÏÌØÚÏ×ÁÔÅÌÑ, ÁÓÓÏÃÉÉÒÕÀÝÉÈ ÎÔËÒÙÔÙÊ ËÌÀÞ Ó ÒÅÁÌØÎÙÍ ÐÅÌ×ÅËÍ. ëÁÖÄÁÑ ÞÁÓÔØ ÓÏÄÅÒÖÉÔ ÄÁÎÎÙÅ Ï ÓÅÅ. äÌÑ ËÌÀÞÁ -- ÜÔÏ ÅÇÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ, ÄÁÔÁ ÓÏÚÄÁÎÉÑ, ÓÒÏË ÄÅÊÓ×ÉÑ É Ô.Ä. äÌÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏØÚÏ×ÁÔÅÌÑ -- ÉÍÑ ÞÅÌÏ×ÅËÁ, ÄÏÐÏÎÉÔÅÌØÎÙÊ ËÏÍÍÅÎÔÁÒÉÊ É ÁÄÒÅ email. óÔÒÏËÔÒÔÁ ÓÅËÅÔÒÏÎÎÏÇÏ ËÌÀÞÁ ÁÎÁÌÏÇÉÞÎÁ, ÎÏ ÓÏÄÅÒÖÉÔ ÓÅËÒÅÔÎÙÅ ÞÁÓÔÉ ËÌÀÞÅÊ É ÎÅ ÓÏÄÅÒÖÉÔ ÉÎÆÏÒÍÁÃÉÀ ÏÂ ÉÄÅÎÔÉÆÉËÁÔÏÒÅ ÐÏØÚÏ×ÁÔÅÌÑ.

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

```
joe% gpg --edit-key joe@duck.zu
Secret key is available.

pub  1024R/3AA48DCE  created: 2002-05-05 expires: never      trust: u/u
sub  1024D/13375D62  created: 2002-05-06 expires: never
sub  2048G/3745CA64  created: 2002-05-06 expires: 2004-05-05
sub  1024g/015418C9  created: 2002-05-06 expires: 2004-05-05
```

```
(1)  Joe Duck <joe@duck.zu>
(2). Joe Duck (cook) <jd@other.mail.zu>

Command>
```

ðÒÉ ÏÔÏÂÒÁÖÅÎÉÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ×Ù×ÏÄÉÔÓÑ ÉÎÆÏÒÍÁÃÉÑ Ï ÔÏÍ, ÄÏÓÔÕÐÅÎ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÉÌÉ ÎÅÔ. úÁÔÅÍ ×Ù×ÏÄÉÔÓÑ ÉÎÆÏÒÍÁÃÉÑ Ï ËÁÖÄÏÍ ËÌÀÞÅ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ðÅÒ×ÁÑ ËÏÌÏÎËÁ ÐÏËÁÚÙ×ÁÅÔ ÔÉÐ ËÌÀÞÁ. óÉÍ×ÏÌÙ `pub` ÏÂÏÚÎÁÞÁÀÔ ÏÔËÒÙÔÕÀ ÞÁÓÔØ ÇÌÁ×ÎÏÇÏ ÐÏÄÐÉÓÙ×ÁÀÝÅÇÏ ËÌÀÞÁ, Á ÓÉÍ×ÏÌÙ `sub` ÏÔËÒÙÔÕÀ ÞÁÓÔØ ÐÏÄÞÉÅÎÎÙÈ ËÌÀÞÅÊ. ÷ÔÏÒÁÑ ËÏÌÏÎËÁ ÐÏËÁÚÙ×ÁÅÔ ÄÌÉÎÕ ËÌÀÞÁ × ÂÉÔÁÈ, ÔÉÐ É ÉÄÅÎÔÉÆÉËÁÔÏÒ. ðÉÐ `D` ÜÔÏ ËÌÀÞ DSA, `R` - ËÌÀÞ RSA, `g` - ËÌÀÞ ElGamal, ÐÒÉÇÌÄÎÛÊ ÔÏÎØËÏ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ, `G` - ËÌÀÞ ElGamal, ËÏÔÏÒÙÊ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ É ÄÌÑ ÐÏÄÐÉÓÉ É ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. äÁÔÁ ÓÏÚÄÁÎÉÑ É ÏËÏÎÞÁÎÉÑ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ÐÏËÁÚÁÎÁ × ËÏÌÏÎËÁÈ ÔÒÉ É ÞÅÔÙÒÅ. éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÒÏÍÅ ËÌÀÞÅÊ.

äÏÐÏÎÉÔÅÌØÎÁÑ ÉÎÆÏÒÍÁÃÉÑ Ï ËÌÀÞÅ ÍÏÖÅ ÂÙÐØ ÐÏÕÐÅÎÁ ÒÁÚÌÉÞÎÙÉ ËÏÍÁÎÄÁÍÉ. ëÏÍÁÎÄ **toggle** ÐÅÒÅËÌÀÞÁÅÔ ÍÅÖÄÕ ÏÔËÒÙÔÏÊ É ÚÁËÒÙÔÏÊ ËÏÍÐÏÎÅÎÔÁÍÉ ÐÁÒÙ ËÌÀÞÅÊ, ÅÓÌÉ ÏÎÁ ÉÊÈ ÄÏÓÔÕÐÎÙ.

```
Command> toggle

sec  1024R/3AA48DCE  created: 2002-05-05 expires: never
ssb  1024D/13375D62  created: 2002-05-06 expires: never
ssb  2048G/3745CA64  created: 2002-05-06 expires: never
ssb  1024g/015418C9  created: 2002-05-06 expires: never
(1)  Joe Duck <joe@duck.zu>
(2)  Joe Duck (cook) <jd@other.mail.zu>

Command>
```

ðÒÅÄÓÔÁ×ÌÅÎÎÁÑ ÉÎÆÏÒÍÁÃÉÑ ÐÏÄÏÂÎÁ ×Ù×ÏÄÉÍÎÊ ÄÌÑ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. óÉÍ×ÏÌÙ `sec` ÕËÁÚÙ×ÁÀÔ ÓÅËÒÅÔÎÙÊ ÇÌÁ×ÎÙÊ ÐÏÄÐÉÓÙ×ÁÀÝÊ ËÌÀÞ, ÓÉÍ×ÏÌÙ `sbb` ÕËÁÚÙ×ÁÀÔ ÓÅËÒÅÔÎÙÅ ÐÏÄÞÉÅÎÎÙÅ ËÌÀÞÉ. ôÁËÖÅ ×Ù×ÏÄÑÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÌØÚÏ×ÁÔÅÌÑ ÉÚ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ.

ãÅÌÏÓÔÏÓÔØ ËÌÀÞÁ.

ðÒÉ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ ÏÔËÒÙÔÕÅ ËÏÍÐØÀÔÅÒÎÕÀ ÷ÁÛÅÇÏ ÇÌÁ×ÎÏÇÏ É ÐÏÄÐÉÓÁÎÎÙÈ ËÌÀÞÅÊ É ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÌØÚÏ×ÁÔÅÌÑ. ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ÜÔÏÇÏ ÍÁÔÅÒÉÁÌÁ, ÏÂÙÞÎÏ, ÒÉÓËÏ×ÁÎÎÏ Ó ÔÏÞËÉ ÚÒÅÎÉÑ ÂÅÚÏÐÁÓÎÏÓÔÉ, Ô.Ë. ÄÅÌÁÅÔ ×ÏÚÍÏÖÎÏ ÐÏÄÍÅÎÕ ËÌÀÞÁ. ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎ ÄÏÂÁ×ÌÅÎÉÑ ÉÌÉ ÚÁÍÅÎÙ ËÌÀÞÅÊ, ÉÌÉ ÄÏÂÁ×ÌÅÉÍ ÉÌÉ ÚÁÍÅÎÙ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÏÌØÚÏ×ÁÔÅÌÑ. ðÏÄÍÅÎÙ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ×ÛÌÍÝÉË ÍÖÅÔ ÉÚÍÅÎÑÔØ ÁÄÒÁ ÜÌÅÔÒÏÎÎÙÅ ÐÏÞÔÙ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÞÔÏÂÙ ÐÒÏÞÁÔØ ÐÅÒÅÐÉÓÁ×ÌÅÎÎÙÅ ÄÏ ÉÚÍÅÎÅÎÉÑ ðÒÉ ÉÚÍÅÎÅÎÉÉ ÏÄÎÏÇÏ ÉÚ ËÌÀÞÅÊ ÛÉÆÒÏ×ÁÎÑ, ×ÛÌÍÝÉË ÓÍÖÅÔ, ÔÁËÖÅ, ÒÁÓÛÉÆÒÏ×Ù×ÁØ ÐÅÒÅÐÉÓÁ×ÌÅÎÎÙÅ ÄÏ ÓÏÂÓÔÅÎÎÏÓÔÉ.

éÓÐÏÌØÚÏ×ÁÎÉÅ ÃÉÆÒÏ×ÙÈ ÐÏÄÐÉÓÅÊ ÒÅÛÁÅÔ ÜÔÏ ÐÒÏÂÌÅÍÕ. ëÏÇÄÁ ÄÁÎÎÙÅ ÐÏÄÐÉÓÁÎÙ ÓÅËÒÅÔÎÙÍ ËÌÀÞÏÍ, ÓÏÎÔ×ÅÔÓ×ÕÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÏÇÒÁÎÉÞÅÎ ÐÏÄÐÉÓÁÎÎÙÍÉ ÄÁÎÎÙÉ. äÒÕÇÉÉ ÓÌÏ×ÁÍÉ, ÔÏÎØËÏ ÓÏÎÔ×ÅÔÓ×ÕÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ É ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ ÄÁÎÎÙÅ ÎÅ ÂÙÌÉ ÉÚÍÅÎÅÎÙ. ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÚÁÝÉÝÅÎ ÏÔ ÉÚÍÅÎÅÎÉÑ ÉÓÐÏÌØÚÏ×ÁÎÉÑ

ÓÏÏÎ×ÅÔÓÔ×ÕÀÝÅÇÏ ÇÌÁ×ÎÏÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÄÌÑ ÐÏÄÐÉÓÉ ËÏÍÐØÎÅÎÔÏ× ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ É ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÏÌØÚÏ×ÁÔÅÌÑ, ÐÒÉ×ÑÚÙ×ÁÑ, ÔÁËÉÍ ÏÂÒÁÚÏÍ, ËÏÍÐØÎÅÎÔÙ ÇÌÁ×ÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ðÏÄÐÉÓØ ËÏÍÐØÎÅÎÔ× ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÓÏÎÔ×ÅÔÓÔ×ÕÀÝÉÍ ÇÌÁ×ÎÙÍ ÓÅËÒÅÔÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ ÎÁÚÙ×ÁÅÔÓÑ *ÓÁÍÏÐÏÄÐÉÓØÀ (self-signing)*, É ÏÔËÒÙÔÙÊ ËÌÀÞ, ÉÍÅÀÝÉÊ ÓÁÍÏÐÏÄÐÉÓÁÎÎÙÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÐÒÉ×ÑÚÁÎÎÙÅ Ë ÎÅÍÕ, ÎÁÚÙ×ÁÅÔÓÑ *ÓÅÒÔÉÆÉËÁÔÏÍ (certificate)*.

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

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

pub  1024R/3AA48DCE  created: 2002-05-05 expires: never      trust: u/u
sub  1024D/13375D62  created: 2002-05-06 expires: never
sub  2048G/3745CA64  created: 2002-05-06 expires: 2004-05-05
sub  1024g/015418C9  created: 2002-05-06 expires: 2004-05-05
(1)  Joe Duck <joe@duck.zu>
(2). Joe Duck (cook) <jd@other.mail.zu>

