ïÐÉÓÁÎÉÅ GNU Privacy Guard

ïÐÉÓÁÎÉÅ GNU Privacy Guard

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

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

÷ËÌÁÄ × ÓÏÚÄÁÎÉÅ ÄÁÎÎÏÇÏ ÒÕËÏ×ÏÄÓÔ×Á ×ÎÅÓÌÉ, ÔÁËÖÅ, íÜÔØÀ ëÏÕÐÌÜÎÄ (Matthew Copeland), êÏÒÇÅÎ çÒÜÎ (Joergen Grahn), äÜ×ÉÄ á. ÷ÉÌÅÒ (David A. Wheeler).

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

Содержание

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
  - ãÅÌÏÓÔÎÏÓÔØ ËÌÀÞÁ. ... 17
  - äÏÂÁ×ÌÅÎÉÅ É ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ ... 18
  - ïÔÚÙ× ËÏÍÐÏÎÅÎÔ ËÌÀÞÁ ... 19
  - éÚÍÅÎÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ ... 21
- ðÒÏ×ÅÒËÁ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ ... 21
  - äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ ... 22
  - éÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏ×ÅÒÉÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ ... 23
- òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÅÊ ... 25

4. åÖÅÄÎÅ×ÎÏÅ ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG ... 28
- ïÐÒÅÄÅÌÅÎÉÅ ÷ÁÛÉÈ ÔÒÅÂÏ×ÁÎÉÊ Ë ÚÁÝÉÔÅ ... 28
  - ÷ÙÂÏÒ ÒÁÚÍÅÒÁ ËÌÀÞÁ ... 29
  - úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ... 29
  - ÷ÙÂÏÒ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ É ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ËÌÀÞÅÊ ... 30
  - õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ ... 31
- ðÏÓÔÒÏÅÎÉÅ ÷ÁÛÅÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ ... 32
- úÁËÏÎÎÏÓÔØ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG ... 33

5. òÁÚÎÉÞÎÙÅ ×ÏÐÒÏÓÙ ... 34
- îÁÐÉÓÁÎÉÅ ÐÏÌØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ ... 34

A. éÚÍÅÎÅÎÉÑ (History) ... 36

B. GNU Free Documentation License ... 37
- 0. PREAMBLE ... 37
- 1. APPLICABILITY AND DEFINITIONS ... 37
- 2. VERBATIM COPYING ... 38
- 3. COPYING IN QUANTITY ... 38

4. MODIFICATIONS....39
5. COMBINING DOCUMENTS....40
6. COLLECTIONS OF DOCUMENTS....40
7. AGGREGATION WITH INDEPENDENT WORKS....41
8. TRANSLATION....41
9. TERMINATION....41
10. FUTURE REVISIONS OF THIS LICENSE....41
How to use this License for your documents....42

Список иллюстраций

3-1. ðÒÉÍÅÒ ÓÅÔÉ ÄÏ×ÅÒÉÑ 25

Глава 1. âÙÓÔÒÙÊ ÓÔÁÒÔ

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

GnuPG ÉÓÐÏÌØÚÕÅÔ ËÒÉÐÔÏÇÒÁÆÉÀ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. ëÁÖÄÙÊ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÅÅÔ ÐÁÒÕ ËÌÀÞÅÊ (keypair), ÓÏÓÔÏÑÝÕÀ ÉÚ *ÓÅËÒÅÔÎÏÇÏ (private)* É *ÏÔËÒÙÔÏÇÏ (public)* ËÌÀÞÅÊ. óÅËÒÅÔÎÙÊ ËÌÀÞ Ñ×ÌÑÅÔÓÑ ÓÅËÒÅÔÏÍ ÐÏÌØÚÏ×ÁÔÅÌÑ É ÎÅ ÍÏÖÅÔ ÂÙÔØ ÐÅÒÅÄÁÎ ÄÒÕÇÉÍ ÌÉÃÁÍ, ÎÉ ÐÒÉ ËÁËÉÈ ÏÂÓÔÏÑÔÅÌØÓÔ×ÁÈ. ïÔËÒÙÔÙÊ ËÌÀÞ ÐÅÒÅÄÁÅÔÓÑ ×ÓÅÍ ÌÀÄÑÍ, Ó ËÏÔÏÒÙÍÉ ÐÏÌØÚÏ×ÁÔÅÌØ ÂÕÄÅÔ ÏÂÍÅÎÉ×ÁÔØÓÑ ÓÏÏÂÝÅÎÉÑÍÉ. GnuPG ÉÓÐÏÌØÚÕÅÔ ÎÅÓËÏÌØËÏ ÂÏÌÅÅ ÈÉÔÒÏÕÍÎÕÀ ÓÈÅÍÕ, ÐÒÉ ËÏÔÏÒÏÊ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÅÅÔ ÐÅÒ×ÉÞÎÕÀ ÐÁÒÕ ËÌÀÞÅÊ É, ×ÏÚÍÏÖÎÏ, ÄÏÐÏÌÎÉÔÅÌØÎÏ ÎÅÓËÏÌØËÏ ÐÏÄÞÉÎÅÎÎÙÈ. ðÅÒ×ÉÞÎÁÑ É ÐÏÄÞÉÎÅÎÎÙÅ ÐÁÒÙ ÏÂßÅÄÉÎÅÎÙ, ÄÌÑ ÕÐÒÏÝÅÎÉÑ ÉÈ ÉÓÐÏÌØÚÏ×ÁÎÉÑ, É ÜÔÁ Ó×ÑÚËÁ, ÚÁÞÁÓÔÕÀ, ÍÏÖÅÔ ÒÁÓÓÍÁÔÒÉ×ÁÔØÓÑ ÐÒÏÓÔÏ, ËÁË ÏÄÎÁ ÐÁÒÁ ËÌÀÞÅÊ.

çÅÎÅÒÁÃÉÑ ÎÏ×ÏÊ ÐÁÒÙ ËÌÀÞÅÊ

äÌÑ ÓÏÚÄÁÎÉÑ ÐÅÒ×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×ÉÞÎÙÊ 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 - ÐÏÄÞÉÎÅÎÎÁÑ, 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, ÐÏÚÖÅ ÍÏÖÎÏ ÓÏÚÄÁÔØ ÄÏÐÏÌÎÉÔÅÌØÎÙÅ ÐÁÒÙ ËÌÀÞÅÊ ÄÌÑ ÐÏÄÐÉÓÉ É ÛÉÆÒÏ×ÁÎÉÑ. îÁÉÂÏÌÅÅ ÈÏÒÏÛÉÍ, ÐÏÖÁÌÕÊ, 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 ÉÍÅÔØ ÌÀÂÏÊ ÒÁÚÍÅÒ. GnuPG ÎÅ ÄÏÐÕÓËÁÅÔ ÄÌÉÎÕ ËÌÀÞÅÊ ÍÅÎÅÅ 768 ÂÉÔ. åÓÌÉ ÷Ù ×ÙÂÒÁÌÉ ×ÁÒÉÁÎÔ 1, ÔÏ ÒÁÚÍÅÒ DSA ËÌÀÞÁ ÐÏÌÁÇÁÅÔÓÑ 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 ×ÚÌÏÍÁ, ÎÏ ÒÁÚÍÅÒ ÐÏ ÕÍÏÌÞÁÎÉÀ ÄÏÓÔÁÔÏÞÅÎ ÐÒÁËÔÉÞÅÓËÉ ÄÌÑ ÌÀÂÙÈ ÃÅÌÅÊ. âÏÌØÛÁÑ ÄÌÉÎÁ ËÌÀÞÁ ÚÁÍÅÄÌÑÅÔ ÚÁÛÉÆÒÏ×ËÕ É ÒÁÓÛÉÆÒÏ×ËÕ É ÍÏÖÅÔ ÏÔÒÁÚÉÔØÓÑ ÎÁ ÄÌÉÎÅ ÐÏÄÐÉÓÅÊ. òÁÚÍÅÒ ËÌÀÞÁ ÎÅÌØÚÑ ÂÕÄÅÔ ×ÐÏÓÌÅÄÓÔ×ÉÉ ÉÚÍÅÎÉÔØ.

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

```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
```

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

÷ ÄÏÐÏÌÎÅÎÉÅ Ë ÐÁÒÁÍÅÔÒÁÍ ËÌÀÞÁ, ÷Ù ÄÏÌÖÎÙ ÕËÁÚÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ. éÄÅÎÔÉÆÉËÁÔÏÒ ÎÕÖÅÎ, ÞÔÏÂÙ Ó×ÑÚÁÔØ ÓÏÚÄÁÎÎÙÊ ËÌÀÞ Ó ËÏÎËÒÅÔÎÙÍ ÌÉÃÏÍ.

```
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 ÏÄÉÎ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÎÏ ×ÏÚÍÏÖÎÏ ÓÏÚÄÁÎÉÅ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ×, ÅÓÌÉ ÷Ù ÈÏÔÉÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ ËÌÀÞ × ÎÅÓËÏÌØËÉÈ ËÏÎÔÅËÓÔÁÈ; ÎÁÐÒÉÍÅÒ, ËÁË ÉÎÖÅÎÅÒ ÎÁ ÒÁÂÏÔÅ É ËÁË ÐÏÌÉÔÉÞÅÓËÉÊ ÄÅÑÔÅÌØ ÐÏÓÌÅ ÎÅÅ. éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÎÅ ÍÏÖÅÔ ÂÙÔØ ÏÔÒÅÄÁËÔÉÒÏ×ÁÎ ÐÏÓÌÅ ÓÏÚÄÁÎÉÑ.

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

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

Enter passphrase:
```

îÁ ÄÌÉÎÕ ÐÁÒÏÌÑ ÎÅÔ ÏÇÒÁÎÉÞÅÎÉÊ, É ÅÇÏ ÓÌÅÄÕÅÔ ×ÙÂÉÒÁÔØ ÔÝÁÔÅÌØÎÏ. ó ÔÏÞËÉ ÚÒÅÎÉÑ ÂÅÚÏÐÁÓÎÏÓÔÉ, ÐÁÒÏÌØ ÄÌÑ ÚÁÝÉÔÙ ËÌÀÞÁ ÏÞÅÎØ ×ÁÖÅÎ × GnuPG (É ÄÒÕÇÉÈ ÓÉÓÔÅÍÁÈ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ), Ô.Ë. ÜÔÏ ÷ÁÛÁ ÅÄÉÎÓÔ×ÅÎÎÁÑ ÚÁÝÉÔÁ × ÓÌÕÞÁÅ, ÅÓÌÉ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÐÏÐÁÄÅÔ × ÞÕÖÉÅ ÒÕËÉ. îÅ ÓÌÅÄÕÅÔ ÂÒÁÔØ ÓÌÏ×Á ÉÚ âóü, ÞÅÒÅÄÕÊÔÅ ÒÅÇÉÓÔÒ ÂÕË× É ÉÓÐÏÌØÚÕÊÔÅ ÎÅÁÌÆÁ×ÉÔÎÙÅ ÓÉÍ×ÏÌÙ. èÏÒÏÛÉÊ ÐÁÒÏÌØ ËÒÉÔÉÞÅÎ ÄÌÑ ÎÁÄÅÖÎÏÓÔÉ GnuPG.

ðÏÓÌÅ ÜÔÏÇÏ GnuPG ÇÅÎÅÒÉÒÕÅÔ ËÌÀÞ. ÷ ÓÌÕÞÁÅ ÅÓÌÉ × ÷ÁÛÅÊ ÓÉÓÔÅÍÅ ÎÅ ÏÞÅÎØ ÈÏÒÏÛÉÊ ÇÅÎÅÒÁÔÏÒ ÓÌÕÞÁÊÎÙÈ ÞÉÓÅÌ, ÐÒÏÇÒÁÍÍÁ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÍÏÖÅÔ ÚÁÎÑÔØ ÄÏ×ÏÌØÎÏ ÍÎÏÇÏ ×ÒÅÍÅÎÉ. ÷ ÎÅËÏÔÏÒÙÈ ÓÌÕÞÁÑÈ ÐÏÍÏÇÁÅÔ ÛÅ×ÅÌÅÎÉÅ ÍÙÛËÏÊ, × ÎÅËÏÔÏÒÙÈ ÎÁÇÒÕÚËÁ ÓÉÓÔÅÍÙ.

óÏÚÄÁÎÉÅ ÏÔÚÙ×ÁÀÝÅÇÏ ÓÅÒÔÉÆÉËÁÔÁ

ðÏÓÌÅ ÓÏÚÄÁÎÉÑ ÐÁÒÙ ËÌÀÞÅÊ, ÷ÁÍ ÓÌÅÄÕÅÔ ÓÏÚÄÁÔØ ÏÔÚÙ×ÁÀÝÉÊ ÓÅÒÔÉÆÉËÁÔ (revokation certificate) ÄÌÑ ÐÅÒ×ÉÞÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÉÓÐÏÌØÚÕÑ ËÌÀÞ `--gen-revoke`. åÓÌÉ ÷Ù ÚÁÂÕÄÅÔÅ ÐÁÒÏÌØ, ÌÉÂÏ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÂÕÄÅÔ ÐÏÈÉÝÅÎ ÉÌÉ ÕÔÅÒÑÎ, ÜÔÏÔ ÓÅÒÔÉÆÉËÁÔ ÍÏÖÅÔ ÂÙÔØ ÒÁÚÏÓÌÁÎ ÄÌÑ Õ×ÅÄÏÍÌÅÎÉÑ Ï ÔÏÍ, ÞÔÏ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÅÌØÚÑ ÂÏÌØÛÅ ÉÓÐÏÌØÚÏ×ÁÔØ. ïÔÏÚ×ÁÎÎÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÓÄÅÌÁÎÎÙÈ ÷ÁÍÉ ÐÏÄÐÉÓÅÊ É ÄÁÌØÛÅ, ÎÏ ÎÅ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÓÏÏÂÝÅÎÉÊ ÄÌÑ ÷ÁÓ. ðÒÉ ÜÔÏÍ, ÷Ù ÓÏÈÒÁÎÑÅÔÅ ×ÏÚÍÏÖÎÏÓÔØ ÒÁÓÛÉÆÒÏ×ËÉ ÐÒÉÓÌÁÎÎÙÈ ÷ÁÍ ÓÏÏÂÝÅÎÉÊ, ÐÒÉ ÎÁÌÉÞÉÉ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ.

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

áÒÇÕÍÅÎÔ **`mykey`** - ÉÄÅÎÔÉÆÉËÁÔÏÒ ÷ÁÛÅÊ ÐÅÒ×ÉÞÎÏÊ ÐÁÒÙ ËÌÀÞÅÊ ÉÌÉ ÌÀÂÁÑ ÞÁÓÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ ÷ÁÛÅÊ ÐÁÒÙ ËÌÀÞÅÊ. óÇÅÎÅÒÉÒÏ×ÁÎÎÙÊ ÓÅÒÔÉÆÉËÁÔ ÂÕÄÅÔ ÓÏÈÒÁÎÅÎ × ÆÁÊÌÅ *`revoke.asc`*. åÓÌÉ ÏÐÃÉÑ `--output` ÏÐÕÝÅÎÁ, ÒÅÚÕÌØÔÁÔ ÐÏÍÅÝÁÅÔÓÑ × ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ. ëÒÏÍÅ ÔÏÇÏ, GnuPG ÚÁÐÒÁÛÉ×ÁÅÔ ÐÒÉÞÉÎÕ ÇÅÎÅÒÁÃÉÉ ÏÔÚÙ×ÁÀÝÅÇÏ 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 ÓÅÊÆ ÐÏÄÏÊÄÅÔ). åÓÌÉ ÓÅÒÔÉÆÉËÁÔ ÐÏÐÁÄÅÔ × ÞÕÖÉÅ ÒÕËÉ É ÂÕÄÅÔ ÏÐÕÂÌÉËÏ×ÁÎ, ÔÏ ÏÔËÒÙÔÙÊ ËÌÀÞ ÕÔÒÁÔÉÔ Ó×ÏÀ ÄÅÊÓÔ×ÉÅ.

ïÂÍÅÎ ËÌÀÞÁÍÉ

äÌÑ ÏÂÝÅÎÉÑ 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 ÐÏÓÌÁÔØ ËÏÍÕ-ÌÉÂÏ ÏÔËÒÙÔÙÊ ËÌÀÞ, ÷Ù ÄÏÌÖÎÙ ÅÇÏ ÜËÓÐÏÒÔÉÒÏ×ÁÔØ. äÌÑ ÜÔÏÇÏ ÉÓÐÏÌØÚÕÅÔÅ ËÏÍÁÎÄÕ `--export`. åÊ ÔÒÅÂÕÅÔÓÑ, ÄÏÐÏÌÎÉÔÅÌØÎÏ, ÁÒÇÕÍÅÎÔ, ÉÄÅÎÔÉÆÉÃÉÒÕÀÝÉÊ ÜËÓÐÏÒÔÉÒÕÅÍÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, ËÁË É ÄÌÑ `--gen-revoke`.

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

ëÌÀÞ ÜËÓÐÏÒÔÉÒÕÅÔÓÑ × Ä×ÏÉÞÎÏÍ ÆÏÒÍÁÔÅ, ÞÔÏ ÂÙ×ÁÅÔ ÎÅÕÄÏÂÎÏ. GnuPG ÉÍÅÅÔ ÏÐÃÉÀ ËÏÍÁÎÄÎÏÊ ÓÔÒÏËÉ `--armor`, ËÏÔÏÒÁÑ ÕËÁÚÙ×ÁÅÔ ÎÁ ÎÅÏÂÈÏÄÉÍÏÓÔØ ×Ù×ÏÄÁ × ÆÏÒÍÁÔÅ ASCII. ðÒÁËÔÉÞÅÓËÉ ÌÀÂÏÊ ×Ù×ÏÄ GnuPG, Ô.Å. ËÌÀÞÉ, ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÏËÕÍÅÎÔÙ, ÐÏÄÐÉÓÉ, ÍÏÖÅÔ ÐÒÅÄÓÔÁ×ÌÑÔØ × 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×ÑÚËÅ ÷ÁÛÉÈ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÐÒÉ ÐÏÍÏÝÉ 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 ÄÏÌÖÎÁ ÂÙÔØ ÐÏÄÔ×ÅÒÖÄÅÎÁ. GnuPG ÉÓÐÏÌØÚÕÅÔ ÇÉÂËÕÀ É ÍÏÝÎÕÀ ÍÏÄÅÌØ ÐÒÏ×ÅÒËÉ ÐÏÄÌÉÎÎÏÓÔÉ, ÎÅ ÔÒÅÂÕÀÝÕÀ, ÞÔÏÂÙ ÷Ù ÌÉÞÎÏ ÐÒÏ×ÅÒÑÌÉ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÁÖÄÏÇÏ ÉÍÐÏÒÔÉÒÏ×ÁÎÎÏÇÏ ËÌÀÞÁ. ôÅÍ ÎÅ ÍÅÎÅÅ, ÄÏÓÔÏ×ÅÒÎÏÓÔØ ÎÅËÏÔÏÒÙÈ ËÌÀÞÅÊ ÷ÁÍ ÐÒÉÄÅÔÓÑ ÐÒÏ×ÅÒÉÔØ ÓÁÍÏÍÕ. óÎÁÞÁÌÁ ÐÒÏ×ÅÒÑÅÔÓÑ ÏÔÐÅÞÁÔÏË (fingerprint) ËÌÀÞÁ, ÚÁÔÅÍ ËÌÀÞ ÚÁ×ÅÒÑÅÔÓÑ ÐÏÄÐÉÓØÀ, ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÔÏÇÏ, ÞÔÏ ÏÎ ÄÏÓÔÏ×ÅÒÅÎ. ïÔÐÅÞÁÔÏË ËÌÀÞÁ ÍÏÖÎÏ ÂÙÓÔÒÏ ÐÒÏÓÍÏÔÒÅÔØ 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 ×ÌÁÄÅÌØÃÅÍ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÓÄÅÌÁÎÏ ÐÒÉ ÌÉÞÎÏÊ ×ÓÔÒÅÞÅ, ÐÏ ÔÅÌÅÆÏÎÕ, ÉÌÉ ÌÀÂÙÍ ÄÒÕÇÉÍ ÓÐÏÓÏÂÏÍ, ÇÁÒÁÎÔÉÒÕÀÝÉÍ, ÞÔÏ ÷Ù ÏÂÝÁÅÔÅÓØ Ó ×ÌÁÄÅÌØÃÅÍ ËÌÀÞÁ. åÓÌÉ ÏÔÐÅÞÁÔËÉ ÐÏÌÕÞÅÎÎÙÅ ÷ÁÍÉ ÓÏ×ÐÁÄÁÀÔ Ó ÕËÁÚÁÎÎÙÍÉ ×ÌÁÄÅÌØÃÅÍ ËÌÀÞÁ, ÔÏ ÍÏÖÅÔÅ ÂÙÔØ Õ×ÅÒÅÎÙ, ÞÔÏ ÉÍÅÅÔÅ ÄÏÓÔÏ×ÅÒÎÕÀ ËÏÐÉÀ ËÌÀÞÁ.

ðÏÓÌÅ ÐÒÏ×ÅÒËÉ ÏÔÐÅÞÁÔËÁ ÷Ù ÍÏÖÅÔÅ ÐÏÄÐÉÓÁÔØ ËÌÀÞ. ôÁË ËÁË ÐÒÏ×ÅÒËÁ ËÌÀÞÁ ÓÌÁÂÏÅ Ú×ÅÎÏ × ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÔÏ ÷Ù ÄÏÌÖÎÙ ÂÙÔØ Ó×ÅÒÛÅÎÎÏ Õ×ÅÒÅÎÙ × ËÌÀÞÅ ÐÅÒÅÄ ÔÅÍ, ËÁË ÅÇÏ ÐÏÄÐÉÓÙ×ÁÔØ, É ×*ÓÅÇÄÁ* ÐÒÏ×ÅÒÑÊÔÅ 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 ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÁ É ÐÏÐÒÏÓÉÔ ÐÏÄÔ×ÅÒÄÉÔØ ÷ÁÛÅ ÖÅÌÁÎÉÅ ÐÏÄÐÉÓÁÔØ ËÌÀÞ. ðÏÄÐÉÓÁ× ËÌÀÞ, ÷Ù ÍÏÖÅÔÅ ÐÒÏÓÍÏÔÒÅÔØ 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 ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÔÏÌØËÏ ÄÌÑ ÐÏÄÐÉÓÉ. äÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÷ÁÛÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÍÏÇÌÉ ÚÁÛÉÆÒÏ×Ù×ÁÔØ ÎÁÐÒÁ×ÌÑÅÍÙÅ ÷ÁÍ ÓÏÏÂÝÅÎÉÑ, ÎÅÏÂÈÏÄÉÍÏ ÓÏÚÄÁÔØ ÄÏÐÏÌÎÉÔÅÌØÎÙÊ ËÌÀÞ, ËÏÔÏÒÙÊ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. çÅÎÅÒÁÃÉÑ ÄÏÐÏÌÎÉÔÅÌØÎÏÇÏ 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 ÒÅÖÉÍÁ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ, ÓÏÈÒÁÎÉ× ÉÚÍÅÎÅÎÉÑ, ×ÏÓÐÏÌØÚÕÊÔÅÓØ 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 ÓÏÏÂÝÅÎÉÅ ÐÒÉ ÐÏÍÏÝÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÜÔÏ ÓÏÏÂÝÅÎÉÅ ÐÏÍÅÝÁÅÔÓÑ × ÓÅÊÆ É ÓÅÊÆ ÚÁËÒÙ×ÁÅÔÓÑ. óÏÏÔ×ÅÔÓÔ×ÕÀÝÉÊ ÚÁËÒÙÔÙÊ ËÌÀÞ - ËÏÍÂÉÎÁÃÉÑ, ÎÅÏÂÈÏÄÉÍÁÑ ÄÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÏÔËÒÙÔØ ÓÅÊÆ É ÐÏÌÕÞÉÔØ ÄÏËÕÍÅÎÔ. äÒÕÇÉÍÉ ÓÌÏ×ÁÍÉ, ÔÏÌØËÏ ÞÅÌÏ×ÅË ÏÂÌÁÄÁÀÝÉÊ ÚÁËÒÙÔÙÍ ËÌÀÞÏÍ ÍÏÖÅÔ ×ÏÓÓÔÁÎÏ×ÉÔØ ÄÏËÕÍÅÎÔ, ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÉÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ.

åÓÌÉ ÷Ù ÈÏÔÉÔÅ ÐÏÓÌÁÔØ ÓÏÏÂÝÅÎÉÅ äÖÏÎÕ, ÔÏ ÷Ù ÚÁÛÉÆÒÏ×Ù×ÁÅÔÅ ÅÇÏ ÐÒÉ ÐÏÍÏÝÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ äÖÏÎÁ, Á ÏÎ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ ÅÇÏ ÐÒÉ ÐÏÍÏÝÉ Ó×ÏÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ. åÓÌÉ äÖÏÎ ÚÁÈÏÞÅÔ ÏÔ×ÅÔÉÔØ, ÔÏ ÏÎ ÚÁÛÉÆÒÕÅÔ ÏÔ×ÅÔ ÐÒÉ ÐÏÍÏÝÉ ÷ÁÛÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, Á ÷Ù ÒÁÓÛÉÆÒÕÅÔÅ ÅÇÏ Ó×ÏÉÍ ÓÅËÒÅÔÎÙÍ.

