PGP-Pretty Good Privacy - 1

Разработил: Джейлян Адемова №13384

PGP е комбинирана (хибридна) криптосистема. Тя използва криптиране с публичен ключ за защита на електронна поща и файлове с данни. Програмата е с много добри възможности и е доста бърза, притежава интелигентно ключово управление и инструменти за цифрови подписи и компресиране на данни, както и сравнително лесни за използване команди. PGP притежава версии за MS-DOS, Unix, Windows и Macintosh [1].

1. Исторически обзор

Pretty Good Privacy е софтуерно реализирана криптографска система за защита на предаваните по електронна поща съобщения и на съхраняваните върху различни носители данни. Първоначално е била създадена като инструмент за защита на човешките права, като е публикувана през 1991 година за свободен достъп. Създадена е от Филип Цимерман, който е обявен за един от водещите 10 изобретатели в електронната индустрия и е сред най-влиятелните „Net 50“ хора [2].

Цимерман е бил подложен на три годишно следствие, защото по мнение на правителството на САЩ е бил нарушил законът за забрана експорта на криптографски програми. Независимо от липсата на финансова поддръжка, изпълнителен персонал, фирма която да го подкрепи и преследването от страна на правителството, PGP се наложи като най-разпространяваната в световен мащаб технология за криптиране на данните предавани чрез електронна поща. След прекратяване на следствието в началото на 1996 година Цимерман основава компания наречена PGP Inc. През декември 1997 PGP Inc е закупена от Network Associates Inc (NAI). Цимерман е работил за NAI в продължение на три години като старши консултант. През август 2002 PGP е закупен от PGP Corporation, където автора продължава да работи и до днес като специален сътрудник и консултант [2, 3].

PGP се налага като най-разпространяваната в световен мащаб технология за криптиране на данните предавани чрез електронна поща. Системата притежава както платена, така и безплатна версия.

2. Принцип на работа на PGP

Основи на криптографията

Смята се, че когато Юлий Цезар е изпращал съобщения до генералите си, поради това че не имал доверие на вестоносците си, той решил да промени облика на съобщенията. Той заместил всяко А в неговото съобщение с Д, а всяко Б с И и така с всички букви. Само някой, който бил наясно с метода на изместване с три позиции надясно, можел да ги разчете [1].

Криптиране и декриптиране

Информация, която може да бъде прочетена и разбрана без предприемането на някакви по специални мерки се нарича “първичен текст”. Криптиране (ще използваме кодиране като синоним) наричаме метода на прикриване смисъла му. Криптираният текст представлява нечетима последователност от символи, която наричаме шифриран текст. Кодирането се извършва, за да се подсигури липсата на директен достъп до информацията от всеки, за когото не е предназначена. Процесът по възстановяването на изначалния вид на криптиран текст наричаме декрпитиране [2].

Фиг. 1. Криптиране и декриптиране

Какво е криптография

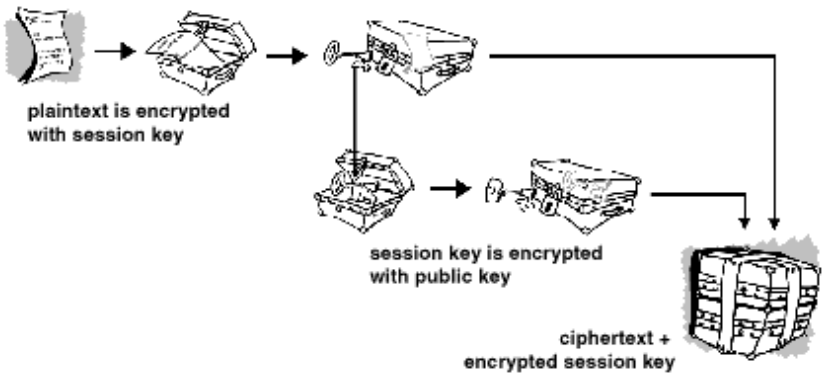
Криптографията е наука, която използва математиката, за да криптира и/или декриптира информация. Криптографията позволява да се съхранява или да изпраща тайна информация в неустойчива

мрежа във вид, непозволяващ да бъде разчетен от някой друг освен от предназначения получател.