Command> check
uid  Joe Duck <joe@duck.zu>
sig!3       3AA48DCE 2002-05-05   [self-signature]
uid  Joe Duck (cook) <jd@other.mail.zu>
sig!3       3AA48DCE 2002-05-06   [self-signature]
```

ëÁË É ÏÖÉÄÁÌÏÓØ, ×ÓÅ ÐÏÄÐÉÓÉ ÓÄÅÌÁÎÙ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ Ó ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ËÌÀÞÁ `0x3AA48DCE`. óÁÍÏÐÏÄÐÉÓÉ ÎÁ ÐÏÄËÌÀÞÁÈ ÔÁËÖÅ ÐÒÅÄÓÔÁ×ÌÅÎÙ × ÏÔËÒÙÔÏÍ ËÌÀÞÅ, ÎÏ ÏÎÉ ÎÅ ÐÏËÁÚÙ×ÁÀÔÓÑ × GnuPG.

äÏÂÁ×ÌÅÎÉÅ É ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔÏ ËÌÀÞÁ

ëÁË ÎÏ×ÙÅ ÐÏÄËÌÀÞÉ, ÔÁË É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ ÍÏÇÕÔ ÂÙÔØ ÄÏÂÁ×ÌÅÎÙ Ë ÷ÁÛÅÊ ÐÁÒÅ ËÌÀÞÅÊ ÐÏÓÌÅ ÅÅ ÓÏÚÄÁÎÉÑ. éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÄÏÂÁ×ÌÑÅÔÓÑ ËÏÍÁÎÄÏÊ **adduid**. ÷ÁÍ ÂÕÄÅÔ ×ÙÄÁÎ ÚÁÐÒÏÓ ÏÔÏÓÔÅÎØÏÏ ÷ÁÛÅÇÏ ÉÍÅÎÉ, ÁÄÒÅÓÁ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÙ É ËÏÍÍÅÎÔÁÒÉÑ, ÔÁËÖÅ ËÁË ÐÓÉ ÓÏÚÄÁÎÉÉ ÐÁÒÙ ËÌÀÞÅÊ. ðÏÄËÌÀÞ ÄÏÂÁ×ÌÑÅÔÓÑ ËÏÍÁÎÄÏÊ **addkey**. ðÒÏÃÅÄÕÒÁ ÁÎÁÌÏÇÉÞÎÁ ÉÓÐÏÌØÚÕÅÍÏÊ ÐÒÉ ÐÅÒ×ÉÞÎÏÍ ÓÏÚÄÁÎÉÉ ÐÁÒÙ ËÌÀÞÅÊ. ðÏÄËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÐÏÄÐÉÓÁÎ DSA ËÌÀÞÏÍ, ElGamal ËÌÀÞÏÍ ÐÒÉÇÏÄÎÙÍ ÔÏÌØËÏ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ, ËÌÀÞÏÍ ElGamal ÐÒÉÇÏÄÎÙÍ É ÄÌÑ ÐÏÄÐÉÓÉ É ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ ÉÌÉ ËÌÀÞÏÍ RSA ÐÒÉÇÏÄÎÙÍ ÌÉÂÏ ÄÌÑ ÐÏÄÐÉÓÉ, ÌÉÂÏ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ëÏÇÁ ÓÏÚÄÁÀÔÓÑ ÐÏÄËÌÀÞ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÏÎÉ ÐÏÄÐÉÓÙ×ÁÀÔÓÑ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ, ÐÒÉ ÜÔÏÍ ÷Ù ÄÏÌÖÎÙ ××ÅÓÉ ÐÁÒÏÌØ, ËÏÔÏÒÙÊ ÚÁÝÉÝ£Î ÇÌÁ×ÎÙÊ ËÌÀÞ.

äÏÐÏÌÎÉÔÅÌØÎÙÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÒÉÍÅÎÉÍÙ, ËÏÇÄÁ ÷Ù ×ÙÓÔÒÐÁÅÔÅ × ÎÅÓËÏÌØËÉÈ ËÁÞÅÓÔ×ÁÈ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ ÒÁÄÏÔÉËÏÍ ËÁËÏÊ-ÌÉÂÏ ÆÉÒÍÙ É, × ÔÏ ÖÅ ×ÒÅÍÑ, ÐÏÌÉÓÉÞÁÓËÉÍ ÄÅÑÔÅÌÅÍ. ëÌÌÌÅÇ ÐÏ ÓÏÏÔ×ÅÔÓÔ×ÕÝÁÍÕ ×ÉÄÕ ÄÅÑÔÅÌØÎÏÓÔÉ ÂÕÄÕÔ ÚÎÁÔØ ÷ÁÓ ÐÏ ÓÏÏÔ×ÅÔÓÔ×ÕÝÁÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒ. ôÁË ËÁË ÜÔÉ ÇÒÕÐÐÙ ÌÀÄÅÊ ÎÅ ÐÒÏÔÅÓÔÉÒÕÀÔÓÑ, ÔÏ ËÁÖÄÁÑ ÇÒÕÐÐÁ ÍÏÅÔ ÎÅ ÄÏ×ÅÒÑØ ÄÒÕÇÉÍ ÉÄÅÎÔÉÆÉËÁÔÏÒ. óÌÅÄÏ×ÁÔÅÌØÎÏ, ÏÂÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÎÕÖÎÙ.

äÏÐÏÎÎÉÔÅÌØÎÙÅ ÐÏÄËÌÀÞÉ ÔÁËÖÅ ÍÏÇÕÔ ÂÙÔØ ÐÏÌÅÚÎÙ. éÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÁÓÓÏÃÉÉÒÏ×ÁÎÙÅ Ó ÷ÁÛÉÍ ÇÌÁ×ÎÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÚÁ×ÅÒÑÀÔÓÑ ÄÒÕÇÉÍ ÌÀÄØÍÉ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÅÅÔÅØ, É ÓÍÅÎÁ ÇÌÁ×ÎÏÇÏ ËÌÀÞÁ, ÓÌÅÄÏ×ÁÔÅÌØÎÏ, ÐÏÒÒÅÂÕÅÔ ÐÅÒÅÐÏÄÔ×ÅÒÖÄÅÎÑ. üÔÏ ÍÏÖÅÔ ÏÐÁÓÁÔØÓÑ ÓÌÏÎÙÍ É ÚÁÎÑÔØ ÍÍÇÏ ×ÒÅÍÅÎÉ, ÅÓÌÉ ÷Ù ÏÂÝÅÅÔÅÓØ ÓÏ ÍÍÇÉÍÉ ÌÀÄØÍÉ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÎÅÐÌÈÏ ÐÅÒÉÄÉÞÅÓËÉ ÍÅÎÑÔØ ÐÏÄËÌÀÞÉ ÛÉÆÒÏ×ÁÎÉÑ. åÓÌÉ ÐÏÄËÌÀÞ ×ÚÌÍÁÎ, ×ÓÅ ÄÁÎÎÙÅ, ÚÁÛÉÆÒÏ×ÁÎÙÅ ÉÍ, ÓÔÁÎÕ ÕÑÚ×ÉÍÙ. ðÒÉ ÓÍÅÎÅ ÐÏÄËÌÀÞÁ, ÕÑÚ×ÉÍÊ ÓÛÁÎÅÎ ÔÏÎØËÏ ÞÁÓÔØ ÄÁÎÎÙÈ.

ðÏÄËÌÀÞÉ É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÌØÚÏ×ÁÔÅÌÑ ÍÏÇÕÔ ÂÙÔØ ÕÄÁÌÅÎÙ. äÌÑ ÕÄÁÌÅÎÉÑ ÐÏÄËÌÀÞÁ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÌØÚÏ×ÁÔÅÌÑ, ÷Ù ÄÏÌÖÎÙ ÓÎÁÞÁÌÁ ×ÙÂÒÁÔØ ÅÇÏ, ÉÓÐÏÌØÚÕÑ ËÏÍÁÎÄÕ **key** ÉÌÉ **uid**. üÔÏ ËÏÍÁÎÄÙ ÐÅÒÅËÌÀÞÁÔÅÌÉ. îÁÐÒÉÍÅÒ, ËÏÍÁÎÄÁ **key *2*** ×ÙÂÅÒÅÔ ×ÔÏÒÏÊ ÐÏÄËÌÀÞ, ÐÏ×ÔÏÒÎÁÑ ËÏÍÁÎÄÁ **key *2*** ÏÓÔÁÅÔÓÑ ×ÙÂÏÒ. åÓÌÉ ÎÅ ÚÁÄÁÎÙ ÄÐÏÏÉÓÅÙÅ ÁÒÇÕÍÅÎÔÙ, ×ÙÂÏÒ ×ÓÅ ÐÏÄËÌÀÞÅÊ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ×ÐÌØÚÏ×ÁÔÅÌÑ ÂÕÄÅÔ ÏÐÅÌÅÎ. åÓÌÉ ÉÄÅÎÔÉÆÉËÁÔÏ ÐÌØÚÏ×ÁÔÅÌÑ, ËÏÔÏÔÙÊ ÎÁÄÏ ÕÄÁÌÉÔØ, ×ÙÀÔÁÎ, ÔÏ ËÏÍÁÎÄÁ **deluid** ÕÄÁÌÉÔ ÅÇÏ ÉÚ ËÌÀÞÁ. áÎÁÌÏÇÉÞÎÏ, ËÏÍÁÎÄÁ **delkey** ÕÄÁÌÑÅÔ ×ÓÅ ×ÙÀÔÁÎÎÙÅ ÐÏÄËÌÀÞÉ ÉÚ ÏÂÏÉÈ, ÏÔËÒÙÔÏÇÏ É ÓÅËÅÔÁÎÏÇÏ, ËÌÀÞÅÊ.

äÌÑ ÕÐÒÁ×ÌÅÎÉÑ ÌÏËÁÌØÎÙÍÉ ÎÁÂÏÒÁÍÉ ËÌÀÞÅÊ, ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔÏ× ËÌÀÞÁ -- ËÏÒÏÛÉÊ ÓÐÏÓÏÂ ÏÞÉÓÔÉÔØ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÄÒÕÇÉÈ ÌÀÄÅÊ ÏÔ ÎÅÎÕÖÏÇÏ ÍÁÔÅÒÉÁÌÁ. õÄÁÌÅÎÉÅ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÌØÚÏ×ÁÔÅÌÑ É ÐÏÄËÌÀÞÅÊ ÉÚ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ ËÌÀÞÁ, ÏÔÏ ÏÎÏ ÎÅ ÓÏÈÒÁÎÑÅÔÓÑ ÎÁ ÄÉÓËÅ, Ô.Ë. ÕÓÌÏÖÎÑÅÔ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÁ. ðÏ ÕÍÌÞÁÎÉÀ, ËÏÇÄÁ ÐÌØÚÏ×ÁÔÅÌÀ ÉÍÐÏÒÔÉÒÕÅÔ ÷ÁÛ ÏÂÎ×ÌÅÎÎÙÊ ÎÔËÒÙÔÙÊ ËÌÀÞ, ÔÏÔ ÏÂßÄÉÑÅÔ ÓÏ ÓÔÁÒÙÍ ËÌÀÞÏÍ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÅÓÌÉ ÏÎ ÅÓÔØ × ÅÇÏ ÎÁÂÏÒÅ. ëÌÉÐÎÌÅÎÔÙ ÏÂÏÉÈ ËÌÀÞÅÊ ÏßßÄÉÑÀÔÓÑ, É ÜÔÏ ÜÆÆÄËÔÉ×ÎÙÊ ÓÐÏÓÏÂ ×ÏÓÔÁÎÏ×ÉÔØ ÕÄÁÌÅÎÎÙÅ ÷ÁÉ ËÌÍÐÎÌÅÎÔÙ. þÔÏÂÙ ÐÓÁ×ÉÌØÎÏ ÏÂÎ×ÉÔØ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÅÓÌÉ ÏÎ ÅÓÔØ × ÅÇÏ ÎÁÂÏÒÅ ÄÎÏÅÎ ÓÎÁÐÁÍ ÕÄÁÌÉÔØ ÓÔÁÒÙÅ ÓÏÂÓÔÀ ×ÅÓÓÉÀ ÷ÁÛÅÇÏ ËÌÀÞÁ É ÔÏÌØËÏ ÚÁÔÅÍ ÉÍÐÏÒÔÉÒÕÅÔ ÎÏ×ÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ. üÔÏ ÄÏÂÁ×ÌÑÅÔ ÍÎÏÇÏ ÓÌÏÖÎÏÓÔÉ, Ó ËÌÎÔÏÒÙÍÉ ÷Ù ÏÂÝÅÅÔÅØ. ëÒÌÍÅ ÔÏÇÏ, ÅÓÌÉ ÷Ù ÏÐÒÁ×ÌÑÅÔÅ ËÌÀÞ ÍÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ, ÏßßÄÉÎÅÎÉÅ ÐÒÏÉÚÏÊÄÅÔ ÎÅÉÉÎÓÁÍÏ, É ÎÉËÔÏ ÉÚ ÐÌÕÐÅ×ÛÉÈ ÷ÁÛ ËÌÀÞ Ó ÓÅÒ×ÅÒÁ ÎÅ ÓÍÏÖÅÔ ÏÐÒÅÄÅÌÉÔØ, ÞÔÏ ÷Ù ÐÒÏ-ÔÏ ÔÁÍ ÕÄÁÌÉÌÉ. óÌÅÄÕ×ÁÔÅÌØÎÏ, ÄÌÑ ÏÂÝÅÇÏ ×ÙÂÏÒ×ÅÎÎÏÇÏ ËÌÀÞÁ ÌÕÞÛÅ ÏÔÏÚ×ÁÔØ ÓÏÌÔ×ÅÓÓ×ÕÀÉÅ ËÏÍÐÏÎÅÎÔÙ ËÌÀÞÁ, ÎÅÖÅÌÉ ÕÄÁÌÑÔØ ÉÈ.

ïÔÚÙ× ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ

äÌÑ ÏÔÚÙ×Á ÐÏÄËÌÀÞÁ ÏÎ ÄÏÌÖÅÎ ÂÙÔØ ×ÙÂÒÁÎ. âÕÄÕÞÉ ×ÙÂÒÁÎ, ÏÎ ÍÏÖÅÔ ÂÙÔØ ÏÔÏÚ×ÁÎ ËÏÍÁÎÄÏÊ **revkey**. ëÌÀÞ ÏÔÚÙ×ÁÅÔÓÑ ÄÏÂÁ×ÌÅÎÉÍ ÏÔÚÙ×ÁÀÝÅÊ ÓÁÍÏÐÏÄÐÉÓÉ Ë ËÌÀÞÕ. ÷ ÏÔÌÉÞÉÅ ÏÔ ÐÃÁÉÉ ËÏÍÁÎÄÏÊ ÓÔÒÏËÉ `--gen-revoke`, ÜÆÆÅËÔ ÎÁÓÔÕÐÁÅÔ ÎÅÍÅÄÌÅÎÎÏ.

```
Command> revkey
Do you really want to revoke this key? y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
Your decision? 2
Enter an optional description; end it with an empty line:
>
```

```
Reason for revocation: Key is superseded
(No description given)
Is this okay? y

You need a passphrase to unlock the secret key for
user: "Joe Duck (cook) <jd@other.mail.zu>"
1024-bit RSA key, ID 3AA48DCE, created 2002-05-05

pub  1024R/3AA48DCE  created: 2002-05-05 expires: never      trust: u/u
sub  1024D/13375D62  created: 2002-05-06 expires: never
sub  2048G/3745CA64  created: 2002-05-06 expires: 2004-05-05
rev! subkey has been revoked: 2002-05-07
sub  1024g/015418C9  created: 2002-05-06 expires: 2004-05-05
(1)  Joe Duck <joe@duck.zu>
(2). Joe Duck (cook) <jd@other.mail.zu>
```

éÄÅÎÔÉÆÉËÁÔÌÒ ÐÎÌØÚÏ×ÁÔÅÌÑ ÏÔÍÅÎÑÅÔÓÑ ÉÎÁÞÅ. ëÁË ÐÒÁ×ÉÌÏ, ÎÁ ÉÄÅÎÔÉÆÉËÁÔÌÒ ÐÎÌØÚÏ×ÁÔÅÌÑ ÓÔÁ×ÑÔÓÑ ÐÏÄÐÉÓÉ, ÕÄÏÓÔÏ×ÅÒÑÅÔ ÌÉÞÎÏÓÔØ ÏÂÌÁÄÁÔÅÌÑ ËÌÀÞÁ. ôÅÏÒÅÔÉÞÅÓËÉ, ÉÄÅÎÔÉÆÉËÁÔÌÒ ×ÅÞÅÎ, Ô.Ë. ÞÅÌ×ÅË ×ÓÅÇÄÁ ÏÓÔÁ£ÔÓÑ ÓÏÂÏÊ. îÁ ÐÒÁËÔÉËÅ, ÏÄÎÁËÏ, ÜÌÅÍÅÎÔÙ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÎØÚÏ×ÁÔÅÌÑ, ÔÁËÉÅ, ËÁË ÁÄÒÅÓ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÙ É ËÏÍÅÎÔÁÒÉÊ ÍÇÕÔ ÉÚÍÅÎÑØÓÑ, ÄÅÌÁÑ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÎØÚÏ×ÁÔÅÌÑ ÎÅÄÅÉÓÔ×ÉÔÅÌØÎÙÍ.

óÐÅÃÉÆÉËÁÃÉÑ OpenPGP

* *ðÅÒ×ÁÑ ÓÓÙÌËÁ ÎÁ OpenPGP*

ÎÅ ÐÏÄÄÅÒÖÉ×ÁÅÔ ÏÔÚÙ× ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÎØÚÏ×ÁÔÅÌÑ, ÎÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÍÏÖÅÔ ÂÙÔØ ÜÆÆÅËÔÉ×ÎÏ ÏÔÚÙ×ÁÎ ÏÔÚÙ×ÍÏ ÓÁÍÏÐÏÄÐÉÓÉ ÎÁ ÎÅÍ. ðÏ ÐÒÉÞÉÎÁÍ ÂÅÚÐÁÓÎÏÓÔÉ, ÏÐÉÓÁÎÙÍ **ÒÁÎÅÅ**, ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕ ÄÏ×ÅÒÑÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ ÐÎØÚÏ×ÁÔÅÌÑ ÎÅ ÉÍÅÀÝÅÍ ÓÁÍÏÐÏÄÐÉÓÉ.

ðÏÄÐÉÓØ ÏÔÚÙ×ÅÂÓÑ ËÏÍÁÎÄÏÊ **revsig**. ô.Ë. ÷Ù ÍÏÖÅÅ ÉÍÅÔØ ÌÀÂÏÅ ÞÉÓÌÏ ÐÏÄÐÉÓÅÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ× ÐÎØÚÏ×ÁÔÅÌÑ, ÐÒÏÇÒÁÍÍÁ ÚÁÐÒÏÓÉÔ ÷ÁÓ Ï ËÁÖÄÏÊ ÐÏÄÐÉÓÉ.

```
Command> revsig
You have signed these user IDs:
     Joe Duck <joe@duck.zu>
   signed by 3AA48DCE at 2002-05-05
     Joe Duck (cook) <jd@other.mail.zu>
   signed by 3AA48DCE at 2002-05-06
user ID: "Joe Duck <joe@duck.zu>"
signed with your key 3AA48DCE at 2002-05-05
Create a revocation certificate for this signature? (y/N) n
user ID: "Joe Duck (cook) <jd@other.mail.zu>"
signed with your key 3AA48DCE at 2002-05-06
Create a revocation certificate for this signature? (y/N) y
You are about to revoke these signatures:
     Joe Duck (cook) <jd@other.mail.zu>
   signed by 3AA48DCE at 2002-05-06
Really create the revocation certificates? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  4 = User ID is no longer valid
  Q = Cancel
Your decision? 4
Enter an optional description; end it with an empty line:
>
Reason for revocation: User ID is no longer valid
(No description given)
Is this okay? y
```

```
You need a passphrase to unlock the secret key for
user: "Joe Duck (cook) <jd@other.mail.zu>"
1024-bit RSA key, ID 3AA48DCE, created 2002-05-05


pub  1024R/3AA48DCE  created: 2002-05-05 expires: never      trust: u/u
sub  1024D/13375D62  created: 2002-05-06 expires: never
sub  2048G/3745CA64  created: 2002-05-06 expires: 2004-05-05
rev! subkey has been revoked: 2002-05-07
sub  1024g/015418C9  created: 2002-05-06 expires: 2004-05-05
(1)  Joe Duck <joe@duck.zu>
(2). Joe Duck (cook) <jd@other.mail.zu>
```

ïÔÏÚ×ÁÎÎÙÊ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÎØÚÏ×ÁÔÅÌÑ ÕËÁÚÁÎ ÏÔÚÙ×ÁÀÝÅÊ ÐÏÄÐÉÓØÀ ÐÒÉ ÐÅÒÅÐÉÌÅÉÉ ÐÏÄÐÉÓÅ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁÈ ÐÎØÚÏ×ÁÔÅÌÑ.