äÌÑ ÚÁÛÉÆÒÏ×ÁÎÉÑ ÄÏËÕÍÅÎÔÁ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--encrypt`. ÷Ù ÄÏÌÖÎÙ ÉÍÅÔØ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÐÒÅÄÐÏÌÁÇÁÅÍÙÈ ÐÏÌÕÞÁÔÅÌÅÊ. ðÒÏÇÒÁÍÍÁ ÏÖÉÄÁÅÔ × ËÁÞÅÓÔ×Å ÐÁÒÁÍÅÔÒÁ ÉÍÑ ÛÉÆÒÕÅÍÏÇÏ ÄÏËÕÍÅÎÔÁ ÉÌÉ, × ÓÌÕÞÁÅ ÅÇÏ ÏÔÓÕÔÓÔ×ÉÑ, ÛÉÆÒÕÅÔ ÓÔÁÎÄÁÒÔÎÙÊ ××ÏÄ. úÁÛÉÆÒÏ×ÁÎÎÙÊ ÒÅÚÕÌØÔÁÔ ÐÏÍÅÝÁÅÔÓÑ × ÓÔÁÎÄÁÒÔÎÙÊ ×Ù×ÏÄ, ÅÓÌÉ ÎÅ ÕËÁÚÁÎÁ ÏÐÃÉÑ `--output`. äÌÑ ÐÏ×ÙÛÅÎÉÑ ÚÁÝÉÔÙ ÄÏËÕÍÅÎÔ ÄÏÐÏÌÎÉÔÅÌØÎÏ ÓÖÉÍÁÅÔÓÑ.

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

ïÐÃÉÑ `--recipient` ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ËÁÖÄÏÇÏ ÐÏÌÕÞÁÔÅÌÑ É ÉÍÅÅÔ ÁÒÇÕÍÅÎÔ, ÉÄÅÎÔÉÆÉÃÉÒÕÀÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, ËÏÔÏÒÙÍ ÄÏÌÖÅÎ ÂÙÔØ ÚÁÛÉÆÒÏ×ÁÎ ÄÏËÕÍÅÎÔ. úÁÛÉÆÒÏ×ÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÍÏÖÅÔ ÂÙÔØ ÒÁÓÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÔÅÍ, ÞÅÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÓÏÏÔ×ÅÔÓÔ×ÕÅÔ ÏÄÎÏÍÕ ÉÚ ÕËÁÚÁÎÎÙÈ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ. ÷ ÞÁÓÔÎÏÓÔÉ, ÷Ù ÎÅ

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

äÌÑ ÒÁÓÛÉÆÒÏ×ÁÎÉÑ ÓÏÏÂÝÅÎÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--decrypt`. ÷ÁÍ ÎÕÖÅÎ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÄÌÑ ËÏÔÏÒÏÇÏ ÜÔÏ ÓÏÏÂÝÅÎÉÅ 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 ÚÁÛÉÆÒÏ×Ù×ÁÔØ ÂÅÚ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ÷ÍÅÓÔÏ ÜÔÏÇÏ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÉÍÍÅÔÒÉÞÎÙÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÄÏËÕÍÅÎÔÁ. ëÌÀÞ, ÉÓÐÏÌØÚÕÅÍÙÊ ÐÒÉ ÚÁÛÉÆÒÏ×ÁÎÉÉ, ÏÂÒÁÚÕÅÔÓÑ ÉÚ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ. äÌÑ ÂÏÌØÛÅÊ ÂÅÚÏÐÁÓÎÏÓÔÉ ÜÔÁ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÎÅ ÄÏÌÖÎÁ Ó×ÐÁÄÁÔØ Ó ÔÅÍ, ËÏÔÏÒÕÀ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ ÄÌÑ ÚÁÝÉÔÙ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ. óÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ ÐÒÉÍÅÎÉÍ, ËÏÇÄÁ ÎÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ ÏÂÍÅÎÉ×ÁÔØÓÑ ËÌÀÞÅ×ÙÍÉ ÆÒÁÚÁÍÉ. äÌÑ ÉÓÐÏÌØÚÏ×ÁÎÉÑ 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 ÄÁÔÕ ÓÏÚÄÁÎÉÑ ÄÏËÕÍÅÎÔÁ. åÓÌÉ ÄÏËÕÍÅÎÔ ÂÕÄÅÔ ËÁËÉÍ-ÌÉÂÏ ÏÂÒÁÚÏÍ ÉÚÍÅÎÅÎ, ÔÏ ÐÒÏ×ÅÒËÁ ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓÉ ÂÕÄÅÔ ÎÅÕÄÁÞÎÏÊ. ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ × ÔÁÈ ÖÅ ÃÅÌÑÈ, ÞÔÏ É ÏÂÙÞÎÁÑ ÐÏÄÐÉÓØ. éÓÈÏÄÎÙÅ ÔÅËÓÔÙ GnuPG, ÎÁÐÒÉÍÅÒ, ÐÏÄÐÉÓÁÎÙ, É ÷Ù ÍÏÖÅÔÅ ÕÂÅÄÉÔØÓÑ, ÞÔÏ ÏÎÉ ÄÏÛÌÉ ÄÏ ÷ÁÓ ÎÅÉÚÍÅÎ£ÎÎÙÍÉ.

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

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

```
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. ðÅÒÅÄ ÐÏÄÐÉÓØÀ ÄÏËÕÍÅÎÔ ÓÖÉÍÁÅÔÓÑ. ðÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ×Ù×ÏÄÉÔÓÑ × Ä×ÏÉÞÎÏÍ ÆÏÒÍÁÔÅ.

éÍÅÑ ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ, ÷Ù ÍÏÖÅÔÅ ÌÉÂÏ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ÌÉÂÏ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ É ×ÏÓÓÔÁÎÏ×ÉÔØ ÉÓÈÏÄÎÙÊ ÄÏËÕÍÅÎÔ. äÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ ÉÓÐÏÌØÚÕÅÔÓÑ ËÏÍÁÎÄÁ `--verify`. äÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ 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 ÓÏÏÂÝÅÎÉÊ usenet É e-mail. ðÒÉ ÜÔÏÍ ÎÅÖÅÌÁÔÅÌØÎÏ ÓÖÉÍÁÔØ 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 - ÉÎÓÔÒÕÍÅÎÔ ÄÌÑ ÚÁÝÉÔÙ ËÏÍÍÕÎÉËÁÃÉÊ. üÔÁ ÇÌÁ×Á ËÒÁÔËÏ ÏÐÉÓÙ×ÁÅÔ ÏÓÎÏ×Ù
ÒÁÂÏÔÙ Ó GnuPG, ×ËÌÀÞÁÑ ÓÏÚÄÁÎÉÅ ÐÁÒ ËÌÀÞÅÊ, ÏÂÍÅÎ ËÌÀÞÁÍÉ É ÉÈ ÐÒÏ×ÅÒËÕ,
ÚÁÛÉÆÒÏ×ËÕ É ÒÁÓÛÉÆÒÏ×ËÕ ÄÏËÕÍÅÎÔÏ×, Á×ÔÏÒÉÚÁÃÉÀ 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, ÔÁËÖÅ, 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£ÎÎÁÑ ÐÏÄÐÉÓØ

ðÒÉÍÅÎÅÎÉÅ ÐÏÄÐÉÓÁÎÎÙÈ ÄÏËÕÍÅÎÔÏ× ÏÇÒÁÎÉÞÅÎÎÏ. ðÏÌÕÞÁÔÅÌØ ÄÏÌÖÅÎ ×ÏÓÓÔÁÎÁ×ÌÉ×ÁÔØ ÄÏËÕÍÅÎÔ ÉÚ ÐÏÄÐÉÓÁÎÎÏÊ ×ÅÒÓÉÉ, É ÄÁÖÅ × ÓÌÕÞÁÅ ÐÒÏÚÒÁÞÎÏÊ ÐÏÄÐÉÓÉ, ÐÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÄÏÌÖÅÎ ÂÙÔØ ÏÔÒÅÄÁËÔÉÒÏ×ÁÎ ÄÌÑ ÐÏÌÕÞÅÎÉÑ ÏÒÉÇÉÎÁÌÁ. ðÏÜÔÏÍÕ ÉÍÅÅÔÓÑ ÔÒÅÔÉÊ ÍÅÔÏÄ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÏ×, ËÏÔÏÒÙÊ 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>"
```

Примечания

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

Глава 2. ïÂÝÉÅ ÐÏÎÑÔÉÑ

GnuPG ÉÓÐÏÌØÚÕÅÔ ÎÅÓËÏÌØËÏ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÈ ÍÅÔÏÄÏ×, ×ËÌÀÞÁÑ *ÓÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ*, *ÛÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ*, É *ÏÄÎÏÎÁÐÒÁ×ÌÅÎÎÏÅ ÈÜÛÉÒÏ×ÁÎÉÅ*. ÷Ù ÍÏÖÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ ÜÔÉ ÍÅÔÏÄÙ, ÉÓÐÏÌØÚÕÑ GnuPG, ÎÏ ÄÌÑ ÌÕÞÛÅÇÏ ÐÏÎÉÍÁÎÉÑ ×ÁÛÅÊ ÚÁÝÉÔÙ ÓÌÅÄÕÅÔ ÏÚÎÁËÏÍÉÔØÓÑ Ó ÎÉÍÉ.

üÔÁ ÇÌÁ×Á - ××ÅÄÅÎÉÅ × ÏÓÎÏ×ÎÙÅ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÅ ÍÅÔÏÄÙ, ÉÓÐÏÌØÚÕÅÍÙÅ × GnuPG. âÏÌÅÅ ÐÏÄÒÏÂÎÏ ÜÔÉ ×ÏÐÒÏÓÙ ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ × ÄÒÕÇÉÈ ÉÓÔÏÞÎÉËÁÈ. èÏÒÏÛÁÑ ËÎÉÇÁ, ÄÌÑ ÄÁÌØÎÅÊÛÅÇÏ ÉÚÕÞÅÎÉÑ: Bruce Schneier
(http://www.counterpane.com/schneier.html) “Applied Cryptography”
(http://www.counterpane.com/applied.html). (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, ÏÂÍÅÎÉ×ÁÀÝÉÅÓÑ ÐÒÉ ÐÏÍÏÝÉ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ, ÄÏÌÖÎÙ ÄÏÇÏ×ÏÒÉÔØÓÑ Ï ËÌÀÞÅ ÄÏ ÎÁÞÁÌÁ ÏÂÍÅÎÁ ÓÏÏÂÝÅÎÉÑÍÉ. ðÏÓÌÅ ÔÏÇÏ ËÁË ÏÎÉ ÄÏÇÏ×ÏÒÉÌÉÓØ, ÏÔÐÒÁ×ÉÔÅÌØ ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÏÂÝÅÎÉÅ, ÉÓÐÏÌØÚÕÑ ËÌÀÞ, ÏÔÐÒÁ×ÌÑÅÔ ÐÏÌÕÞÁÔÅÌÀ, É ÐÏÌÕÞÁÔÅÌØ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ ÓÏÏÂÝÅÎÉÅ, ÉÓÐÏÌØÚÑ ÔÏÔ ÖÅ ÓÁÍÙÊ ËÌÀÞ. îÁÐÒÉÍÅÒ, ÎÅÍÅÃËÁÑ Enigma - ÓÉÍÍÅÔÒÉÞÎÙÊ ÛÉÆÒ, ÅÖÅÄÎÅ×ÎÙÅ ËÌÀÞÉ ÒÁÓÐÒÏÓÔÒÁÎÑÌÉÓØ ËÁË ËÎÉÇÉ ËÏÄÏ×. ëÁÖÄÙÊ ÄÅÎØ ÐÏÓÙÌÁÀÝÉÊ ÉÌÉ ÐÒÉÎÉÍÁÀÝÉÊ ÒÁÄÉÓÔ ÄÏÌÖÅÎ ÂÙÌ ÎÁÊÔÉ × Ó×ÏÅÊ ËÏÐÉÉ ËÎÉÇÉ ËÏÄÏ× ËÌÀÞ ÎÁ ÔÅËÕÝÉÊ ÄÅÎØ. òÁÄÉÏÇÒÁÍÍÙ × ÜÔÏÔ ÄÅÎØ ÚÁÛÉÆÒÏ×Ù×ÁÌÉÓØ É ÒÁÓÛÉÆÒÏ×Ù×ÁÌÉÓØ ÜÔÉÍ ËÌÀÞÏÍ. óÏ×ÒÅÍÅÎÎÙÅ ÐÒÉÍÅÒÙ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ×: 3DES, Blowfish, IDEA É çïóô.

èÏÒÏÛÉÊ ÛÉÆÒ ÚÁËÌÀÞÁÅÔ ×ÓÀ ÚÁÝÉÔÕ × ËÌÀÞÅ, ÎÏ ÎÅ × ÁÌÇÏÒÉÔÍÅ. äÒÕÇÉÍÉ ÓÌÏ×ÁÍÉ, ÚÎÁÎÉÅ ÉÓÐÏÌØÚÕÅÍÏÇÏ ÁÌÇÏÒÉÔÍÁ ÎÅ ÄÏÌÖÎÏ ÐÏÍÏÇÁÔØ ×ÚÌÏÍÝÉËÕ. úÎÁÎÉÅ ÁÌÇÏÒÉÔÍÁ ÐÏÍÏÇÁÅÔ ÅÍÕ, ÔÏÌØËÏ ËÏÇÄÁ ÏÎ ÐÏÌÕÞÉÔ ËÌÀÞ. ûÉÆÒÙ, ÉÓÐÏÌØÚÕÅÍÙÅ × GnuPG, ÏÂÌÁÄÁÀÔ ÜÔÉÍ Ó×ÏÊÓÔ×ÏÍ.

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

âÒÉÔÁÎÉÑ ÉÓÐÏÌØÚÏ×ÁÌÁ ÍÁÛÉÎÙ ÄÌÑ ÐÏÄÂÏÒÁ ËÌÀÞÅÊ, ×Ï ×ÒÅÍÑ ÷ÔÏÒÏÊ íÉÒÏ×ÏÊ ×ÏÊÎÙ. îÅÍÅÃËÁÑ Enigma ÉÍÅÌÁ ÏÞÅÎØ ÂÏÌØÛÏÅ ÐÒÏÓÔÒÁÎÓÔ×Ï ËÌÀÞÅÊ, ÎÏ áÎÇÌÉÞÁÎÅ ÐÏÓÔÒÏÉÌÉ ÓÐÅÃÉÁÌØÎÙÅ ×ÙÞÉÓÌÉÔÅÌØÎÙÅ ÍÁÈÉÎÉÓÙ, "Bombes", ËÏÔÏÒÙÅ ÐÅÒÅÂÉÒÁÌÉ ËÌÀÞÉ ÐÏËÁ ÎÁ ÎÁÈÏÄÉÌÉ ÎÕÖÎÙÊ. éÍÇÄÁ ÏÎÉ ÎÁÈÏÄÉÌÉ ËÌÀÞ ÎÁ ÔÅËÕÝÉÊ ÄÅÎØ ÞÁÒÅÚ ÎÅÓËÏÌØËÏ ÞÁÓÏ× ÐÏÓÌÅ ÎÁÞÁÌÁ ÅÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ, Á ÉÎÏÇÄÁ ÎÅ ÎÁÈÏÄÉÌÉ ÓÏ×ÓÅÍ. "Bombes" ÎÅ Ñ×ÌÑÌÉÓØ ËÏÍÐØÀÔÅÒÁÍÉ, ÎÏ ÂÙÌÉ ÉÈ ÐÒÅÄÛÅÓÔ×ÅÎÎÉËÁÍÉ.

óÏ×ÒÅÍÅÎÎÙÅ ËÏÍÐØÀÔÅÒÙ ÍÏÇÕÔ ÐÅÒÅÂÉÒÁÔØ ËÌÀÞÉ Ó ÏÇÒÏÍÎÏÊ ÓËÏÒÏÓÔØÀ, ÐÏÜÔÏÍÕ ÒÁÚÍÅÒ ËÌÀÞÁ ÔÁË ×ÁÖÅÎ × ÓÏ×ÒÅÍÅÎÎÙÈ ËÒÉÐÔÏÓÉÓÔÅÍÁÈ. ûÉÆÒ DES ÉÓÐÏÌØÚÕÅÔ ËÌÀÞ ÄÌÉÎÏÊ 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 ÐÅÒÅÂÒÁÔØ ÉÈ ÚÁ ÓÞÉÔÁÎÎÙÅ ÄÎÉ, Á ÓÐÅÃÉÁÌÉÚÉÒÏ×ÁÎÎÙÊ ÚÁ ÞÁÓÙ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÂÏÌÅÅ ÐÏÚÄÎÉÅ ÁÌÇÏÒÉÔÍÙ - 3DES, Blowfish É IDEA ÉÓÐÏÌØÚÕÀÔ ËÌÀÞÉ ÄÌÉÎÏÊ 128 ÂÉÔ, ÞÔÏ ÏÚÎÁÞÁÅÔ 2^{128} ×ÏÚÍÏÖÎÙÈ ËÌÀÞÅÊ. üÔÏ ÎÁÍÎÏÇÏ ÂÏÌØÛÅ, É, ÄÁÖÅ, ÅÓÌÉ ×ÓÅ ËÏÍÐØÀÔÅÒÙ ÎÁ ÎÁÛÅÊ ÐÌÁÎÅÔÅ ÏÂßÅÄÉÎÉÔØ, ÉÍ ÐÏÔÒÅÂÕÅÔÓÑ ×ÒÅÍÅÎÉ ÂÏÌØÛÅ, ÞÅÍ ×ÏÚÒÁÓÔ ×ÓÅÌÅÎÎÏÊ, ÄÌÑ ÎÁÈÏÖÄÅÎÉÑ ËÌÀÞÁ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ

ïÓÎÏ×ÎÁÑ ÐÒÏÂÌÅÍÁ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× - ÏÂÍÅÎ ËÌÀÞÁÍÉ. ïÔÐÒÁ×ÉÔÅÌØ É ÐÏÌÕÞÁÔÅÌØ ÄÏÌÖÎÙ ÏÂÍÅÎÑÔØÓÑ ËÌÀÞÁÍÉ, ËÏÔÏÒÙÅ ÂÕÄÕÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÚÁÝÉÝÅÎÎÏÇÏ ÏÂÍÅÎÁ ÉÎÆÏÒÍÁÃÉÅÊ, ÎÏ ËÁËÉÍ ÚÁÝÉÝÅÎÎÙÍ ËÁÎÁÌÏÍ ÏÎÉ ÍÏÇÕÔ ×ÏÓÐÏÌØÚÏ×ÁÔØÓÑ ÄÌÑ ÏÂÍÅÎÁ ÓÁÍÉÍÉ ËÌÀÞÁÍÉ? ÷ ÞÁÓÔÎÏÓÔÉ, ×ÚÌÏÍÝÉËÕ ÍÏÖÅÔ ÂÙÔØ ÌÅÇÞÅ ÐÅÒÅÈ×ÁÔÉÔØ ËÌÀÞ, ÎÅÖÅÌÉ ÅÇÏ ÐÏÄÂÉÒÁÔØ. äÒÕÇÁÑ ÐÒÏÂÌÅÍÁ - ËÏÌÉÞÅÓÔ×Ï ÎÅÏÂÈÏÄÉÍÙÈ ËÌÀÞÅÊ. åÓÌÉ *n* ÞÅÌÏ×ÅË ÈÏÔÑÔ ÏÂÍÅÎÉ×ÁÔØÓÑ ÍÅÖÄÕ ÓÏÂÏÊ ÓÏÏÂÝÅÎÉÑÍÉ, ÔÏ ÎÅÏÂÈÏÄÉÍÏ *n(n-1)/2* ËÌÀÞÅÊ, ÐÏ ÏÄÎÏÍÕ ÄÌÑ ËÁÖÄÏÊ ÐÁÒÙ, ÕÞÁ×ÓÔ×ÕÀÝÉÈ × ÐÅÒÅÐÉÓËÅ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÐÒÉÅÍÌÅÍÏ ÄÌÑ ÎÅÂÏÌØÛÏÊ ÇÒÕÐÐÙ ÌÀÄÅÊ, ÎÏ ÓÔÁÎÏ×ÉÔ ÎÅÕÄÏÂÎÙÍ ÐÒÉ ÅÅ Õ×ÅÌÉÞÅÎÉÉ.

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

üÔÏÔ ÍÅÔÏÄ ÒÅÛÁÅÔ ÐÒÏÂÌÅÍÕ ÏÂÍÅÎÁ ËÌÀÞÁÍÉ, ÐÒÉÓÕÝÕÀ ÓÉÍÍÅÔÒÉÞÎÙÍ ÛÉÆÒÁÍ. ïÔÐÁÄÁÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔØ ÄÏÇÏ×ÏÒÉÔØÓÑ Ï ËÌÀÞÅ ÍÅÖÄÕ ÏÔÐÒÁ×ÉÔÅÌÅÍ É ÐÏÌÕÞÁÔÅÌÅÍ. ÷ÓÅ ÞÔÏ ÔÒÅÂÕÅÔÓÑ, ÜÔÏ ÞÔÏÂÙ ÏÔÐÒÁ×ÉÔÅÌØ ÄÏ ÎÁÞÁÌÁ ÓÅËÒÅÔÎÏÇÏ ÏÂÝÅÎÉÑ ÐÏÌÕÞÉÌ ËÏÐÉÀ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÐÏÌÕÞÁÔÅÌÑ. ëÒÏÍÅ ÔÏÇÏ, ÏÄÉÎ ÏÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ×ÓÅÍÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍÉ ÐÏÌÕÞÁÔÅÌÑ. ôÁËÉÍ ÏÂÒÁÚÏÍ, ÔÏÌØËÏ *n* ÐÁÒ ËÌÀÞÅÊ ÎÅÏÂÈÏÄÉÍÏ ÄÌÑ *n* ÞÅÌÏ×ÅË, ÐÅÒÅÐÉÓÙ×ÁÀÝÉÈÓÑ ÄÒÕÇ Ó ÄÒÕÇÏÍ.

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÏÓÎÏ×ÁÎÙ ÎÁ ÏÄÎÏÓÔÏÒÏÎÎÉÈ ÆÕÎËÃÉÑÈ "c ÌÁÚÅÊËÏÊ". ïÄÎÏÓÔÏÒÏÎÎÑÑ ÆÕÎËÃÉÑ ÜÔÏ ÆÕÎËÃÉÑ, ËÏÔÏÒÕÀ ÌÅÇËÏ ×ÙÞÉÓÌÉÔØ, ÎÏ ÔÒÕÄÎÏ ×ÙÞÉÓÌÉÔØ ÅÅ ÏÂÒÁÔÎÕÀ ÆÕÎËÃÉÀ, Ô.Å. ÐÏ ÚÎÁÞÅÎÉÀ ÆÕÎËÃÉÉ ÎÁÊÔÉ ÚÎÁÞÅÎÉÅ ÁÒÇÕÍÅÎÔÁ. îÁÐÒÉÍÅÒ, ÌÅÇËÏ ×ÙÞÉÓÌÉÔØ ÐÒÏÉÚ×ÅÄÅÎÉÅ Ä×ÕÈ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, ÎÏ ÔÒÕÄÎÏ ÒÁÚÌÏÖÉÔØ ÜÔÏ ÐÒÏÉÚ×ÅÄÅÎÉÅ ÎÁ ÍÎÏÖÉÔÅÌÉ. ïÄÎÏÓÔÏÒÏÎÎÉÅ ÆÕÎËÃÉÉ "Ó ÌÁÚÅÊËÏÊ" ÐÏÈÏÖÉ, ÎÏ ÉÍÅÀÔ ÌÁÚÅÊËÕ. ïÎÁ ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏ ÅÓÌÉ ÎÅËÏÔÏÒÁÑ ÞÁÓÔØ ÉÎÆÏÒÍÁÃÉÉ ÉÚ×ÅÓÔÎÁ, ÔÏ ×ÙÞÉÓÌÅÎÉÅ ÏÂÒÁÔÎÏÊ ÆÕÎËÃÉÉ ÓÔÁÎÏ×ÉÔÓÑ ÌÅÇËÉÍ. îÁÐÒÉÍÅÒ, ÅÓÌÉ ÷ÁÍ ÉÚ×ÅÓÔÎÏ ÏÄÎÏ ÉÚ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, × ÐÒÉÍÅÒÅ ×ÙÛÅ, ÔÏ, ÚÎÁÑ ÐÒÏÉÚ×ÅÄÅÎÉÅ, ÷Ù ÌÅÇËÏ ÎÁÊÄÅÔÅ ×ÔÏÒÏÅ ÞÉÓÌÏ. äÁÎÎÙÊ ÛÉÆÒ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÏÓÎÏ×ÁÎ ÎÁ ÐÒÏÓÔÙÈ ÍÎÏÖÉÔÅÌÑÈ, ÏÔËÒÙÔÙÊ ËÌÀÞ ÓÏÄÅÒÖÉÔ ÐÒÏÉÚ×ÅÄÅÎÉÅ Ä×ÕÈ

ÂÏÌØÛÉÈ ÐÒÏÓÔÙÈ ÞÉÓÅÌ, ÁÌÇÏÒÉÔÍ ÛÉÆÒÏ×ÁÎÉÑ ÉÓÐÏÌØÚÕÅÔ ÜÔÏ ÞÉÓÌÏ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÓÏÏÂÝÅÎÉÑ. áÌÇÏÒÉÔÍ ÒÁÓÛÉÆÒÏ×ËÉ ÔÒÅÂÕÅÔ ÚÎÁÎÉÑ ÐÒÏÓÔÙÈ ÍÎÏÖÉÔÅÌÅÊ, ÔÁË, ÒÁÓÛÉÆÒÏ×ËÁ ÓÔÁÎÏ×ÉÔÓÑ ÌÅÇËÏÊ, ÅÓÌÉ Õ ÷ÁÓ ÅÓÔØ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÓÏÄÅÒÖÁÝÉÊ ÏÄÉÎ ÉÚ ÍÎÏÖÉÔÅÌÅÊ, ÎÏ ÞÒÅÚ×ÙÞÁÊÎÏ ÚÁÔÒÕÄÎÅÎÁ ÅÓÌÉ ÅÇÏ Õ ÷ÁÓ ÎÅÔ.