От своя страна криптоанализът е наука за анализ и дифтонгизация на надеждната комуникация. Класическият криптоанализ е интересна комбинация от аналитични разсъждения, подбор от математически инструменти, търсене по образец, търпение, отдаденост и малко късмет. Често като синоним на тази наука се ползва термина „атаки”. Криптологията обхваща както криптографията, така и криптоанализа [2, 5].

Как работи PGP

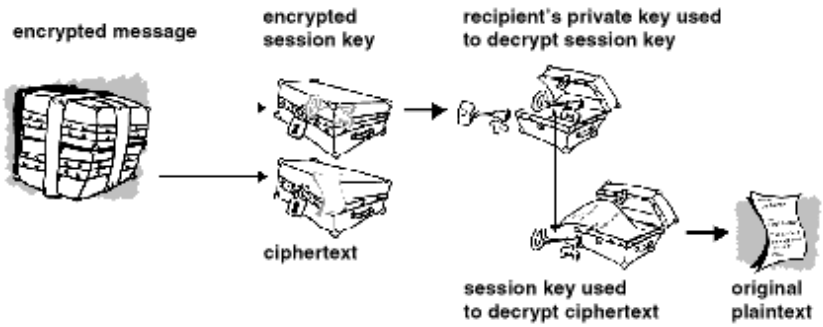
PGP комбинира най-добрите черти на двете криптосистеми: симетричната и асиметричната. PGP е хибридна криптосистема. Когато криптираме текст с нея, той бива първо компресиран. Компресирането на информацията спестява време и дисково пространство по време на предаването на данни, но най-важното – засилва сигурността. Повечето техники за криптоанализ разработват начини за разбиване на повторения, намерени в шифъра. Компресирането намалява броя на повторенията в „първичния текст”, което увеличава устойчивостта на криптирания текст спрямо атаки [2].



Фиг. 2. Как работи PGP криптирането

След което PGP създава сесиен ключ, който е „one-time-only” секретен ключ. Този ключ е произволно число, генерирано чрез движенията на мишката или чрез натиснат клавиш от клавиатурата. Сесийният ключ работи с много бърз и сигурен алгоритъм за криптиране на „първичния текст”, в резултат на което имаме шифриран текст. След като информацията е криптирана, сесийният

ключ се криптира с публичния ключ. Криптираният сесиен ключ се изпраща заедно с криптирания текст на получателя [5, 6].



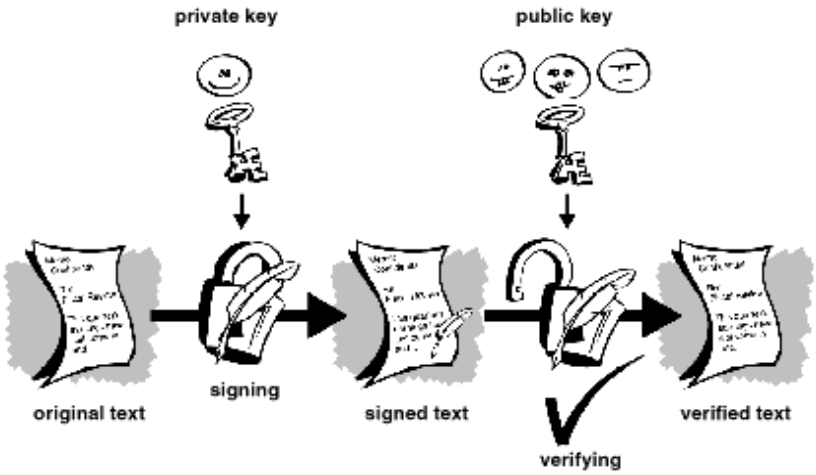
Фиг. 3. Как работи PGP декриптирането

Ако обърнем процеса ще получим принципа на декриптирането (Фиг. 3.). Получателят използва частния си ключ, за да декриптира сесийния ключ, а сесийния, за да декриптира криптирания текст.