```
Command> check
uid  Joe Duck <joe@duck.zu>
sig!3       3AA48DCE 2002-05-05   [self-signature]
uid  Joe Duck (cook) <jd@other.mail.zu>
rev!        3AA48DCE 2002-05-07   [revocation]
sig!3       3AA48DCE 2002-05-06   [self-signature]
```

ïÔÚÙ× É ÐÏÄËÌÀÞÅÊ, É ÓÁÍÏÐÏÄÐÉÓÅÊ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÅ ÐÎØÚÏ×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×ÌÅÎÉÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ É ÏÂßÄÉÎÅÎÉÉ ÅÇÏ Ó ÒÁÎÎÉÍÉ ËÏÐÉÑÍÉ. ïÔÚÙ×, ÔÁËÉÍ ÏÀÓÁÚÉÍ, ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ Õ ×ÓÅÈ ÂÕÄÅÔ ÎÅÐÒÏÔÉ×ÏÔÅÞ×ÁÑ ËÏÐÉÑ ÷ÁÛÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ.

éÚÍÅÎÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ

óÒÏË ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎ ËÏÍÁÎÄÏÊ **expire** ÉÚ ÍÅÎÀ ÒÅÄÁËÔÉÒ×ÁÎÉÑ ËÌÀÞÁ. åÓÌÉ ÎÅÔ ×ÙÂÒÁÎÎÙÈ ËÌÀÞÅÊ, ÔÏ ÂÕÄÅÔ ÉÚÍÅÎÅÎ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ÐÒ×ÉÞÎÏÇÏ ËÌÀÞÁ. éÎÁÞÅ ÉÚÍÅÎÑÅÔÓÑ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ×ÙÂÒÁÎÎÏÇÏ ÐÏÄÞÉÎÅÎÎÏÇÏ ËÌÀÞÁ.

÷ÒÅÍÑ ÏËÏÎÞÁÎÉÑ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ Ó×ÑÚÁÎÏ Ó ÓÁÍÏÐÏÄÐÉÓØÀ ÎÁ ËÌÀÞÅ. ïËÏÎÞÁÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ÉÚÍÅÎÑÅÔÓÑ ÕÄÁÌÅÎÉÍ ÓÔÁÒÏÊ ÐÏÄÐÉÓÉ É ÄÏÂÁ×ÌÅÎÉÅÍ ÎÏ×ÏÊ. ôÁË ËÁË ÷ÁÛÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕÔ ÕÄÁÌÑÔÓØ ÓÔÁÒÙÅ ÐÏÄÐÉÓÉ É ÄÏÂÁ×ÌÅÎÉÅ ÎÏ×ÏÊ. ôÁË ËÁË ÷ÁÛÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕÔ ×ÉÄÅÎÙ ÐÏÄÐÉÓÅÊ ÓÔÁÒÙÈ ËÌÀÞÅÊ, ÐÏÓËÏÌØËÕ ÏÎÉ ÎÅ ÂÕÄÕÔ ÐÒÉÎÉÍÁÔØÓÑ ÐÒÉ ÐÒÏ×ÅÒËÅ ÐÏÄÐÉÓÅÊ. ðÒÉÄÅÔÓÑ ÏÂÎÏ×ÉÔØ ÉÈ ÏÔ ÓÅÒ×ÅÒÏ×, ÐÒÉÕÞÉÔÏ ×ÁÛÉ ËÏÌÌÅÇÉ ÄÅÊÓÔ×ÉÑ ÷ÁÛÅÇÏ ËÌÀÞÁ.

ðÒÏ×ÅÒËÁ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ

÷ ÇÌÁ×Å 1 ÂÙÌÁ ÏÐÉÓÁÎÁ ÐÒÏÃÅÄÕÒÁ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÏÐÅÒÁÃÉÏÎÎÏÊ ÓÉÓÔÅÍÙ: ËÏÒÒÅÓÐÏÎÄÅÎÔ ÌÉÞÎÏ ÐÒÏ×ÅÒÑÅÔ ÏÐÅÒÁÃÉÏÎÎÕÀ ÓÉÓÔÅÍÕ, ÞÔÏ ÏÎ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÉÍÅÅÔ ÄÏÓÔÕÐ Ë ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÅÍÕ ËÌÀÞÕ, É ÚÁÔÅÍ ÷Ù ÐÏÄÐÉÓÕ×ÁÅÔÅ ÅÇÏ ÏÐÅÒÁÃÉÏÎÎÕÀ ÓÉÓÔÅÍÕ. ðÒÉ ÌÉÞÎÏÊ ÐÒÏ×ÅÒËÅ ÏÐÅÒÁÃÉÏÎÎÁÑ ×ÌÁÄÅÌØÃÅÍ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ Õ×ÅÒÅÎÙ, ÞÔÏ ËÌÀÞ

ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÐÒÉÎÁÄÌÅÖÉÔ ÅÍÕ, É, ÐÏÄÐÉÓÁ× ÅÇÏ, ÷Ù ÓÍÏÖÅÔÅ ÏÂÎÁÒÕÖÉÔØ ÌÀÂÏÅ ÉÚÍÅÎÅÎÉÅ ËÌÀÞÁ × ÂÕÄÕÝÅÍ. ë ÓÏÖÁÌÅÎÀ, ÜÔÁ ÐÒÏÃÅÄÕÒÁ ÐÒÁËÔÉÞÅÓËÉ ÎÅ×ÏÚÍÏÖÎÁ ÅÓÌÉ ÷Ù ËÏÎÔÒÏÌÉÒÕÅÔÅ Ó ÂÎØÛÉÍ ÞÉÓÌÏÍ ÌÀÄÅÊ, ÌÉÂÏ ÎÅ ÚÎÁËÏÍÙ ÓÏ ×ÓÅÍÉ ÉÚ ÎÉÈ ÌÉÞÎÏ.

GnuPG ÒÅÛÁÅÔ ÜÔÕ ÐÒÏÂÌÅÍÕ ÐÒÉ ÐÏÍÏÝÉ ÍÅÈÁÎÉÚÍÁ ÉÍÅÎÕÅÍÏÇÏ *ÓÅÔØ ÄÏ×ÅÒÉÑ (web of trust)*. ÷ ÍÏÄÅÌÉ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÏÔ×ÅÔÓÔ×ÅÎÎÏÓÔØ ÚÁ ÐÒÏ×ÅÒÅÎÎÕÀ ËÌÀÞÅÊ ×ÍÚÌÏÖÅÎÁ ÎÁ ÌÀÄÅÊ, ËÏÔÏÒÕÍ ÷Ù ÄÏ×ÅÒÑÅÔÅ. îÁÐÒÉÍÅÒ, ÐÒÄÐÏÏÖÉÍ

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

åÓÌÉ üÌÉÓ Õ×ÅÒÎÁ, ÞÔÏ âÌÜÊË ÐÒÏ×ÅÒÑÅÔ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÅÊ, ËÏÔÏÒÙÅ ÏÎ ÐÏÄÐÉÓÙ×ÁÅÔ, ÔÏ üÌÉÓ ÍÏÖÅÔ ÂÙÔØ Õ×ÅÒÅÎÁ, ÞÔÏ ËÌÀÞÉ èÌÏÊ É äÈÁÒÍÙ ÄÏÓÔÏ×ÅÒÎÙ ÎÅ ÐÒÏ×ÅÒÑÀÔ ÉÓÐÏÌØÚÕÅÔ Ó×ÏÀ ÄÏÓÔÏ×ÅÒÎÕÀ ËÏÐÉÀÖÏÇÏ ËÌÀÞÁ âÌÜÊËÁ ÄÌÑ ÐÒÏ×ÅËÉ ÅÇÏ ÐÏÄÐÉÓÉ ÎÁ ËÌÀÞÁÈ èÌÏÊ É äÈÁÒÍÙ. ÷ÏÎÂÝÅ, ÐÒÅÄÐÌÁÇÁÑ, ÞÔÏ üÌÉÓ ÓÏ×ÅÒÛÅÎÎÏ Õ×ÅÒÅÎÁ, ÞÔÏ ×ÓÅ ÐÒÁ×ÉÌØÎÏ ÐÒÏ×ÅÑÀÔ ËÌÀÞÉ, ÐÅÒÅÄ ÔÅÍ ËÁË ÉÈ ÐÏÄÐÉÓÁÔØ, ÔÏ ÌÀÂÏÊ ËÌÀÞ, ÐÏÄÐÉÓÁÎÎÙÊ ÄÏÓÔÏ×ÅÒÎÕÀ ËÌÀÞÏÍ, ÂÕÄÅÔ ÄÏÓÔÏ×ÅÒÎÙÍ.

äÏ×ÅÒÅÁ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ

îÁ ÐÒÁËÔÉËÅ ÄÏ×ÅÒÅÁ ÓÕÂßÅËÔÉ×ÎÏ. îÁÐÒÉÍÅÒ, ËÌÀÞ âÌÜÊËÁ ÄÏÓÔÏ×ÅÒÅÎ, Ô.Ë. üÌÉÓ ÐÏÄÐÉÓÁÌ ÅÇÏ, ÎÏ ÎÁ ÍÏÖÅÔ ÎÅ ÂÙÔØ Õ×ÅÒÅÎ, ÞÔÏ âÌÜÊË ÐÒÁ×ÉÌØÎÏ ÐÒÏ×ÅÒÑÅÔ ËÌÀÞÉ, ËÏÔÏÒÙÅ ÏÎ ÐÏÄÐÉÓÙ×ÁÅÔ. ÷ ÜÔÏÍ ÓÌÕÞÁÅ, ÎÁ ÂÕÄÕÝÅÍ ÓÏÂÓÔÖÎÉÊ ÐÒÉ×Ù×ÁÑØ ÎÁ ÐÏÄÐÉÓÉ âÌÜÊËÁ. íÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÒÅÚÕÌØÔÁÔÕ Ó×ÑÚÙ×ÁÑ Ó ËÁÖÄÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ × ÷ÁÛÅÍ ÎÁÂÏÒÅ ÚÎÁÞÅÎ ÕÒÏ×ÅÎØ ÷ÁÛÅÇÏ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ. éÍÅÅÔÓÑ ÐÑÔØ ÕÒÏ×ÎÅÊ ÄÏ×ÅÒÉÑ.

unknown (ÎÅÉÚ×ÅÓÔÎÅ)

> îÉÞÅÇÏ ÎÅ ÉÚ×ÅÓÔÎÏ Ï ÐÌÎÉÔÉËÅ ÐÏÄÐÉÓÁÎÉÑ ËÌÀÞÅÊ ÄÁÎÎÙÍ ×ÌÁÄÅÌØÃÅÍ. ëÌÀÞÁÍ × ÷ÁÛÅÍ ÎÁÂÏÒÅ, ËÏÎÅ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÇÏ, ÐÀÒ×ÏÎÁÞÁÌØÎÏ ÐÒÉÓ×ÁÉ×ÁÅÔÓÑ ÜÔÏÔ ÕÒÏ×ÅÎØ ÄÏ×ÅÒÉÑ.

none (ÎÅÔ)

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

marginal (ÇÒÁÎÉÞÎÏÅ)

> ðÏÎÉÍÅÔ ÓÍÙÓÌ ÐÏÄÐÉÓÁÎÉÑ ËÌÀÞÅÊ É ÐÒÏ×ÅÒÑÔ ÉÈ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ÐÅÒÅÄ ÔÅÍ, ËÁË ÐÏÄÐÉÓÙ×ÁÔØ.

full (ÐÎÎÏÅ)

> ÷ÌÄÅÌÅÃ ÏÞÅÎØ ÒÁÚÂÏÒÞÉ× × ÐÏÄÐÉÓÉ ËÌÀÞÅÊ É ÔÝÁÔÅÌØÎÏ ÐÒÏ×ÅÒÑÔ ÉÈ ÐÅÒÅÄ ÔÅÍ, ËÁË ÐÏÄÐÉÓÙ×ÁÔØ.

ultimate (ÂÅÚÏÇÏ×ÏÒÏÞÎÅ)

÷ÌÁÄÅÌØÃÕ ÄÁÎÎÏÇÏ ËÌÀÞÁ ÷Ù ×ÅÒÉÔÅ ËÁË ÓÁÍÏÍÕ ÓÅÂÅ.

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 ËÏÍÁÎÄÁ **trust** ÒÅÖÉÍ ÒÅÄÁËÔÉÒ×ÁÎÉÑ ËÌÀÞÁ. ÷ ÜÔÏÍ ÐÒÉÍÅÒÅ üÌÉÓ ÒÅÄÁËÔÉÒÕÅÔ ÕÒÏ×ÎØ Ó×ÏÅÇÏ ÄÏ×ÅÒÉÑ âÌÜÊËÕ É ÚÁÔÅÍ ÏÂÎÏ×ÌÑÅÔ ÂÁÚÕ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ, ÞÔÏÂÙ ÐÒÅÄÏÔ×ÒÁÔÉÔØ ËÌÀÞÅÊ ÏÓÎ×Ù×ÁÑØ ÎÁ ÎÏ×ÏÍ ÚÎÁÞÅÎÉÉ ÄÏ×ÅÒÉÑ âÌÜÊËÕ.

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

pub  1024R/01A1FE63  created: 2002-05-01 expires: never      trust: -/f
sub  1024R/526C7F7F  created: 2002-05-01 expires: 2003-05-01
(1). Blake (dumb) <blake@anywhere.ru>

Command> trust
pub  1024R/01A1FE63  created: 2002-05-01 expires: never      trust: -/f
sub  1024R/526C7F7F  created: 2002-05-01 expires: 2003-05-01
(1). Blake (dumb) <blake@anywhere.ru>

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
 5 = I trust ultimately
 i = please show me more information
 m = back to the main menu

Your decision? 3

pub  1024R/01A1FE63  created: 2002-05-01 expires: never      trust: m/f
sub  1024R/526C7F7F  created: 2002-05-01 expires: 2003-05-01
(1). Blake (dumb) <blake@anywhere.ru>
```

äÏ×ÅÒÅÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ É ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÁ ×Ù×ÏÄÑÔÓÑ ÓÐÒÁ×Á ÏÔ ËÌÀÞÁ, ËÏÇÄÁ ×Ù×ÏÄÉÔÓÑ ËÌÀÞ. äÏ×ÅÒÅ ×ÌÁÄÅÌØÃÕ ×Ù×ÏÄÉÔÓÑ ÐÅÒ×ÙÍ, ÄÏÓÔ×ÅÒÎÏÓÔØ ËÌÀÞÁ ×ÔÏÒÏÊ[1]. ðÑÔØ ÕÒÏ×ÎÅ ÄÏ×ÅÒÉÑ/ÄÏÓÔ×ÅÒÎÏÓÔÉ ÏÂÏÚÎÁÞÁÀÔÓÑ ÓÉÍ×ÏÌÁÍÉ: ÎÅÉÚ×ÅÓÔÎÙÊ (q), ÎÅÔ (n), ÇÒÁÎÉÞÎÙÊ (m), ÐÏÌÎÙÊ (f), ÂÅÚÏÇÏ×ÏÌÎÙÊ (u). ÷ ÜÔÏÍ ÓÌÕÞÁÅ, ËÌÀÞ âÌÜÊËÁ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÅÎ, Ô.Ë. üÌÉÓ ÓÁÍÁ ÐÏÄÐÉÓÁÌÁ ÅÇÏ. éÚÍÁÞÁÌØÎÏ ÕÓÔÁÎÏ×ÌÅÎÏ ÎÅÉÚ×ÅÓÔÎÏÅ ÄÏ×ÅÒÅ ÏÔÎÏÓÉÔÅÌØÎÏ ÐÒÁ×ÉØÎÏÓÔÉ ÐÏÄÐÉÓÉ âÌÜÊËÍÍ ËÌÀÞÅÊ, ÎÏ üÌÉÓ ÒÅÛÁÅÔ ÕÓÔÁÎÏ×ÉÔØ ÇÒÁÎÉÞÎÙÊ ÕÒÏ×ÅÎØ ÄÏ×ÅÒÑ.

éÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏ×ÅÒÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ

óÅÔØ ÄÏ×ÅÒÑ ÐÏÚ×ÏÌÑÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ ×ÅØÍÁ ÇÉÂËÉÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ. åÓÌÉ ÐÒÅÄÄ ÄÏÓÔÏ×ÅÒÎÙÍ ÓÞÉÔÁÌÉÓØ ÔÏØËÏ ÔÅ ËÌÀÞÉ,

ËÏÔÏÒÙÅ ÷Ù ÐÏÄÐÉÓÁÌÉ ÌÉÞÎÏ, ÔÏ ÔÅÐÅØ ÉÓÐÏØÚÕÅÔÓÑ ÓÌÅÄÕÀÝÉÅ ÁÌÇÏÒÉÔÍÉ. ëÌÀÞ *K* ÓÞÉÔÁÅÔÓÑ ÄÏÓÔÏ×ÅÒÎÙÍ, ÅÓÌÉ ÎÅ ÕÄÌ×ÌÅÔ×ÏÑÅÔ ÓÌÅÄÕÀÝÅÍ Ä×ÕÍ ÕÓÌÏ×ÉÑÍ:

1. ÏÎ ÐÏÄÐÉÓÁÎ ÄÏÔÁÔÏÞÎÙÍ ËÏÌÉÞÅÓÔ×ÏÍ ÄÏÔÏ×ÅÒÙÈ ËÌÀÞÅÊ, Ô.Å.

   - ÷Ù ÐÏÄÐÉÓÁÌÉ ÅÇÏ ÌÉÞÎÏ (ÉÌÉ ÏÂÌÁÄÁÔÅÌØ ËÌÀÞÁ, ËÏÔÏÒÏÍÕ ÷Ù ÂÅÚÏÇÏ×ÏÒÞÎÏ ÄÏ×ÅÒÑÅÔÅ),
   - ÏÎ ÂÙÌ ÐÏÄÐÉÓÁÎ ËÌÀÞÏÍ ×ÌÁÄÅÌØÃÅÍ ËÏÔÏÒÏÇÏ ÷Ù ÐÏÌÎÏÓÔØÀ ÄÏ×ÅÒÑÅÔÅ, ÉÌÉ
   - ÏÎ ÂÙÌ ÐÏÄÐÉÓÁÎ ÔÒÅÍ ËÌÀÞÁÍ Ó ÇÒÁÎÉÞÎÙÍ ÕÒÏ×ÎÅÍ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÅ; É

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

äÌÉÎÁ ÃÅÐÏÞËÉ, ÞÉÓÌÏ ÔÒÅÂÕÅÍÙÈ ËÌÀÞÅÊ Ó ÇÒÁÎÉÞÎÙÍ ÕÒÏ×ÎÅÍ ÄÏ×ÅÒÉÑ É ÞÉÓÌÏ ËÌÀÞÅÊ Ó ÐÏÌÎÏÍ ÄÏ×ÅÒÅÍ ÍÏÔÅÔ ÂÙÔ ÉÚÍÅÎÅÎÏ ÐÒÉ ÐÏÍÏÝÉ ÐÁÒÁÍÅÔÒ× `--max-cert-depth`, `--marginals-needed` É `--completes-needed`. ãÉÆÒÙ ÐÒÉ×ÅÄÅÎÎÙÅ ×ÙÛÅ - ÚÎÁÞÅÎÉÑ ÉÓÐÏÌØÚÕÅÍÙÅ GnuPG ÐÏ ÕÍÍÏÞÁÎÉÀ.

. 3-1 ÒÁÓÓÍÏÔÒÉÍ ÓÅÔØ ÄÏ×ÅÒÑ ÎÁÞÉÎÁÀÝÕÀÓÑ Ó üÌÉÓ. çÒÁÆ ÉÌÌÀÓÔÒÉÒÕÅÔ ËÔÏ ÐÏÄÐÉÓÁÌ ÞÅÊ ËÌÀÞ. ôÁÂÌÉÃÁ ÐÏËÁÚÙ×ÁÅÔ ËÌÀÞÉ, ËÏÔÏÒÙÅ üÌÉÓ ÐÒÉÚÎÁÅÔ ÄÏÓÔÏ×ÅÒÎÙÍ ÄÏ×ÅÒÉÔÅÌÅÍ ÄÒÕÇÉÈ ÞÌÅÎÏ×. ÇÒÁÆ ÉÌÌÀÓÔÒÉÒÕÅÔ ÔÁËÖÅ, ÞÔÏ ÄÌÑ ÐÒÉÚÎÁÎÉÑ ËÌÀÞÁ ÄÏÓÔÁÔÏÞÎÏ ÔÒÅÈ ÐÏÄÐÉÓÅÊ.

* *ðÏÊÌÅÔÅÁÌØÎÁÑ ÏÛÉÂËÁ: ÏÐÃÉÑ `--completes-needed` × ËÏÍÁÎÄÅ ÓÔÒÏËÅ ÂÕÄÕÐ ÐÒÉÇÎÏÒÉÒÏ×ÁÍÁ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ Ó ËÏÍÁÎÄÏÊ `--update-trustdb`. úÎÁÞÅÎÉÅ ×ÙÞÉÓÌÅÔÓÑ ËÏÒÒÅËÔÎÏ ÅÓÌÉ ÕËÁÚÁÔØ ÅÇÏ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.*

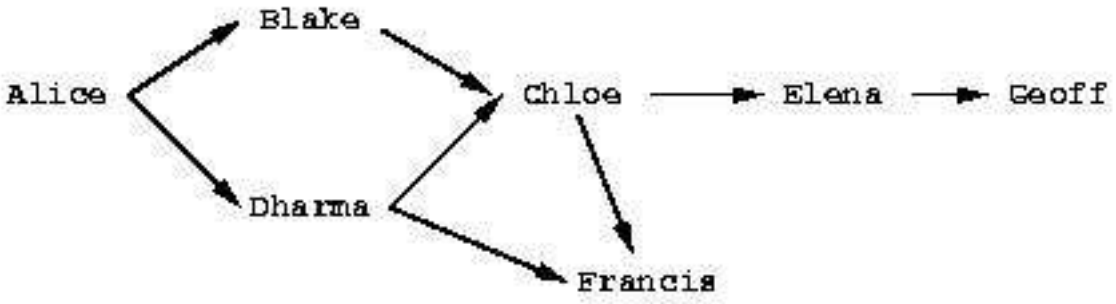
üÔÏÔ ÐÒÉÍÅÒ ÐÒÅÄÐÏÌÁÇÁÅÔ, ÞÔÏ ÄÌÑ ÐÒÉÚÎÁÎÉÑ ÄÒÕÇÏÇÏ ËÌÀÞÁ ÄÏÓÔÁÔÏÞÎÙ ÔÒÅÂÕÅÔÓÑ Ä×Á ËÌÀÞÁ Ó ÇÒÁÎÉÞÎÙÍ ÄÏ×ÅÒÅÍ ÉÌÉ ÏÄÎÏ Ó ÐÏÌÎÙÍ. íÁËÓÉÍÁÌØÎÁÑ ÄÌÉÎÁ ÃÅÐÏÞËÉ ÒÁ×ÎÁ ÔÒÅÍ.