ëÁË É × ÓÌÕÞÁÅ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ×, ×ÓÑ ÚÁÝÉÔÁ ÈÏÒÏÛÅÇÏ ÛÉÆÒÁ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÚÁËÌÀÞÅÎÁ × ËÌÀÞÅ. îÁÄÅÖÎÏÓÔØ ÚÁ×ÉÓÉÔ ÏÔ ÒÁÚÍÅÒÁ ËÌÀÞÁ, ÎÏ ÎÅÌØÚÑ ÓÒÁ×ÎÉ×ÁÔØ ÄÌÉÎÙ ËÌÀÞÅÊ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× É ÛÉÆÒÏ× Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ËÁË ÍÅÒÕ ÉÈ ÏÔÎÏÓÉÔÅÌØÎÏÊ ÎÁÄÅÖÎÏÓÔÉ. ðÒÉ ÇÒÕÂÏÍ ×ÚÌÏÍÅ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÛÉÆÒÁ Ó ËÌÀÞÏÍ ÄÌÉÎÏÊ 80 ÂÉÔ, ×ÚÌÏÍÝÉË ÄÏÌÖÅÎ ÐÅÒÅÂÒÁÔØ ÄÏ 2^{81}-1 ËÌÀÞÅÊ ÄÌÑ ÎÁÈÏÖÄÅÎÉÑ ÐÒÁ×ÉÌØÎÏÇÏ. ðÒÉ ×ÚÌÏÍÅ ÛÉÆÒÁ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ Ó ÄÌÉÎÏÊ ËÌÀÞÁ 512 ÂÉÔ, ×ÚÌÏÍÝÉË ÄÏÌÖÅÎ ÒÁÚÌÏÖÉÔØ ÎÁ ÍÎÏÖÉÔÅÌÉ ÞÉÓÌÏ ÚÁËÏÄÉÒÏ×ÁÎÎÏÅ × 512 ÂÉÔÁÈ (ÄÏ 155 ÄÅÓÑÔÉÞÎÙÈ ÚÎÁËÏ×). äÅÊÓÔ×ÉÑ ×ÚÌÏÍÝÉËÁ ÓÉÌØÎÏ ÒÁÚÌÉÞÁÀÔÓÑ × ÚÁ×ÉÓÉÍÏÓÔÉ ÏÔ ÛÉÆÒÁ. åÓÌÉ ÄÌÑ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ×, ÎÁ ÓÅÇÏÄÎÑÛÎÉÊ ÄÅÎØ, ÄÏÓÔÁÔÏÞÎÁ ÄÌÉÎÁ ËÌÀÞÁ 128 ÂÉÔ, ÔÏ ÄÌÑ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ÒÅËÏÍÅÎÄÕÅÔÓÑ ÄÌÉÎÁ 1024 ÂÉÔÁ.

óÍÅÛÁÎÎÙÅ ÛÉÆÒÙ

ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÎÅ ÐÁÎÁÃÅÑ. íÎÏÇÉÅ ÓÉÍÍÅÔÒÉÞÎÙÅ ÛÉÆÒÙ ÂÏÌÅÅ ÕÓÔÏÊÞÉ×Ù ÐÒÏÔÉ× ×ÚÌÏÍÁ, É, ËÒÏÍÅ ÔÏÇÏ ÚÁÛÉÆÒÏ×ÁÎÉÅ/ÒÁÓÛÉÆÒÏ×ÁÎÉÅ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÔÒÅÂÕÅÔ ÂÏÌØÛÉÈ ÚÁÔÒÁÔ, ÞÅÍ ÁÎÁÌÏÇÉÞÎÙÅ ÏÐÅÒÁÃÉÉ × ÓÉÍÍÅÔÒÉÞÎÙÈ ÓÉÓÔÅÍÁÈ. ûÉÆÒÙ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÔÅÍ ÎÅ ÍÅÎÅÅ, ÜÆÆÅËÔÉ×ÎÙ ÐÒÉ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ËÌÀÞÅÊ ÓÉÍÍÅÔÒÉÞÎÙÈ ÛÉÆÒÏ× É ÉÍÅÎÎÏ ÔÁË ÏÎÉ ÉÓÐÏÌØÚÕÀÔÓÑ × ÓÉÓÔÅÍÁÈ ÓÏ ÓÍÅÛÁÎÎÙÍ ÛÉÆÒÏÍ.

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

é PGP É GnuPG ÉÓÐÏÌØÚÕÀÔ ÉÍÅÎÎÏ ÓÍÅÛÁÎÎÙÅ ÛÉÆÒÙ. óÅÁÎÓÏ×ÙÊ ËÌÀÞ, ÚÁÛÉÆÒÏ×ÁÎÎÙÊ ÛÉÆÒÏÍ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, É ÓÏÏÂÝÅÎÉÅ, ÚÁÛÉÆÒÏ×ÁÎÎÏÅ ÓÉÍÍÅÔÒÉÞÎÙÍ ÛÉÆÒÏÍ, Á×ÔÏÍÁÔÉÞÅÓËÉ ÏÂßÅÄÉÎÑÀÔÓÑ ×ÍÅÓÔÅ. ðÏÌÕÞÁÔÅÌØ ÉÓÐÏÌØÚÕÅÔ Ó×ÏÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÓÅÁÎÓÏ×ÏÇÏ ËÌÀÞÁ É, ÚÁÔÅÍ, ÉÓÐÏÌØÚÕÅÔ ÐÏÌÕÞÅÎÎÙÊ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÓÏÏÂÝÅÎÉÑ.

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

ãÉÆÒÏ×ÙÅ ÐÏÄÐÉÓÉ

èÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ ÜÔÏ ÆÕÎËÃÉÑ "ÍÎÏÇÉÅ-Ë-ÏÄÎÏÍÕ", ÏÔÏÂÒÁÖÁÀÝÁÑ Ó×ÏÉ

ÁÒÇÕÍÅÎÔÙ ÎÁ ÏÇÒÁÎÉÞÅÎÎÏÅ ÍÎÏÖÅÓÔ×Ï ÚÎÁÞÅÎÉÊ. ïÂÙÞÎÏ ÜÔÏ ÍÎÏÖÅÓÔ×Ï - ÄÉÁÐÁÚÏÎ ÎÁÔÕÒÁÌØÎÙÈ ÞÉÓÅÌ. ðÒÏÓÔÁÑ ÈÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ - $f(x) = 0$ ÄÌÑ ×ÓÅÈ ÃÅÌÙÈ x. âÏÌÅÅ ÉÎÔÅÒÅÓÎÁ ÆÕÎËÃÉÑ $f(x) = x \; mod \; 37$, ËÏÔÏÒÁÑ ÏÔÏÂÒÁÖÁÅÔ x × ÏÓÔÁÔÏË ÏÔ ÄÅÌÅÎÉÑ x ÎÁ 37.

ãÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÄÏËÕÍÅÎÔÁ - ÒÅÚÕÌØÔÁÔ ÐÒÉÍÅÎÅÎÉÑ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ Ë ÄÏËÕÍÅÎÔÕ. äÌÑ ÔÏÇÏ ÞÔÏÂÙ ÂÙÔØ ÐÒÉÍÅÎÉÍÏÊ × ËÒÉÐÔÏÇÒÁÆÉÉ, ÈÅÛÉÒÕÀÝÁÑ ÆÕÎËÃÉÑ ÄÏÌÖÎÁ ÕÄÏ×ÌÅÔ×ÏÒÑÔØ Ä×ÕÍ ×ÁÖÎÙÍ ÕÓÌÏ×ÉÑÍ. ÷Ï-ÐÅÒ×ÙÈ, ÎÁÊÔÉ Ä×Á ÄÏËÕÍÅÎÔÁ Ó ÏÄÉÎÁËÏ×ÙÍ ÚÎÁÞÅÎÉÅÍ ÆÕÎËÃÉÉ ÄÏÌÖÎÏ ÂÙÔØ ÐÒÁËÔÉÞÅÓËÉ ÎÅ×ÏÚÍÏÖÎÙÍ. ÷Ï-×ÔÏÒÙÈ, ×ÏÓÓÔÁÎÏ×ÌÅÎÉÅ ÄÏËÕÍÅÎÔÁ ÐÏ ÉÍÅÀÝÅÊÓÑ ÐÏÄÐÉÓÉ ÄÏÌÖÎÏ ÂÙÔØ ÎÅ×ÏÚÍÏÖÎÙÍ.

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

÷ ËÁÞÅÓÔ×Å ÁÌØÔÅÒÎÁÔÉ×Ù ÉÓÐÏÌØÚÕÀÔÓÑ ÈÅÛÉÒÕÀÝÉÅ ÆÕÎËÃÉÉ, ÕÄÏ×ÌÅÔ×ÏÒÑÀÝÉÅ Ä×ÕÍ ×ÙÛÅÕËÁÚÁÎÎÙÍ ÕÓÌÏ×ÉÑÍ. SHA É MD5 ÐÒÉÍÅÒÙ ÔÁËÉÈ ÆÕÎËÃÉÊ. ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÄÁÎÎÏÇÏ ÁÌÇÏÒÉÔÍÁ ÄÌÑ ÐÏÄÐÉÓÉ ÄÏËÕÍÅÎÔÁ, ÓÎÁÞÁÌÁ ×ÙÞÉÓÌÑÅÔÓÑ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ, Á ÚÁÔÅÍ ÜÔÏ ÚÎÁÞÅÎÉÅ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÌÉÎÎÏÓÔÉ ÄÏËÕÍÅÎÔÁ. ðÏÌÕÞÁÔÅÌØ ÍÏÖÅÔ ÐÒÏ×ÅÒÉÔØ ÐÏÄÐÉÓØ, ×ÙÞÉÓÌÉ× ÚÎÁÞÅÎÉÅ ÆÕÎËÃÉÉ ÄÌÑ ÄÏËÕÍÅÎÔÁ É ÓÒÁ×ÎÉ× ÅÇÏ ÓÏ ÚÎÁÞÅÎÉÅÍ, ×ÙÞÉÓÌÅÎÎÙÍ ÏÔÐÒÁ×ÉÔÅÌÅÍ ÄÌÑ ÎÁÓÔÏÑÝÅÇÏ ÄÏËÕÍÅÎÔÁ. åÓÌÉ ÏÎÉ ÓÏ×ÐÁÄÕÔ, ÔÏ ÐÏÞÔÉ ÎÁ×ÅÒÎÑËÁ ÄÏËÕÍÅÎÔÙ ÉÄÅÎÔÉÞÎÙ.

ôÅÐÅÒØ ÐÒÏÂÌÅÍÁ ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏÂÙ ÐÒÅÄÏÔ×ÒÁÔÉÔØ ÉÚÍÅÎÅÎÉÅ ÐÏÄÐÉÓÉ ÚÌÏÕÍÙÛÌÅÎÎÉËÏÍ. åÓÌÉ ÄÏËÕÍÅÎÔ É ÐÏÄÐÉÓØ ÐÏÓÙÌÁÀÔÓÑ ÎÅÚÁÛÉÆÒÏ×ÁÎÎÙÍÉ, ×ÚÌÏÍÝÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÄÏËÕÍÅÎÔ É ×ÙÞÉÓÌÉÔØ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÅÅ ÚÎÁÞÅÎÉÅ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ, ÂÅÚ ×ÅÄÏÍÁ ÐÏÌÕÞÁÔÅÌÑ. åÓÌÉ ÚÁÛÉÆÒÏ×ÁÎ ÔÏÌØËÏ ÄÏËÕÍÅÎÔ, ×ÚÌÏÍÝÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÚÎÁÞÅÎÉÅ ÐÏÄÐÉÓÉ É ÐÒÏ×ÁÌÉÔØ ÅÅ ÐÒÏ×ÅÒËÕ. ôÒÅÔÉÊ ÐÕÔØ - ÉÓÐÏÌØÚÏ×ÁÔØ ÓÍÅÛÁÎÎÙÊ ÍÅÔÏÄ ÛÉÆÒÏ×ÁÎÉÑ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÄÌÑ ÚÁÛÉÆÒÏ×ËÉ ÐÏÄÐÉÓÉ É ÄÏËÕÍÅÎÔÁ. ïÔÐÒÁ×ÉÔÅÌØ ÉÓÐÏÌØÚÕÅÔ Ó×ÏÊ ÚÁËÒÙÔÙÊ ËÌÀÞ, É ÌÀÂÏÊ ÍÏÖÅÔ ×ÏÓÐÏÌØÚÏ×ÁÔØÓÑ ÅÇÏ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÄÌÑ ÐÒÏ×ÅÒËÉ ÐÏÄÐÉÓÉ É ÄÏËÕÍÅÎÔÁ. ú×ÕÞÉÔ ÎÅÐÌÏÈÏ, ÎÏ ÎÁ ÄÅÌÅ ÅÓÔØ ÎÅÂÏÌØÛÁÑ ÐÒÏÂÌÅÍÁ. åÓÌÉ ÂÙ ÜÔÏÔ ÁÌÇÏÒÉÔÍ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÚÁÝÉÝÁÌ ÄÏËÕÍÅÎÔ, ÔÏ, ÔÁËÖÅ, ÚÁÝÉÝÁÌ ÂÙ ÅÇÏ ÏÔ ÐÒÏÞÔÅÎÉÑ, É ÎÅ ÂÙÌÏ ÂÙ ÎÅÏÂÈÏÄÉÍÏÓÔÉ ÅÇÏ ÐÏÄÐÉÓÙ×ÁÔØ. ÷ ÄÅÊÓÔ×ÉÔÅÌØÎÏÓÔÉ, ÜÔÏÔ ÍÅÔÏÄ ÎÅ ÚÁÝÉÝÁÅÔ ÄÏËÕÍÅÎÔ ÏÔ ÐÒÏÞÔÅÎÉÑ. úÁËÒÙÔÙÍ ËÌÀÞÏÍ ÏÔÐÒÁ×ÉÔÅÌÑ ÛÉÆÒÕÅÔÓÑ ÔÏÌØËÏ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ ÓÉÍÍÅÔÒÉÞÎÏÇÏ ÁÌÇÏÒÉÔÍÁ. ìÀÂÏÊ ÞÅÌÏ×ÅË, ÉÓÐÏÌØÚÕÑ ÏÔËÒÙÔÙÊ ËÌÀÞ ÏÔÐÒÁ×ÉÔÅÌÑ, ÍÏÖÅÔ ×ÏÓÓÔÁÎÏ×ÉÔØ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ. îÅÔÒÕÄÎÏ, ÚÁÔÅÍ, ÉÚÍÅÎÉÔØ ÄÏËÕÍÅÎÔ, ÚÁÛÉÆÒÏ×ÁÔØ ÅÇÏ ÎÁÒÁÔÎÏ, ÉÓÐÏÌØÚÕÑ ÐÏÌÕÞÅÎÎÙÊ ÓÅÁÎÓÏ×ÙÊ ËÌÀÞ, É ÐÅÒÅÓÌÁÔØ ÄÁÌØÛÅ ÏÔ ÉÍÅÎÉ ÏÔÐÒÁ×ÉÔÅÌÑ.

áÌÇÏÒÉÔÍ, ËÏÔÏÒÙÊ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÒÁÂÏÔÁÅÔ, ÉÓÐÏÌØÚÕÅÔ ÍÅÔÏÄ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ ÔÏÌØËÏ ÚÎÁÞÅÎÉÑ ÈÅÛÉÒÕÀÝÅÊ ÆÕÎËÃÉÉ. ðÏÄÐÉÓÁÎÎÙÊ ÄÏËÕÍÅÎÔ ÍÏÖÅÔ ÂÙÔØ ÏÔÐÒÁ×ÌÅÎ Ó ÉÓÐÏÌØÚÏ×ÁÎÉÅÍ ÌÀÂÏÇÏ ÄÒÕÇÏÇÏ ÁÌÇÏÒÉÔÍÁ ÛÉÆÒÏ×ÁÎÉÑ, ÌÉÂÏ × ÞÉÓÔÏÍ ×ÉÄÅ, ÅÓÌÉ ÄÏËÕÍÅÎÔ ÎÅ ÓÏÄÅÒÖÉÔ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏÊ ÓÏ×ÅÄÅÎÉÉ. åÓÌÉ ÄÏËÕÍÅÎÔ ÉÚÍÅÎÅÎ ÐÏÓÌÅ ÐÏÄÐÉÓÉ ÐÒÏÔÅÒÐÉÔ ÎÅÕÄÁÞÕ. óÔÁÎÄÁÒÔ ÃÉÆÒÏ×ÏÊ ÐÏÄÐÉÓÉ DSA ÒÁÂÏÔÁÅÔ ÔÁË, ËÁË ÂÙÌÏ ÏÐÉÓÁÎÏ. DSA - ÏÓÎÏ×ÎÏÊ ÁÌÇÏÒÉÔÍ ÃÉÆÒÏ×ÏÊ

ÐÏÄÐÉÓÉ, ÉÓÐÏÌØÚÕÅÍÙÊ × GnuPG.

Примечания

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

Глава 3. õÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ

ðÏÄÄÅÌËÁ ËÌÀÞÁ - ÎÁÉÂÏÌÅÅ ÓÌÁÂÏÅ ÍÅÓÔÏ × ËÒÉÐÔÏÇÒÁÆÉÉ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÌÏÕÍÙÛÌÅÎÎÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÅ Ó×ÑÚËÉ ËÌÀÞÅÊ ÉÌÉ ÐÏÄÄÅÌÁÔØ ÏÔËÒÙÔÙÊ ËÌÀÞ ÐÏÌØÚÏ×ÁÔÅÌÑ É ÐÏÓÌÁÔØ ÅÇÏ ÄÒÕÇÉÍ ÄÌÑ ÚÁÇÒÕÚËÉ É ÉÓÐÏÌØÚÏ×ÁÎÉÑ. îÁÐÒÉÍÅÒ, ÐÒÅÄÐÏÌÏÖÉÍ, ÞÔÏ èÌÏÊ ÈÏÞÅÔ ÏÔÓÌÅÖÉ×ÁÔØ ÓÏÏÂÝÅÎÉÑ, ËÏÔÏÒÙÅ üÌÉÓ ÐÏÓÙÌÁÅÔ âÌÜËÕ. ïÎÁ ÍÏÇÌÁ ÂÙ ÉÓÐÏÌØÚÏ×ÁÔØ ÁÔÁËÕ, ÎÁÚÙ×ÁÅÍÕÀ *ÞÅÌÏ×ÅË × ÓÅÒÅÄÉÎÅ (man in the middle)*. äÌÑ ÜÔÏÇÏ èÌÏÊ ÓÏÚÄÁÅÔ Ó×ÏÀ ÐÁÒÕ ËÌÀÞÅÊ. ïÎÁ ÚÁÍÅÎÑÅÔ ËÏÐÉÀ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ âÌÜËÁ, ÐÒÉÎÁÄÌÅÖÁÝÅÇÏ üÌÉÓ, ÎÁ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞÏÍ. úÁÔÅÍ ÏÎÁ ÐÅÒÅÈ×ÁÔÙ×ÁÅÔ ÓÏÏÂÝÅÎÉÑ, ËÏÔÏÒÙÅ üÌÉÓ ÐÏÓÙÌÁÅÔ âÌÜËÕ. ëÁÖÄÏÅ ÐÅÒÅÈ×ÁÞÅÎÎÏÅ ÓÏÏÂÝÅÎÉÅ ÏÎÁ ÒÁÓÛÉÆÒÏ×Ù×ÁÅÔ, ÉÓÐÏÌØÚÕÑ Ó×ÏÊ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÚÁÛÉÆÒÏ×Ù×ÁÅÔ ÎÁÓÔÏÑÝÉÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ âÌÜËÁ É ÎÁÐÒÁ×ÌÑÅÔ ÅÍÕ ÅÇÏ. ÷ÓÅ ÓÏÏÂÝÅÎÉÑ, ÎÁÐÒÁ×ÌÅÎÎÙÅ üÌÉÓ âÌÜËÕ, ÔÅÐÅÒØ ÍÏÇÕÔ ÂÙÔØ ÐÒÏÞÉÔÁÎÙ èÌÏÊ.

ðÒÁ×ÉÌØÎÏÅ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ Ñ×ÌÑÅÔÓÑ ÒÅÛÁÀÝÉÍ ÄÌÑ ÏÂÅÓÐÅÞÅÎÉÑ ÃÅÌÏÓÔÎÏÓÔÉ ÎÅ ÔÏÌØËÏ ÷ÁÛÉÈ Ó×ÑÚÏË ËÌÀÞÅÊ, ÎÏ É Ó×ÑÚÏË ËÌÀÞÅÊ ÄÒÕÇÉÈ ÐÏÌØÚÏ×ÁÔÅÌÅÊ. ïÓÎÏ×ÏÊ ÕÐÒÁ×ÌÅÎÉÑ ËÌÀÞÁÍÉ × GnuPG Ñ×ÌÑÅÔÓÑ ÐÏÄÐÉÓÙ×ÁÎÉÅ ËÌÀÞÅÊ. ðÏÄÐÉÓÁÎÉÅ ËÌÀÞÅÊ ÉÍÅÅÔ Ä×Á ÏÓÎÏ×ÎÙÈ ÐÒÉÍÅÎÅÎÉÑ: ÜÔÏ ÐÏÚ×ÏÌÑÅÔ ÷ÁÍ ÏÂÎÁÒÕÖÉ×ÁÔØ ×ÍÅÛÁÔÅÌØÓÔ×Ï × ÷ÁÛÕ Ó×ÑÚËÕ ËÌÀÞÅÊ, Á ÔÁËÖÅ ÐÏÚ×ÏÌÑÅÔ ÕÄÏÓÔÏ×ÅÒÉÔØ, ÞÔÏ ËÌÀÞ ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÐÒÉÎÁÄÌÅÖÉÔ ÞÅÌÏ×ÅËÕ, ÞØÉÍ ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ÐÏÌØÚÏ×ÁÔÅÌÑ ÏÎ ÐÏÍÅÞÅÎ. ðÏÄÐÉÓÉ ÎÁ ËÌÀÞÁÈ ÔÁËÖÅ ÉÓÐÏÌØÚÕÀÔÓÑ × ÓÈÅÍÅ ÉÚ×ÅÓÔÎÏÊ ËÁË *ÓÅÔØ Ä×ÅÒÉÑ (web of trust)*, ËÏÔÏÒÁÑ ÐÏÚ×ÏÌÑÅÔ ÓÞÉÔÁÔØ ÄÏÐÕÓÔÉÍÙÍÉ ÎÅ ÔÏÌØËÏ ËÌÀÞÉ ÐÏÄÐÉÓÁÎÎÙÅ ÌÉÞÎÏ ×ÁÍÉ, ÎÏ É ÐÏÄÐÉÓÁÎÎÙÅ ÌÀÄØÍÉ, ËÏÔÏÒÙÍ ×Ù ÄÏ×ÅÒÑÅÔÅ. áËËÕÒÁÔÎÙÅ ÐÏÌØÚÏ×ÁÔÅÌÉ, ÐÒÁ×ÉÌØÎÏ ÒÅÁÌÉÚÏ×Á×ÛÉÅ ÕÐÒÁ×ÌÅÎÉÅ ËÌÀÞÁÍÉ, ÍÏÇÕÔ ÉÓËÌÀÞÉÔØ ÐÏÄÍÅÎÕ ËÌÀÞÅÊ ËÁË ×ÉÄ ÁÔÁËÉ ÎÁ ËÏÎÆÉÄÅÎÃÉÁÌØÎÕÀ Ó×ÑÚØ ÐÒÉ ÐÏÍÏÝÉ GnuPG.

õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÐÁÒÏÊ ËÌÀÞÅÊ

ðÁÒÁ ËÌÀÞÅÊ ÓÏÓÔÏÉÔ ÉÚ ÏÔËÒÙÔÏÇÏ É ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÅÊ. ïÔËÒÙÔÙÊ ËÌÀÞ ÓÏÓÔÏÉÔ ÉÚ ÏÔËÒÙÔÏÊ ÞÁÓÔÉ ÇÌÁ×ÎÏÇÏ ÐÏÄÐÉÓÙ×ÁÀÝÅÇÏ ËÌÀÞÁ, ÏÔËÒÙÔÙÈ ÞÁÓÔÅÊ ÐÏÄÞÉÎÅÎÎÙÈ ÐÏÄÐÉÓÙ×ÁÀÝÉÈ É ÛÉÆÒÕÀÝÉÈ ËÌÀÞÅÊ, ÎÁÂÏÒÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÏÌØÚÏ×ÁÔÅÌÑ, ÁÓÓÏÃÉÉÒÕÀÝÉÈ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó ÒÅÁÌØÎÙÍ ÞÅÌÏ×ÅËÏÍ. ëÁÖÄÁÑ ÞÁÓÔØ ÓÏÄÅÒÖÉÔ ÄÁÎÎÙÅ Ï ÓÅÂÅ. äÌÑ ËÌÀÞÁ -- ÜÔÏ ÅÇÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ, ÄÁÔÁ ÓÏÚÄÁÎÉÑ, ÓÒÏË ÄÅÊÓÔ×ÉÑ É Ô.Ä. äÌÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ -- ÉÍÑ ÞÅÌÏ×ÅËÁ, ÄÏÐÏÌÎÉÔÅÌØÎÙÊ ËÏÍÍÅÎÔÁÒÉÊ É ÁÄÒÅÓ email. óÔÒÕËÔÕÒÁ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÁÎÁÌÏÇÉÞÎÁ, ÎÏ ÓÏÄÅÒÖÉÔ ÓÅËÒÅÔÎÙÅ ÞÁÓÔÉ ËÌÀÞÅÊ É ÎÅ ÓÏÄÅÒÖÉÔ ÉÎÆÏÒÍÁÃÉÀ ÏÂ ÉÄÅÎÔÉÆÉËÁÔÏÒÅ ÐÏÌØÚÏ×ÁÔÅÌÑ.

äÌÑ ÕÐÒÁ×ÌÅÎÉÑ ÐÁÒÏÊ ËÌÀÞÅÊ ÉÓÐÏÌØÚÕÅÔÓÑ 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 ËÏÍÐÏÎÅÎÔÅ 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 ÐÏÄÞÉÎÅÎÎÙÈ ËÌÀÞÅÊ. ÷ÔÏÒÁÑ ËÏÌÏÎËÁ ÐÏËÁÚÙ×ÁÅÔ ÄÌÉÎÕ ËÌÀÞÁ × ÂÉÔÁÈ, ÔÉÐ É ÉÄÅÎÔÉÆÉËÁÔÏÒ. ôÉÐ `D` ÜÔÏ ËÌÀÞ DSA, `R` - ËÌÀÞ RSA, `g` - ËÌÀÞ ElGamal, ÐÒÉÇÏÄÎÙÊ ÔÏÌØËÏ 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. éÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÅÒÅÞÉÓÌÅÎÙ ÐÏÓÌÅ ËÌÀÞÅÊ.

äÏÐÏÌÎÉÔÅÌØÎÁÑ ÉÎÆÏÒÍÁÃÉÑ Ï ËÌÀÞÅ ÍÏÖÅÔ ÂÙÔØ ÐÏÌÕÞÅÎÁ ÒÁÚÌÉÞÎÙÍÉ ËÏÍÁÎÄÁÍÉ. ëÏÍÁÎÄÁ **toggle** ÐÅÒÅËÌÀÞÁÅÔ ÍÅÖÄÕ ÏÔËÒÙÔÏÊ É ÚÁËÒÙÔÏÊ ËÏÍÐÏÎÅÎÔÁÍÉ ÐÁÒÙ ËÌÀÞÅÊ, ÅÓÌÉ ÏÂÅ ÉÚ ÎÉÈ 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×ÏÄÉÍÏÊ ÄÌÑ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. óÉÍ×ÏÌÙ `sec` ÕËÁÚÙ×ÁÀÔ ÓÅËÒÅÔÎÙÊ ÇÌÁ×ÎÙÊ ÐÏÄÐÉÓÙ×ÁÀÝÉÊ ËÌÀÞ, ÓÉÍ×ÏÌÙ `sbb` ÕËÁÚÙ×ÁÀÔ ÓÅËÒÅÔÎÙÅ ÐÏÄÞÉÎÅÎÎÙÅ ËÌÀÞÉ. ôÁËÖÅ ×Ù×ÏÄÑÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ ÉÚ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ.

ãÅÌÏÓÔÎÏÓÔØ ËÌÀÞÁ.

ðÒÉ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ ÏÔËÒÙÔÙÅ ËÏÍÐÏÎÅÎÔÙ ÷ÁÛÅÇÏ ÇÌÁ×ÎÏÇÏ É ÐÏÄÞÉÎÅÎÎÙÈ ËÌÀÞÅÊ É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ. òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ÜÔÏÇÏ ÍÁÔÅÒÉÁÌÁ, ÏÄÎÁËÏ, ÒÉÓËÏ×ÁÎÎÏ Ó ÔÏÞËÉ ÚÒÅÎÉÑ ÂÅÚÏÐÁÓÎÏÓÔÉ, Ô.Ë. ÄÅÌÁÅÔ ×ÏÚÍÏÖÎÏÊ ÐÏÄÍÅÎÕ ËÌÀÞÁ. ïÔËÒÙÔÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎ ÄÏÂÁ×ÌÅÎÉÅÍ ÉÌÉ ÚÁÍÅÎÏÊ ËÌÀÞÅÊ, ÉÌÉ ÄÏÂÁ×ÌÅÎÉÅÍ ÉÌÉ ÚÁÍÅÎÏÊ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÏÌØÚÏ×ÁÔÅÌÑ. ðÏÄÍÅÎÏÊ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ, ×ÚÌÏÍÝÉË ÍÏÖÅÔ ÉÚÍÅÎÉÔØ ÁÄÒÅÓ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÙ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÞÔÏÂÙ ÐÏÌÕÞÁÔØ ÐÅÒÅÎÁÐÒÁ×ÌÅÎÎÕÀ ÅÍÕ ÐÏÞÔÕ. ðÒÉ ÉÚÍÅÎÅÎÉÉ ÏÄÎÏÇÏ ÉÚ ËÌÀÞÅÊ ÛÉÆÒÏ×ÁÎÉÑ, ×ÚÌÏÍÝÉË ÓÍÏÖÅÔ, ÔÁËÖÅ, ÒÁÓÛÉÆÒÏ×Ù×ÁÔØ ÐÅÒÅÎÁÐÒÁ×ÌÅÎÎÙÅ ÅÍÕ ÓÏÏÂÝÅÎÉÑ.

éÓÐÏÌØÚÏ×ÁÎÉÅ ÃÉÆÒÏ×ÙÈ ÐÏÄÐÉÓÅÊ ÒÅÛÁÅÔ ÜÔÕ ÐÒÏÂÌÅÍÕ. ëÏÇÄÁ ÄÁÎÎÙÅ ÐÏÄÐÉÓÁÎÙ ÓÅËÒÅÔÎÙÍ ËÌÀÞÏÍ, ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÉÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÏÇÒÁÎÉÞÅÎ ÐÏÄÐÉÓÁÎÎÙÍÉ ÄÁÎÎÙÍÉ. äÒÕÇÉÍÉ ÓÌÏ×ÁÍÉ, ÔÏÌØËÏ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÉÊ 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×ÁÎÉÅÍ

ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÅÇÏ ÇÌÁ×ÎÏÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÄÌÑ ÐÏÄÐÉÓÉ ËÏÍÐÏÎÅÎÔÏ× ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ É ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÏÌØÚÏ×ÁÔÅÌÑ, ÐÒÉ×ÑÚÙ×ÁÑ, ÔÁËÉÍ ÏÂÒÁÚÏÍ, ËÏÍÐÏÎÅÎÔÙ ÇÌÁ×ÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ. ðÏÄÐÉÓØ ËÏÍÐÏÎÅÎÔÏ× ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÓÏÏÔ×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 ÐÏÄËÌÀÞÁ. 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 ËÏÍÐÏÎÅÎÔ 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 ÏÔÎÏÓÉÔÅÌØÎÏ ÷ÁÛÅÇÏ ÉÍÅÎÉ, ÁÄÒÅÓÁ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÙ É ËÏÍÍÅÎÔÁÒÉÑ, ÔÁËÖÅ ËÁË ÐÒÉ ÓÏÚÄÁÎÉÉ ÐÁÒÙ ËÌÀÞÅÊ. ðÏÄËÌÀÞ ÄÏÂÁ×ÌÑÅÔÓÑ ËÏÍÁÎÄÏÊ **addkey**. ðÒÏÃÅÄÕÒÁ ÁÎÁÌÏÇÉÞÎÁ ÉÓÐÏÌØÚÕÅÍÏÊ ÐÒÉ ÐÅÒ×ÉÞÎÏÍ ÓÏÚÄÁÎÉÉ ÐÁÒÙ ËÌÀÞÅÊ. ðÏÄËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ DSA 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. ëÏÇÄÁ ÓÏÚÄÁÅÔÓÑ ÐÏÄËÌÀÞ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÏÎÉ ÐÏÄÐÉÓÙ×ÁÀÔÓÑ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ, ÐÒÉ ÜÔÏÍ ÷Ù ÄÏÌÖÎÙ ××ÅÓÔÉ ÐÁÒÏÌØ, ËÏÔÏÒÙÍ ÚÁÝÉÝ£Î ÇÌÁ×ÎÙÊ ËÌÀÞ.

äÏÐÏÌÎÉÔÅÌØÎÙÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌÅÚÎÙ, ËÏÇÄÁ ÷Ù ×ÙÓÔÕÐÁÅÔÅ × ÎÅÓËÏÌØËÉÈ ËÁÞÅÓÔ×ÁÈ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ ÒÁÂÏÔÎÉËÏÍ ËÁËÏÊ-ÌÉÂÏ ÆÉÒÍÙ É, × ÔÏ ÖÅ ×ÒÅÍÑ, ÐÏÌÉÔÉÞÅÓËÉÍ ÄÅÑÔÅÌÅÍ. ëÏÌÌÅÇÉ ÐÏ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÅÍÕ ×ÉÄÕ ÄÅÑÔÅÌØÎÏÓÔÉ ÂÕÄÕÔ ÚÎÁÔØ ÷ÁÓ ÐÏ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÅÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ. ôÁË ËÁË ÜÔÉ ÇÒÕÐÐÙ ÌÀÄÅÊ ÎÅ ÐÅÒÅÓÅËÁÀÔÓÑ, ÔÏ ËÁÖÄÁÑ ÇÒÕÐÐÁ ÍÏÖÅÔ ÎÅ ÄÏ×ÅÒÑÔØ ÄÒÕÇÏÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ. óÏÏÔ×ÅÔÓÔ×ÅÎÎÏ, ÏÂÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÎÕÖÎÙ.

äÏÐÏÌÎÉÔÅÌØÎÙÅ ÐÏÄËÌÀÞÉ ÔÁËÖÅ ÍÏÇÕÔ ÂÙÔØ ÐÏÌÅÚÎÙ. éÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÁÓÓÏÃÉÉÒÏ×ÁÎÎÙÅ Ó ÷ÁÛÉÍ ÇÌÁ×ÎÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÚÁ×ÅÒÛÁÔÓÑ ÄÌÑ ÄÏÌÇÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ ÉÌÉ ×ÏÏÂÝÅ ÅÇÏ ÓÌÅÄÕÅÔ ÄÅÌÁÔØ ÏÎÌÁÊÎ, ÄÏÓÔÁÔÏÞÎÏ ÎÅÏÂÈÏÄÉÍÏ ÄÌÑ ÒÅÇÕÌÑÒÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ. üÔÏ ÎÕÖÎÏ ÄÌÑ ÏÂÌÁÓÔÉ ÐÏÔÅÒÉ ÏÄÎÏÇÏ ÉÌÉ ÎÅÓËÏÌØËÉÈ ÐÏÄËÌÀÞÅÊ. ÷ ÄÁÎÎÏÍ ÓÌÕÞÁÅ ÔÏÌØËÏ ÏÎÉ ÂÕÄÕÔ ÏÔÏÚ×ÁÎÙ. åÓÌÉ ÐÏÄËÌÀÞ ×ÙÛÅÌ, ×ÓÅ ÄÁÎÎÙÅ, ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÉÍ, ÓÔÁÎÕÔ ÈÌÁÍÏÍ. ðÏ×ÔÏÒÉÍ ÐÒÏÃÅÄÕÒÕ ×ÏÓÓÔÁÎÏ×ÌÅÎÉÑ ËÌÀÞÁ, ÈÏÔÑ ÂÙ ÂÅÚÏÐÁÓÎÏÓÔØ ÎÅ ÐÏÓÔÒÁÄÁÅÔ.

ðÏÄËÌÀÞÉ É ÉÄÅÎÔÉÆÉËÁÔÏÒÙ ÐÏÌØÚÏ×ÁÔÅÌÑ ÍÏÇÕÔ ÂÙÔØ ÕÄÁÌÅÎÙ. äÌÑ ÕÄÁÌÅÎÉÑ ÐÏÄËÌÀÞÁ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÷Ù ÄÏÌÖÎÙ ÓÎÁÞÁÌÁ ×ÙÂÒÁÔØ ÅÇÏ, ÉÓÐÏÌØÚÕÑ ËÏÍÁÎÄÕ **key** ÉÌÉ **uid**. üÔÉ ËÏÍÁÎÄÙ ÐÅÒÅËÌÀÞÁÔÅÌÉ. îÁÐÒÉÍÅÒ, ËÏÍÁÎÄÁ **key *2*** ×ÙÂÅÒÅÔ ×ÔÏÒÏÊ ÐÏÄËÌÀÞ, ÐÏ×ÔÏÒÎÁÑ ËÏÍÁÎÄÁ **key *2*** ÏÔÍÅÎÉÔ ×ÙÂÏÒ. åÓÌÉ ÎÅ ÚÁÄÁÎÙ ÄÏÐÏÌÎÉÔÅÌØÎÙÅ ÁÒÇÕÍÅÎÔÙ, ×ÙÂÏÒ ×ÓÅÈ ÐÏÄËÌÀÞÅÊ ÉÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÏÌØÚÏ×ÁÔÅÌÑ ÂÕÄÅÔ ÏÔÍÅÎÅÎ. åÓÌÉ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ, ËÏÔÏÒÙÊ ÎÁÄÏ ÕÄÁÌÉÔØ, ×ÙÂÒÁÎ, ÔÏ ËÏÍÁÎÄÁ **deluid** ÕÄÁÌÉÔ ÅÇÏ ÉÚ ËÌÀÞÁ. áÎÁÌÏÇÉÞÎÏ, ËÏÍÁÎÄÁ **delkey** ÕÄÁÌÑÅÔ ×ÓÅ ×ÙÂÒÁÎÎÙÅ ÐÏÄËÌÀÞÉ ÉÚ ÎÁÛÅÇÏ, ÏÔËÒÙÔÏÇÏ É ÓÅËÒÅÔÎÏÇÏ, ËÌÀÞÅÊ.