Комбинацията от двата метода за криптиране предлага удобството на асиметричното криптиране и скоростта на симетричното. Симетричното криптиране е около 1000 пъти по-бързо от асиметричното. От своя страна асиметричното разрешава проблемите, свързани с обмяната на ключа и данните.

Квалифициран електронен подпис

Асиметричните криптосистми осигуряват метод за използването на цифрови подписи. Квалифицираният електронен подпис позволява на получателя на информация да потвърди автентичността на документа (включително, че и информацията, която носи е непокътната). Вместо да се криптира информация с нечий публичен ключ, се използва личния частен ключ. Ако дадено лице може да декриптира информацията със своя публичен ключ, то следва, че то я е и криптирало.



Фиг. 4. Принцип на електронния подпис

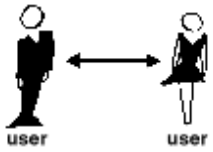
X.509 certificate format

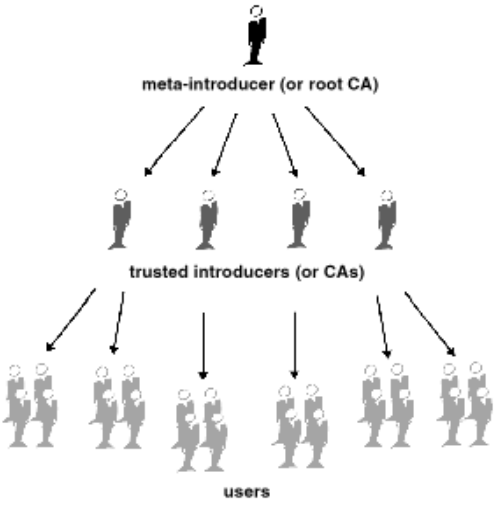
X.509 е ITU-T стандарт за инфраструктура на публичния ключ (PKI).

> •ITU Telecommunication Standardization Sector (ITU-T) координира стандартите в телекомуникациите от името на International Telecommunication Union (ITU). Базиран е в Женева.
>
> •Инфраструктура на публичните ключове (PKI) е спогодба, която обвързва публичните ключове със съответния потребител от Certificate Authority (CA) чрез сертификати, издавани от CA.

Модели на доверие

- Direct Trust
- Hierarchical Trust
- A Web of Trust





Фиг. 5. Модели на доверие

Какво е Мрежа на Доверие

Мрежа на Доверие (Web of Trust) е термин, използван за описание на връзките на доверие между група от ключове. Всяка сигнатура върху ключ е връзка в тази мрежа. Колкото повече връзки има, толкова повече нараства мрежата на доверие. В идеалната ситуация в група от ключове всеки вярва на всеки. Често софтуерът, който управлява работата с ключове, предлага възможност за имплицитно доверие, тоест ако достатъчно от вашите контакти вярват и са подписали даден ключ, то и вие имплицитно може да се доверите на този ключ.

Web of trust (мрежа на доверие)

При използването на публични ключове е много важно удостоверяването на собственика на ключа. Още от самото си създаване PGP включва в системата за разпространение на публичните ключове и “сертификат за идентичност”. Включването на публичния ключ в сертификат дава сигурност на потребителите, че ключът е валиден. Тази мрежа от сертификати е наречена WEB OF TRUST. Даден сертификат може да бъде подписан и от трета страна за заверка, като в тези подписи могат да бъдат включени няколко нива на сигурност.

•WEB OF TRUST протоколът е описан най-напред от Zimmermann в Ръководство за PGP version 2.0.

•WEB OF TRUST механизмът има предимства пред централизираната PKI схема, които се използват от S/MIME (Secure / Multipurpose Internet Mail Extensions) стандарта, но не се използва масово. Проблемът е, че потребителите трябва да проверят валидността на сертификатите ръчно, или просто да ги приемат [2,4].