ðÒÉ ×ÙÞÉÓÌÅÎÉÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ, × ÜÔÏÍ ÐÒÉÍÅÒÅ, ËÌÀÞÉ âÌÜÊËÁ É äÈÁÒÍÙ ×ÓÅÇÄÁ ÓÞÉÔÁÀÔÓÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÍÉ, Ô.Ë. ÏÎÉ ÐÏÄÐÉÓÁÎÙ üÌÉÓ. äÏÓÔÏ×ÅÒÎÏÓÔØ ÄÒÕÇÉÈ ËÌÀÞÅÊ ÚÁ×ÉÓÉÔ ÏÔ ÄÏ×ÅÒÉÑ. ÷ ÐÅÒ×ÏÍ ÓÌÕÞÁÅ, ÄÏ×ÅÒÑÑ äÈÁÒÍÅ ÐÏÌÎÏÅ, ÞÔÏ ÄÅÌÁÅÔ ËÌÀÞ èÏÎÊ É æÒÜÎÓÉÓÁ ÐÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙÍÉ. ÷Ï ×ÔÏÒÏÍ ÓÌÕÞÁÅ, ÄÏ×ÅÒÑÑ âÌÜÊËÕ É äÈÁÒÍÅ ÇÒÁÎÉÞÎÅ. ô.Ë. Ä×Á ËÌÀÞÁ Ó ÇÒÁÎÉÞÎÙÍ ÄÏ×ÅÒÅÍ ÔÒÅÂÕÅÔÓÑ ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ, ËÌÀÞ èÏÎÊ ÂÕÄÅÔ ÐÒÉÎÉÍÁÔØÓÑ ÄÏÓÔÏ×ÅÒÎÙÍ, ÎÏ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÁ æÒÜÎÓÉÓÁ ÂÕÄÅÔ ÔÏÌØËÏ ÞÁÓÔÉÞÎÏÊ ÐÏÄÔ×ÅÒÖÄÅÎÁ. ÷ ÓÌÕÞÁÅ ÇÒÁÎÉÞÎÏÇÏ ÄÏ×ÅÒÑ èÏÎÊ É äÈÁÒÍÅ, ËÌÀÞ èÏÎÊ ÂÕÄÅÔ ÞÁÓÔÉÞÎÏÊ ÄÏÓÔÏ×ÅÒÎÏ, Á ËÌÀÞ äÈÁÒÍÙ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎ. ëÌÀÞ æÒÜÎÓÉÓÁ ÂÕÄÅÔ ÞÁÓÔÉÞÎÏÊ ÄÏÓÔÏ×ÅÒÎÏ, Ô.Ë. ÔÏÌØËÏ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙÅ ËÌÀÞ ÍÖÅÂ ÂÙÔ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÒÉÚÎÁÎÉÑ ÄÒÕÇÉÈ ËÌÀÞÅÊ, Á ÅÄÉÎÓÔ×ÅÎÎÙÅ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙÅ ËÌÀÞ, ËÏÔÏÒÙÍ ÐÄÐÉÓÁÎ ËÌÀÞ æÒÜÎÅÁ, ÜÔÏ ËÌÀÞ äÈÁÒÍÙ. ðÏÌÅ ÄÏÂÁ×ÌÅÎÉÑ ÇÒÁÎÉÞÎÏÇÏ ÄÏ×ÅÒÑ âÌÜÊËÕ ËÌÀÞ èÏÎÊ ÓÔÁÎÏ×ÉÔÓÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÙÍ É ÍÖÅÂ ÂÙÔ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÅÎÎÏÇÏ ËÌÀÞÁ æÒÜÎÓÉÓÁ É ÞÁÓÔÉÞÎÏÇÏ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÉÔÅÌÅÍ ËÌÀÞÁ åÌÅÎÙ. îÁËÏÎÅÃ, ÅÓÌÉ ÄÏ×ÅÒÅ âÌÜÊËÕ, èÏÎÊ É åÌÅÎÅ ÐÏÌÎÏÊ, ÜÔÏÇÏ ×ÓÅ ÅÝÅ ÎÅ ÄÏÓÔÁÔÏÞÎÏ ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ äÕÆÁ, Ô.Ë. ÍÁËÓÉÍÁÌØÎÁÑ ÄÌÉÎÁ ÃÅÐÏÞËÉ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÒÁ×ÎÁ ÔÒÅÍ, ÎÏ ÐÕÔÏ ÏÎ äÕÆÁ Ë üÌÉÓ ÒÁ×ÅÎ ÞÅÔÙÒÅÍ.

íÏÄÅÌØ ÓÅÔÉ Ä×ÅÒÉÑ ÒÅÁÌÉÚÕÅÔ ÇÉÂÒÉÄ Ë ÐÒÏÂÌÅÍÅ ÂÅÚÏÐÁÓÎÏÇÏ ÏÂÍÅÎÁ ËÌÀÞÁÍÉ. ïÎ ÐÚ×ÏÑÅÔ ÎÁÓÔÒÁÉ×ÁÔØ GnuPG × ÓÏÔÔ×ÅÔÓÔ×ÉÉ Ó ÷ÁÛÉÍÉ

ÐÏÔÒÅÂÎÏÓÔÑÍÉ. ÷Ù ÍÏÖÅÔÅ ÔÒÅÂÏ×ÁÔØ ÍÎÏÇÏ ËÏÒÏÔËÉÈ ÃÅÐÏÞÅË ÏÔ ÷ÁÛÅÇÏ ËÌÀÞÁ ÄÏ ËÌÀÞÁ *K* ÄÌÑ ÐÒÉÚÍÁÎÉÑ ÅÇÏ ÄÏÓÔÏ×ÅÒÎÙ. 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 ÐÎØÚÏ×ÁÔÅÌÑ. ãÅÎÁ ÚÁ ÔÁËÕÀ ÎÁÄÅÖÎÓÔØ, ËÏÎÅÞÎÏ, ×ÙÛÅ, Ô.Ë. ÷Ù ÌÉÞÎÏ ÄÏÔÏÙ ÐÒÏ×ÅÒÑÔ É ÐÏÄÐÉÓÁÔØ ÂÎØÛÅÅ ËÏÌÉÞÅÓÔ×Ï ËÌÀÞÅÊ, ÞÅÍ × ÓÌÕÞÁÅ ËÏÇÄÁ ÷ÁÓ ÕÓÔÒÁÉ×ÁÅÔ ÎÅÂÎØÛÏÅ ÞÉÓÌÏ ÄÌÉÎÙÈ ÃÅÐÏÞÅË.

3-1. ðÒÉÍÅÒ ÓÅÔÉ ÄÏ×ÅÒÉÑ



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

òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÅÊ

÷ ÉÄÅÁÌÅ, ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ ÷ÁÛÉ ËÌÀÞÉ ÐÅÒÓÏÎÁÌØÎÏ ÐÅÒÅÄ×ÁÑ ÅÇÏ ÷ÁÛÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ. îÁ ÐÒÁËÔÉËÅ, ÏÄÎÁËÏ, ËÌÀÞÉ ÞÁÓÔÏ ÒÁÓÐÒÏÓÔÒÁÎÑÀÔÓÑ ÐÏ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÅ ÉÌÉ ÄÒÕÇÉÍ ÓÐÏÓÏÂÁÍ ÜÌÅËÔÒÏÎÎÏÊ Ó×ÑÚÉ. òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ÐÏ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÅ ÈÌÏÛÏ ËÏÇÄÁ ÷Ù ÉÍÅÅÔÅ ÔÏÌØËÏ ÎÅÓËÏÌØËÉÈ ËÌÀÞÁÓÐÒÉÄÅÎÏ×, ÅÓÌÉ ËÏÒÒÅÓÐÏÎÄÅÎÔ× ÍÏÇÏ, ÷Ù ÍÏÖÅÔÅ ÒÁÚÅÓÔÉÔØ Ó×ÏÊ ËÌÀÞ ÎÁ ÐÅÒÓÏÎÁÌØÎÏÊ ×ÅÂ-ÓÔÒÁÎÉÃÅ. üÔÏ ÎÅ ÐÒÉÍÅÎÍÏ, 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 ÒÁÓÐÒÏÓÒÁÎÑÀÔ ÏÔËÒÙÔÙÅ ËÌÀÞÉ. ïÔËÒÙÔÙÊ ËÌÀÞ ÌÉÂÏ ÄÏÂÁ×ÌÑÅÔÓÑ Ë ÂÁÚÅ ÄÁÎÎÙÈ ÓÅÒ×ÅÒÁ, ÌÉÂÏ ÏÂßÅÄÉÑÅÔÓÑ Ó ÓÕÝÅÓÔ×ÕÀÝÉÍ ËÌÀÞÏÍ, ÅÓÌÉ ÔÁËÏÊ ÓÕÝÅÓÔ×ÕÅÔ. ëÏÇÄÁ ÎÁ ÓÅÒ×ÅÒ ÐÒÉÈÏÄÉÔ ÚÁÐÒÏÓ ËÌÀÞÁ, ÓÅÒ×ÅÒ ÐÒÏÓÍÁÔÒÉ×ÁÅÔ ÂÁÚÕ ÄÁÎÙÈ É, ÅÓÌÉ ÎÁÈÏÄÉÔ, ×ÏÚ×ÒÁÝÁÅÔ ÚÁÐÒÏÛÅÎÎÙÊ ËÌÀÞ.

óÅÒ×ÅÒÙ ËÌÀÞÅÊ ÔÁËÖÅ ÐÎÌÅÚÎÙ ËÏÇÄÁ ÍÎÇÅÅ ÌÀÄÉ ÞÁÓÔÏ ÐÏÄÐÉÓÙ×ÁÀÔ ËÌÀÞÉ ÄÒÕÇÉÈ ÌÀÄÅÊ. âÅÚ ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ, ËÏÇÄÁ âÌÜÊÊ ÐÏÄÐÉÓÙ×ÁÂÔ ËÌÀÞ ǜÉÓ, ÏÎ ÄÎÌÖÅÎ ÐÏÓÌÁÔØ ÅÊ ÐÏÄÐÉÓÁÎÎÕÀ ÉÍ ËÏÐÉÀ ÅÅ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ËÏÔÏÒÕÀ ǜÉÓ ÍÏÖÅÔ ÄÏÂÁ×ÉÔØ Ë Ó×ÏÍÕ ÎÁÂÏÒÕ É ÐÅÒÅÄ×ÁÔØ, ÚÁÔÅÍ, ×ÓÅÍ Ó×ÏÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ. ÷ÙÐÏÎÅÎÉ ÜÔÉÈ ÄÅÊÔ×ÉÊ ÓÐÏÓÏÂÁÔ×ÕÂ ÐÏÔÔÒÅÎÉÀ ÐÏÔÔÙÈ ÓÅÔÅÊ ÄÏ×ÅÒÉÑ É ÐÏ×ÙÛÅÎÉÀ ÂÅÚÏÐÁÓÏÓÔÉ PGP. ïÄÎÁËÏ ÎÉ ÓÔÁÎÏ×ÑÔÓÑ ÐÍÅÈÏÊ ËÏÇÄÁ ËÌÀÞÉ ÐÏÄÐÉÓÙ×ÁÀÔÓÑ ÞÁÓÔÏ.

éÓÐÏÎØÚÏ×ÁÎÉÅ ÓÅÒ×ÅÒÏ× ËÌÀÞÅÊ ÏÂÌÅÇÞÁÅÔ ÜÔÏÔ ÐÒÏÃÅÓÓ. ëÏÇÄÁ âÌÜÊË ÐÏÄÐÉÓÙ×ÁÅÔ ËÌÀÞ ǜÉÓ ÏÎ ÐÏÓÙÌÁÅÔ ÐÏÄÐÉÓÁÎÎÙÊ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ. óÅÒ×ÅÒ ËÌÀÞÅÊ ÄÏÂÁ×ÌÑÅÔ ËÌÀÞ ÐÏÄÐÉÓØ âÌÜÊËÁ Ë Ó×ÏÅÊ ËÏÐÉÉ ËÌÀÞÁ ǜÉÓ. ôÅ ËÔÏ ÉÎÔÅÒÅÓÕÅÔÓÑ ÏÂÎ×ÌÅÉÍ ËÏÐÉÉ ËÌÀÞÅÊ ǜÉÓ, ÐÏ Ó×ÏÅÊ ÉÎÉÃÉÁÔÉ×Å Ó×ÑÚÙ×ÁÀÔÓÑ Ó ÓÅÒ×ÅÒÏÍ ËÌÀÞÅÊ É ÐÎÕÞÁÔ ÏÔÐÒÁ×ËÕ ÐÏÄÐÉÓÁÎÎÙÊ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ. óÅÒ×ÅÒ ÌÅ ÐÒÉÎÉÍÁÅÔ ÔÏÌØËÏ ÐÏÄÐÉÓÁÎÎÙÅ ËÌÀÞÁ É ÍÏÖÅÔ ÐÒÏÐÅÔØ ÐÏÄÐÉÓÉ ÎÁ Ó×ÏÅÍ ËÌÀÞÅ ÐÒÏÓÏ ÚÁÐÒÏÓ× ÓÅÒ×ÅÒ.

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

ïÄÉÎ ÉÌÉ ÂÏÌÅÅ ËÌÀÞÅÊ ÍÇÕÔ ÂÙÔØ ÏÐÒÁ×ÌÅÎÙ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ ËÍÍÁÎÄÏÊ `--send-keys`. ÷ ËÁÞÅÓÔ×Å ÁÒÇÕÍÅÎÔÁ ÕËÁÚÙ×ÁÀÔÓÑ ÏÄÉÎ ÉÌÉ ÂÏÌÅÅ ÓÐÅÃÉÆÉËÁÔÏÒ×. ÷ ËÁÞÅÓÔ×Å ËÌÀÞÅÊ, ËÏÔÏÒÙÍÕ ÂÕÃÕÔ ÐÅÒÅÄÁÎÙ ËÌÀÞÉ ÚÁÄÁÅÔÓÑ ÏÐÃÉÑ `--keyserver`. áÎÁÌÏÇÉÞÎÏ, ËÍÍÁÎÄÁ `--recv-keys` ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÏÌÕÞÅÎÉÑ ËÌÀÞÅÊ Ó ÓÅÒ×ÅÒÁ, ÎÉ ËÍÍÁÎÄÅ `--recv-keys` ÔÒÅÂÕÅÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒ ËÌÀÞÁ. ÷ ÓÌÅÄÕÀÝÅÍ ÐÒÉÍÅÒÅ ǜÉÓ ÏÂÎ×ÌÑÅÔ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó ÎÍ×ÙÍÉ ÐÏÄÐÉÓÑÍÉ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ *`certserver.pgp.com`* É ÚÁÔÅÍ ÐÏÚÌÅÅÓ Ó×ÏÀ ËÍÐÉÀ 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 B115BDB6 from certserver.pgp.com ...
gpg: key B115BDB6: 1 new signature

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

óÕÝÅÓÔ×ÕÀÔ ÎÅÓËÏÌØËÏ ÐÏÐÕÌÑÒÎÙÈ ÓÅÒ×ÅÒÏ× ËÌÀÞÅÊ. ïÓÎÏ×ÎÙÅ ÓÅÒ×ÅÒÙ ËÌÀÞÅÊ ÓÉÎÈÒÏÎÉÚÉÒÕÀÔÓÑ ÄÒÕÇ Ó ÄÒÕÇÎÍ, ÐÏÜÔÍÕ ÌÕÞÛÅ ×ÙÂÒÁÔØ ÂÌÉÖÁÉÛÉÊ Ë ÷ÁÍ É ÒÅÇÕÌÑÒÎÏ ÉÓÐÏÌØÚÏ×ÁÔØ ÅÇÏ ÄÌÑ ÎÔÐÒÁ×ËÉ É ÐÏÌÕÞÅÎÉÑ ËÌÀÞÅÊ.

1. GnuPG ÐÅÒÅÇÒÕÖÁÅÔ ÓÌÏ×Ï “ÄÏ×ÅÒÉÅ” ÉÓÐÏÌØÚÕÑ ÅÇÏ × ÓÍÙÓÌÅ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ É × ÓÍÙÓÌÅ ÄÏ×ÅÒÉÑ ËÌÀÞÕ. üÔÏ ÍÏÖÅÔ ×ÙÚ×ÁÔØ ÐÕÔÁÍÉÃÕ. éÍÏÇÁ ÄÏ×ÅÒÅÅ ×ÌÁÄÅÌØÃÕ ÕËÁÚÙ×ÁÂÔÓÑ ÐÒÑÍÏ. ÷ ÏÓÎÏ×ÎÏÍ, × ÙÔÏÍ ÒÕËÏ×ÏÄÓÔ×Å, ÔÅÒÍÉÎ “ÄÏ×ÅÒÅÅ” ÉÓÐÏÌØÚÕÅÔÓÑ × ÓÍÙÓÌÅ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ É ÔÅÒÍÉÎ “ÄÏÓ×ÅÒÏÔÓØ” ÄÌÑ ÎÂÏÚÎÁÞÅÎÉÑ Õ×ÅÒÅÎÎÏÓÔÉ × ÔÏÍ, ÞÔÏ ËÌÀÞ ÐÒÉÁÄÌÅÖÉÔ ÞÅÌÏ×ÅËÕ ÕËÁÁÎÎÏÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ ÐÌØÚÏ×ÁÔÅÌÑ.