äÌÑ ÕÐÒÁ×ÌÅÎÉÑ ÌÏËÁÌØÎÙÍÉ ÎÁÂÏÒÁÍÉ ËÌÀÞÅÊ, ÕÄÁÌÅÎÉÅ ËÏÍÐÏÎÅÎÔÏ× ËÌÀÞÁ -- ÈÏÒÏÛÉÊ ÓÐÏÓÏÂ ÏÞÉÓÔÉÔØ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÄÒÕÇÉÈ ÌÀÄÅÊ ÏÔ ÎÅÎÕÖÎÏÇÏ ÎÁÔÅÒÉÁÌÁ. õÄÁÌÅÎÉÅ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÏÌØÚÏ×ÁÔÅÌÑ É ÐÏÄËÌÀÞÅÊ ÉÚ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ ËÌÀÞÁ, ÏÄÎÁËÏ, ÎÅ ×ÓÅÇÄÁ ÒÁÚÕÍÎÏ, Ô.Ë. ÕÓÌÏÖÎÑÅÔ ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ËÌÀÞÁ. ðÏ ÕÍÏÌÞÁÎÉÀ, ËÏÇÄÁ ÐÏÌØÚÏ×ÁÔÅÌØ ÉÍÐÏÒÔÉÒÕÅÔ ÷ÁÛ ÏÂÎÏ×ÌÅÎÎÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ, ÔÏÔ ÏÂßÅÄÉÎÑÅÔÓÑ Ó ÓÔÁÒÏÊ ËÏÐÉÅÊ ÷ÁÛÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ÅÓÌÉ ÏÎÁ ÅÓÔØ × ÅÇÏ ÎÁÂÏÒÅ ËÌÀÞÅÊ. ëÏÍÐÏÎÅÎÔÙ ÏÂÏÉÈ ËÌÀÞÅÊ ÏÂßÅÄÉÎÑÀÔÓÑ, É ÜÔÏ ÜÆÆÅËÔÉ×ÎÙÊ ÓÐÏÓÏÂ ×ÏÓÓÔÁÎÏ×ÉÔØ ÕÄÁÌÅÎÎÙÅ ÷ÁÍÉ ËÏÍÐÏÎÅÎÔÙ. þÔÏÂÙ ÒÅÁ×ÉÌØÎÏ ÏÂÎÏ×ÉÔØ ËÌÀÞ, ÐÏÌØÚÏ×ÁÔÅÌØ ÄÏÌÖÅÎ ÓÎÁÞÁÌÁ ÕÄÁÌÉÔØ ÓÔÁÒÕÀ ×ÅÒÓÉÀ ÷ÁÛÅÇÏ ËÌÀÞÁ É ÔÏÌØËÉ ÚÁÔÅÍ ÉÍÐÏÒÔÉÒÏ×ÁÔØ ÎÏ×ÕÀ. üÔÏ ÄÏÂÁ×ÌÑÅÔ ÎÁÇÒÕÚËÉ ÌÀÄÑÍ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÁÅÔÅÓØ. ëÒÏÍÅ ÔÏÇÏ, ÅÓÌÉ ÷Ù ÏÔÐÒÁ×ÌÑÅÔÅ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ, ÏÂßÅÄÉÎÅÎÉÅ ÐÒÏÉÚÏÊÄÅÔ ÎÅÚÁ×ÉÓÉÍÏ, É ÎÉËÔÏ ÉÚ ÐÏÌÕÞÉ×ÛÉÈ ÷ÁÛ ËÌÀÞ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ ÎÉËÏÇÄÁ ÎÅ ÕÚÎÁÅÔ Ï ÔÏÍ, ÞÔÏ ÷Ù ÞÔÏ-ÔÏ ÔÁÍ ÕÄÁÌÉÌÉ. óÌÅÄÏ×ÁÔÅÌØÎÏ, ÄÌÑ ÏÂÎÏ×ÌÅÎÉÑ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ ËÌÀÞÁ ÌÕÞÛÅ ÏÔÏÚ×ÁÔØ ÓÏÏÔ×ÅÔÓÔ×ÕÀÝÉÅ 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×ÌÅÎÉÅÍ ÏÔÚÙ×ÁÀÝÅÊ ÓÁÍÏÐÏÄÐÉÓÉ Ë ËÌÀÞÕ. ÷ ÏÔÌÉÞÉÅ ÏÔ ÏÐÃÉÉ ËÏÍÁÎÄÎÏÊ 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>
```

éÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÏÔÍÅÎÑÅÔÓÑ ÉÎÁÞÅ. ëÁË ÐÒÁ×ÉÌÏ, ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÓÔÁ×ÑÔÓÑ ÐÏÄÐÉÓÉ, ÕÄÏÓÔÏ×ÅÒÑÀÝÉÅ ÌÉÞÎÏÓÔØ ÏÂÌÁÄÁÔÅÌÑ ËÌÀÞÁ. ôÅÏÒÅÔÉÞÅÓËÉ, ÉÄÅÎÔÉÆÉËÁÔÏÒ ×ÅÞÅÎ, Ô.Ë. ÞÅÌÏ×ÅË ×ÓÅÇÄÁ ÏÓÔÁ£ÔÓÑ ÓÏÂÏÊ. îÁ ÐÒÁËÔÉËÅ, ÏÄÎÁËÏ, ÜÌÅÍÅÎÔÙ ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÔÁËÉÅ, ËÁË ÁÄÒÅÓ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÙ É ËÏÍÍÅÎÔÁÒÉÊ ÍÏÇÕÔ ÉÚÍÅÎÑÔØÓÑ, ÄÅÌÁÑ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ ÎÅÄÅÊÓÔ×ÉÔÅÌØÎÙÍ.

óÐÅÃÉÆÉËÁÃÉÑ OpenPGP

* *ðÅÒ×ÁÑ ÓÓÙÌËÁ ÎÁ OpenPGP*

ÎÅ ÐÏÄÄÅÒÖÉ×ÁÅÔ ÏÔÚÙ× ÉÄÅÎÔÉÆÉËÁÔÏÒÁ ÐÏÌØÚÏ×ÁÔÅÌÑ, ÎÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÍÏÖÅÔ ÂÙÔØ ÜÆÆÅËÔÉ×ÎÏ ÏÔÏÚ×ÁÎ ÏÔÚÙ×ÏÍ ÓÁÍÏÐÏÄÐÉÓÉ ÎÁ ÎÅÍ. ðÏ ÐÒÉÞÉÎÁÍ ÂÅÚÏÐÁÓÎÏÓÔÉ, ÏÐÉÓÁÎÎÙÍ ÒÁÎÅÅ, ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕÔ ÄÏ×ÅÒÑÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒÕ ÐÏÌØÚÏ×ÁÔÅÌÑ ÎÅ ÉÍÅÀÝÅÍÕ ÓÁÍÏÐÏÄÐÉÓÉ.

ðÏÄÐÉÓØ ÏÔÚÙ×ÁÅÔÓÑ ËÏÍÁÎÄÏÊ **revsig**. ô.Ë. ÷Ù ÍÏÖÅÔÅ ÉÍÅÔØ ÌÀÂÏÅ ÞÉÓÌÏ ÐÏÄÐÉÓÁÎÎÙÈ ÉÄÅÎÔÉÆÉËÁÔÏÒÏ× ÐÏÌØÚÏ×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 ÐÏÌØÚÏ×ÁÔÅÌÑ ÕËÁÚÁÎ ÏÔÚÙ×ÁÀÝÅÊ ÐÏÄÐÉÓØÀ ÐÒÉ ÐÅÒÅÞÉÓÌÅÎÉÉ ÐÏÄÐÉÓÅÊ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÁÈ ÐÏÌØÚÏ×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 ÐÏÄÐÉÓÅÊ, É ÓÁÍÏÐÏÄÐÉÓÅÊ ÎÁ ÉÄÅÎÔÉÆÉËÁÔÏÒÅ ÐÏÌØÚÏ×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 ÏÂÎÏ×ÌÅÎÎÏÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ É ÏÂßÅÄÉÎÅÎÉÉ ÅÇÏ Ó ÓÔÁÒÏÊ ËÏÐÉÅÊ. ïÔÚÙ×, ÔÁËÉÍ ÏÂÒÁÚÏÍ, ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ Õ ×ÓÅÈ ÂÕÄÅÔ ÎÅÐÒÏÔÉ×ÏÒÅÞÉ×ÁÑ ËÏÐÉÑ ÷ÁÛÅÇÏ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ.

éÚÍÅÎÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ

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

÷ÒÅÍÑ ÖÉÚÎÉ ËÌÀÞÁ Ó×ÑÚÁÎÏ Ó ÓÁÍÏÐÏÄÐÉÓØÀ ÎÁ ËÌÀÞÅ. ïÂÎÏ×ÌÅÎÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ÉÚÍÅÎÑÅÔÓÑ ÕÄÁÌÅÎÉÅÍ ÓÔÁÒÏÊ ÐÏÄÐÉÓÉ É ÄÏÂÁ×ÌÅÎÉÅÍ ÎÏ×ÏÊ. ôÁË ËÁË ÷ÁÛÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÎÅ ÂÕÄÕÔ ÕÄÁÌÑÔØ ÓÔÁÒÕÀ ËÏÐÉÀ ËÌÀÞÁ, ÏÎÉ ÂÕÄÕÔ ×ÉÄÅÔØ ÄÏÐÏÌÎÉÔÅÌØÎÕÀ ÓÁÍÏÐÏÄÐÉÓØ ÎÁ ËÌÀÞÅ ÐÏÓÌÅ ÅÇÏ ÏÂÎÏ×ÌÅÎÉÑ. ðÏÚÄÎÅÊÛÁÑ ÓÁÍÏÐÏÄÐÉÓØ ÉÍÅÅÔ ÐÒÉÏÒÉÔÅÔ, ÐÏÜÔÏÍÕ ×ÓÅ ËÏÒÒÅÓÐÏÎÄÅÎÔÙ ÂÕÄÕÔ ÏÄÎÏÚÎÁÞÎÏ ÏÓ×ÅÄÏÍÌÅÎÙ Ï ×ÒÅÍÅÎÉ ÄÅÊÓÔ×ÉÑ ÷ÁÛÅÇÏ ËÌÀÞÁ.

ðÒÏ×ÅÒËÁ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ

÷ ÇÌÁ×Å 1 ÂÙÌÁ ÏÐÉÓÁÎÁ ÐÒÏÃÅÄÕÒÁ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ ÷ÁÛÅÇÏ ËÏÒÒÅÓÐÏÎÄÅÎÔÁ: ËÏÒÒÅÓÐÏÎÄÅÎÔ ÌÉÞÎÏ ÐÒÏ×ÅÒÑÅÔ ÏÔÐÅÞÁÔËÉ ÎÁ ÷ÁÛÅÊ ËÏÐÉÉ ËÌÀÞÁ, É ÚÁÔÅÍ ÷Ù ÐÏÄÐÉÓÙ×ÁÅÔÅ ÅÇÏ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó×ÏÉÍ ÓÅËÒÅÔÎÙÍ. ðÒÉ ÌÉÞÎÏÊ ÐÒÏ×ÅÒËÅ ÏÔÐÅÞÁÔËÏ× ×ÌÁÄÅÌØÃÅÍ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ Õ×ÅÒÅÎÙ, ÞÔÏ ËÌÀÞ

ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÐÒÉÎÁÄÌÅÖÉÔ ÅÍÕ, É, ÐÏÄÐÉÓÁ× ÅÇÏ, ÷Ù ÓÏÏÂÝÁÅÔÅ ÏÂÏÁÒÕÖÉÔØ ÌÀÂÏÅ ÉÚÍÅÎÅÎÉÅ ËÌÀÞÁ × ÂÕÄÕÝÅÍ. ë ÓÏÖÁÌÅÎÉÀ, ÜÔÁ ÐÒÏÃÅÄÕÒÁ ÐÒÁËÔÉÞÅÓËÉ ÎÅ×ÏÚÍÏÖÎÁ ÅÓÌÉ ÷Ù ËÏÎÔÁËÔÉÒÕÅÔÅ Ó ÂÏÌØÛÉÍ 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×ÅÒËÕ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ ×ÏÚÌÏÖÅÎÁ ÎÁ ÌÀÄÅÊ, ËÏÔÏÒÙÍ ÷Ù ÄÏ×ÅÒÑÅÔÅ. îÁÐÒÉÍÅÒ, ÐÒÅÄÐÏÌÏÖÉÍ

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

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

äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ

îÁ ÐÒÁËÔÉËÅ ÄÏ×ÅÒÉÅ ÓÕÂßÅËÔÉ×ÎÏ. îÁÐÒÉÍÅÒ, ËÌÀÞ âÌÜÊËÁ ÄÏÓÔÏ×ÅÒÅÎ, Ô.Ë. üÌÉÓ ÐÏÄÐÉÓÁÌÁ ÅÇÏ, ÎÏ ÏÎÁ ÍÏÖÅÔ ÎÅ ÂÙÔØ Õ×ÅÒÅÎÁ, ÞÔÏ âÌÜÊË ÐÒÁ×ÉÌØÎÏ ÐÒÏ×ÅÒÑÅÔ ËÌÀÞÉ, ËÏÔÏÒÙÅ ÏÎ ÐÏÄÐÉÓÙ×ÁÅÔ. ÷ ÜÔÏÍ ÓÌÕÞÁÅ, ÏÎÁ ÎÅ ÂÕÄÅÔ ÓÞÉÔÁÔØ ËÌÀÞÉ èÌÏÊ É äÈÁÒÍÙ ÄÏÓÔÏ×ÅÒÎÙÍÉ, ÏÓÎÏ×Ù×ÁÑÓØ ÎÁ ÐÏÄÐÉÓÉ âÌÜÊËÁ. íÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÒÅÛÁÅÔ ÜÔÕ ÚÁÄÁÞÕ Ó×ÑÚÙ×ÁÑ Ó ËÁÖÄÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ × ÷ÁÛÅÍ ÎÁÂÏÒÅ ÚÎÁÞÅÎÉÅ ÕËÁÚÙ×ÁÀÝÅÅ ÕÒÏ×ÅÎØ ÷ÁÛÅÇÏ ÄÏ×ÅÒÉÑ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ. éÍÅÅÔÓÑ ÐÑÔØ ÕÒÏ×ÎÅÊ ÄÏ×ÅÒÉÑ.

unknown (ÎÅÉÚ×ÅÓÔÎÏÅ)

îÉÞÅÇÏ ÎÅ ÉÚ×ÅÓÔÎÏ Ï ÐÏÌÉÔÉËÅ ÐÏÄÐÉÓÁÎÉÑ ËÌÀÞÅÊ ÄÁÎÎÙÍ ×ÌÁÄÅÌØÃÅÍ. ëÌÀÞÁÍ × ÷ÁÛÅÍ ÎÁÂÏÒÅ, ËÒÏÍÅ ÷ÁÛÅÇÏ ÓÏÂÓÔ×ÅÎÎÏÇÏ, ÐÅÒ×ÏÎÁÞÁÌØÎÏ ÐÒÉÓ×ÁÉ×ÁÅÔÓÑ ÜÔÏÔ ÕÒÏ×ÅÎØ ÄÏ×ÅÒÉÑ.

none (ÎÅÔ)

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

marginal (ÇÒÁÎÉÞÎÏÅ)

ðÏÎÉÍÁÅÔ ÓÍÙÓÌ ÐÏÄÐÉÓÁÎÉÑ ËÌÀÞÅÊ É ÐÒÏ×ÅÒÑÅÔ ÉÈ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ÐÅÒÅÄ ÔÅÍ, ËÁË ÐÏÄÐÉÓÙ×ÁÔØ.

full (ÐÏÌÎÏÅ)

÷ÌÁÄÅÌÅÃ ÏÞÅÎØ ÒÁÚÂÏÒÞÉ× × ÐÏÄÐÉÓÉ ËÌÀÞÅÊ É ÔÝÁÔÅÌØÎÏ ÐÒÏ×ÅÒÑÅÔ ÉÈ ÐÅÒÅÄ ÔÅÍ, ËÁË ÐÏÄÐÉÓÙ×ÁÔØ.

ultimate (ÂÅÚÏÇÏ×ÏÒÏÞÎÏÅ)

÷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** ÒÅÖÉÍÁ ÒÅÄÁËÔÉÒÏ×ÁÎÉÑ ËÌÀÞÁ. ÷ ÜÔÏÍ ÐÒÉÍÅÒÅ üÌÉÓ ÒÅÄÁËÔÉÒÕÅÔ ÕÒÏ×ÅÎØ Ó×ÏÅÇÏ ÄÏ×ÅÒÉÑ âÌÜÊËÕ É ÚÁÔÅÍ ÏÂÎÏ×ÌÑÅÔ ÂÁÚÕ ÄÁÎÎÙÈ ÄÏ×ÅÒÉÑ, ÞÔÏÂÙ ÐÅÒÅÓÞÉÔÁÔØ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÅÊ ÏÓÎÏ×Ù×ÁÑÓØ ÎÁ ÎÏ×ÏÍ ÕÒÏ×ÎÅ 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×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ËÌÀÞÁ É ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÁ ×Ù×ÏÄÑÔÓÑ ÓÐÒÁ×Á ÏÔ ËÌÀÞÁ, ËÏÇÄÁ ×Ù×ÏÄÉÔÓÑ ËÌÀÞ. äÏ×ÅÒÉÅ ×ÌÁÄÅÌØÃÕ ×Ù×ÏÄÉÔÓÑ ÐÅÒ×ÙÍ, ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÁ ×ÔÏÒÙÍ[1]. ðÑÔØ ÕÒÏ×ÎÅÊ ÄÏ×ÅÒÉÑ/ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÏÂÏÚÎÁÞÁÀÔÓÑ ÓÉÍ×ÏÌÁÍÉ: ÎÅÉÚ×ÅÓÔÎÙÊ (q), ÎÅÔ (n), ÇÒÁÎÉÞÎÙÊ (m), ÐÏÌÎÙÊ (f), ÂÅÚÏÇÏ×ÏÒÏÞÎÙÊ (u). ÷ ÜÔÏÍ ÓÌÕÞÁÅ, ËÌÀÞ âÌÜÊËÁ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÅÎ, Ô.Ë. üÌÉÓ ÓÁÍÁ ÐÏÄÐÉÓÁÌÁ ÅÇÏ. éÚÎÁÞÁÌØÎÏ ÕÓÔÁÎÏ×ÌÅÎÏ ÎÅÉÚ×ÅÓÔÎÏÅ ÄÏ×ÅÒÉÅ ÏÔÎÏÓÉÔÅÌØÎÏ ÐÒÁ×ÉÌØÎÏÓÔÉ ÐÏÄÐÉÓÉ âÌÜÊËÏÍ ËÌÀÞÅÊ, ÎÏ üÌÉÓ ÒÅÛÁÅÔ ÕÓÔÁÎÏ×ÉÔØ ÇÒÁÎÉÞÎÙÊ ÕÒÏ×ÅÎØ ÄÏ×ÅÒÉÑ.

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

óÅÔØ ÄÏ×ÅÒÉÑ ÐÏÚ×ÏÌÑÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ ×ÅÓØÍÁ ÇÉÂËÉÊ ÁÌÇÏÒÉÔÍ ÄÌÑ ÐÒÏ×ÅÒËÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ. òÁÎØÛÅ ÄÏÓÔÏ×ÅÒÎÙÍÉ ÓÞÉÔÁÌÉÓØ ÔÏÌØËÏ ÔÅ ËÌÀÞÉ,

ËÏÔÏÒÙÅ ÷Ù ÐÏÄÐÉÓÁÌÉ ÌÉÞÎÏ, ÔÏ ÔÅÐÅÒØ ÉÓÐÏÌØÚÕÅÔÓÑ ÓÌÅÄÕÀÝÉÊ ÁÌÇÏÒÉÔÍ. ëÌÀÞ *K* ÓÞÉÔÁÅÔÓÑ ÄÏÓÔÏ×ÅÒÎÙÍ, ÅÓÌÉ ÏÎ ÕÄÏ×ÌÅ×ÏÒÑÅÔ ÓÌÅÄÕÀÝÉÍ Ä×ÕÍ ÕÓÌÏ×ÉÑÍ:

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

   - ÷Ù ÐÏÄÐÉÓÁÌÉ ÅÇÏ ÌÉÞÎÏ (ÉÌÉ ÏÂÌÁÄÁÔÅÌØ ËÌÀÞÁ, ËÏÔÏÒÏÍÕ ÷Ù ÂÅÚÏÇÏ×ÏÒÏÞÎÏ ÄÏ×ÅÒÑÅÔÅ),
   - ÏÎ ÂÙÌ ÐÏÄÐÉÓÁÎ ËÌÀÞÏÍ ×ÌÁÄÅÌØÃÁ ËÏÔÏÒÏÇÏ ÷Ù ÐÏÌÎÏÓÔØÀ ÄÏ×ÅÒÑÅÔÅ, ÉÌÉ
   - ÏÎ ÂÙÌ ÐÏÄÐÉÓÁÎ ÔÒÅÍÑ ËÌÀÞÁÍÉ 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 ÄÏ×ÅÒÉÅÍ É ÞÉÓÌÏ ËÌÀÞÅÊ Ó ÐÏÌÎÙÍ ÄÏ×ÅÒÉÅÍ ÍÏÇÕÔ ÂÙÔØ ÉÚÍÅÎÅÎÙ ÐÒÉ ÐÏÍÏÝÉ ÐÁÒÁÍÅÔÒÏ× `--max-cert-depth`, `--marginals-needed` É `--completes-needed`. ãÉÆÒÙ ÐÒÉ×ÅÄÅÎÎÙÅ ×ÙÛÅ - ÚÎÁÞÅÎÉÑ ÉÓÐÏÌØÚÕÅÍÙÅ GnuPG ÐÏ ÕÍÏÌÞÁÎÉÀ.

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

* *ðÏÔÅÎÃÉÁÌØÎÁÑ ÏÛÉÂËÁ: ÏÐÃÉÑ `--completes-needed` × ËÏÎÆÉÇÕÒÁÃÉÏÎÎÏÍ ÆÁÊÌÅ ÂÕÄÅÔ ÐÒÏÉÇÎÏÒÉÒÏ×ÁÎÁ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ Ó ËÏÍÁÎÄÏÊ `--update-trustdb`. úÎÁÞÅÎÉÅ ×ÙÞÉÓÌÑÅÔÓÑ ËÏÒÒÅËÔÎÏ ÅÓÌÉ ÕËÁÚÁÔØ ÅÇÏ × ÆÁÊÌÅ ËÏÎÆÉÇÕÒÁÃÉÉ.*

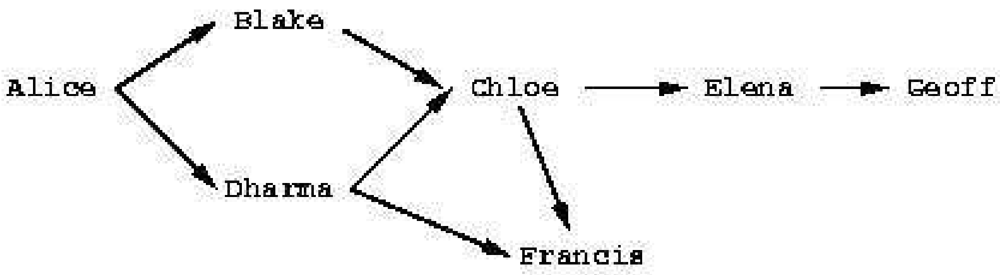