3. Работа с PGP Desktop

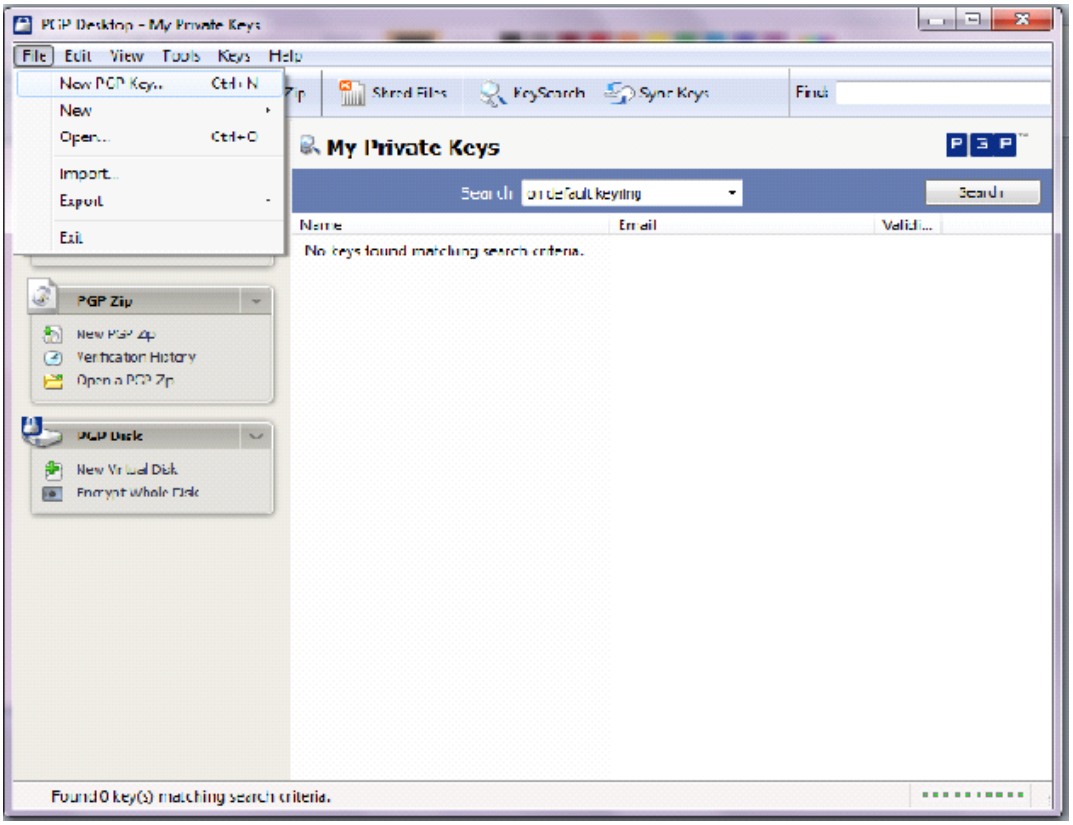
По-горе обяснихме понятията публичен и частен ключ, сега ще преминем към реалното им ползване. Public-key криптографията използва два ключа за криптиране и декриптиране.

Голяма част от дейността с PGP Desktop изисква наличието на keypair. Все пак трябва да се ограничи броят на потребителски създадените **keypair**, защото наличието на прекалено много такива може да доведе до объркване и на потребителите, и на желаещите

да се свържат. Желателно е създаването само на един keypair за имейла, по който да се изпрати криптираното съобщение.