4. åÖÅÄÎÅ×ÎÏÅ ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG

GnuPG ÓÌÏÖÎÙÊ ÉÎÓÔÒÕÍÅÎÔ Ó ÎÁÂÏÒÎÏÍ ÔÅÈÎÉÞÅÓËÉÈ, ÓÏÃÉÁÌØÎÙÈ É ÚÁËÏÎÏÔÄÁÔÅÌØÎÙÈ ÔÏÎËÏÓÔÅÊ, ×ÏÚÎÉËÁÀÝÉÈ ÐÒÉ ÅÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÉ. ôÅÈÎÉÞÅÓËÉ, ÏÎ ÂÙÌ ÒÁÚÒÁÂÏÔÁÎ ÄÌÑ ÕÄ×ÌÅÔ×ÏÒÅÎÉÑ ÏÞÅÎØ ÒÁÚÌÉÞÁÀÝÉÈÓÑ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ. üÔÏ ÕÓÌÏÖÎÑÅÔ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ. óÏÃÉÁÌØÎÏ, ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG ÎÅ Ñ×ÌÑÅÔÓÑ ÔÏÌØËÏ ÐÒÒÓÏÎÁÌØÎÙÍ ÒÅÛÅÎÉÅÍ. äÌÑ ÜÆÆÅËÔÉ×ÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG, ÅÇÏ ÄÏÌÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ ÏÂÅ ÓÔÒÏÎÙ. îÁËÏÎÅÃ, ÚÁËÏÎÏÄÁÔÅÌØÓÔ×Ï ÏÇÒÁÎÉÞÉ×ÁÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÃÉÆÒÏ×ÏÇÏ ÛÉÆÒÏ×ÁÎÉÑ, É, × ÞÁÓÔÉÓÔÉ, ÏÔ×ÅÔ ÎÁ ×ÏÐÒÏÓ Ï ÚÁËÏÎÎÏÓÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG ÒÁÚÌÉÞÅÎ × ÒÁÚÎÙÈ ÇÏÓÕÄÁÒÓÔ×ÁÈ.

úÄÅÓØ ÒÁÓÍÁÔÒ×ÁÀÔÓÑ ÜÔÉ ×ÏÐÒÏÓÙ. ôÁËÖÅ ÄÁÀÔÓÑ ÐÒÁËÔÉÞÅÓËÉÅ ÓÏ×ÅÔÙ ËÁË ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ÄÌÑ ÕÄ×ÌÅÔ×ÏÒÅÎÑ Ó×ÏÉÈ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ. òÁÓÍÁÔÒÉ×ÁÀÔÓÑ ÐÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG ÄÌÑ ÚÁÝÉÝÅÎÎÏÇÏ ÏÂÍÅÎ ÉÎÆÏÒÍÁÃÉÅÊ ÍÅÖÄÕ ÷ÁÍÉ É ÷ÁÛÉÍÉ ËÌÌÌÅÇÁÍÉ ÅÓÌÉ ÎÉ ÅÝÅ ÎÅ ÉÓÐÏÌØÚÕÀÔ GnuPG. ÷ ÚÁËÌÀÞÅÎÉÅ, ×ÙÄÅÌÅÎ ÚÁËÎÎÏÄÁÔÅÌØÎÛÊ ÓÔÁÔÕÓ GnuPG, ÏÐÒÅÄÅÌÑÅÔÓÑ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÍÉ ÚÁËÎÎÁÍÉ × ÍÉÒÅ.

ïÐÒÅÄÅÌÅÎÉÅ ÷ÁÛÉÈ ÔÒÅÂ×ÁÎÉÊ Ë ÚÁÝÉÔÅ

GnuPG ÉÎÓÔÒÕÍÅÎÔ ÄÌÑ ÚÁÝÉÔÙ ÷ÁÛÉÈ ÓÅËÒÅÔÏ×. ÷ÁÛÉ ÓÅËÒÅÔÙ ÚÁÝÉÝÅÎÙ ÅÓÌÉ ÷ÁÛÉ ÓÏÌÂÝÅÎÉÑ ÎÅ ÄÏÓÔÁÔÏÞÎÏ ÐÏÓÔÏÑÎÎÏÍÕ ÇÌÁÚÕ.

ôÏ, ËÁË ÷ÁÍ ÓÌÅÄÕÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, ÚÁ×ÉÓÉÔ ÏÔ ÖÅÌÁÎÉÑ É ×ÏÚÍÏÖÎÏÓÔÅÊ ÔÅÈ, ËÔÏ ÍÏÖÅÔ ÚÁËÏÔÅÔØ ÐÒÏÐÅÓÔØ ÷ÁÛÉ ÓÏÌÂÝÅÎÉÑ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÂÅÓÅÄÏÎÅÍÎÙÊ ÓÉÓÔÅÍÎÙÊ ÁÄÍÉÎÉÓÔÒÁÔÏÒ, ÎÅÂÏÅÖÎÏ ÐÒÏÍÁÔÒÉ×ÁÀÝÉÊ ÷ÁÛ ÐÏÞÔÕ, ÐÒÍÍÙÛÌÅÎÎÙÊ ÛÐÉÎÍ, ÐÙÔÁÀÝÉÊÓÑ ÐÏÈÉÔÉØ ÓÅÒÖÅÎÔ ÷ÁÛÅÇÏ ÐÒÅÄÐÒÉÑÔÉÑ, ÉÌÉ ÇÏÓÕÄÁÓÓÔ×ÅÎÎÙÅ ÓÐÅÃÉÁÌÉÓÔÙ, ÉÎÔÅÒÅÓÀÝÅÓÑ ÷ÁÍÉ. éÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG ÄÌÑ ÚÁÝÉÔÙ ÏÔ ÓÌÕÞÁÊÎÏÇÏ ÐÒÏÍÁÔÒ×ÁÎÉÑ ÏÔ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG × ÓÌÕÞÁÅ ÅÓÌÉ ËÔÏ-ÔÏ ÃÅÌÅÎÁÐÒÁ×ÌÅÎÎÏ ÐÙÔÁÅÔÓÑ ÐÒÏÞÅÓÔØ ÷ÁÛÕ ÐÏÞÔÕ. ÷ÁÛÁ ÃÅÌØ, × ËÏÎÅÞÎÏÍ ÓÞÅÔÅ, ÓÏÓÔÏÊ × ÔÏÍ, ÞÔÂÙ ÓÄÅÌÁÔØ ÒÁÓÛÉÆÒÏ×ËÕ ÄÅÎÛÅ ÂÎÅÅ ÄÏÒÇÏÊ ÞÅÍ ÉÈ ÓÏÏÉÎÓÔÓÔ.

îÁÓÔÒÏÊËÁ GnuPG ×ËÌÀÞÁÅÔ ÒÅÛÅÎÉÅ ÞÂÔÙÒÅÈ ÚÁÄÁÞ:

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

ðÒÁ×ÉÌØÎÏ ×ÙÂÒÁÎÎÙÊ ÒÁÚÍÅÒ ËÌÀÞÁ ÚÁÝÉÝÁÅÔ ÷ÁÓ ÏÔ ÌÎÁÏ×ÙÈ ÁÔÁË ÍÁ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÓÏÎÂÝÅÎÉÑ. úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÐÒÅÄÓÔ×ÌÑÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÅÇÏ-ÔÏ ÄÕÕÇÉÍ ÄÌÑ ÒÁÛÉÆÒÏ×ËÉ ÎÁÐÒÁ×ÌÅÎÎÙÈ ÷ÁÍ ÓÏÎÂÝÅÎÉÊ É ÐÏÄÐÉÓÉ Ó×ÏÉÈ ÓÏÎÂÝÅÎÉÊ ÷ÁÛÅÊ ÐÏÄÐÉØÀ. ðÒÁ×ÉÌØÎÏ ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÐÒÅÄÓÔ×ÌÑÅÔ ÓÏÂÏÊ ÄÏÓÔÁÔÏÞÎÏ ÓÌÏÖÎÕÀ ÚÁÄÁÞÕ. ÷ ËÎÉÇÅ ÄÁÀÔÓÑ ÓÐÅÃÉÆÉÞÅÓËÉÅ ÒÅÛÅÎÉÑ ÄÌÑ ÒÁÚÎÙÈ ÓÉÔÕÁÃÉÊ, ÚÁ×ÉÓÉÔ ÂÁÌÁÎÓ ÍÅÖÄÕ

ÄÏÐÏÌÎÉÔÅÌØÎÏÊ ÒÁÂÏÔÏÊ, Ó×ÑÚÁÎÎÏÊ Ó ÉÓÐÏÌØÚÏ×ÁÎÉÅÍ GnuPG, É ÚÁÝÉÔÏÊ, ËÏÔÏÒÕÀ ÷ÁÍ ÜÔÏ ÄÁÅÔ.

÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ

÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ ÚÁ×ÉÓÉÔ ÏÔ ÔÉÐÁ ËÌÀÞÁ. ÷ OpenPGP, ÐÁÒÁ ÏÔËÒÙÔÏÇÏ/ÚÁËÒÙÔÏÇÏ ËÌÀÞÅÊ ÏÂÙÞÎÏ ÓÏÓÔÉÔ ÉÚ ÎÁÓËÏÌØËÉÈ ËÌÀÞÅÊ. ëÁË ÍÉÎÉÍÕÍ × ÎÅÅ ×ÈÏÄÉÔ ÇÌÁ×ÎÙÊ ËÌÀÞ ÄÌÑ ÐÏÄÐÉÓÉ, ËÒÏÍÅ ÔÏÇÏ, ÏÂÙÞÎÏ ÏÎÁ ÓÏÄÅÒÖÉÔ ÏÄÉÎ ÉÌÉ ÎÅÓËÏÌØËÏ ÄÏÐÏÎÉÔÅÌØÎÙÈ ËÌÀÞÅÊ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÐÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÐÁÒÁÍÅÔÒÏ× ÐÏ ÕÍÌÞÁÎÉÀ, ÇÌÁ×ÎÙÊ ËÌÀÞ ÂÕÄÅÔ DSA ËÌÀÞÍÍ, Á ÐÏÄËÌÀÞÉ ÂÕÄÕÔ ElGamal ËÌÀÞÁÍÉ.

DSA ÄÏÐÕÓËÁÅÔ ËÌÀÞÉ ÄÌÉÎÎÏ ÄÏ 1024 ÂÉÔ. üÔÏ ÎÅ ÓÌÉÛËÎÍ ÍÎÇÏ, ÕÞÉÔÙ×ÁÑ ÓÅÇÏÄÍÑÛÎÅÅ ÒÁÚ×ÉÔÉÅ ÔÅÈÎÏÌÏÇÉÉ, ÎÏ ÜÔÏ ÔÏ, ÞÔÏ ÏÐÉÓÙ×ÁÅÔ ÓÔÁÎÄÁÒÔ. åÓÌÉ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ DSA ËÌÀÞÉ, ÔÏ ÉÈ ÄÌÉÎÁ ÄÏÌÖÎÁ ÂÙÔØ 1024 ÂÉÔÁ.

ElGamal É RSA 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 ÓËÏÒÓÔØ ÚÁÛÉÆÒÏ×ÁÎÉÑ É ÒÁÓÛÉÆÒÏ×ÁÎÉÑ, Ô.Ë. ÓÔÏÉÍÓÔÔ ÜÔÉÈ ÁÌÇÏÒÉÔÍ× ÜËÓÐÏÎÅÎÃÁÌØÎÁ ÏÔÎÓÉÔÅÌØÎÏ ÒÁÚÍÅÒÁ ËÌÀÞÁ. âÏÌØÛÉÁ ËÌÀÞÉ ÔÁËÅ ÔÒÅÂÕÀÔ ÂÏÌØÛÅ ×ÒÅÍÅÎÉ ÄÌÑ ÇÅÎÅÒÁÃÉÉ É ÂÏÌØÛÅ ÍÅÓÔÁ ÄÌÑ ÈÒÁÎÅÎÉÑ. îÁËÏÎÅÃ, ÅÓÌÉ ËÌÀÞ ÓÌÉÛËÍÍ ×ÅÌÉË ÄÌÑ ÁÔÁË × ÏÏÂ, ÐÏÈÔÉÔÅÌØ ÐÒÏÔÏ ÎÁÐÁÄÁÅÔ ÌÉÞÎÏ ÎÁ ÷ÁÓ. 1024 ÂÉÔ - ÒÅËÍÅÎÄÕÅÍÙÊ ÒÁÚÍÅÒ ËÌÀÞÁ. åÓÌÉ ÷Ù ÄÅÊÓ×ÉÔÅÌØÎÏ ÎÕÖÄÁÅÔÅÓØ × ËÌÀÞÅ ÂÏÌØÛÅÇÏ ÒÁÚÍÅÒÁ, ÔÏ ÓËÏÒÅÅ ×ÓÅÇÏ ÕÖÅ ÚÍÁÂÔÅ ÎÁ ÜÔÏÍ É ÄÏÌÔÙ ÐÒÏËÎÓÕÎØÔÉÒÌ×ÁÔØÓÑ Ó ÜËÓÐÅÒÔÎÏÍ ÐÏ ÚÁÝÉÔÅ ÄÁÎÎÙÈ.

úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ

úÁÝÉÔÁ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÏÄÎÁ ÉÚ ÎÁÉÂÏÌØÅ ×ÁÖÎÙÈ ÚÁÄÁÞ ÄÌÑ ÎÁÄ£ÖÎÎÊ ÒÁÂÏÔÙ GnuPG. åÓÌÉ ËÔÏ-ÌÉÂÏ ÐÏÑÞÉÔ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÔÏ ÏÎ ÓÍÏÖÅÔ ÒÁÓÛÉÆÒÏ×Ù×ÁØ ×ÓÅ ÎÁÐÒÁ×ÌÅÎÎÙÅ ÷ÁÍ ÓÏÏÂŸÅÉÑ É ÓÍÏÖÅÔ ÐÏÄÐÉÓÙ×ÁØÓÑ ÷ÁÛÅ ÐÏÄÐÉÓØÀ. åÓÌÉ ÷Ù ÐÎÔÅÒÑÅÅ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÔÏ ÎÅ ÓÍÏÖÅÅ ÂÏÌØÛÅ ÒÁÓÛÉÆÒÏ×Ù×ÁØ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÌÑ ÷ÁÓ Ó×ÏÉ ÓÏÏÂŸÅÎÉÑ. ðÏÅÒÑ ÅÄÉÎÓ×ÅÎÎÏÊ ËÌÀÞ ÄÅÊÓ×ÉÔÅÌØÎÏ ÚÁÝÉÝÁÅÔ ÏÔ ÚÁÐÉÓÅÊ ÎÅÓÁÎÃÉÏÎÉÒÏ×ÁÎÎÙÈ ÓÏÏÂŸÅÎÉÊ É ÒÁÓÛÉÆÒÏ×ÁÎÎÙÈ ÓÅÓÓÉÊ.

îÅÚ×ÉÓÉÍÍ ÏÔ ÔÏÇÏ, ËÁË ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG ÷Ù ÄÏÌÖÎÙ ÓÏÈÒÁÎÑÔØ ÓÅÒÔÉÆÉËÁÔ ÏÔÚÙ×Á ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ É ÒÅÚÅÒ×ÎÕÀ ËÏÐÍÀ ÷ÂÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÎÁ ÚÁÝÉÝÅÎÎÙÅ ÏÔ ÚÁÐÉÓÅÊ ÎÅÓÁÎÃÉÏÎÉÒÏ×ÁÎÎÙÈ ÓÏÏÂŸÅÎÉÊ É ÈÒÁÎÉÔØ ÅÇÏ × ÎÁÄÅÖÎÏÍ ÍÅÓÔÅ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÚÁÐÉÓÁÔØ ËÏÐÉÑ ËÌÀÞÁ ÎÁ ËÏÍÐÁËÔ-ÄÉÓË É ÈÒÁÎÉÔØ ÅÇÏ × ÂÁÎËÏ×ÓËÏÍ ÓÅÊÆÅ. íÏÖÎ, ÔÁËÅ, ÚÁÐÉÓÁÔØ ÉÈ ÎÁ ÄÉÓËÅÔÕ É ÓÐÒÑÔÁÔØ ÅÅ ÄÍÍÁ. þÔÏÂÙ ÷Ù ÎÉ ÄÅÌÁÌÉ, ËÌÐÉÉ ÄÏÌÖÎÙ ÂÙÔØ ÓËÏÐÉÒÏ×ÁÎÙ ÎÁ ÎÍÓÉÔÅÌØ, ÎÁ ËÌÓÏÒÍÍ ÍÍÉ ÓÍÍÇÕÔ ÎÁÄÅÖÎÏ ÈÒÁÎÉÔØÓÑ ÎÁ ÐÒÍÔÑÔÉÉ ×ÓÅÇÏ ÓÒÌËÁ ÉÓÐÍÌØÚÏ×ÁÎÑ ËÌÀÞÁ, É ÉÈ ÓÌÅÄÕÅÔ ÓÐÒÑÔÁÔØ ÂÍÅÅ ÔÝÁÔÀÌØÍÍ, ÞÅÍ ËÌÐÉÀ ÷ÁÛÅÇÏ ÓÅËÒÅÔÍÇÏ ËÌÀÞÁ ÄÌÑ ÅÖÅÄÅÎ×ÍÇÏ ÉÓÐÍÌØÚÏ×ÁÎÑ.

þÔÏÂÙ ÚÁÝÉÔÉÔØ ÷ÁÛ ËÌÀÞ, GnuPG ÎÅ ÓÏÈÒÁÎÑÅÔ ÅÇÏ ÎÁ ÄÉÓË × ÞÉÓÔÏÍ ×ÉÄÅ. ÷ÍÅÓÔÏ ÜÔÏÇÏ ÏÎ ÛÉÆÒÕÅÔÓÑ ÓÉÍÅÔÒÉÞÎÙÍ ÁÌÇÏÒÉÔÍÏÍ. ÷ÏÔ ÚÁÞÅÍ ÎÕÖÎÁ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÄÌÑ ÄÏÓÔÕÐÁ Ë ËÌÀÞÕ. ðÏÜÔÏÍÕ ×ÚÌÍÝÉË ÄÎÌÖÅÎ ÒÅÛÉÔ Ä×Å ÐÒÏÂÌÅÍÙ, ÞÔÂÙ ÐÏÌÕÞÉÔØ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ: (1) ÏÎ ÄÏÌÖÅÎ ÐÏÕÞÉÔØ ËÌÀÞ, (2) Ï Ñ ÄÎÌÖÅÎ ÒÁÓÛÉÆÒÏ×ÁÔØ ËÌÀÞ.