üÔÏÔ ÐÒÉÍÅÒ ÐÒÅÄÐÏÌÁÇÁÅÔ, ÞÔÏ ÄÌÑ ÐÒÉÚÎÁÎÉÑ ÄÒÕÇÏÇÏ ËÌÀÞÁ ÄÏÓÔÏ×ÅÒÎÙÍ ÔÒÅÂÕÅÔÓÑ Ä×Á ËÌÀÞÁ Ó ÇÒÁÎÉÞÎÙÍ ÄÏ×ÅÒÉÅÍ ÉÌÉ ÏÄÉÎ Ó ÐÏÌÎÙÍ. íÁËÓÉÍÁÌØÎÁÑ ÄÌÉÎÁ ÃÅÐÏÞËÉ ÒÁ×ÎÁ ÔÒÅÍ.

ðÒÉ ×ÙÞÉÓÌÅÎÉÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÅÊ, × ÜÔÏÍ ÐÒÉÍÅÒÅ, ËÌÀÞÉ âÌÜËÁ É äÖÁÒÏÎÙ ×ÓÅÇÄÁ ÓÞÉÔÁÀÔÓÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÍÉ, Ô.Ë. ÏÎÉ ÐÏÄÐÉÓÁÎÙ üÌÉÓ. äÏÓÔÏ×ÅÒÎÏÓÔØ ÄÒÕÇÉÈ ËÌÀÞÅÊ ÚÁ×ÉÓÉÔ ÏÔ ÄÏ×ÅÒÉÑ. ÷ ÐÅÒ×ÏÍ ÓÌÕÞÁÅ, ÄÏ×ÅÒÉÅ äÖÁÒÏÎÅ ÐÏÌÎÏÅ, ÞÔÏ ÄÅÌÁÅÔ ËÌÀÞÉ èÌÏÅ É æÒÜÎÓÉÓ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÍÉ. ÷Ï ×ÔÏÒÏÍ ÓÌÕÞÁÅ, ÄÏ×ÅÒÉÅ âÌÜËÕ É äÖÁÒÏÎÅ ÇÒÁÎÉÞÎÏÅ. Ô.Ë. Ä×Á ËÌÀÞÁ Ó ÇÒÁÎÉÞÎÙÍ ÄÏ×ÅÒÉÅÍ ÔÒÅÂÕÅÔÓÑ ÄÌÑ ÐÒÅÄÓÔÁ×ÌÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ, ËÌÀÞ èÌÏÅ ÂÕÄÅÔ ÐÒÉÚÎÁÎ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÍ, ÎÏ ÄÏÓÔÏ×ÅÒÎÏÓÔØ ËÌÀÞÁ æÒÜÎÓÉÓÁ ÂÕÄÅÔ ÔÏÌØËÏ ÞÁÓÔÉÞÎÏ ÐÏÄÔ×ÅÒÖÄÅÎÁ. ÷ ÓÌÕÞÁÅ ÇÒÁÎÉÞÎÏÇÏ ÄÏ×ÅÒÉÑ èÌÏÅ É äÖÁÒÏÎÅ, ËÌÀÞ èÌÏÅ ÂÕÄÅÔ ÞÁÓÔÉÞÎÏ ÄÏÓÔÏ×ÅÒÅÎ, Á ËÌÀÞ äÖÁÒÏÎÙ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÅÎ. ëÌÀÞ æÒÜÎÓÉÓÁ ÂÕÄÅÔ ÞÁÓÔÉÞÎÏ ÄÏÓÔÏ×ÅÒÅÎ, Ô.Ë. ÔÏÌØËÏ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÊ ËÌÀÞ ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ÄÒÕÇÉÈ ËÌÀÞÅÊ, Á ÅÄÉÎÓÔ×ÅÎÎÙÊ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÊ ËÌÀÞ, ËÏÔÏÒÙÍ ÐÏÄÐÉÓÁÎ ËÌÀÞ æÒÜÎËÁ, ÜÔÏ ËÌÀÞ äÖÁÒÏÎÙ. ðÏÓÌÅ ÄÏÂÁ×ÌÅÎÉÑ ÇÒÁÎÉÞÎÏÇÏ ÄÏ×ÅÒÉÑ âÌÜËÕ ËÌÀÞ èÌÏÅ ÓÔÁÎÏ×ÉÔÓÑ ÐÏÌÎÏÓÔØÀ ÄÏÓÔÏ×ÅÒÎÙÍ É ÍÏÖÅÔ ÂÙÔØ ÉÓÐÏÌØÚÏ×ÁÎ ÄÌÑ ÐÏÌÎÏÇÏ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ æÒÜÎÓÉÓÁ É ÞÁÓÔÉÞÎÏÇÏ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ åÌÅÎÙ. îÁËÏÎÅÃ, ÅÓÌÉ ÄÏ×ÅÒÉÅ âÌÜËÕ, èÌÏÅ É åÌÅÎÅ ÐÏÌÎÏÅ, ÜÔÏÇÏ ×ÓÅ ÅÝÅ ÎÅ ÄÏÓÔÁÔÏÞÎÏ ÄÌÑ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ ËÌÀÞÁ äÖÅÆÁ, Ô.Ë. ÍÁËÓÉÍÁÌØÎÁÑ ÄÌÉÎÁ ÃÅÐÏÞËÉ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ÒÁ×ÎÁ ÔÒÅÍ, ÎÏ ÐÕÔØ ÏÔ äÖÅÆÁ Ë üÌÉÓ ÒÁ×ÅÎ ÞÅÔÙÒÅÍ.

íÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÒÅÁÌÉÚÕÅÔ ÇÉÂËÉÊ ÐÏÄÈÏÄ Ë ÐÒÏÂÌÅÍÅ ÂÅÚÏÐÁÓÎÏÇÏ ÏÂÍÅÎÁ ËÌÀÞÁÍÉ. ïÎÁ ÐÏÚ×ÏÌÑÅÔ ÎÁÓÔÒÁÉ×ÁÔØ GnuPG × ÓÏÏÔ×ÅÔÓÔ×ÉÉ Ó ÷ÁÛÉÍÉ

ÐÏÔÒÅÂÎÏÓÔÑÍÉ. ÷Ù ÍÏÖÅÔÅ ÔÒÅÂÏ×ÁÔØ ÍÎÏÇÏ ËÏÒÏÔËÉÈ ÃÅÐÏÞÅË ÏÔ ÷ÁÛÅÇÏ ËÌÀÞÁ ÄÏ ËÌÀÞÁ *K* ÄÌÑ ÐÒÉÚÎÁÎÉÑ ÅÇÏ ÄÏÓÔÏ×ÅÒÎÙÍ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÷Ù ÍÏÖÅÔÅ ÂÙÔØ ÕÄÏ×ÌÅÔ×ÏÒÅÎÙ ÏÄÎÏÊ ÄÌÉÎÎÏÊ ÃÅÐÏÞËÏÊ. ôÒÅÂÏ×ÁÎÉÅ ÍÎÏÇÏÞÉÓÌÅÎÎÙÈ ËÏÒÏÔËÉÈ ÃÅÐÏÞÅË - ÓÉÌØÎÁÑ ÇÁÒÁÎÔÉÑ ÔÏÇÏ, ÞÔÏ ËÌÀÞ *K* ÐÒÉÎÁÄÌÅÖÉÔ ÔÏÍÕ, ÎÁ ËÏÇÏ ÕËÁÚÙ×ÁÅÔ ÅÇÏ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÐÏÌØÚÏ×ÁÔÅÌÑ. ãÅÎÁ ÚÁ ÔÁËÕÀ ÎÁÄÅÖÎÏÓÔØ, ËÏÎÅÞÎÏ, ×ÙÛÅ, Ô.Ë. ÷Ù ÌÉÞÎÏ ÄÏÌÖÎÙ ÐÒÏ×ÅÒÉÔØ É ÐÏÄÐÉÓÁÔØ ÂÏÌØÛÅ ËÌÀÞÅÊ, ÞÅÍ × ÓÌÕÞÁÅ ËÏÇÄÁ ÷ÁÓ ÕÓÔÒÁÉ×ÁÅÔ ÎÅÏÂÈÏÄÉÍÏÅ ÞÉÓÌÏ ÄÌÉÎÎÙÈ ÃÅÐÏÞÅË.

Рисунок 3-1. ðÒÉÍÅÒ ÓÅÔÉ ÄÏ×ÅÒÉÑ



ÄÏ×ÅÒÉÅ		ÄÏÓÔÏ×ÅÒÎÏÓÔØ	
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 ÷ÁÛ ËÌÀÞ ÐÅÒÓÏÎÁÌØÎÏ ÐÅÒÅÄÁ×ÁÑ ÅÇÏ ÷ÁÛÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ. îÁ ÐÒÁËÔÉËÅ, ÏÄÎÁËÏ, ËÌÀÞÉ ÞÁÓÔÏ ÒÁÓÐÒÏÓÔÒÁÎÑÀÔÓÑ ÐÏ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÅ ÉÌÉ ÄÒÕÇÉÍ ÓÒÅÄÓÔ×ÁÍ ÜÌÅËÔÒÏÎÎÏÊ Ó×ÑÚÉ. òÁÓÐÒÏÓÔÒÁÎÅÎÉÅ ÐÏ ÜÌÅËÔÒÏÎÎÏÊ ÐÏÞÔÅ ÈÏÒÏÛÏ ËÏÇÄÁ ÷Ù ÉÍÅÅÔÅ ÔÏÌØËÏ ÎÅÓËÏÌØËÉÈ ËÏÒÒÅÓÐÏÎÄÅÎÔÏ×, ÅÓÌÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÏ× ÍÎÏÇÏ, ÷Ù ÍÏÖÅÔÅ ÒÁÚÍÅÓÔÉÔØ Ó×ÏÊ ËÌÀÞ ÎÁ ÐÅÒÓÏÎÁÌØÎÏÊ ×Å÷-ÓÔÒÁÎÉÃÅ. üÔÏ ÎÅ ÐÒÉÅÍÌÅÍÏ, ÏÄÎÁËÏ, ÅÓÌÉ ÌÀÄÉ, ËÏÔÏÒÙÍ ÎÕÖÅÎ ÷ÁÛ ÏÔËÒÙÔÙÊ ËÌÀÞ, ÎÅ ÚÎÁÀÔ ÇÄÅ ÎÁÊÔÉ ÅÇÏ × ÓÅÔÉ.

äÌÑ ÒÅÛÅÎÉÑ ÜÔÏÊ ÐÒÏÂÌÅÍÙ ÉÓÐÏÌØÚÕÀÔÓÑ ÓÅÒ×ÅÒÙ ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ, ËÏÔÏÒÙÅ ÓÏÂÉÒÁÀÔ É ÒÁÓÐÒÏÓÔÒÁÎÑÀÔ ÏÔËÒÙÔÙÅ ËÌÀÞÉ. ïÔËÒÙÔÙÊ ËÌÀÞ ÌÉÂÏ ÄÏÂÁ×ÌÑÅÔÓÑ

Ë ÂÁÚÅ ÄÁÎÎÙÈ ÓÅÒ×ÅÒÁ, ÌÉÂÏ ÏÂßÅÄÉÎÑÅÔÓÑ Ó ÓÕÝÅÓÔ×ÕÀÝÉÍ ËÌÀÞÏÍ, ÅÓÌÉ ÔÁËÏÊ ÓÕÝÅÓÔ×ÕÅÔ. ëÏÇÄÁ ÎÁ ÓÅÒ×ÅÒ ÐÒÉÈÏÄÉÔ ÚÁÐÒÏÓ ËÌÀÞÁ, ÓÅÒ×ÅÒ ÐÒÏÓÍÁÔÒÉ×ÁÅÔ ÂÁÚÕ ÄÁÎÎÙÈ É, ÅÓÌÉ ÎÁÈÏÄÉÔ, ×ÏÚ×ÒÁÝÁÅÔ ÚÁÐÒÏÛÅÎÎÙÊ ËÌÀÞ.

óÅÒ×ÅÒÙ ËÌÀÞÅÊ ÔÁËÖÅ ÐÏÌÅÚÎÙ ËÏÇÄÁ ÍÎÏÇÉÅ ÌÀÄÉ ÞÁÓÔÏ ÐÏÄÐÉÓÙ×ÁÀÔ ËÌÀÞÉ ÄÒÕÇÉÈ ÌÀÄÅÊ. âÅÚ ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ, ËÏÇÄÁ âÏÂËË ÐÏÄÐÉÓÙ×ÁÅÔ ËÌÀÞ üÌÉÓ, ÏÎ ÄÏÌÖÅÎ ÐÏÓÌÁÔØ ÅÊ ÐÏÄÐÉÓÁÎÎÕÀ ÉÍ ËÏÐÉÀ ÅÅ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ, ËÏÔÏÒÕÀ üÌÉÓ ÍÏÖÅÔ ÄÏÂÁ×ÉÔØ Ë Ó×ÏÅÊ ÎÁÂÏÒÕ É ÐÅÒÅÄÁ×ÁÔØ, ÚÁÔÅÍ, ×ÓÅÍ Ó×ÏÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ. ÷ÙÐÏÌÎÅÎÉÅ ÜÔÉÈ ÄÅÊÓÔ×ÉÊ ÓÏÐÒÏ×ÏÖÄÁÅÔ ÐÒÉÎÃÉÐÁÍ ÐÏÄÄÅÒÖËÉ ÓÅÔÅÊ ÄÏ×ÅÒÉÑ É ÐÏ×ÙÛÅÎÉÀ ÂÅÚÏÐÁÓÎÏÓÔÉ PGP. ïÄÎÁËÏ ÏÎÉ ÓÔÁÎÏ×ÑÔÓÑ ÐÏÍÅÈÏÊ ËÏÇÄÁ ËÌÀÞÉ ÐÏÄÐÉÓÙ×ÁÀÔÓÑ ÞÁÓÔÏ.

éÓÐÏÌØÚÏ×ÁÎÉÅ ÓÅÒ×ÅÒÏ× ËÌÀÞÅÊ ÏÂÌÅÇÞÁÅÔ ÜÔÏÔ ÐÒÏÃÅÓÓ. ëÏÇÄÁ âÏÂËË ÐÏÄÐÉÓÙ×ÁÅÔ ËÌÀÞ üÌÉÓ ÏÎ ÐÏÓÙÌÁÅÔ ÐÏÄÐÉÓÁÎÎÙÊ ËÌÀÞ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ. óÅÒ×ÅÒ ËÌÀÞÅÊ ÄÏÂÁ×ÌÑÅÔ ÐÏÄÐÉÓØ âÏÂËËÁ Ë Ó×ÏÅÊ ËÏÐÉÉ ËÌÀÞÁ üÌÉÓ. ôÅ ËÔÏ ÉÎÔÅÒÅÓÕÅÔÓÑ ÏÂÎÏ×ÌÅÎÉÅÍ ËÏÐÉÉ ËÌÀÞÅÊ üÌÉÓ, ÐÏ Ó×ÏÅÊ ÉÎÉÃÉÁÔÉ×Å Ó×ÑÚÙ×ÁÀÔÓÑ Ó ÓÅÒ×ÅÒÏÍ ËÌÀÞÅÊ É ÐÏÌÕÞÁÀÔ ÏÔÔÕÄÁ ÏÂÎÏ×ÌÅÎÎÙÊ ËÌÀÞ üÌÉÓ. üÌÉÓ ÎÅ ÐÒÉÎÉÍÁÅÔ ÕÞÁÓÔÉÑ × ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÉ ËÌÀÞÁ É ÍÏÖÅÔ ÐÏÌÕÞÉÔØ ÐÏÄÐÉÓÉ ÎÁ Ó×ÏÊ ËÌÀÞÅ ÐÒÏÓÔÏ ÚÁÐÒÏÓÉ× ÓÅÒ×ÅÒ.

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

ïÄÉÎ ÉÌÉ ÂÏÌÅÅ ËÌÀÞÅÊ ÍÏÇÕÔ ÂÙÔØ ÏÔÐÒÁ×ÌÅÎÙ ÎÁ ÓÅÒ×ÅÒ ËÌÀÞÅÊ ËÏÍÁÎÄÏÊ `--send-keys`. ÷ ËÁÞÅÓÔ×Å ÁÒÇÕÍÅÎÔÁ ÕËÁÚÙ×ÁÀÔÓÑ ÏÄÉÎ ÉÌÉ ÂÏÌÅÅ ÓÐÅÃÉÆÉËÁÔÏÒÏ× ËÌÀÞÅÊ. óÅÒ×ÅÒ ËÌÀÞÅÊ, ËÏÔÏÒÏÍÕ ÂÕÄÕÔ ÐÅÒÅÄÁÎÙ ËÌÀÞÉ ÚÁÄÁÅÔÓÑ ÏÐÃÉÅÊ `--keyserver`. áÎÁÌÏÇÉÞÎÏ, ËÏÍÁÎÄÁ `--recv-keys` ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÐÏÌÕÞÅÎÉÑ ËÌÀÞÅÊ Ó ÓÅÒ×ÅÒÁ, ÎÏ ËÏÍÁÎÄÅ `--recv-keys` ÔÒÅÂÕÅÔÓÑ ÉÄÅÎÔÉÆÉËÁÔÏÒ ËÌÀÞÁ. ÷ ÓÌÅÄÕÀÝÅÍ ÐÒÉÍÅÒÅ üÌÉÓ ÏÂÎÏ×ÌÑÅÔ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ Ó ÎÏ×ÙÍÉ ÐÏÄÐÉÓÑÍÉ Ó ÓÅÒ×ÅÒÁ ËÌÀÞÅÊ *certserver.pgp.com* É ÚÁÔÅÍ ÐÏÓÙÌÁÅÔ Ó×ÏÀ ËÏÐÉÀ ÏÔËÒÙÔÏÇÏ ËÌÀÞÁ âÏÂËËÁ 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 ÄÒÕÇÏÍ, ÐÏÜÔÏÍÕ ÌÕÞÛÅ ×ÙÂÒÁÔØ ÂÌÉÖÁÊÛÉÊ Ë ÷ÁÍ É ÒÅÇÕÌÑÒÎÏ ÉÓÐÏÌØÚÏ×ÁÔØ ÅÇÏ ÄÌÑ ÏÔÐÒÁ×ËÉ É ÐÏÌÕÞÅÎÉÑ ËÌÀÞÅÊ.

Примечания

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

“ÄÏÓÔÏ×ÅÒÎÏÓÔØ” ÄÌÑ ÏÂÏÚÎÁÞÅÎÉÑ Õ×ÅÒÅÎÎÏÓÔÉ × ÔÏÍ, ÞÔÏ ËÌÀÞ ÐÒÉÎÁÄÌÅÖÉÔ ÞÅÌÏ×ÅËÕ ÕËÁÚÁÎÎÏÍÕ ÉÄÅÎÔÉÆÉËÁÔÏÒÏÍ ÐÏÌØÚÏ×ÁÔÅÌÑ.

Глава 4. åÖÅÄÎÅ×ÎÏÅ ÉÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG

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

úÄÅÓØ ÒÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ ÜÔÉ ×ÏÐÒÏÓÙ. ôÁËÖÅ ÄÁÀÔÓÑ ÐÒÁËÔÉÞÅÓËÉÅ ÓÏ×ÅÔÙ ËÁË ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ÄÌÑ ÕÄÏ×ÌÅÔ×ÏÒÅÎÉÑ Ó×ÏÉÈ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ. òÁÓÓÍÁÔÒÉ×ÁÀÔÓÑ ÐÕÔÉ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG ÄÌÑ ÚÁÝÉÝÅÎÎÏÇÏ ÏÂÍÅÎÁ ÉÎÆÏÒÍÁÃÉÅÊ ÍÅÖÄÕ ÷ÁÍÉ É ÷ÁÛÉÍÉ ËÏÌÌÅÇÁÍÉ ÅÓÌÉ ÏÎÉ ÅÝÅ ÎÅ ÉÓÐÏÌØÚÕÀÔ GnuPG. ÷ ÚÁËÌÀÞÅÎÉÅ, ×ÙÄÅÌÅÎ ÚÁËÏÎÏÄÁÔÅÌØÎÙÊ ÓÔÁÔÕÓ GnuPG, ÐÒÅÄÓÔÁ×ÌÅÎÎÙÊ ËÒÉÐÔÏÇÒÁÆÉÞÅÓËÉÍÉ ÚÁËÏÎÁÍÉ × ÍÉÒÅ.

ïÐÒÅÄÅÌÅÎÉÅ ÷ÁÛÉÈ ÔÒÅÂÏ×ÁÎÉÊ Ë ÚÁÝÉÔÅ

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

ôÏ, ËÁË ÷ÁÍ ÓÌÅÄÕÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, ÚÁ×ÉÓÉÔ ÏÔ ÖÅÌÁÎÉÑ É ×ÏÚÍÏÖÎÏÓÔÅÊ ÔÅÈ, ËÔÏ ÍÏÖÅÔ ÚÁÈÏÔÅÔØ ÐÒÏÞÅÓÔØ ÷ÁÛÉ ÓÏÏÂÝÅÎÉÑ. üÔÏ ÍÏÖÅÔ ÂÙÔØ ÂÅÓÃÅÒÅÍÏÎÎÙÊ ÓÉÓÔÅÍÎÙÊ ÁÄÍÉÎÉÓÔÒÁÔÏÒ, ÎÅÂÒÅÖÎÏ ÐÒÏÓÍÁÔÒÉ×ÁÀÝÉÊ ÷ÁÛÕ ÐÏÞÔÕ, ÐÒÏÍÙÛÌÅÎÎÙÊ ÛÐÉÏÎ, ÐÙÔÁÀÝÉÊÓÑ ÐÏÈÉÔÉÔØ ÓÅËÒÅÔÙ ÷ÁÛÅÇÏ ÐÒÅÄÐÒÉÑÔÉÑ, ÉÌÉ ÇÏÓÕÄÁÒÓÔ×ÅÎÎÙÅ ÓÌÕÖÂÙ, ÉÎÔÅÒÅÓÕÀÝÉÅÓÑ ÷ÁÍÉ. éÓÐÏÌØÚÏ×ÁÎÉÅ GnuPG ÄÌÑ ÚÁÝÉÔÙ ÏÔ ÓÌÕÞÁÊÎÏÇÏ ÐÒÏÓÍÁÔÒÉ×ÁÎÉÑ ÏÔÌÉÞÁÅÔÓÑ ÏÔ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG × ÓÌÕÞÁÅ ÅÓÌÉ ËÔÏ-ÔÏ ÃÅÌÅÎÁÐÒÁ×ÌÅÎÎÏ ÐÙÔÁÅÔÓÑ ÐÒÏÞÅÓÔØ ÷ÁÛÕ ÐÏÞÔÕ. ÷ÁÛÁ ÃÅÌØ, × ËÏÎÅÞÎÏÍ ÓÞÅÔÅ, ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏÂÙ ÓÄÅÌÁÔØ ÒÁÓÛÉÆÒÏ×ËÕ ÄÁÎÎÙÈ ÂÏÌÅÅ ÄÏÒÏÇÉÍ ÞÅÍ ÉÈ ÓÔÏÉÍÏÓÔØ.

îÁÓÔÒÏÊËÁ GnuPG ×ËÌÀÞÁÅÔ ÒÅÛÅÎÉÅ ÞÅÔÙÒÅÈ ÚÁÄÁÞ:

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

ðÒÁ×ÉÌØÎÏ ×ÙÂÒÁÎÎÙÊ ÒÁÚÍÅÒ ËÌÀÞÁ ÚÁÝÉÝÁÅÔ ÷ÁÓ ÏÔ ÍÎÏÇÉÈ ÁÔÁË ÎÁ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÓÏÏÂÝÅÎÉÑ. úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÐÒÅÄÏÔ×ÒÁÝÁÅÔ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÅÇÏ ËÅÍ-ÔÏ ÄÒÕÇÉÍ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÎÁÐÒÁ×ÌÅÎÎÙÈ ÷ÁÍ ÓÏÏÂÝÅÎÉÊ É ÐÏÄÐÉÓÉ Ó×ÏÉÈ ÓÏÏÂÝÅÎÉÊ ÷ÁÛÅÊ ÐÏÄÐÉÓØÀ. ðÒÁ×ÉÌØÎÏÅ ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ ÐÒÅÄÏÔ×ÒÁÝÁÅÔ ÍÁÓËÉÒÏ×ËÕ ÁÔÁËÕÀÝÅÇÏ ÐÏÄ ÞÅÌÏ×ÅËÁ Ó ËÏÔÏÒÙÍ ÷Ù ÐÅÒÅÐÉÓÙ×ÁÅÔÅÓØ. ÷ ËÏÎÅÞÎÏÍ ÓÞÅÔÅ, ÐÏ ÔÏÍÕ ËÁË ÷Ù ÓÏÏÔÎÏÓÉÔÅ ÒÅÛÅÎÉÅ ÜÔÉÈ ÐÒÏÂÌÅÍ Ó ÐÏÔÒÅÂÎÏÓÔÑÍÉ ÚÁÝÉÔÙ, 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 ÓÏÓÔÏÉÔ ÉÚ ÎÅÓËÏÌØËÉÈ ËÌÀÞÅÊ. ëÁË ÍÉÎÉÍÕÍ × ÎÅÅ ×ËÌÀÞÅÎ ÇÌÁ×ÎÙÊ ËÌÀÞ ÄÌÑ ÐÏÄÐÉÓÉ, ËÒÏÍÅ ÔÏÇÏ, ÏÂÙÞÎÏ ÏÎÁ ÓÏÄÅÒÖÉÔ ÏÄÉÎ ÉÌÉ ÎÅÓËÏÌØËÏ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ËÌÀÞÅÊ ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. ðÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ ÐÒÉ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÐÁÒÁÍÅÔÒÏ× ÐÏ ÕÍÏÌÞÁÎÉÀ, ÇÌÁ×ÎÙÊ ËÌÀÞ ÂÕÄÅÔ DSA ËÌÀÞÏÍ, Á ÐÏÄËÌÀÞÉ ÂÕÄÕÔ ElGamal ËÌÀÞÁÍÉ.