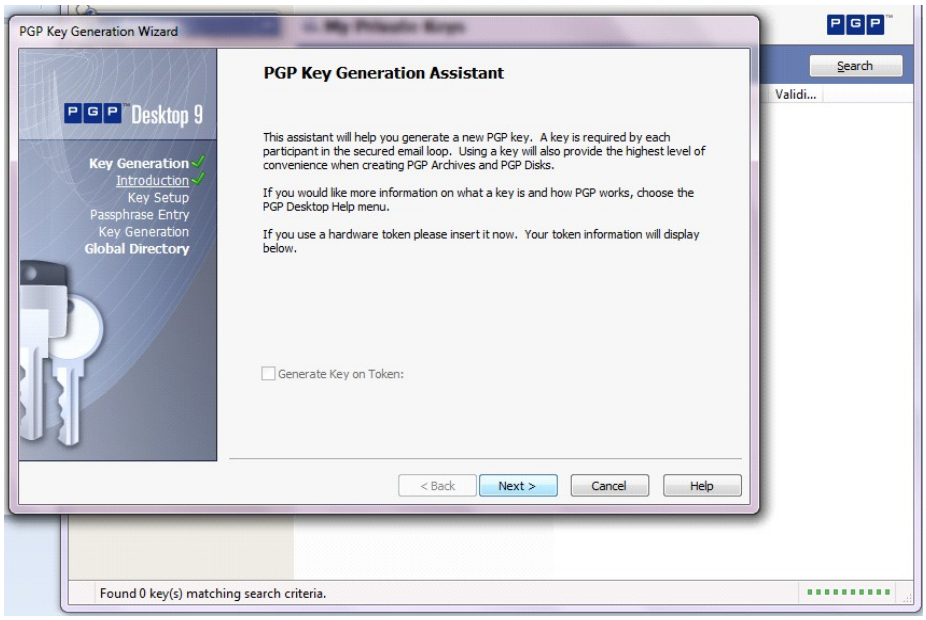
Как се създава PGP keypair:

В началния прозорец от меню File се избира New PGP Key {Ctrl+N}. Отваря се диалогов прозорец за генериране на ключове (Key Generation Assistant) [7].



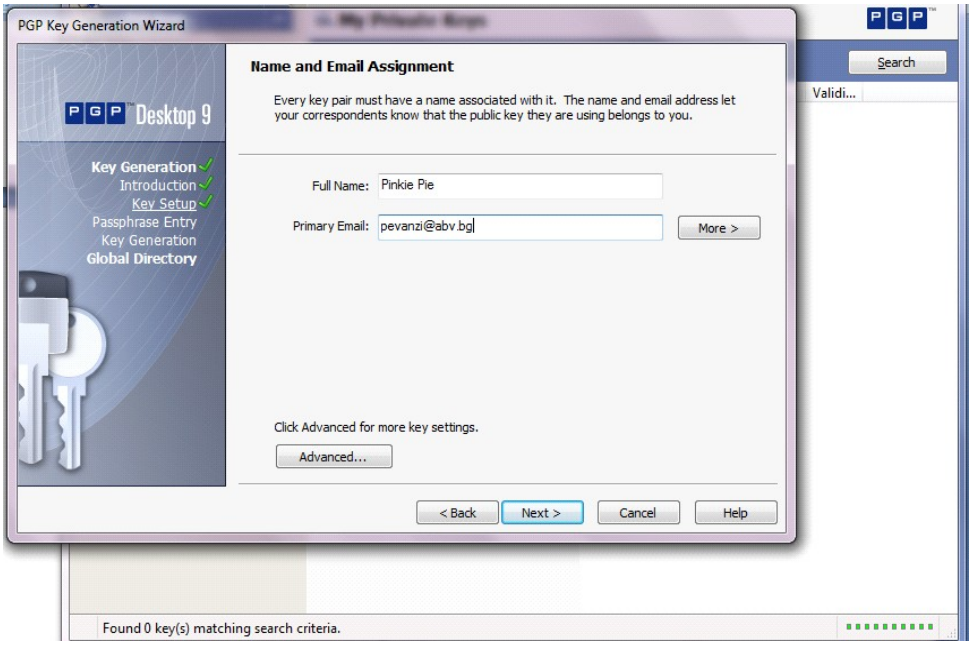
Фиг. 6. Създаване на PGP keypair

При желание за генериране на ключа върху карта памет или друг преносим източник, се проверява дали той е свързан със системата и след това се отбелязва в checkbox-а Generate Key on Token.