îÁÄÅÖÎÅ ÈÒÁÎÅÎÉÅ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ - ÓÌÏÖÎÁÑ ÚÁÄÁÞÁ. ÷ ÉÄÅÁÌÅ, ÷Ù ÄÎÖÎÙ ÈÒÁÎÉÔØ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÎÁ ÓÍÅÎÎÏÍ, ÚÁÝÉÝÅÎÎÏÍ ÏÔ ÚÁÐÉÓÉ Ä ÉÓÐÏÌØÚÏ×ÁÔØ ÅÇÏ ÔÎØËÏ ÎÁ ÎÁ ÏÄÎÐÎÌØÚÏ×ÁÔÅÌØÓÏÉÎÅÉÅ ÎÅ ÐÏÄËÀÞÅÎÎÏÊ Ë ÓÅÂÉ. üÔÏ ÍÏÖÅÔ ÏÅÁÚÁÔØÓÑ ÎÅÕÄÏÂÎÙÍ ÉÌÉ ÎÅ×ÏÚÍÏÖÎÙÍ ÄÌÑ ÷ÁÓ. îÁÐÒÉÍÅÒ, Õ ÷ÁÓ ÍÏÖÅÔ ÎÅ ÂÙÔØ Ó×ÏÅÇÏ ËÏÍÐØÀÔÅÒÁ É ÷Ù ÉÓÐÏÌØÚÕÅÔÅ ËÏÍÐØÀÔÅÒ ÎÁ ÒÁÂÏÅÍ, ÉÌÉ ÜÔÏ ÍÏÖÅÔ ÏÚÎÁÞÁÔØ, ÞÔÏ ÷ÁÍ ÐÒÉÊÄÅÔÓÑ ÏÔËÌÀÞÁÔØ ËÏÍÐØÀÔÅÒ ÏÔ ÓÅÔÉ ËÁÖÄÙÊ ÒÁÚ ËÏÇÄÁ ÷Ù ÚÁÐÕÓËÁÅÔÅ GnuPG

üÔÏ ÎÅ ÏÚÎÁÞÁÅÔ, ÞÔÏ ÷Ù ÍÏÖÅÔÅ ÉÌÉ ÎÅ ÄÏÌÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG. üÔÏ ÏÚÎÁÞÁÅÔ ÔÏÌØËÏ, ÞÔÏ ÷Ù ÓÞÉÔÁÅÔÅ Ó×ÏÉ ÄÁÎÎÙÅ ÄÏÓÔÁÔÏÞÎÏ ×ÁÖÎÙÍÉ, ÞÔÏÂÙ ÛÉÆÒÏ×ÁÔØ, ÏÏ ÎÅ ÎÁÓÔÌØËÏ ×ÁÖÎÙÍÉ, ÞÔÏÂÙ ÐÒÉÎÉÁÔØ ÏÓÏÂÙÅ ÍÅÒÙ ÐÒÅÄÏÓÔÏÒÏÖÎÏÓÔÉ ÄÌÑ ÕÓÏÓÑ ÐÒÏ×ÏÚÉÒÕÅÔ. üÔÏ ÷ÁÛ ×ÙÂÏÒ.

èÏÒÏÛÁÑ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÏÞÅÎØ ËÒÉÔÉÞÎÁ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ GnuPG. ìÀÂÏÊ ×ÚÌÍÝÉË, ÐÌÕÞÉ×ÛÉÊ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÄÏÌÖÅÎ ×ÚÌÍÁÔØ ÛÉÆÒ ÎÁ ÓÅËÒÅÔÎÏÍ ËÌÀÞÅ. ÷ÍÅÓÔÏ ÁÔÁËÉ × ÌÏÂ, ×ÚÌÍÝÉË, ÎÁ×ÅÒÎËÁ, ÐÏÐÒÎÂÔÅ ÕÇÁÄÁÔØ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ.

íÏÉ×ÁÃÉÅÊ ÄÌÑ ÐÏÄÂÏÒÁ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ Ñ×ÌÑÅÔÓÑ ÔÏ, ÞÔÏ ÂÏØÛÉÎÓÔ×Ï ÌÀÄÅÊ ×ÙÂÉÒÁÀÔ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ, ËÏÔÒÕÀ ÐÒÏÐÏÐÏÂÒÁÔØ, ÞÅÍ ÐÒÏÉÚ×ÏØÛÕÔÅÓÑ ÓÏÏ×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 ÐÅÒÅÍÅÎÎÏ×ÏË. ôÁÖÅ ÐÒÏÂÌÅÍÁ Ó ÃÉÔÉÒÏ×ÁÍÉÅÍ. ÷ ÏÂÝÅÍ ÓÌÕÞÁÅ, ËÌÀÞÅ×ÙÅ ÆÒÁÚÙ ÏÓÎ×ÁÎÙÅ ÎÁ ÅÓÔÅÓÔ×ÅÎÎÏÍ ÑÚÙËÅ ÎÅÄÏÔÁÔÏÞÎÙ, Ô.Ë. × ÅÓÔÅÓÔ×ÅÎÎÙÈ ÑÚÙËÁÈ ÎÅ È×ÁÔÁÅÔ ÓÌÕÞÁÊÎÏÓÔÉ É ÉÚÂÙÔÏÞÎÏÓÔÉ. ÷Ù ÄÎÖÎÙ ÉÚÂÅÇÁØ 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 ÄÎÖÎÁ ×ËÌÀÞÁØ ÓÉÍ×ÎÙ ÉÚ ×ÓÅÇÏ ÄÉÁÐÁÚÏÎÁ ÐÅÞÁÔÎÙÈ ÓÉÍ×ÎÏ× ÎÁ ×ÁÛÅÊ ËÌÁ×ÉÁÔÕÒÅ. óÀÄÁ ×ÈÏÄÑÔ ÁÌÆÁ×ÉÔÎÅ ÓÉÍ×ÎÙ, × ÒÁÚÎÙÈ ÒÅÇÉÔÎÙÈ ÑÉÍ×ÎÏÈ ÃÉÆÒÙ É ÓÐÅÃÉÁÌØÎÙÅ ÓÉÍ×ÎÙ, ÔÁËÉÅ ËÁË } É |. ðÒÏÑ×ÉÔÅ Ô×ÏÞÁÓËÉÊ ÐÏÄËÏÄ É ÚÁÔÒÁÔØÔÅ ÎÅÍÎÏÇÏ ×ÒÅÍÅÎÉ ÎÁÄÕÍ×ÁÑ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ, ÈÏÒÏÛÉÊ ×ÙÂÏÒ ×ÁÖÅÎ ÄÎÑ ÏÂÅÓÐÅÞÅÎÉÑ ÷ÁÛÅÊ ÓÅËÒÅÔÎÏÓÔÉ.

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

ðÏ ÕÍÍÏÞÁÎÉÀ, ËÏÇÄÁ ÷Ù ÓÏÚÄÁÅÔÅ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ, ÇÅÎÅÒÉÒÕÅÔÓÑ ÇÌÁ×ÎÙÊ ËÌÀÞ DSA ÄÌÑ ÐÏÄÐÉÓÉ É ÐÏÄÐÉÎÁÎÎÙÊ ËÌÀÞ ElGamal ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. üÔÏ ÕÄÏÂÎÏ, Ô.Ë. ÒÎÉ 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, ÓÏÂÉÓÀÀÔÓÑ ÐÏÄÐÉÓÉ ÔÅÈ, ËÔÏ ÐÏÄÔ×ÅÒÖÄÁÅÔ ÐÒÉÁÄÌÅÖÎÏÓÔØ ËÌÀÞÁ ÷ÁÍ. ëÌÀÞ ÛÉÆÒÏ×ÁÎÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÒÁÓÛÉÆÒÏ×ÁÎÉÑ ÚÁÛÉÆÒÏ×ÁÎÎÙÈ ÄÏËÕÍÅÎÔÏ×, ÏÔÐÒÁ×ÌÅÎÙÈ ÷ÁÍ. ïÂÙÞÎÏ, ÃÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÉÍÅÅÔ ÐÒÏÄÏÌÖÉÔÅÌØÎÙÊ ÓÒÏË ÄÅÉÓÔ×ÉÑ, ÎÁÐÒÉÍÅÒ, ÎÅÏÇÒÁÎÉÞÅÎÎÙÊ, É ÷Ù, ÔÁËÖÅ, ÎÅ ÈÏÔÉÔÅ ÕÔÒÁÔÉÔØ ÐÏÄÐÉÓÉ ÎÁ ÷ÁÛÅÍ ËÌÀÞÅ, ÓÏÂÒÁÎÙÅ Ó ÂÏØÛÉÍ ÔÒÕÄÏÍ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÐÏÄËÌÀÞ ÛÉÆÒÏ×ÁÎÑ ÍÏÖÅÔ ÐÅÒÅÄÁÓÔÅ ÉÚÍÅÎÎÔØÓÑ, ÞÔÏ ÐÏ×ÙÓÉÔ ÂÅÚÏÐÁÓÎÏÓÔØ, Ô.Ë. ×ÚÌÍÁÎÎÛÊ ËÌÀÞ ÛÉÆÒÏ×ÁÎÑ ÐÏÚ×ÌÉÔ ×ÚÌÍÝÉËÕ ÐÒÌÞÁÓÔØ ×ÓÅ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÌÑ ÜÔÏÇÏ ËÌÀÞÁ, ËÁË × ÂÕÄÕÝÅÍ, ÔÁË É × ÐÒÏÛÌÍ.

ðÏÜÔÍÕ ÷Ù ÐÏÞÔÉ ×ÓÅÇÄÁ ÚÁÈÏÔÉÔÅ ÏÓÔÁ×ÉÔØ ÇÌÁ×ÎÙÊ ËÌÀÞ Ó ÎÅÏÇÒÁÍÉÞÅÎÎÙÍ ÓÒÏËÍÍ ÄÅÊÓ×ÉÑ. åÓÔØ Ä×Å ÐÒÉÞÉÎÙ ÐÏ ËÏÔÏÒÙÍ ÷Ù ÍÏÖÅÅ ÏÇÒÁÍÉÞÉÔØ ÓÒÏË ÄÅÊÓ×ÉÑ ËÌÀÞÁ. ÷Ï-ÐÅÒ×ÙÈ, ÷ÁÍ ÍÏÖÅÔ ÐÏÎÁÄÏÂÉÔØÓÑ ËÌÀÞ ÎÁ ÏÐÒÅÄÅÌÅÎÎÙÊ ÐÅÒÉÄ. îÁÐÒÍÅÒ, ËÌÀÞ ÂÕÄÕ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ×Ï ×ÒÅÍÑ ÉÚÂÉÒÁÔÅÌØÎÏÊ ËÁÍÐÁÎÉÉ É ÎÅ ÐÏÎÁÄÏÂÉÔÓÑ ÐÏÓÌÅ ÅÅ ÏÎÉÐÁÎÑ. äÒÕÇÁÑ ÐÒÉÞÉÎÁ ÓÏÓÔÏÑ × ÔÏÍ, ÞÔÏ ÅÓÌÉ ÷Ù ÔÅÒÑÅÔÅ ËÌÀÞÏÍ É, ÐÒÉ ÜÔÏÍ, ÎÅ ÉÍÅÅÔÅ ÓÀÒÔÉÆÉËÁÔÁ ÏÚÙ×Á, ÎÁÉÞÉÅ ÓÒÏËÁ ÄÅÊÓ×ÉÑ ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ × ËÏÎÅÞÎÍ ÓÞÅÔÅ ËÌÀÞ ÓÔÁÎÅÔ ÎÅÄÅÊÓ×ÉÔÅÌÅÎ.

óÍÅÎÁ ÐÏÄËÌÀÞÅÊ ÛÉÆÒÏ×ÁÎÑ ÐÒÏÓÔÁ, ÎÏ ÍÏÖÅÔ ×ÙÚ×ÁÔØ ÎÅÑÄÏÔÓÔÁ. åÓÌÉ ÷Ù ÓÏÚÄÁÅÔÅ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ ÓÏ ÓÒÏËÍÍ ÄÅÊÓ×ÉÑ ÐÏÄËÌÀÞÅÊ, ÜÔÏ ÓÒÏË ÒÁÎÏ ÉÌÉ ÐÏÚÄÁÎÏ ÉÓÔÅÞÅÔ ÓÒÏË ÄÅÊÓÔ×ÉÑ ÐÏÄÐÉÓÉ. îÅÚÁÄÎÏÇÏ ÄÏ ÉÓÔÅÞÅÎÉÑ ÓÒÏËÁ, ÷ÁÍ ÓÌÅÄÕÅÔ ÄÏÂÁ×ÉÔØ ÎÏ×ÙÊ ÐÐÕÂÌÉËÏ×ÁÔØ ÏÔÐÅÞÁÔÏË ËÌÀÞ. ðÏÓÌÅ ÉÓÔÅÞÅÎÉÑ ÓÒÏËÁ ÄÅÊÓ×ÉÑ, ÔÅ, ËÔÏ ÈÏÑÔ ÏÐÒÁ×ÉÔØ ÎÏ×ÙÊ ÐÐÕÂÌÉËÏ×ÁÔØ ÏÔÐÅÞÁÔÏË ËÌÀÞ, Ô.Ë. ÎÅ ÓÍÏÇÕÔ ÂÏÌÅÅ ÚÉÆÒÏ×ÁÔØ ËÌÀÞÏÍ Ó ÐÒÏÓÒÏÞÅÎÎÙÍ ÓÒÏËÏÍ ÄÅÊÓ×ÉÑ. üÔÏ ÍÏÖÅÔ ÎÁÕÄÏÂÎÙÍ, × ÚÁ×ÉÓÍÍÓÔÉ ÏÔ ÔÏÇÏ, ËÁË ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ. ïÄÎÁËÏ ÎÅ ÔÒÅÂÕÅÔÓÑ ÎÉËÁËÉÈ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ÐÏÄÐÉÓÅÊ, Ô.Ë. ÐÏÄËÌÀÞ ÐÏÄÐÉÓÁÎ ÷ÁÛÉÍ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ, ËÏÔÏÒÙÊ, ×ÅÒÑÔÎÏÍ, ÕÖÅ ÂÙÌ ÐÏÄÔ×ÅÒÖÄÅÎ ÷ÁÛÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÏÍ.

üÔÉ ÎÅÕÄÏÂÓ×Á ÍÇÕÔ ÏÐÒÁ×ÄÙ×ÁÔØ, Á ÍÇÕÔ É ÎÅ ÏÐÒÁ×ÄÙ×ÁÔØ ÐÌÕÞÁÅÍÕÀ ÄÏÐÏÌÎÉÔÅÌØÎÕÀ ÚÁÝÉÔÕ. ôÁË ÖÅ ËÁË É ÷Ù, ×ÚÌÍÝËË ÍÏÖÅÔ ÞÉÔÁØ ×ÓÅ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÙÅ ÉÓÔÅËÛÉÍ ËÌÀÞÏÍ. óÍÅÍ ÐÏÄËÌÀÞ ÚÁÝÉÝÅÔ ÔÏÌØËÏ ÎÏ×ÙÅ ÄÏËÕÍÅÎÔÙ. äÌÑ ÞÔÅÎÉÑ ÄÏËÕÍÅÎÔÏ×, ÚÁÛÉÆÒÏ×ÁÎÙÈ ÎÏ×ÙÍ ÐÏÄËÌÀÞÍ, ×ÚÌÍÝËÕ ÐÒÉÊÄÅÔÓÑ ×ÚÌÁÍÙ×ÁØ ÎÏ×ÙÊ ËÌÀÞ, ÉÓÐÌØÚÕÑ ÔÅ ÖÅ ÍÅÔÏÄÙ, ÞÔÏ É × ÐÅÒ×ÙÊ ÒÁÚ.

îÁËÌÎÅÃ, ×ÓÅ ÜÔÏ ÉÍÅÅÔ ÓÍÙÓÌ, ÅÓÌÉ × Ó×ÑÚËÅ ÉÍÅÅÔÓÑ ÔÌØËÏ ÏÄÎÁ ÄÅÊÓÔ×ÙÝÉÊ ÐÏÄËÌÀÞ. ÷Ù ÎÅ ÐÌÕÞÉÔÅ ÎÉËÁËÏÊ ÄÏÐÌÎÉÔÅÌØÎÏÊ ÚÁÝÉÔÙ ÐÓÉ ÎÁÌÉÞÉÉ Ä×ÕÈ É ÂÏÌÅ ÁËÔÉ×ÎÙÊ ËÌÀÞÅÊ. ÷Ù, ËÏÎÅÞÎÏ, ÍÏÖÅÔÅ ÉÍÅØ ÌÀÂÏÅ ÞÉÓÌÏ ÉÓÔÅËÛÉÈ ËÌÀÞÅÊ × Ó×ÑÚËÅ, ÞÔÏÂÙ ÞÉÔÁØ ÄÏÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÀ ÒÁÂÏÔÕ ÎÅ ÔÒÅÂÏÖÁÌÁ ×ÒÁÍ.

õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ.

ëÁË É ÚÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÕÐÒÁ×ÌÅÎÉÅ ÓÅÔØÀ ÄÏ×ÅÒÉÑ Ñ×ÌÑÅÔÓÑ ÔÅÍ ÁÓÐÅËÔÏÍ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG, ËÏÔÏÒÛÊ ÔÒÅÂÕÅÔ ÓÏÂÌÀÄÅÎÉÑ ÂÁÌÁÎÓÁ ÍÅÖÄÕ ÚÁÝÉÔÏÊ É ÌÅÇËÏÓÔØÀ ÉÓÐÏÌØÚÏ×ÁÎÉÑ. åÓÌÉ ÷Ù ÉÓÐÏÌØÚÕÅÅ GnuPG ÄÌÑ ÚÁÝÉÔÙ ÏÔ ÓÌÕÞÁÊÎÏÇÏ ÐÏÄÓÌÕÛÉ×ÁÎÉÑ É ÐÏÄÄÅÌËÉ, ÔÏ ÍÏÖÅÔÅ ÐÏ×ÙÓÉÔØ ÓÏÌÉÄÎÏÓÔØ ÓÏÂÓÔ×ÅÎÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ × ÄÏ×ÅÒÉÑ ÐÒÏÉÓÈÏÄÉÔ ÎÁ ËÌÀÞÁÈ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÅÓÌÉ ÷Ù

ÓÞÉÔÁÅÔÅ, ÞÔÏ ËÔÏ-ÌÉÂÏ ÚÁÉÎÔÅÒÅÓÏ×ÁÎ × ÐÏÌÕÞÅÎÉÉ ÄÏÓÔÕÐÁ Ë ÷ÁÛÉÍ ÓÅËÒÅÔÁÍ, ÔÏ ÷ÁÍ ÓÌÅÄÕÅÔ ÐÒÏÑ×ÌÑÔØ ÍÅÎØÛÅ ÄÏ×ÅÒÅ × ÏÔÎÏÛÅÎÉÉ ÞÕÖÉÈ ÐÏÄÐÉÓÅÊ É ÔÒÁÔØ ÂÎØÛÅ ×ÒÅÍÅÎÉ ÎÁ ÐÒÏ×ÅÒÕ ËÌÀÞÅÊ.