DSA ÄÏÐÕÓËÁÅÔ ËÌÀÞÉ ÄÌÉÎÏÊ ÄÏ 1024 ÂÉÔ. üÔÏ ÎÅ ÓÌÉÛËÏÍ ÍÎÏÇÏ, ÕÞÉÔÙ×ÁÑ ÓÅÇÏÄÎÑÛÎÅÅ ÒÁÚ×ÉÔÉÅ ÔÅÈÎÏÌÏÇÉÊ, 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 ÓËÏÒÏÓÔØ ÚÁÛÉÆÒÏ×ÁÎÉÑ É ÒÁÓÛÉÆÒÏ×ÁÎÉÑ, Ô.Ë. ÓÔÏÉÍÏÓÔØ ÜÔÉÈ ÁÌÇÏÒÉÔÍÏ× ÜËÓÐÏÎÅÎÃÉÁÌØÎÏ ÏÔÎÏÓÉÔÅÌØÎÏ ÒÁÚÍÅÒÁ ËÌÀÞÁ. âÏÌØÛÉÅ ËÌÀÞÉ ÔÁËÖÅ ÔÒÅÂÕÀÔ ÂÏÌØÛÅ ×ÒÅÍÅÎÉ ÄÌÑ ÇÅÎÅÒÁÃÉÉ É ÂÏÌØÛÅ ÍÅÓÔÁ ÄÌÑ ÈÒÁÎÅÎÉÑ. îÁËÏÎÅÃ, ÅÓÌÉ ËÌÀÞ ÓÌÉÛËÏÍ ×ÅÌÉË ÄÌÑ ÁÔÁËÉ × ÌÏÂ, ÐÒÏÔÉ×ÎÉË ÐÒÏÓÔÏ ÐÒÉÂÅÇÎÅÔ Ë ÄÒÕÇÉÍ ÍÅÔÏÄÁÍ, ÞÔÏÂÙ ÐÏÌÕÞÉÔØ ÉÎÔÅÒÅÓÕÀÝÉÅ ÅÇÏ ÄÁÎÎÙÅ. ðÒÉÍÅÒÁÍÉ ÄÒÕÇÉÈ ÍÅÔÏÄÏ× Ñ×ÌÑÅÔÓÑ ÏÇÒÁÂÌÅÎÉÅ ÷ÁÛÅÇÏ ÄÏÍÁ ÉÌÉ ÏÆÉÓÁ, ÍÉÎÕÑ ÎÁÐÁÄÅÎÉÅ ÌÉÞÎÏ ÎÁ ÷ÁÓ. 1024 ÂÉÔ - ÒÅËÏÍÅÎÄÕÅÍÙÊ ÒÁÚÍÅÒ ËÌÀÞÁ. åÓÌÉ ÷Ù ÄÅÊÓÔ×ÉÔÅÌØÎÏ ÎÕÖÄÁÅÔÅÓØ × ËÌÀÞÅ ÂÏÌØÛÅÇÏ ÒÁÚÍÅÒÁ, ÔÏ ÓËÏÒÅÅ ×ÓÅÇÏ ÕÖÅ ÚÎÁÅÔÅ ÏÂ ÜÔÏÍ É ÄÏÌÖÎÙ ÐÒÏËÏÎÓÕÌØÔÉÒÏ×ÁÔØÓÑ Ó ÜËÓÐÅÒÔÏÍ ÐÏ ÚÁÝÉÔÅ ÄÁÎÎÙÈ.

úÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ

úÁÝÉÔÁ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÏÄÎÁ ÉÚ ÎÁÉÂÏÌÅÅ ×ÁÖÎÙÈ ÚÁÄÁÞ ÄÌÑ ÎÁÄ£ÖÎÏÊ ÒÁÂÏÔÙ GnuPG. åÓÌÉ ËÔÏ-ÌÉÂÏ ÐÏÌÕÞÉÔ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÔÏ ÏÎ ÓÍÏÖÅÔ ÒÁÓÛÉÆÒÏ×Ù×ÁÔØ ×ÓÅ ÎÁÐÒÁ×ÌÅÎÎÙÅ ÷ÁÍ ÓÏÏÂÝÅÎÉÑ É ÓÍÏÖÅÔ ÐÏÄÐÉÓÙ×ÁÔØÓÑ ÷ÁÛÅÊ ÐÏÄÐÉÓØÀ. åÓÌÉ ÷Ù ÐÏÔÅÒÑÅÔÅ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÔÏ ÎÅ ÓÍÏÖÅÔÅ ÂÏÌØÛÅ ÒÁÓÛÉÆÒÏ×Ù×ÁÔØ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÌÑ ÷ÁÓ É ÎÅ ÓÍÏÖÅÔÅ ÐÏÄÐÉÓÙ×ÁÔØ Ó×ÏÉ ÓÏÏÂÝÅÎÉÑ. ðÏÔÅÒÑ ÅÄÉÎÓÔ×ÅÎÎÏÊ ËÏÐÉÉ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ËÁÔÁÓÔÒÏÆÉÞÎÁ.

îÅÚÁ×ÉÓÉÍÏ ÏÔ ÔÏÇÏ, ËÁË ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG ÷Ù ÄÏÌÖÎÙ ÓÏÈÒÁÎÉÔØ ÓÅÒÔÉÆÉËÁÔ ÏÔÚÙ×Á ÏÔËÒÙÔÙÈ ËÌÀÞÅÊ É ÒÅÚÅÒ×ÎÕÀ ËÏÐÉÀ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÎÁ ÚÁÝÉÝÅÎÎÙÊ ÏÔ ÚÁÐÉÓÉ ÎÏÓÉÔÅÌØ É ÈÒÁÎÉÔØ ÅÇÏ × ÎÁÄÅÖÎÏÍ ÍÅÓÔÅ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÚÁÐÉÓÁÔØ ËÏÐÉÀ ÎÁ ËÏÍÐÁËÔ-ÄÉÓË É ÈÒÁÎÉÔØ ÅÇÏ × ÂÁÎËÏ×ÓËÏÍ ÓÅÊÆÅ. íÏÖÎÏ, ÔÁËÖÅ, ÚÁÐÉÓÁÔØ ÉÈ ÎÁ ÄÉÓËÅÔÕ É ÓÐÒÑÔÁÔØ ÅÅ ÄÏÍÁ. þÔÏÂÙ ÷Ù ÎÉ ÄÅÌÁÌÉ, ËÏÐÉÉ ÄÏÌÖÎÙ ÂÙÔØ ÓËÏÐÉÒÏ×ÁÎÙ ÎÁ ÎÏÓÉÔÅÌØ, ÎÁ ËÏÔÏÒÏÍ ÏÎÉ ÓÍÏÇÕÔ ÎÁÄÅÖÎÏ ÈÒÁÎÉÔØÓÑ ÎÁ ÐÒÏÔÑÖÅÎÉÉ ×ÓÅÇÏ ÓÒÏËÁ ÉÓÐÏÌØÚÏ×ÁÎÉÑ ËÌÀÞÁ, É ÉÈ ÓÌÅÄÕÅÔ ÓÐÒÑÔÁÔØ ÂÏÌÅÅ ÔÝÁÔÅÌØÎÏ, ÞÅÍ ËÏÐÉÀ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ ÄÌÑ ÅÖÅÄÎÅ×ÎÏÇÏ ÉÓÐÏÌØÚÏ×ÁÎÉÑ.

þÔÏÂÙ ÚÁÝÉÔÉÔØ ÷ÁÛ ËÌÀÞ, GnuPG ÎÅ ÓÏÈÒÁÎÑÅÔ ÅÇÏ ÎÁ ÄÉÓË × ÞÉÓÔÏÍ ×ÉÄÅ. ÷ÍÅÓÔÏ ÜÔÏÇÏ ÏÎ ÛÉÆÒÕÅÔÓÑ ÓÉÍÍÅÔÒÉÞÎÙÍ ÁÌÇÏÒÉÔÍÏÍ. ÷ÏÔ ÚÁÞÅÍ ÎÕÖÎÁ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÄÌÑ ÄÏÓÔÕÐÁ Ë ËÌÀÞÕ. ðÏÜÔÏÍÕ ×ÚÌÏÍÝÉË ÄÏÌÖÅÎ ÒÅÛÉÔØ Ä×Å ÐÒÏÂÌÅÍÙ, ÞÔÏÂÙ ÐÏÌÕÞÉÔØ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ: (1) ÏÎ ÄÏÌÖÅÎ ÐÏÌÕÞÉÔØ ËÌÀÞ, (2) ÏÎ ÄÏÌÖÅÎ ÒÁÓÛÉÆÒÏ×ÁÔØ ËÌÀÞ.

îÁÄÅÖÎÏÅ ÈÒÁÎÅÎÉÅ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ - ÓÌÏÖÎÁÑ ÚÁÄÁÞÁ. ÷ ÉÄÅÁÌÅ, ÷Ù ÄÏÌÖÎÙ ÈÒÁÎÉÔØ ÓÅËÒÅÔÎÙÊ ËÌÀÞ ÎÁ ÓÍÅÎÎÏÍ, ÚÁÝÉÝÅÎÎÏÍ ÏÔ ÚÁÐÉÓÉ ÄÉÓËÅ É ÉÓÐÏÌØÚÏ×ÁÔØ ÅÇÏ ÔÏÌØËÏ ÎÁ ÎÁ ÏÄÎÏÐÏÌØÚÏ×ÁÔÅÌØÓËÏÊ ÍÁÛÉÎÅ ÎÅ ÐÏÄËÌÀÞÅÎÎÏÊ Ë ÓÅÔÉ. üÔÏ ÍÏÖÅÔ ÏËÁÚÁÔØÓÑ ÎÅÕÄÏÂÎÙÍ ÉÌÉ ÎÅ×ÏÚÍÏÖÎÙÍ ÄÌÑ ÷ÁÓ. îÁÐÒÉÍÅÒ, Õ ÷ÁÓ ÍÏÖÅÔ ÎÅ ÂÙÔØ Ó×ÏÅÇÏ ËÏÍÐØÀÔÅÒÁ É ÷Ù ÉÓÐÏÌØÚÕÅÔÅ ËÏÍÐØÀÔÅÒ ÎÁ ÒÁÂÏÔÅ, ÉÌÉ ÜÔÏ ÍÏÖÅÔ ÏÚÎÁÞÁÔØ, ÞÔÏ ÷ÁÍ ÐÒÉÄÅÔÓÑ ÏÔËÌÀÞÁÔØ ËÏÍÐØÀÔÅÒ ÏÔ ÓÅÔÉ ËÁÖÄÙÊ ÒÁÚ ËÏÇÄÁ ÷Ù ÚÁÐÕÓËÁÅÔÅ GnuPG

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

èÏÒÏÛÁÑ ËÌÀÞÅ×ÁÑ ÆÒÁÚÁ ÏÞÅÎØ ËÒÉÔÉÞÎÁ ÐÒÉ ÉÓÐÏÌØÚÏ×ÁÎÉÉ GnuPG. ìÀÂÏÊ ×ÚÌÏÍÝÉË, ÐÏÌÕÞÉ×ÛÉÊ ÷ÁÛ ÓÅËÒÅÔÎÙÊ ËÌÀÞ, ÄÏÌÖÅÎ ×ÚÌÏÍÁÔØ ÛÉÆÒ ÎÁ ÓÅËÒÅÔÎÏÍ ËÌÀÞÅ. ÷ÍÅÓÔÏ ÁÔÁËÉ × ÌÏÂ, ×ÚÌÏÍÝÉË, ÎÁ×ÅÒÎÑËÁ, ÐÏÐÒÏÂÕÅÔ ÕÇÁÄÁÔØ ËÌÀÞÅ×ÕÀ ÆÒÁÚÕ.

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

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

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

ðÏ ÕÍÏÌÞÁÎÉÀ, ËÏÇÄÁ ÷Ù ÓÏÚÄÁÅÔÅ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ, ÇÅÎÅÒÉÒÕÅÔÓÑ ÇÌÁ×ÎÙÊ ËÌÀÞ DSA ÄÌÑ ÐÏÄÐÉÓÉ É ÐÏÄÞÉÎÅÎÎÙÊ ËÌÀÞ ElGamal ÄÌÑ ÛÉÆÒÏ×ÁÎÉÑ. üÔÏ ÕÄÏÂÎÏ, Ô.Ë. ÒÏÌÉ Ä×ÕÈ ËÌÀÞÅÊ ÒÁÚÌÉÞÎÙ, É ÷Ù ÍÏÖÅÔÅ ÐÏÖÅÌÁÔØ, ÞÔÏÂÙ ÏÎÉ ÉÍÅÌÉ ÒÁÚÌÉÞÎÙÅ ÓÒÏËÉ ÄÅÊÓÔ×ÉÑ. çÌÁ×ÎÙÊ ËÌÀÞ ÄÌÑ ÐÏÄÐÉÓÉ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÓÏÚÄÁÎÉÑ ÃÉÆÒÏ×ÙÈ

ÐÏÄÐÉÓÁÎ, ÎÁ ÎÅÍ, ÔÁËÖÅ, ÓÏÂÉÒÁÀÔÓÑ ÐÏÄÐÉÓÉ ÔÅÈ, ËÔÏ ÐÒÏÔ×ÅÒÖÄÁÅÔ ÐÒÉÎÁÄÌÅÖÎÏÓÔØ ËÌÀÞÁ ÷ÁÍ. ëÌÀÞ ÛÉÆÒÏ×ÁÎÉÑ ÉÓÐÏÌØÚÕÅÔÓÑ ÄÌÑ ÒÁÓÛÉÆÒÏ×ËÉ ÚÁÛÉÆÒÏ×ÁÎÎÙÈ ÄÏËÕÍÅÎÔÏ×, ÏÔÐÒÁ×ÌÅÎÎÙÈ ÷ÁÍ. ïÂÙÞÎÏ, ÃÉÆÒÏ×ÁÑ ÐÏÄÐÉÓØ ÉÍÅÅÔ ÐÒÏÄÏÌÖÉÔÅÌØÎÙÊ ÓÒÏË ÄÅÊÓÔ×ÉÑ, ÎÁÐÒÉÍÅÒ, ÎÅÏÇÒÁÎÉÞÅÎÎÙÊ, É ÷Ù, ÔÁËÖÅ, ÎÅ ÈÏÔÉÔÅ ÕÔÒÁÔÉÔØ ÐÏÄÐÉÓÉ ÎÁ ÷ÁÛÅÍ ËÌÀÞÅ, ÓÏÂÒÁÎÎÙÅ Ó ÂÏÌØÛÉÍ ÔÒÕÄÏÍ. ó ÄÒÕÇÏÊ ÓÔÏÒÏÎÙ, ÐÏÄËÌÀÞ ÛÉÆÒÏ×ÁÎÉÑ ÍÏÖÅÔ ÐÅÒÉÏÄÉÞÅÓËÉ ÉÚÍÅÎÑÔØÓÑ, ÞÔÏ ÐÏ×ÙÓÉÔ ÂÅÚÏÐÁÓÎÏÓÔØ, Ô.Ë. ×ÚÌÏÍÁÎÎÙÊ ËÌÀÞ ÛÉÆÒÏ×ÁÎÉÑ ÐÏÚ×ÏÌÉÔ ×ÚÌÏÍÝÉËÕ ÐÒÏÞÅÓÔØ ×ÓÅ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÄÌÑ ÜÔÏÇÏ ËÌÀÞÁ, ËÁË × ÂÕÄÕÝÅÍ, ÔÁË É × ÐÒÏÛÌÏÍ.

ðÏÜÔÏÍÕ ÷Ù ÐÏÞÔÉ ×ÓÅÇÄÁ ÚÁÈÏÔÉÔÅ ÏÓÔÁ×ÉÔØ ÇÌÁ×ÎÙÊ ËÌÀÞ Ó ÎÅÏÇÒÁÎÉÞÅÎÎÙÍ ÓÒÏËÏÍ ÄÅÊÓÔ×ÉÑ. åÓÔØ Ä×Å ÐÒÉÞÉÎÙ ÐÏ ËÏÔÏÒÙÍ ÷Ù ÍÏÖÅÔÅ ÏÇÒÁÎÉÞÉÔØ ÓÒÏË ÄÅÊÓÔ×ÉÑ ËÌÀÞÁ. ÷Ï-ÐÅÒ×ÙÈ, ÷ÁÍ ÍÏÖÅÔ ÐÏÎÁÄÏÂÉÔØÓÑ ËÌÀÞ ÎÁ ÏÐÒÅÄÅÌÅÎÎÙÊ ÐÅÒÉÏÄ. îÁÐÒÉÍÅÒ, ËÌÀÞ ÂÕÄÅÔ ÉÓÐÏÌØÚÏ×ÁÔØÓÑ ×Ï ×ÒÅÍÑ ÉÚÂÉÒÁÔÅÌØÎÏÊ ËÁÍÐÁÎÉÉ É ÎÅ ÐÏÎÁÄÏÂÉÔÓÑ ÐÏÓÌÅ ÅÅ ÏËÏÎÞÁÎÉÑ. äÒÕÇÁÑ ÐÒÉÞÉÎÁ ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏ ÅÓÌÉ ÷Ù ÔÅÒÑÅÔÅ ËÏÎÔÒÏÌØ ÎÁÄ ËÌÀÞÏÍ É, ÐÒÉ ÜÔÏÍ, ÎÅ ÉÍÅÅÔÅ ÓÅÒÔÉÆÉËÁÔÁ ÏÔÚÙ×Á, ÎÁÌÉÞÉÅ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ ÇÁÒÁÎÔÉÒÕÅÔ, ÞÔÏ × ËÏÎÅÞÎÏÍ ÓÞÅÔÅ ËÌÀÞ ÓÔÁÎÅÔ ÎÅÄÅÊÓÔ×ÉÔÅÌÅÎ.

óÍÅÎÁ ÐÏÄËÌÀÞÅÊ ÛÉÆÒÏ×ÁÎÉÑ ÐÒÏÓÔÁ, ÎÏ ÍÏÖÅÔ ×ÙÚ×ÁÔØ ÎÅÕÄÏÂÓÔ×Á. åÓÌÉ ÷Ù ÓÏÚÄÁÅÔÅ ÎÏ×ÕÀ ÐÁÒÕ ËÌÀÞÅÊ ÓÏ ÓÒÏËÏÍ ÄÅÊÓÔ×ÉÑ ÐÏÄËÌÀÞÅÊ, ÜÔÏÔ ÓÒÏË ÒÁÎÏ ÉÌÉ ÐÏÚÄÎÏ ÉÓÔÅÞÅÔ. îÅÚÁÄÏÌÇÏ ÄÏ ÉÓÔÅÞÅÎÉÑ ÓÒÏËÁ, ÷ÁÍ ÓÌÅÄÕÅÔ ÄÏÂÁ×ÉÔØ ÎÏ×ÙÊ ÐÏÄËÌÀÞ É ÏÐÕÂÌÉËÏ×ÁÔØ ÏÂÎÏ×ÌÅÎÎÙÊ ÏÔËÒÙÔÙÊ ËÌÀÞ. ðÏÓÌÅ ÉÓÔÅÞÅÎÉÑ ÓÒÏËÁ ÄÅÊÓÔ×ÉÑ, ÔÅ, ËÔÏ ÈÏÔÑÔ ÏÔÐÒÁ×ÉÔØ ÷ÁÍ ËÏÒÒÅÓÐÏÎÄÅÎÃÉÀ, ÄÏÌÖÎÙ ÎÁÊÔÉ ÷ÁÛ ÏÂÎÏ×ÌÅÎÎÙÊ ËÌÀÞ, Ô.Ë. ÎÅ ÓÍÏÇÕÔ ÂÏÌØÛÅ ÛÉÆÒÏ×ÁÔØ ËÌÀÞÏÍ Ó ÐÒÏÓÒÏÞÅÎÎÙÍ ÓÒÏËÏÍ ÄÅÊÓÔ×ÉÑ. üÔÏ ÍÏÖÅÔ ÎÅÕÄÏÂÎÙÍ, × ÚÁ×ÉÓÉÍÏÓÔÉ ÏÔ ÔÏÇÏ, ËÁË ÷Ù ÒÁÓÐÒÏÓÔÒÁÎÑÅÔÅ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ. ïÂÎÁËÏ ÎÅ ÔÒÅÂÕÅÔÓÑ ÎÉËÁËÉÈ ÄÏÐÏÌÎÉÔÅÌØÎÙÈ ÐÏÄÐÉÓÅÊ, Ô.Ë. ÐÏÄËÌÀÞ ÐÏÄÐÉÓÁÎ ÷ÁÛÉÍ ÇÌÁ×ÎÙÍ ÐÏÄÐÉÓÙ×ÁÀÝÉÍ ËÌÀÞÏÍ, ËÏÔÏÒÙÊ, ×ÅÒÏÑÔÎÏ, ÕÖÅ ÂÙÌ ÐÒÏÔ×ÅÒÖÄÅÎ ÷ÁÛÉÍÉ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍÉ.

üÔÉ ÎÅÕÄÏÂÓÔ×Á ÍÏÇÕÔ ÐÒÅ×ÙÛÁÔØ, Á ÍÏÇÕÔ É ÎÅ ÐÒÅ×ÙÛÁÔØ ÐÏÌÕÞÁÅÍÕÀ ÄÏÐÏÌÎÉÔÅÌØÎÕÀ ÚÁÝÉÔÕ. ôÁË ÖÅ ËÁË É ÷Ù, ×ÚÌÏÍÝÉË ÍÏÖÅÔ ÐÒÉÏÂÒÅÓÔÉ ×ÓÅ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÉÓÐÏÌØÚÕÑ ËÌÀÞ. óÍÅÎÁ ÐÏÄËÌÀÞÁ ÚÁÝÉÝÁÅÔ ÔÏÌØËÏ ÎÏ×ÙÅ ÄÏËÕÍÅÎÔÙ. äÌÑ ÞÔÅÎÉÑ ÄÏËÕÍÅÎÔÏ×, ÚÁÛÉÆÒÏ×ÁÎÎÙÈ ÎÏ×ÙÍ ÐÏÄËÌÀÞÏÍ, ×ÚÌÏÍÝÉËÕ ÐÒÉÊÄÅÔÓÑ ×ÚÌÁÍÙ×ÁÔØ ÎÏ×ÙÊ ËÌÀÞ, ÉÓÐÏÌØÚÕÑ ÔÅ ÖÅ ÍÅÔÏÄÙ, ÞÔÏ É × ÐÅÒ×ÙÊ ÒÁÚ.

îÁËÏÎÅÃ, ×ÓÅ ÜÔÏ ÉÍÅÅÔ ÓÍÙÓÌ, ÅÓÌÉ × Ó×ÑÚËÅ ÉÍÅÅÔÓÑ ÔÏÌØËÏ ÏÄÉÎ ÄÅÊÓÔ×ÕÀÝÉÊ ÐÏÄËÌÀÞ. ÷Ù ÎÅ ÐÏÌÕÞÉÔÅ ÎÉËÁËÏÊ ÄÏÐÏÌÎÉÔÅÌØÎÏÊ ÚÁÝÉÔÙ ÐÒÉ ÎÁÌÉÞÉÉ Ä×ÕÈ É ÂÏÌÅÅ ÁËÔÉ×ÎÙÈ ËÌÀÞÅÊ. ÷Ù, ËÏÎÅÞÎÏ, ÍÏÖÅÔÅ ÉÍÅÔØ ÌÀÂÏÅ ÞÉÓÌÏ ÉÓÔÅËÛÉÈ ËÌÀÞÅÊ × Ó×ÑÚËÅ, ÞÔÏÂÙ ÞÉÓÁÔØ ÄÏËÕÍÅÎÔÙ ÚÁÛÉÆÒÏ×ÁÎÎÙÅ ÒÁÎÅÅ, ÎÏ ÔÏÌØËÏ ÏÄÉÎ ÐÏÄËÌÀÞ ÄÏÌÖÅÎ ÂÙÔØ ÁËÔÉ×ÎÙÍ × ÄÁÎÎÙÊ ×ÒÅÍÑ.

õÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ.

ëÁË É ÚÁÝÉÔÁ ÷ÁÛÅÇÏ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÕÐÒÁ×ÌÅÎÉÅ ÓÅÔØÀ ÄÏ×ÅÒÉÑ Ñ×ÌÑÅÔÓÑ ÅÝÅ ÏÄÎÏÊ ÁÓÐÅËÔÏÍ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG, ËÏÔÏÒÙÊ ÔÒÅÂÕÅÔ ÓÏÂÌÀÄÅÎÉÑ ÂÁÌÁÎÓÁ ÍÅÖÄÕ ÚÁÝÉÔÏÊ É ÌÅÇËÏÓÔØÀ ÉÓÐÏÌØÚÏ×ÁÎÉÑ. åÓÌÉ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG ÄÌÑ ÚÁÝÉÔÙ ÏÔ ÓÌÕÞÁÊÎÏÇÏ ÐÒÏÓÌÕÛÉ×ÁÎÉÑ É ÐÏÄÄÅÌËÉ, ÔÏ ÍÏÖÅÔÅ ÐÏÚ×ÏÌÉÔØ ÓÅÂÅ ÍÎÏÇÏÓÔÅÐÅÎÎÏÅ ÌÅÇËÏÓÔØ × ÄÏ×ÅÒÉÉ ÞÕÖÉÍ ÐÏÄÐÉÓÑÍ 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×ÅÒÉÑ × ÏÔÎÏÛÅÎÉÉ ÞÕÖÉÈ ÐÏÄÐÉÓÅÊ É ÔÒÁÔÉÔØ ÂÏÌØÛÅ ×ÒÅÍÅÎÉ ÎÁ ÐÒÏ×ÅÒËÕ ËÌÀÞÅÊ.

îÅÚÁ×ÉÓÉÍÏ ÏÔ ÷ÁÛÉÈ ÌÉÞÎÙÈ ÐÏÔÒÅÂÎÏÓÔÅÊ × ÚÁÝÉÔÅ, ÷Ù *×ÓÅÇÄÁ ÄÏÌÖÎÙ ÂÙÔØ ×ÎÉÍÁÔÅÌØÎÙ* ÐÏÄÐÉÓÙ×ÁÑ ÞÕÖÉÅ ËÌÀÞÉ. ðÏÄÐÉÓÙ×ÁÔØ ËÌÀÞ ÏÐÉÒÁÑÓØ ÎÁ ÓÏÂÓÔ×ÅÎÎÙÅ ÐÏÔÒÅÂÎÏÓÔÉ × ÚÁÝÉÔÅ ÜÇÏÉÓÔÉÞÎÏ. îÁ ÷ÁÛÕ ÐÏÄÐÉÓØ ÍÏÇÕÔ ÐÏÌÁÇÁÔØÓÑ ÄÒÕÇÉÅ, ÞØÉ ÔÒÅÂÏ×ÁÎÉÑ, ×ÏÚÍÏÖÎÏ, ÂÏÌÅÅ ×ÙÓÏËÉ. åÓÌÉ ÏÎÉ ÎÅ ÓÍÏÇÕÔ ÐÏÌÁÇÁÔØÓÑ ÎÁ ÷ÁÓ, ÜÔÏ ÏÓÌÁÂÉÔ ÓÅÔØ ÄÏ×ÅÒÉÑ É ÚÁÔÒÕÄÎÉÔ ÏÂÝÅÎÉÅ ×ÓÅÇÏ ÓÏÏÂÝÅÓÔ×Á ÐÏÌØÚÏ×ÁÔÅÌÅÊ GnuPG. éÓÐÏÌØÚÕÊÔÅ ÔÅ ÖÅ ÍÅÒÙ ÐÒÅÄÏÓÔÏÒÏÖÎÏÓÔÉ, ÐÏÄÐÉÓÙ×ÁÑ ËÌÀÞÉ, ËÁËÉÅ ÷Ù ÈÏÔÅÌÉ ÂÙ, ÞÔÏÂÙ ÐÒÉÎÉÍÁÌÉ ÔÅ, ÎÁ ÞØÉ ÐÏÄÐÉÓÉ ÐÏÌÁÇÁÅÔÅÓØ ÷Ù.

îÁ ÐÒÁËÔÉËÅ, ÕÐÒÁ×ÌÅÎÉÅ ÷ÁÛÅÊ ÓÅÔØÀ ÄÏ×ÅÒÉÑ Ó×ÏÄÉÔÓÑ Ë ÐÒÉÓ×ÏÅÎÉÀ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ ÎÅËÏÔÏÒÏÍÕ ÍÉÎÉÍÁÌØÎÏÍÕ ÞÉÓÌÕ ÄÒÕÇÉÈ ÌÉÃ É ÎÁÓÔÒÏÊËÅ ÐÁÒÁÍÅÔÒÏ× `--marginals-needed` É `--completes-needed`. ìÀÂÏÊ ËÌÀÞ, ÐÏÄÐÉÓÁÎÎÙÊ ÷ÁÍÉ ÌÉÞÎÏ, ÓÞÉÔÁÅÔÓÑ ÐÏÄÔ×ÅÒÖÄÅÎÎÙÍ, ÎÏ, ËÒÏÍÅ ËÁË ÄÌÑ ÎÁÉÍÅÎØÛÉÈ ÇÒÕÐÐ, ÎÅ Ñ×ÌÑÅÔÓÑ ÐÒÁËÔÉÞÎÙÍ ÐÏÄÐÉÓÙ×ÁÔØ ËÌÀÞ ËÁÖÄÏÇÏ, Ó ËÅÍ ÷Ù ÐÅÒÅÐÉÓÙ×ÁÅÔÅÓØ. ÷Ù ÂÕÄÅÔÅ, ÓÌÅÄÏ×ÁÔÅÌØÎÏ, ÄÏÌÖÎÙ ÐÏÌÁÇÁÔØÓÑ ÎÁ ÄÒÕÇÉÈ.