îÅÚÁ×ÉÓÉÍÏ ÏÔ ÷ÁÛÉÈ ÌÉÞÎÙÈ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ, ÷Ù ×*ÓÅÇÄÁ ÄÏÖÎÙ ÂÙÔØ ×ÎÉÍÁÔÅÌØÎÙ* ÐÏÄÐÉÓÙ×ÁÑ ÞÕÖÉÅ ËÌÀÞ. ðÏÄÐÉÓÙ×ÁÔØ ËÌÀÞ ÏÐÅÒÁÃÉÏÎÎÏÊ ÓÉÓÔÅÍÙ ÎÁ ÓÏÂÓÔ×ÅÎÎÙÅ ÐÏÔÒÅÂÎÏÓÔÉ × ÚÁÝÉÔÅ ÜÇÏÉÓÔÉÞÎÏ. îÁ ÷ÁÛÕ ÐÏÄÐÉÓØ ÍÏÇÔ ÐÏÌÁÇÁÔØÓÑ ÄÒÕÇÉÅ, ÞØÉ ÔÒÅÂÏ×ÁÎÉÑ, ×ÏÚÍÏÖÎÏ, ÂÏÌÅÅ ×ÙÓÏËÉ. åÓÌÉ ÏÎÉ ÎÅ ÓÍÇÕÔ ÐÏÌÁÇÁÔØÓÑ ÎÁ ÷ÁÓ, ÜÔÏ ÏÔÌÁÂÉÔ ÓÅÔØ ÄÏ×ÅÒÑ É ÚÁÔÒÕÄÎÉÔ ÏÎÝÅÎÉÅ ×ÓÅÇÏ ÓÏÎÝÅÓÔ×Á ÐÏÌØÚÏ×ÁÔÅÌÅÊ GnuPG. éÓÐÏØÚÕÊÔÅ ÔÅ ÖÅ ÍÅÒÙ ÐÒÅÄÏÔÖÏÐÏÓÔÉ, ÐÏÄÐÉÓÙ×ÁÑ ËÌÀÞÉ, ËÁËÉÅ ÷Ù ÈÏÔÅÌÉ ÂÙ, ÞÔÏÂÙ ÐÒÉÎÉÍÁÌÉ ÔÅ, ÎÁ ÞØÉ ÐÏÄÐÉÓÉ ÐÌÁÇÁÂÔÅÓØ ÷Ù.

îÁ ÐÒÁËÔÉËÅ, ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÑ Ó×ÅÄÅÎÏ Ë ÐÒÉ×ÏÅÎÉÀ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÑ ÎÅËÏÔÏÒÏÍÕ ÍÉÎÉÍÁÌØÎÏÍÕ ÞÉÓÌÕ ÄÒÕÇÉÈ ÌÉÃ É ÎÁÓÔÒÏËÅ ÐÁÒÁÍÅÔÒÏ× `--marginals-needed` É `--completes-needed`. ìÀÂÏÊ ËÌÀÞ, ÐÏÄÐÉÓÁÎÎÙÊ ÷ÁÍÉ ÌÉÞÎÏ, ÓÞÉÔÁÅÔÓÑ ÐÏÄÔ×ÅÒÖÄÅÎÎÙÍ, ÎÏ, ËÒÏÍÅ ËÁË ÄÌÑ ÍÁÌÅÎØËÉÈ ÇÒÕÐÐ, ÎÅ Ñ×ÌÑÅÔÓÑ ÐÒÁËÔÉÞÅÓËÉ ÐÏÄÐÉÓÙ×ÁÔØ ËÌÀÞ ËÁÖÄÏÇÏ, Ó ËÅÍ ÷Ù ÐÀÒÅÐÉÓÙ×ÁÅÔÅÓØ. ÷Ù ÂÕÄÅÔÅ, ÓÌÅÄÏ×ÁÔÅÌØÎÏ, ÄÏÖÎÙ ÐÏÄÔÖÕÄÅÎÙ ÎÁ ÄÒÕÇÉÈ.

îÁÉÂÏÌÅÅ ÒÁÚÕÍÎÏ, ÐÒÏÑ×ÉÔØ ÁËËÕÒÁÔÎÏÓÔØ ÐÒÉÓ×ÉÓ×ÁÑ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÑ É ÚÁÔÅÍ ÎÁÓÔÒÏÉÔØ GnuPG ÓÔÒÏÇÏÓÔØ ÐÒÏ×ÅÒÏÑÅÔ ËÌÀÞÅÊ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÐÏÌÏÖÉÔØ ÕÒÏ×ÅÎØ ÕÚÅÌÏÕ ÒÁ×ÎÙÍ ÄÖÅÊÍÓÕ ÉÚ ÐÑÔÉ ÉÌÉ ÓÅÍÉ ÐÏÄÐÉÓÅÊ, É ÎÅÚÎÁÐÏÓÌÉØÎÏ ÄÏ×ÅÒÑÔÅ ËÌÀÞÁÍ, Ó ËÏÔÏÒÙÍÉ ×ÙÈÏÄÉÔÅ ÌÉÞÎÏ. ôÏÇÄÁ, ÷Ù ÍÏÖÅÔÅ Õ×ÎÕËÉ. ÷Ù ÍÏÖÅÔÅ ÓÏÚÄÁÔØ ÓÐÉÓÏË ÐÏÄÐÉÓÅÊ, ÎÁ ËÏÔÏÒÙÅ ×ÙÂÙ ÄÏ×ÅÒÑÅÔÅ, ÉÌÉ ÐÏÌÎÙÊ ÓÐÉÓÏË ÐÏÄÐÉÓÅÊ, ÎÁ ËÏÔÏÒÙÅ ×ÙÂÙ ÄÏ×ÅÒÑÅÔÅ, ÉÌÉ ÐÏÌÎÙÊ ÓÐÉÓÏË ÐÏÄÐÉÓÅÊ, ÎÁ ËÏÔÏÒÙÅ ×ÙÂÙ ÎÅ ÄÏ×ÅÒÑÅÔÅ. ÷Ù ÔÁËÖÅ ÍÏÖÅÔÅ ÕËÁÚÁÔØ ÓÔÅÐÅÎØ ÄÏ×ÅÒÉÑ, ËÏÔÏÒÕÀ ×Ù ÈÏÔÉÔÅ ÐÒÉÍÅÎÉÔØ ËÏ ×ÓÅÍ ÐÏÄÐÉÓÑÍ, ÉÌÉ ÍÏÖÅÔÅ ÕËÁÚÁÔØ ÒÁÚÎÙÅ ÕÒÏ×ÎÉ ÄÏ×ÅÒÉÑ ÄÌÑ ÒÁÚÎÙÈ ÐÏÄÐÉÓÅÊ.

ðÏÄÐÉÓÙÁÎÉÅ ÷ÁÛÅÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ

ïÄÎÏÇÏ ÖÅÌÁÁÝÅÇÏ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ÎÅÄÏÓÔÁÔÏÞÎÏ. äÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÓÏÏÂÝÁÔØÓÑ ÚÁÝÉÝÅÎÎÏ Ó ÄÒÕÇÉÍÉ, ÷Ù ÄÏÌÖÎÙ ÉÍÅÔØ ÓÅÔØ ÄÏ×ÅÒÑ. ðÏÓÌÅÄÎÅÅ ÓÅÔÉ ÄÏ×ÅÒÑ ÐÏÈÏÄÅ ÎÁ ÕËÏÎÙÅ ÓÅÒÖÅÒÙ, ÁÎÏÎÉÍÎÙÅ ÉÓÈÏÄÎÙÅ ÔÏÞËÉ ÐÏÄÄÅÒÖÉ×ÁÀÔ ÐÒÏÔÏËÏÌ ÈÁÛÉÒÏ×ÁÎÉÑ ÐÏÒÔÏ×, ÞÔÏÂÙ ÌÀÄÉ, Ó ËÏÔÏÒÙÍÉ ×Ù ÌÉÞÎÏ ÎÅ ÚÎÁËÏÍÙ, ÍÏÇÌÉ ÓÏÚÄÁÔØ ÓÅËÒÅÔÎÙÅ ËÌÀÞÉ ÄÌÑ ×ÁÛÅÇÏ ÉÍÅÎÉ. üÔÏ ÔÁËÖÅ ÐÏÚ×ÏÌÑÅÔ ÐÒÅÄÏÔ×ÒÁÔÉÔØ ÐÏÐÙÔËÉ ËÔÏ-ÔÏ ÄÅÌÁÔØ ×ÉÄ, ÞÔÏ ×Ù ÐÏÄÐÉÓÁÌÉ ÓÏÏÂÝÅÎÉÅ, ËÏÔÏÒÏÅ ÏÎÏ ÎÅ ÐÏÌÕÞÁÌÏ.

ëÒÏÍÅ ÷Ù ÎÁÞÅÎÁÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, ×ÁÖÎÏ ÐÏÑÎÔØ, ÞÔÏ ÎÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ × ÚÁÝÉÔÅ ÐÅÒÅÐÉÓÅË Ó ËÁÖÄÙÍ ËÌÀÞÁÍÉ ÏÔ ÎÅÂÏÛÏÇÏ ËÒÕÇÁ ÌÀÄÅÊ, ×ÏÚÍÏÖÎÏ ÔÏÌØËÏ ÷Ù É ÏÄÎÏ ÉÌÉ Ä×Á ÷ÁÛÉÈ ÔÏ×ÁÒÉÝÁ, ÔÏÖÅ ÖÅÌÁÀÝÉÈ ÒÅÁÌØÎÙ×ÁÔØ Ó×ÏÅ ÐÒÁ×Ï ÎÁ ÔÁÊÎÕ ÐÅÒÅÐÉÓËÕ. üÔÏ ÷ÁÛÁ ÎÁÞÁÌØÎÁÑ ÓÅÔØ ÄÏ×ÅÒÑ. äÅÌÁÑ ÔÁË, ÷Ù ÏÃÅÎÉÔÅ

ÚÎÁÞÅÎÉÅ ÍÁÌÅÎØËÏÊ, ÎÁÄÅÖÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ É ÂÕÄÅÔ ÂÏÌÅ ÏÓÔÏÒÏÛ × ÂÕÄÙÝÅÍ, ËÏÇÄÁ ÷ÁÛÁ ÓÅÔØ ÓÔÁÎÅÔ ÒÁÓÔÉ.

÷ ÄÏÐÏÎÅÎÉÅ Ë ÜÔÏÊ ÎÁÞÁÌØÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ, ÷Ù ÍÏÖÅÔÅ ÚÁÈÏÔÅØ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏ ÐÅÒÅÐÉÓÙ×ÁÔØÓÑ Ó ÄÒÕÇÉÍÉ ÌÀÄØÍÉ, ÔÁËÖÅ ÉÓÐÏÌØÚÕÀÝÉÍÉ GnuPG. òÅÁÌÉÚÁÃÉÑ ÜÔÏÇÏ ÖÅÌÁÎÉÑ, ÏÄÎÁËÏ, ÍÏÖÅÔ ÏËÁÚÁÔØÓÑ ÎÅÕÄÏÂÎÏÊ ÐÏ Ä×ÕÍ ÐÒÉÞÉÎÁÍ: (1) ÷Ù ÎÅ ×ÓÅÇÄÁ ÚÎÁÅÔÅ, ÐÔÏ ÞÅÌÏ×ÅË ÉÓÐÏÌØÚÕÅÔ ÉÌÉ ÖÅÌÁÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, É (2) ÅÓÌÉ ÷Ù É ÚÎÁÅÔÅ, ÐÔÏ ÞÅÌÏ×ÅË ÉÓÐÏÌØÚÕÅÔ ÅÇÏ, ÍÏÇÕÔ ×ÏÚÎÉËÎÕÔØ ÓÌÏÖÎÏÓÔÉ Ó ÐÏÄÔ×ÅÒÖÄÅÎÉÅÍ ËÌÀÞÅÊ. ðÅÒ×ÁÑ ÐÒÉÞÉÎÁ Ñ×ÌÑÅÔÓÑ ÓÌÅÄÔ×ÉÁÍ ÔÏÇÏ, ÞÔÏ ÌÀÄÉ ÎÅ ×ÓÅÇÄÁ ÏÂßÑ×ÌÑÀÔ Ï ÔÏÍ, ÞÔÏ ÉÓÐÏÌØÚÕÀÔ GnuPG. ÷ÏÚÍÏÖÎÙÊ ×ÁÖÉÁÎÔ ÒÅÛÅÎÉÑ ÜÔÏÊ ÐÒÏÂÌÅÍÙ, ÐÏÄÄÅØ ÐÒÉÅÍ É ÏÂß×ÉÔØ, ÞÔÏ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG. åÓÔØ ËÁË ÍÉÎÉÍÕÍ ÔÒÉ ÓÐÏÓÏÂÁ ÓÄÅÌÁÔØ ÜÔÏ: ÷Ù ÍÏÖÅÔÅ ÐÏÄÐÉÓÙ×ÁÔØ Ó×ÏÉ ÓÏÏÂÝÅÎÉÑ, ÷Ù ÍÏÖÅÔÅ ÐÏÌÏÉÔØ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÁ Ó×ÌÅÊ ×ÂÅ-ÓÔÒÁÎÉÃÅ, ÷Ù ÍÏÖÅÔÅ ÕËÁÚÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÷ÁÛÅÇÏ ËÌÀÞÁ × ÐÏÄÐÉÓÉ ÐÞÔÏ×ÏÇÏ ÓÏÏÂÝÅÎÉÑ. åÓÌÉ ÷Ù ÓÏÏÂÝÁÅÔÅ Ï Ó×ÏÅÍ ËÌÀÞÅ, ÔÏ ÄÅÌÁÅÔÅ ÂÏÌÅÅ ÕÍÅÎØÛÉÔÅÌÙÍ ÄÌÑ ÄÒÕÇÉÈ ÓÏÏÂÝÉÔÅÌÅÊ ÏÔÐÒÁ×ÉÔØ ÓÏÏÂÝÅÎÉÑ ÐÏ ÉÈ ËÌÀÞÁÈ. âÏÌÅ ÔÏÇÏ, ÷ÁÛÉÍ ËÌÀÞÏÍ ÔÁÉÌÅ ÕÄÁÌÑÔØ ÎÁÐÁÔØ Ó ÷ÁÍÉ ÐÅÒÅÐÉÓ×ÁÎÎÙÅ ÓÏÏÂÝÅÎÉÑ, ÅÓÌÉ ÷Ù ÐÒÏÑ×ÉÌÉ ÉÎÔÅÒÅÓ Ë ÓÄÅÌÁÎÎÏÍÕ ÷ÁÍÉ GnuPG.

ðÒÏ×ÅÒÁ ÐÓ×ÉÌØÎÏÓÔÉ ËÌÀÞÁ ÂÏÌÅ ÓÌÏÖÎÁ. åÓÌÉ ÷Ù ÎÅ ÚÎÁËÏÍÙ ÌÉÞÎÏ Ó ÞÅÌÏ×ÅËÍ, ÞÅÊ ËÌÀÞ ÓÏÂÉÓÁÅÔÅÓØ ÐÏÄÉÓÁÔØ, ÔÏ ÎÅ ÍÏÖÅÔÅ ÐÏÄÉÓÁÔØ ËÌÀÞ ÓÁÍÉ. ÷Ù ÄÏÔÏÙ ÏÐÉÓÁÔØÓÑ ÎÁ ÞÕÖÉÅ ÐÏÄÉÓÉ É ÐÏÓÔÁÔÅØÓÑ ÎÁÊÔÉ ÃÅÐÏÞËÕ ÐÏÄÉÓÅÊ, ÎÁÞÉÎÁÑ Ó ËÌÀÞÁ ÐÏÄ ×ÏÐÒÏÍ É ÚÁËÁÎÞÉ×ÁÑ ÷ÁÛÉÍ. äÌÑ ÎÁÈÏÄÅÎÉÑ ÃÅÐÏÞËÉ, ÷Ù ÄÏÌÖÎÙ ÐÒÏÑ×ÉÔØ ÉÎÔÅÇÒÁÔÉ×Ñ ÷ÁÛÉÍ ËÌÀÞÏÍ ÐÏÄÐÉÓÁÎÎÙÊ ËÅÍ-ÌÉÂÏ ÚÁ ÐÒÅÄÅÌÁÍÉ ÷ÁÛÅÊ ÎÁÞÁÌØÎÏÊ ÓÅÔÉ Ä×ÅÒÉ.

éÍÅÊÔÅ ÏÄÎÁËÏ × ×ÉÄÕ, ÞÔÏ ×ÓÅ ÜÔÏ × ÚÁ×ÉÓÉÍÓÔÉ ÏÔ ÐÏÔÒÅÂÎÏÓÔÅÊ. ÷Ù ÎÅ ÏÂÑÚÁÔÅÌØÎÏ ÄÏÌÖÎÙ ÚÁÑ×ÌÑÔØ Ï Ó×ÏÅÍ ËÌÀÞÅ ÉÌÉ ÐÏÄÐÉÓÙ×ÁÔØ ÞÕÖÅÅ ËÌÀÞÉ. óÉÌÁ GnuPG ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏ ÎÎ ÄÏÓÔÁÔÏÞÎÏ ÇÉÂÏÉ É ÍÏÖÅÔ ÂÙÔØ ÁÄÁÐÔÉÒÏ×ÁÎ Ë ÷ÁÛÉÍ ÐÏÔÒÅÂÎÏÓÑÍ, ËÁËÉÍ ÂÙ ÏÎÉ ÎÅ ÂÙÌÉ. ðÒÉ ÜÔÏÍ ÄÅÓÔ×ÉÔÅÌØÎÏÓÔØ ÔÁËÏ×Á, ÞÔÏ ÷Ù ÄÏÌÖÎÙ ÐÒÏÑ×ÌÑÔØ ÉÎÉÃÉÁÔÉ×Õ, ÅÓÌÉ ÈÏÉÅÅ ÒÁÓÛÉÒÅÎÎÙÊ ÓÔÁÎÄÁÒÔ Ó×ÏÀ ÓÅÔØ ÄÏ×ÅÒÑ É ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ËÁË ÍÏÖÎÏ ÂÏÌØÛÅ.

úÁËÌÀÞÅÎÉÅ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG

úÁËÌÀÞÉÔÅÌØÎÙÊ ÓÔÁÔÕÓ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÐÒÏÇÒÁÍÍ ÒÁÚÌÉÞÅÎ × ÒÁÚÎÙÈ ÓÔÒÁÎÁÈ, ËÒÏÍÅ ÔÏÇÏ, ÚÁËÌÀÞÅÎÙ, ÒÅÇÕÌÉÒÕÀÝÁ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÓÒÅÄÓÔ×, ÂÙÓÔÒÏ ÍÅÎÑÀÔÓÑ. Bert-Japp Koops (http://cwis.kub.nl/~frw/people/koops/bertjaap.htm) ÓÄÅÌÁÌ ÎÅÐÌÈÕÀ ÓÔÒÁÎÉÞÕ Crypto Law Survey (http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm), Ë ËÏÔÏÒÏÊ ÷Ù ÍÏÖÅÔÅ ÏÂÒÁÝÁÔØÓÑ, ÞÔÏÂÙ ÕÚÎÁÔØ ÚÁËÏÎÏÄÁÔÅÌØÎÙÊ ÓÔÁÔÕÓ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÐÒÏÇÒÁÍÍ × ÷ÁÛÅÊ ÓÔÒÁÎÅ.

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

5. òÁÚÌÉÞÎÙÅ ×ÏÐÒÏÓÙ

üÔÁ ÇÌÁ×Á ÒÁÓÓÍÁÔÒÉ×ÁÅÔ ÒÁÚÌÉÞÎÙÅ ×ÏÐÒÏÓÙ ËÏÔÏÒÙÍ ÎÅ ÎÁÛÌÏÓØ ÍÅÓÔÁ × ÄÒÕÇÏÍ ÍÅÓÔÅ ÒÕÊÌ×ÏÄÓÔ×Á. äÏÂÁ×ÌÅÎÙÅ ×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 ÞÅÒÎ×ÕÀ ×ÅÒÓÉÀ, ÏÐÉÓÁÎÎÕÀ ÉÎÔÅÒÅÓÕÀÝÉÊ ÷ÁÓ ×ÏÐÒÏÓ!

îÁÐÉÓÁÎÉÅ ÐÏÌØÚÏ×ÁÔÅÌØÓÊÏÇÏ 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) ÐÏÌØÚÏ×ÁÔÅÌØÓÊÏÇÏ ÉÎÔÅÒÆÅÊÓÁ PGP 5.0 É ÐÒÉÛÌÉ Ë ÚÁËÌÀÞÅÎÉÀ, ÞÔÏ ÎÁÞÉÎÁÀÝÉÅ ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÅ ÎÅÐÏÎÑÔÎÙÅ PGP ÓÌÏÖÎÙÍ É ÎÅÐÏÎÑÔÎÙÍ. ðÏ ÒÅÚÕÌØÔÁÔÁÍ ÉÈ ÔÅÓÔÏ×, ÔÏÌØËÏ ÞÅÔ×ÅÒÏ ÉÚ Ä×ÅÎÁÄÃÁÔÉ ÔÅÓÔÉÒÕÅÍÙÈ ÐÒÁ×ÉÌØÎÏ ÏÐÒÁ×ÉÌÉ ÚÁÛÉÆÒÏ×ÁÎÙÅ ÓÏÏÂÝÅÎÉÑ ÞÌÅÎÁÍ ÉÈ ËÏÍÁÎÄÙ, É ÔÒÌÅ ÉÚ Ä×ÅÎÁÄÃÁÔÉ ÏÐÒÁ×ÉÌÉ ÓÅËÒÅÔ ÎÅÚÁÛÉÆÒÏ×ÁÎÙÍ. ðÒÉ ÜÔÏÍ ÐÌÌ×ÉÍÁ ÔÁÓÔÉÒÕÅÍÙÈ ÐÒÏÛÌÉ ÔÅÈÎÉÞÅÓËÕÀ ÐÏÄÇÏÔÏ×ËÕ.

üÔÉ ÒÅÚÕÌØÔÁÔÙ ÎÅ ÕÄÉ×ÌÑÀÔ. PGP 5.0 ÉÍÅÅÔ ÈÏÒÛÉÊ ÐÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ, ËÏÔÏÒÙÊ ÐÒÅ×ÏÓÈÏÄÅÎ ÅÓÌÉ ÷Ù ÕÖÅ ÐÎÎÉÍÅÅÔÅ Ë ÚÁËÌÀÞÅÎÉÀ ÛÉÆÒÏ×ÁÎÎÙÍ ËÌÀÞÏÍ É ÄÒÕÉÅÔ Ó ÍÏÄÅÌØÀ ÐÏÄÔ×ÅÒÖÄÅÎÑ ËÌÀÞÅÊ ÓÐÅÃÉÆÉÃÉÒÏ×ÁÎÎÙÊ OpenPGP. ë ÓÏÖÁÌÅÉÀ, ÎÁÞÉÍÁÀÝÉÅ ÐÌÌØÚÏ×ÁÔÅÌÉ, ÎÅ ÐÎÉÍÁÀÔ ÎÉ ÛÉÆÒÏ×ÁÎÑ Ó ÏÔÈÒÙÔÙÍ ËÌÀÞÏÍ, ÎÉ ÐÒ×ÉÌ ÓÐÒÔ×ÌÅÎÑ ËÌÀÞÁÍÉ, É ÐÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ ÍÁÌÏ ÐÍÍÇÁÂÔ ÉÍ.

÷ÁÍ ÓÌÅÄÕÅÔ ×ÎÉÁÔÅÌØÎÏ ÏÚÎÁËÏÍÉÔÔØÓÑ Ó ×Ù×ÏÄÁÍÉ Whitten'Á É Tygar'Á ÅÓÌÉ ÷Ù ÐÉÛÅÔÅ ÐÌÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ. ïÎÉ ÄÁÀÔ ËÏÍÍÅÎÔÁÒÉÉ ÐÏ ËÁÖÄÏÍÕ ÉÚ ÔÅÓÔÏÖÅÍÙÈ. îÁÐÒÉÍÅÒ, ÏËÁÚÁÏÓØ, ÞÔÏ ÍÏÇÉÅ ×ÅÑÎÕ, ÞÔÏ ÓÏÂÝÅÍÉÅ ÐÏÙÌÁÅÍÏÅ ÄÒÕÇÉÍ ÌÀÄÑÍ ÎÁÄÏ ÚÁÛÉÆÒÏ×Ù×ÁÔØ Ó×ÏÉÍ ÓÏÂÓÔ×ÅÎÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÁÄÕÍÁÊÔÅØ ÎÁÄ ÜÔÉÍ, É ÷Ù ÐÏÊÍÅÔÅ, ÞÔÏ ÌÅÇËÏ ÄÏÕÓÔÉÔØ ÔÛÉÂËÕ. ëÁË ÐÒÁ×ÉÌ, ÎÁÞÉÎÁÀÝÉÅ ÐÎÌØÚÏ×ÁÔÅÌÉ ÉÓÐÙÔÙ×ÁÀÔ ÔÒÕÄÎÏÓÔÉ × ÐÎÍÉÁÎÉÉ ÒÁÚÌÉÞÉÊ ÍÅÖÄÕ ÏÔËÒÙÔÙÍ É ÚÁËÒÙÔÙÍ ËÌÀÞÁÍÉ ËÇÄÁ ÉÓÐÎÌØÚÕÀÔ GnuPG. ëÁË ÄÉÚÂÎÅÀ ÐÎÌØÚÏ×ÁÔÅÌØÓËÉÇÏ ÉÎÔÅÒÆÅÊÓÁ, ÷Ù ÄÏÔÏÙ ÐÏÓÔÁÀÔÓÑ ÓÄÅÌÁÔØ ×ÙÂÏÒ ÔÏÇÏ ÉÌÉ ËÌÀÞÁ ÐÒÏÚÒÁÞÎÙÍ. ÷Ù ÍÏÖÅÔÅ, ÔÁËÅ, ÉÓÐÎÌØÚÏ×ÁÔØ ÍÁÓÔÅÒ ÍÁÓÔÅÒ É ÄÕÇÉÅ ÏÐÅÒÁÔÏÒÙ ÐÏÄÄÅÒÖËÉ ÛÉÆÒÏ×ÁÎÉÑ ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÈ ËÌÀÞÅÊ, ÔÁËÉÅ ËÁË ÇÅÎÅÒÁÃÉÑ ËÌÀÞÁ, ÄÏÐÏÌÎÅÎÉÑ ÇÅÎÅÒÁÃÉÅÊ ÓÅÎÓÏÒÎÙÈ ÔÏÞÅË ÏÔ ÏÐÅÒÁÃÉÏÎÎÏÊ ÓÉÓÔÅÍÙ, ÏÔÅÖÅ, ÓÌÅÄÕÀÝÉÅ ×Ù×ÏÄÙ.

- âÅÚÏÐÁÓÎÏÓÔØ, ÏÂÙÞÎÏ Ñ×ÌÑÅÔÑ ×ÔÏÒÏÓÅÐÅÎÎÏÊ ÚÁÄÁÞÅÊ; ÌÀÄÉ ÈÏÑÔ ÏÔÐÒÁ×ÌÑÔØ ÐÏÞÔÕ, ÐÒÏÍÁÔÒÉ×ÁÔØ É Ô.Ä. îÅ ÄÕÍÁÊÔÅ ÞÔÏ ÐÎÌØÚÏ×ÁÔÅÌÉ ÓÔÁÎÕÔ ÞÉÔÁØ ÔÏÌÓÔÙÅ ÒÕËÏ×ÏÄÓÔ×Á ÉÌÉ ÒÁÚÂÉÒÁÔØÓÑ × ÎÁÓÔÒÏÊËÁÈ ÛÉÆÒÏ×ÁÎÑ.
- úÁÝÉÔÁ ÓÅÅ×ÏÇÏ ËÏÍÐØÀÔÅÒÁ ÎÅ ÓÉÌØÎÅÅ ÓÁÍÏÇÏ ÓÌÁÂÏÇÏ ÉÚ ÅÅ ËÏÍÐÏÎÅÎÔÏ×. ðÏÌØÚÏ×ÁÔÅÌ ÄÏÖÎ ÂÙÔØ ÏÓ×ÅÄÏÍÌÅÎ ÏÂ ×ÓÅÈ ÁÓÐÅËÔÁÈ Ó×ÏÅÊ ÂÅÚÏÐÁÓÎÏÓÔÉ, ÎÅ ÏÇÓÁÍÉÞÉ×ÁÑØ ÞÁÓÔÉÞÎÙÍÉ Ó×ÅÄÅÎÑÍÉ, ËÁË ÜÔÏ ÍÖÅÂ ÂÙÔØ ÓÌÅÄÕÅÔ ÓÄÅÌÁÔØ Ó ÔÅËÓÔÏÍ ÐÏÓÌÅ ÅÇÏ ÛÉÆÒÏ×ÁÎÉÑ.

- ÷ÓÅÇÄÁ ÉÓÐÏÌØÚÕÊÔÅ ÏÄÉÎÁËÏ×ÙÅ ÔÅÒÍÉÎÙ ÄÌÑ ÏÄÉÎÁËÏ×ÙÈ ÄÅÊÓÔ×ÉÊ. éÚÂÅÇÁÊÔÅ ÕÐÏÔÒÅÂÌÅÎÑ ÓÉÎÏÎÉÎÏ×, ÔÉÐÁ “encrypt” É “encipher”.
- äÌÑ ÎÅÉÓËÕÛÅÎÙÈ ÐÏÌØÚÏ×ÁÔÅÌÅÊ ÕÐÒÏÓÔÓÅÔÅ ×Ù×ÏÄ ÉÎÆÏÒÍÁÃÉÉ. óÌÉÛËÏÍ ÂÏØÛÏÅ ËÏÌÉÞÅÓÔ×Ï ÉÎÆÏÒÍÁÃÉÉ ÓËÒÙ×ÁÅÔ ÕÑ, ËÏÔÒÁÑ ×ÁÖÍÁ. îÁÞÁÌØÍÁÑ ËÏÎÆÉÇÕÒÁÃÉÑ ÉÎÔÅÒÆÅÉÁ ÄÏÌÖÍÁ ÏÅÒÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÒÁ×ÉÌØÎÏÊ ÍÄÅÌÌÛÅÎÉÊ ÍÅÄÌÅÎÎÏÇÏ ÐÒÏÃÅÓÓÁ É ÚÁËÒÙÔÙÍ ËÌÀÞÁÍÉ É ÐÒÏÚÁÞÎÙÍ ÐÏÎÉÍÁÎÉÅÍ ÆÕÎËÃÉÊ ÐÌÕÞÅÎÉÑ É ÒÁÓÐÒÏÓÒÁÎÅÎÑ ËÌÀÞÅÊ.

òÁÚÒÁÂÏÔËÁ ÜÆÆÅËÔÉ×ÎÏÇÏ ÐÏÌØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ ÄÌÑ ÕÐÒÁ×ÌÅÎÑ ËÌÀÞÁÍÉ ÅÝÅ ÂÏÌÅÅ ÓÌÏÖÎÁ. íÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ OpenPGP, Ë ÓÏÖÁÌÅÉÀ, ÄÏ×ÎØÎÏ ÔÒÕÄÎÁ ÄÌÑ ÐÏÎÉÍÁÎÉÑ. îÁÐÒÉÍÅÒ, ÓÐÅÃÉÆÉËÁÃÉÑ ÏÐÒÅÄÅÌÑÅÔ ÔÒÉ ÓÔÅÐÅÎÉ ÄÏ×ÅÒÉÑ ÐÏØÚÏ×ÁÔÅÌÀ: ÎÅÔ (none), ÏÔÍÏÉÔÅÌØÎÏÅ (marginal), É ÐÏÌÎÏÅ (Óomplete). ÷ÓÅ ÇÒÁÎÉ ÄÏ×ÅÒÉÑ, ÉÓÐÙÔÙ×ÁÅÍÇÏ ÐÏØÚÏ×ÁÔÅÌÅÍ, ÄÏÌÖÎÙ ÕÍÅÔØ ÕÎÉ ÔÒÅÇÏÔØÓÑ × ÜÔÉ ÔÒÉ ÑÞÅËÉ. áÌÇÏÒÉÔÍ ÐÏÄ×ÅÒÖÄÅÎÉÑ ËÌÀÞÅÊ ÔÁËÖÅ ÓÏÖÅÎ ÄÌÑ ÐÏÎÉÍÁÎÉÑ ÎÅ ÓÐÅÃÉÁÌÉÓÔÏ×, ÏÓÏÂÅÎÎÏ ÐÁÒÁÍÅÔÒÙ “marginals needed” É “completes needed”. ôÁË ËÁË ÍÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÞÅÔËÏ ÐÒÅÄÅÌÅÎÁ É ÎÅ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎÁ, ÷ÁÍ ÐÒÉÊÄÅÔÓÑ ÐÏÔÒÁÔÉÔØÓÑ É ÒÁÚÒÁÂÏÔÁÔØ ÉÎÔÅÒÆÅÓ, ËÏÔÏÙÊ ÐÏÍÏÇÅÔ ÐÏÎÑÔØ ÅÅ ÐÌÌØÚÏ×ÁÔÅÌÀ. ïÐÒÅÄÅÌÅÎÎÁÑ ÆÕÎËÃÉÑ, Ë ÐÒÉÍÅÒÕ, ÍÏÇÌÁ ÂÙ ÏÔÂÒÁÖÁÔØ ÄÉÁÇÒÁÍÍÕ ÔÏÇÏ, ËÁË ÂÙÌ ÐÏÄ×ÅÒÖÄÅÎ ËÌÀÞ, ÐÏ ÚÁÐÒÓÕ ÐÌØÚÏ×ÁÔÅÌÑ. ïÓÎÏ×ÙÅ ×Ù×ÏÄÙ ÓÌÅÄÕÀÝÉÅ.

- ðÏØÚÏ×ÁÔÅÌÉ ÍÇÕÔ ÏÓÁ×ÁÔØÓÑ × ÎÅ×ÅÄÅÎÉÉ ÏÔÏÓÉÔÅÌØÎÏ ÔÏÇÏ, ËÁË É ËÏÇÄÁ ÐÒÅÄÏÓÁ×ÉÔØ ÄÏÓÕÐ.
- ðÒÉÄÁÊÔÅ ×ÙÓÏËÉÊ ÐÒÉÒÉÔÅÔ ÔÍÍÕ, ÞÔÏÂÙ ÚÁÝÉÔÉÔØ ÐÏØÚÏ×ÁÔÅÌÅ ÏÔ ÓÏ×ÅÒØÅÎÉÑ ÄÌÒÏÇÍÓÔÑÝÉÈ ÏÛÉÂÏË, ÔÁËÉÈ ËÁË ÏÛÉÂÏÞÎÏÅ ÕÄÁÌÅÎÉÅ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÐÕÂÌÉËÁÃÉÑ ËÌÀÞÁ, ÏÔÚ× ËÌÀÞÁ, ÐÏÔÅÒÑ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ, ÎÅÐÒÁ×ÉÌØÎÏÁÑ ÁÒÈÉ×ÁÃÉÑ ËÌÀÞÁ.

A. éÚÍÅÎÅÎÉÑ (History)

1. GNU Privacy Handbook. 1999Ç. Mike Ashley.
2. ïÐÉÓÁÎÉÅ GNU Privacy Guard. 2001Ç. ðÁ×ÅÌ ûÁÊÄÏ. ðÅÒÅ×ÏÄ ÎÁ ÒÕÓÓËÉÊ ÑÚÙË.
3. ïÐÉÓÁÎÉÅ GNU Privacy Guard. ÍÁÊ 2002Ç. ðÁ×ÅÌ ûÁÊÄÏ. ðÒÉ×ÅÄÅÎÉ × ÓÏÎÔ×ÅÓÔ×ÉÅ Ó ×ÅÒÓÉÅÊ gnupg 1.0.7. ðÒÏÃÅÄÕÒÁ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÏÐÉÓÁÎÁ ÄÌÑ ÁÌÇÏÒÉÔÍÁ RSA. õÄÁÌÅÎÉ ÏÐÉÓÁÎÉÅ ËÏÍÁÎÄ É ÐÁÒÁÍÅÔÒÏ×, ËÁË ÕÓÔÁÎÏ×ÉÌÅ.

B. 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.