îÁËÏÎÅÃ, ÒÁÚÕÍÎÏ, ÐÒÏÑ×ÉÔØ ÁËËÕÒÁÔÎÏÓÔØ ÐÒÉÓ×ÁÉ×ÁÑ ÚÎÁÞÅÎÉÑ ÄÏ×ÅÒÉÑ É ÚÁÔÅÍ ÎÁÓÔÒÏÉÔØ ÏÐÃÉÉ, ÕËÁÚÙ×ÁÀÝÉÅ GnuPG ÓÔÒÏÇÏÓÔØ ÐÒÏ×ÅÒËÉ ËÌÀÞÅÊ. îÁÐÒÉÍÅÒ, ÷Ù ÍÏÖÅÔÅ ÐÏÌÎÏÓÔØÀ ÄÏ×ÅÒÑÔØ ÕÚËÏÍÕ ËÒÕÇÕ ÄÒÕÚÅÊ, ËÏÔÏÒÙÅ, ËÁË ÷Ù ÚÎÁÅÔÅ, ÏÓÔÏÒÏÖÎÙ ÐÒÉ ÐÏÄÐÉÓÉ ËÌÀÞÅÊ, É ÎÅÚÎÁÞÉÔÅÌØÎÏ ÄÏ×ÅÒÑÔØ ×ÓÅÍ ÏÓÔÁÌØÎÙÍ, ÞØÉ ËÌÀÞÉ ÉÍÅÀÔÓÑ × ÷ÁÛÅÊ Ó×ÑÚËÅ. ôÏÇÄÁ, ÷Ù ÍÏÖÅÔÅ ÕÓÔÁÎÏ×ÉÔØ ÚÎÁÞÅÎÉÑ `--completes-needed` ÒÁ×ÎÙÍ 1 É `--marginals-needed` ÒÁ×ÎÙÍ 2. åÓÌÉ ÷Ù ÂÏÌÅÅ ÏÓÔÏÒÏÖÎÙ, ÔÏ ÍÏÖÅÔÅ ×ÙÂÒÁÔØ ÚÎÁÞÅÎÉÑ 1 É 3 ÉÌÉ 2 É 3 ÓÏÏÔ×ÅÔÓÔ×ÅÎÎÏ. åÓÌÉ ÷Ù ÎÅ ÏÞÅÎØ ÏÚÁÂÏÞÅÎÙ ÓÅËÒÅÔÎÏÓÔØÀ É ÐÒÏÓÔÏ ÚÁÉÎÔÅÒÅÓÏ×ÁÎÙ × ÎÅËÏÔÏÒÏÍ ÐÒÉÅÍÌÅÍÏÍ ÐÏÄÔ×ÅÒÖÄÅÎÉÉ ÄÏÓÔÏ×ÅÒÎÏÓÔÉ, ÕÓÔÁÎÏ×ÉÔÅ ÚÎÁÞÅÎÉÑ 1 É 1. ÷ ÃÅÌÏÍ, ÂÏÌÅÅ ×ÙÓÏËÉÅ ÚÎÁÞÅÎÉÑ ÜÔÉÈ ÐÁÒÁÍÅÔÒÏ× ÏÚÎÁÞÁÀÔ, ÞÔÏ ÂÏÌØÛÅÅ ÞÉÓÌÏ ÌÀÄÅÊ ÄÏÌÖÎÙ ÓÇÏ×ÏÒÉÔØÓÑ ÐÒÏÔÉ× ÷ÁÓ, ÞÔÏÂÙ ÐÏÌÕÞÉÔØ ÐÏÄÔ×ÅÒÖÄÅÎÎÙÊ ËÌÀÞ, ÎÅ ÐÒÉÎÁÄÌÅÖÁÝÉÊ ÔÏÍÕ, ËÏÍÕ ÷Ù ÄÕÍÁÅÔÅ.

ðÏÓÔÒÏÅÎÉÅ ÷ÁÛÅÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ

ïÄÎÏÇÏ ÖÅÌÁÎÉÑ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ÎÅÄÏÓÔÁÔÏÞÎÏ. äÌÑ ÔÏÇÏ, ÞÔÏÂÙ ÓÏÏÂÝÁÔØÓÑ ÚÁÝÉÝÅÎÎÏ Ó ÄÒÕÇÉÍÉ, ÷Ù ÄÏÌÖÎÙ ÉÍÅÔØ ÓÅÔØ ÄÏ×ÅÒÉÑ. ðÏÓÔÒÏÅÎÉÅ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÐÏÈÏÖÅ ÎÁ ÕËÒÏÝÅÎÉÅ. ìÀÄÉ, Ó ËÏÔÏÒÙÍÉ ÷Ù ÏÂÝÁÅÔÅÓØ, ÄÏÌÖÎÙ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG[1], É ÄÏÌÖÎÏ ÉÍÅÔØÓÑ ÄÏÓÔÁÔÏÞÎÏÅ ËÏÌÉÞÅÓÔ×Ï ÐÏÄÐÉÓÁÎÎÙÈ ËÌÀÞÅÊ, ÞÔÏÂÙ ËÌÀÞÉ ÍÏÇÌÉ ÐÏÄÔ×ÅÒÖÄÁÔØÓÑ. üÔÏ ÎÅ ÓÔÏÌØËÏ ÔÅÈÎÉÞÅÓËÉÅ, ÓËÏÌØËÏ ÓÏÃÉÁÌØÎÙÅ ÐÒÏÂÌÅÍÙ. ïÄÎÁËÏ, ÷Ù ÄÏÌÖÎÙ ÐÒÅÏÄÏÌÅÔØ ÜÔÉ ÐÒÏÂÌÅÍÙ, ÅÓÌÉ ÈÏÔÉÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG.

ëÏÇÄÁ ÷Ù ÎÁÞÉÎÁÅÔÅ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, ×ÁÖÎÏ ÐÏÎÑÔØ, ÞÔÏ ÎÅÔ ÎÅÏÂÈÏÄÉÍÏÓÔÉ × ÚÁÝÉÔÅ ÐÅÒÅÐÉÓËÉ Ó ËÁÖÄÙÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÏÍ. îÁÞÎÉÔÅ Ó ÎÅÂÏÌØÛÏÇÏ ËÒÕÇÁ ÌÀÄÅÊ, ×ÏÚÍÏÖÎÏ ÔÏÌØËÏ ÷Ù É ÏÄÉÎ ÉÌÉ Ä×Á ÷ÁÛÉÈ ÔÏ×ÁÒÉÝÁ, ÔÏÖÅ ÖÅÌÁÀÝÉÈ ÒÅÁÌÉÚÏ×ÁÔØ Ó×ÏÅ ÐÒÁ×Ï ÎÁ ÔÁÊÎÕ ÐÅÒÅÐÉÓËÉ. óÏÚÄÁÊÔÅ ÷ÁÛÉ ËÌÀÞÉ É ÐÏÄÐÉÛÉÔÅ ÏÔËÒÙÔÙÅ ËÌÀÞÉ ÄÒÕÇ ÄÒÕÇÁ. üÔÏ ÷ÁÛÁ ÎÁÞÁÌØÎÁÑ ÓÅÔØ ÄÏ×ÅÒÉÑ. äÅÌÁÑ ÔÁË, ÷Ù ÏÃÅÎÉÔÅ

ÚÎÁÞÅÎÉÅ ÍÁÌÅÎØËÉÊ, ÎÁÄÅÖÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ É ÂÕÄÅÔÅ ÂÏÌÅÅ ÏÓÔÏÒÏÖÎÙ × ÂÕÄÕÝÅÍ, ËÏÇÄÁ ÷ÁÛÁ ÓÅÔØ ÓÔÁÎÅÔ ÒÁÓÔÉ.

÷ ÄÏÐÏÌÎÅÎÉÅ Ë ÜÔÏÊ ÎÁÞÁÌØÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ, ÷Ù ÍÏÖÅÔÅ ÚÁÈÏÔÅÔØ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏ ÐÅÒÅÐÉÓÙ×ÁÔØÓÑ Ó ÄÒÕÇÉÍÉ ÌÀÄØÍÉ, ÔÁËÖÅ ÉÓÐÏÌØÚÕÀÝÉÍÉ GnuPG. ðÅÒÅÐÉÓËÁ, ÏÄÎÁËÏ, ÍÏÖÅÔ ÐÏÎÁÄÏÂÉÔØÓÑ ÎÅÓËÏÌØËÉÍÉ ÐÏ ÄÒÕÇÉÍ ÐÒÉÞÉÎÁÍ: (1) ÷Ù ÎÅ ×ÓÅÇÄÁ ÚÎÁÅÔÅ, ÞÔÏ ÞÅÍÕ-ÌÉÂÏ ÉÓÐÏÌØÚÕÅÔ ÉÌÉ ÖÅÌÁÅÔ ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG, É (2) ÅÓÌÉ ÷Ù É ÚÎÁÅÔÅ, ÞÔÏ ÞÅÍÕ-ÌÉÂÏ ÉÓÐÏÌØÚÕÅÔ ÅÇÏ, ÍÏÖÅÔ ×ÏÚÎÉËÎÕÔØ ÓÌÏÖÎÏÓÔÉ Ó ÐÏÄÔ×ÅÒÖÄÅÎÉÅÍ ËÌÀÞÅÊ. ðÅÒ×ÁÑ ÐÒÉÞÉÎÁ Ñ×ÌÑÅÔÓÑ ÓÌÅÄÓÔ×ÉÅÍ ÔÏÇÏ, ÞÔÏ ÌÀÄÉ ÎÅ ×ÓÅÇÄÁ ÏÂßÑ×ÌÑÀÔ Ï ÔÏÍ, ÞÔÏ ÉÓÐÏÌØÚÕÀÔ GnuPG. ÷ÏÚÍÏÖÎÙÊ ×ÁÒÉÁÎÔ ÒÅÛÅÎÉÑ ÜÔÏÊ ÐÒÏÂÌÅÍÙ, ÐÏÄÁÔØ ÐÒÉÍÅÒ É ÏÂßÑ×ÉÔØ, ÞÔÏ ÷Ù ÉÓÐÏÌØÚÕÅÔÅ GnuPG. åÓÔØ ËÁË ÍÉÎÉÍÕÍ ÔÒÉ ÓÐÏÓÏÂÁ ÓÄÅÌÁÔØ ÜÔÏ: ÷Ù ÍÏÖÅÔÅ ÐÏÄÐÉÓÙ×ÁÔØ Ó×ÏÉ ÓÏÏÂÝÅÎÉÑ, ÷Ù ÍÏÖÅÔÅ ÐÏÍÅÓÔÉÔØ Ó×ÏÊ ÏÔËÒÙÔÙÊ ËÌÀÞ ÎÁ Ó×ÏÅÊ ×ÅÂ-ÓÔÒÁÎÉÃÅ, ÷Ù ÍÏÖÅÔÅ ÕËÁÚÁÔØ ÉÄÅÎÔÉÆÉËÁÔÏÒ ÷ÁÛÅÇÏ ËÌÀÞÁ × ÐÏÄÐÉÓÉ ÐÏÞÔÏ×ÏÇÏ ÓÏÏÂÝÅÎÉÑ. åÓÌÉ ÷Ù ÓÏÏÂÝÁÅÔÅ Ï Ó×ÏÅÍ ËÌÀÞÅ, ÔÏ ÄÅÌÁÅÔÅ ÂÏÌÅÅ ÕÍÅÓÔÎÙÍ ÄÌÑ ÄÒÕÇÉÈ ÓÏÏÂÝÉÔØ ÏÂ ÉÈ ËÌÀÞÁÈ. âÏÌÅÅ ÔÏÇÏ, ÷ÁÛÉÍ ËÏÒÒÅÓÐÏÎÄÅÎÔÁÍ ÂÕÄÅÔ ÐÒÏÝÅ ÎÁÞÁÔØ Ó ÷ÁÍÉ ÐÅÒÅÐÉÓÙ×ÁÔØÓÑ ËÏÎÆÉÄÅÎÃÉÁÌØÎÏ, ÅÓÌÉ ÷Ù ÐÒÏÑ×ÉÔÅ ÉÎÉÃÉÁÔÉ×Õ É ÓÄÅÌÁÅÔÅ ÑÓÎÙÍ ÉÓÐÏÌØÚÏ×ÁÎÉÅ ÷ÁÍÉ GnuPG.

ðÒÏ×ÅÒËÁ ÐÒÁ×ÉÌØÎÏÓÔÉ ËÌÀÞÁ ÂÏÌÅÅ ÓÌÏÖÎÁ. åÓÌÉ ÷Ù ÎÅ ÚÎÁËÏÍÙ ÌÉÞÎÏ Ó ÞÅÌÏ×ÅËÏÍ, ÞÅÊ ËÌÀÞ ÓÏÂÉÒÁÅÔÅÓØ ÐÏÄÐÉÓÁÔØ, ÔÏ ÎÅ ÍÏÖÅÔÅ ÐÏÄÐÉÓÁÔØ ËÌÀÞ ÓÁÍÉ. ÷Ù ÄÏÌÖÎÙ ÏÐÉÒÁÔØÓÑ ÎÁ ÞÕÖÉÅ ÐÏÄÐÉÓÉ É ÐÏÓÔÁÒÁÔØÓÑ ÎÁÊÔÉ ÃÅÐÏÞËÕ ÐÏÄÐÉÓÅÊ, ÎÁÞÉÎÁÑ Ó ËÌÀÞÁ ÐÏÄ ×ÏÐÒÏÓÏÍ É ÚÁËÁÎÞÉ×ÁÑ ÷ÁÛÉÍ. äÌÑ ÎÁÈÏÖÄÅÎÉÑ ÃÅÐÏÞËÉ, ÷Ù ÄÏÌÖÎÙ ÐÒÏÑ×ÉÔØ ÉÎÉÃÉÁÔÉ×Õ É ÐÏÌÕÞÉÔØ ÷ÁÛ ËÌÀÞ ÐÏÄÐÉÓÁÎÎÙÊ ËÅÍ-ÌÉÂÏ ÚÁ ÐÒÅÄÅÌÁÍÉ ÷ÁÛÅÊ ÎÁÞÁÌØÎÏÊ ÓÅÔÉ ÄÏ×ÅÒÉÑ.

éÍÅÊÔÅ ÏÄÎÁËÏ × ×ÉÄÕ, ÞÔÏ ×ÓÅ ÜÔÏ × ÚÁ×ÉÓÉÍÏÓÔÉ ÏÔ ÐÏÔÒÅÂÎÏÓÔÅÊ. ÷Ù ÎÅ ÏÂÑÚÁÔÅÌØÎÏ ÄÏÌÖÎÙ ÚÁÑ×ÌÑÔØ Ï Ó×ÏÅÍ ËÌÀÞÅ ÉÌÉ ÐÏÄÐÉÓÙ×ÁÔØ ÞÕÖÉÅ ËÌÀÞÉ. óÉÌÁ GnuPG ÓÏÓÔÏÉÔ × ÔÏÍ, ÞÔÏ ÏÎ ÄÏÓÔÁÔÏÞÎÏ ÇÉÂÏË É ÍÏÖÅÔ ÂÙÔØ ÁÄÁÐÔÉÒÏ×ÁÎ Ë ÷ÁÛÉÍ ÐÏÔÒÅÂÎÏÓÔÑÍ, ËÁËÉÍÉ ÂÙ ÏÎÉ ÎÅ ÂÙÌÉ. ðÒÉ ÜÔÏÍ ÄÅÊÓÔ×ÉÔÅÌØÎÏÓÔØ ÔÁËÏ×Á, ÞÔÏ ÷Ù ÄÏÌÖÎÙ ÐÒÏÑ×ÌÑÔØ ÉÎÉÃÉÁÔÉ×Õ, ÅÓÌÉ ÈÏÔÉÔÅ ÒÁÓÛÉÒÉÔØ Ó×ÏÀ ÓÅÔØ ÄÏ×ÅÒÉÑ É ÉÓÐÏÌØÚÏ×ÁÔØ GnuPG ËÁË ÍÏÖÎÏ ÂÏÌØÛÅ.

úÁËÏÎÎÏÓÔØ ÉÓÐÏÌØÚÏ×ÁÎÉÑ GnuPG

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

Примечания

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

Глава 5. òÁÚÌÉÞÎÙÅ ×ÏÐÒÏÓÙ

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

îÁÐÉÓÁÎÉÅ ÐÏÌØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ

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

üÔÉ ÒÅÚÕÌØÔÁÔÙ ÎÅ ÕÄÉ×ÌÑÀÔ. PGP 5.0 ÉÍÅÅÔ ÈÏÒÏÛÉÊ ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ, ËÏÔÏÒÙÊ ÐÒÅ×ÏÓÈÏÄÅÎ ÅÓÌÉ ÷Ù ÕÖÅ ÐÏÎÉÍÁÅÔÅ ËÁË ÒÁÂÏÔÁÅÔ ÛÉÆÒÏ×ÁÎÉÅ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ É ÄÒÕÖÉÔÅ Ó ÍÏÄÅÌØÀ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ËÌÀÞÅÊ ÓÐÅÃÉÆÉÃÉÒÏ×ÁÎÎÏÊ OpenPGP. ë ÓÏÖÁÌÅÎÉÀ, ÎÁÞÉÎÁÀÝÉÅ ÐÏÌØÚÏ×ÁÔÅÌÉ, ÎÅ ÐÏÎÉÍÁÀÔ ÎÉ ÛÉÆÒÏ×ÁÎÉÑ Ó ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ, ÎÉ ÐÒÁ×ÉÌ ÕÐÒÁ×ÌÅÎÉÑ ËÌÀÞÁÍÉ, É ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ ÍÁÌÏ ÐÏÍÏÇÁÅÔ ÉÍ.

÷ÁÍ ÓÌÅÄÕÅÔ ×ÎÉÍÁÔÅÌØÎÏ ÏÚÎÁËÏÍÉÔØÓÑ Ó ×Ù×ÏÄÁÍÉ Whitten’Á É Tygar’Á ÅÓÌÉ ÷Ù ÐÉÛÅÔÅ ÐÏÌØÚÏ×ÁÔÅÌØÓËÉÊ ÉÎÔÅÒÆÅÊÓ. ïÎÉ ÄÁÀÔ ËÏÍÍÅÎÔÁÒÉÉ ÐÏ ËÁÖÄÏÍÕ ÉÚ ÔÅÓÔÉÒÕÅÍÙÈ. îÁÐÒÉÍÅÒ, ÏËÁÚÁÌÏÓØ, ÞÔÏ ÍÎÏÇÉÅ ×ÅÒÑÔ, ÞÔÏ ÓÏÏÂÝÅÎÉÅ ÐÏÓÙÌÁÅÍÏÅ ÄÒÕÇÉÍ ÌÀÄÑÍ ÎÁÄÏ ÚÁÛÉÆÒÏ×Ù×ÁÔØ Ó×ÏÉÍ ÓÏÂÓÔ×ÅÎÎÙÍ ÏÔËÒÙÔÙÍ ËÌÀÞÏÍ. úÁÄÕÍÁÊÔÅÓØ ÎÁÄ ÜÔÉÍ, É ÷Ù ÐÏÊÍÅÔÅ, ÞÔÏ ÌÅÇËÏ ÄÏÐÕÓÔÉÔØ ÔÁËÕÀ ÏÛÉÂËÕ. ëÁË ÐÒÁ×ÉÌÏ, ÎÁÞÉÎÁÀÝÉÅ ÐÏÌØÚÏ×ÁÔÅÌÉ ÉÓÐÙÔÙ×ÁÀÔ ÔÒÕÄÎÏÓÔÉ × ÐÏÎÉÍÁÎÉÉ ÒÁÚÌÉÞÉÊ ÍÅÖÄÕ ÏÔËÒÙÔÙÍ É ÚÁËÒÙÔÙÍ ËÌÀÞÁÍÉ ËÏÇÄÁ ÉÓÐÏÌØÚÕÀÔ GnuPG. ëÁË ÄÉÚÁÊÎÅÒ ÐÏÌØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ, ÷Ù ÄÏÌÖÎÙ ÐÏÓÔÁÒÁÔØÓÑ ÓÄÅÌÁÔØ ×ÙÂÏÒ ÔÏÇÏ ÉÌÉ ËÌÀÞÁ ÐÒÏÚÒÁÞÎÙÍ. ÷Ù ÍÏÖÅÔÅ, ÔÁËÖÅ, ÉÓÐÏÌØÚÏ×ÁÔØ ÍÁÓÔÅÒÁ É ÄÒÕÇÉÅ ÏÂÝÅÐÒÉÎÑÔÙÅ ÐÒÉÅÍÙ GUI ÄÌÑ ÐÒÏ×ÅÄÅÎÉÑ ÐÏÌØÚÏ×ÁÔÅÌÑ ÓË×ÏÚØ ÏÓÎÏ×ÎÙÅ ÚÁÄÁÞÉ, ÔÁËÉÅ ËÁË ÇÅÎÅÒÁÃÉÑ ËÌÀÞÁ, ÄÏÐÏÌÎÅÎÎÁÑ ÇÅÎÅÒÁÃÉÅÊ ÓÅÒÔÉÆÉËÁÔÁ ÏÔÚÙ×Á ËÌÀÞÁ, É Ô.Ð. éÚ ÄÏËÕÍÅÎÔÁ ÓÌÅÄÕÀÔ, ÔÁËÖÅ, ÓÌÅÄÕÀÝÉÅ ×Ù×ÏÄÙ.

- âÅÚÏÐÁÓÎÏÓÔØ, ÏÂÙÞÎÏ Ñ×ÌÑÅÔÓÑ ×ÔÏÒÏÓÔÅÐÅÎÎÏÊ ÚÁÄÁÞÅÊ; ÌÀÄÉ ÈÏÔÑÔ ÏÔÐÒÁ×ÌÑÔØ ÐÏÞÔÕ, ÐÒÏÓÍÁÔÒÉ×ÁÔØ É Ô.Ä. îÅ ÄÕÍÁÊÔÅ ÞÔÏ ÐÏÌØÚÏ×ÁÔÅÌÉ ÓÔÁÎÕÔ ÞÉÔÁÔØ ÔÏÌÓÔÙÅ ÒÕËÏ×ÏÄÓÔ×Á ÉÌÉ ÒÁÚÂÉÒÁÔØÓÑ × ÎÁÓÔÒÏÊËÁÈ ÛÉÆÒÏ×ÁÎÉÑ.
- úÁÝÉÔÁ ÓÅÔÅ×ÏÇÏ ËÏÍÐØÀÔÅÒÁ ÎÅ ÓÉÌØÎÅÅ ÓÁÍÏÇÏ ÓÌÁÂÏÇÏ ÉÚ ÅÅ ËÏÍÐÏÎÅÎÔÏ×. ðÏÌØÚÏ×ÁÔÅÌÉ ÄÏÌÖÎÙ ÂÙÔØ ÏÓ×ÅÄÏÍÌÅÎÙ ÏÂÏ ×ÓÅÈ ÁÓÐÅËÔÁÈ Ó×ÏÅÊ ÂÅÚÏÐÁÓÎÏÓÔÉ, ÎÅ ÏÇÒÁÎÉÞÉ×ÁÑÓØ ÞÁÓÔÉÞÎÙÍÉ Ó×ÅÄÅÎÉÑÍÉ, ËÁË ÜÔÏ ÍÏÖÅÔ ÂÙÔØ Ó ÔÅËÓÔÏ×ÙÍÉ ÐÒÏÇÒÁÍÍÁÍÉ ÉÌÉ ÜÌÅËÔÒÏÎÎÙÍÉ ÔÁÂÌÉÃÁÍÉ.

- ÷ÓÅÇÄÁ ÉÓÐÏÌØÚÕÊÔÅ ÏÄÉÎÁËÏ×ÙÅ ÔÅÒÍÉÎÙ ÄÌÑ ÏÄÉÎÁËÏ×ÙÈ ÄÅÊÓÔ×ÉÊ. éÚÂÅÇÁÊÔÅ ÕÐÏÔÒÅÂÌÅÎÉÑ ÓÉÎÏÎÉÍÏ×, ÔÉÐÁ “encrypt” É “encipher”.
- äÌÑ ÎÅÉÓËÕÛÅÎÙÈ ÐÏÌØÚÏ×ÁÔÅÌÅÊ ÕÐÒÏÓÔÉÔÅ ×Ù×ÏÄ ÉÎÆÏÒÍÁÃÉÉ. óÌÉÛËÏÍ ÂÏÌØÛÏÅ ËÏÌÉÞÅÓÔ×Ï ÉÎÆÏÒÍÁÃÉÉ ÓËÒÙ×ÁÅÔ ÔÕ, ËÏÔÏÒÁÑ ×ÁÖÎÁ. îÁÞÁÌØÎÁÑ ËÏÎÆÉÇÕÒÁÃÉÑ ÉÎÔÅÒÆÅÊÓÁ ÄÏÌÖÎÁ ÏÂÅÓÐÅÞÉÔØ ÐÏÌØÚÏ×ÁÔÅÌÑ ÐÒÁ×ÉÌØÎÏÊ ÍÏÄÅÌØÀ ÏÔÎÏÛÅÎÉÊ ÍÅÖÄÕ ÏÔËÒÙÔÙÍ É ÚÁËÒÙÔÙÍ ËÌÀÞÁÍÉ É ÐÒÏÚÒÁÞÎÙÍ ÐÏÎÉÍÁÎÉÅÍ ÆÕÎËÃÉÊ ÐÏÌÕÞÅÎÉÑ É ÒÁÓÐÒÏÓÔÒÁÎÅÎÉÑ ËÌÀÞÅÊ.

ðÁÚÒÁÂÏÔËÁ ÜÆÆÅËÔÉ×ÎÏÇÏ ÐÏÌØÚÏ×ÁÔÅÌØÓËÏÇÏ ÉÎÔÅÒÆÅÊÓÁ ÄÌÑ ÕÐÒÁ×ÌÅÎÉÑ ËÌÀÞÁÍÉ ÅÝÅ ÂÏÌÅÅ ÓÌÏÖÎÁ. íÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ OpenPGP, Ë ÓÏÖÁÌÅÎÉÀ, ÄÏ×ÏÌØÎÏ ÔÒÕÄÎÁ ÄÌÑ ÐÏÎÉÍÁÎÉÑ. îÁÐÒÉÍÅÒ, ÓÐÅÃÉÆÉËÁÃÉÑ ÏÐÒÅÄÅÌÑÅÔ ÔÒÉ ÓÔÅÐÅÎÉ ÄÏ×ÅÒÉÑ ÐÏÌØÚÏ×ÁÔÅÌÀ: ÎÅÔ (none), ÏÔÎÏÓÉÔÅÌØÎÏÅ (marginal), É ÐÏÌÎÏÅ (Óomplete). ÷ÓÅ ÇÒÁÎÉ ÄÏ×ÅÒÉÑ, ÉÓÐÙÔÙ×ÁÅÍÏÇÏ ÐÏÌØÚÏ×ÁÔÅÌÅÍ, ÄÏÌÖÎÙ ÕÍÅÓÔÉÔØÓÑ × ÜÔÉ ÔÒÉ ÑÞÅËËÉ. áÌÇÏÒÉÔÍ ÐÏÄÔ×ÅÒÖÄÅÎÉÑ ËÌÀÞÅÊ ÔÁËÖÅ ÓÌÏÖÅÎ ÄÌÑ ÐÏÎÉÍÁÎÉÑ ÎÅ ÓÐÅÃÉÁÌÉÓÔÏ×, ÏÓÏÂÅÎÎÏ ÐÁÒÁÍÅÔÒÙ “marginals needed” É “completes needed”. ôÁË ËÁË ÍÏÄÅÌØ ÓÅÔÉ ÄÏ×ÅÒÉÑ ÞÅÔËÏ ÏÐÒÅÄÅÌÅÎÁ É ÎÅ ÍÏÖÅÔ ÂÙÔØ ÉÚÍÅÎÅÎÁ, ÷ÁÍ ÐÒÉÊÄÅÔÓÑ ÐÏÓÔÁÒÁÔØÓÑ É ÒÁÚÒÁÂÏÔÁÔØ ÉÎÔÅÒÆÅÊÓ, ËÏÔÏÒÙÊ ÐÏÍÏÖÅÔ ÐÏÎÑÔØ ÅÅ ÐÏÌØÚÏ×ÁÔÅÌÀ. ïÐÒÅÄÅÌÅÎÎÁÑ ÆÕÎËÃÉÑ, Ë ÐÒÉÍÅÒÕ, ÍÏÇÌÁ ÂÙ ÏÔÏÂÒÁÖÁÔØ ÄÉÁÇÒÁÍÍÕ ÔÏÇÏ, ËÁË ÂÙÌ ÐÏÄÔ×ÅÒÖÄÅÎ ËÌÀÞ, ÐÏ ÚÁÐÒÏÓÕ ÐÏÌØÚÏ×ÁÔÅÌÑ. ïÓÎÏ×ÎÙÅ ×Ù×ÏÄÙ ÓÌÅÄÕÀÝÉÅ.

- ðÏÌØÚÏ×ÁÔÅÌÉ ÍÏÇÕÔ ÏÓÔÁ×ÁÔØÓÑ × ÎÅ×ÅÄÅÎÉÉ ÏÔÎÏÓÉÔÅÌØÎÏ ÔÏÇÏ, ËÁË É ËÏÇÄÁ ÐÒÅÄÏÓÔÁ×ÉÔØ ÄÏÓÔÕÐ.
- ðÒÉÄÁÊÔÅ ×ÙÓÏËÉÊ ÐÒÉÏÒÉÔÅÔ ÔÏÍÕ, ÞÔÏÂÙ ÚÁÝÉÔÉÔØ ÐÏÌØÚÏ×ÁÔÅÌÅÊ ÏÔ ÓÏ×ÅÒÛÅÎÉÑ ÄÏÒÏÇÏÓÔÏÑÝÉÈ ÏÛÉÂÏË, ÔÁËÉÈ ËÁË ÏÛÉÂÏÞÎÏÅ ÕÄÁÌÅÎÉÅ ÓÅËÒÅÔÎÏÇÏ ËÌÀÞÁ, ÐÕÂÌÉËÁÃÉÑ ËÌÀÞÁ, ÏÔÚÙ× ËÌÀÞÁ, ÐÏÔÅÒÑ ËÌÀÞÅ×ÏÊ ÆÒÁÚÙ, ÎÅÐÒÁ×ÉÌØÎÁÑ ÁÒÈÉ×ÁÃÉÑ ËÌÀÞÁ.

Приложение 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×ÅÄÅÎÏ × ÓÏÏÔ×ÅÔÓÔ×ÉÅ Ó ×ÅÒÓÉÅÊ gnupg 1.0.7. ðÒÏÃÅÄÕÒÁ ÇÅÎÅÒÁÃÉÉ ËÌÀÞÁ ÏÐÉÓÁÎÁ ÄÌÑ ÁÌÇÏÒÉÔÍÁ RSA. õÄÁÌÅÎÏ ÏÐÉÓÁÎÉÅ ËÏÍÁÎÄ É ÐÁÒÁÍÅÔÒÏ×, ËÁË ÕÓÔÁÒÅ×ÛÅÅ.

Приложение B. GNU Free Documentation License

Version 1.1, March 2000

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.