Фиг. 7.1. Генериране на ключа

Натиска се Next. Появява се диалогов прозорец „The Name and Email Assignment”. Въвеждат се име в полето Full Name и адекватен имейл в Primary Email [7].



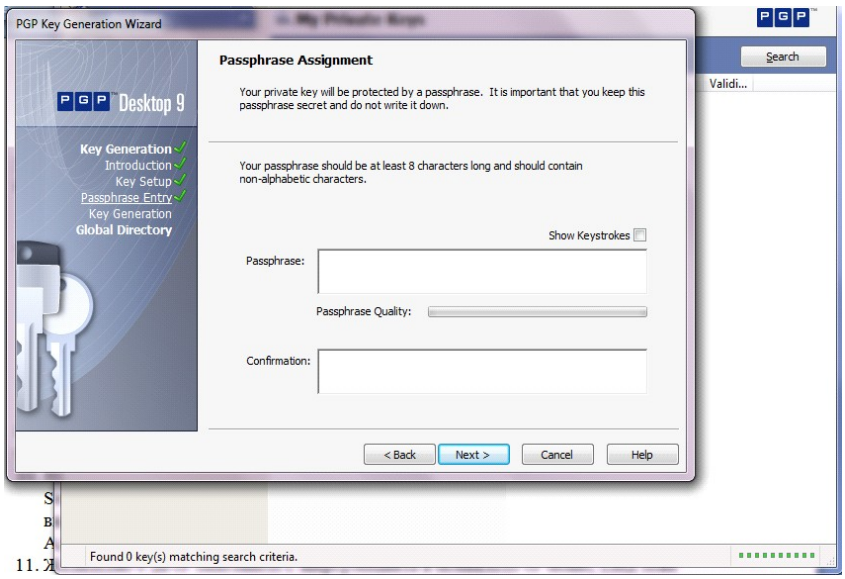
Фиг. 7.2. Генериране на ключа

За добавяне на още настройки към създавания ключ, се натиска Advanced, където може да се променят следните характеристики:

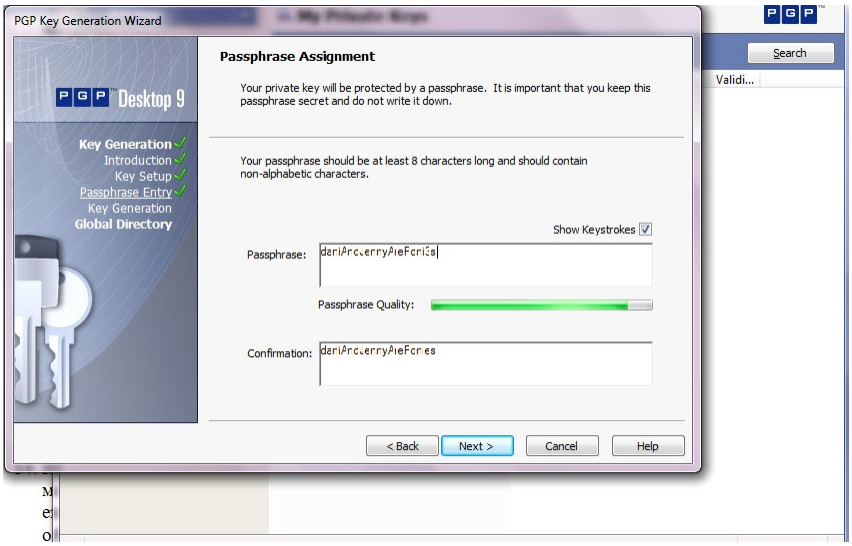
- Тип на ключа (избор между Diffie-Hellman/DSS и RSA).

- Размер на ключа. от 1024 bits до 4096 bits. Колкото е по-голям толкова по-сигурен ще е ключа, но и ще отнеме повече време да се генерира.
- Срок на годност (имаме опция и да е безсрочен).
- Разрешени алгоритми. Отбележи, ако има алгоритми, които не искаш твоя ключ да поддържа.
- Препрочитан алгоритъм. Избор на алгоритъм по подразбиране.

Натиска се OK за затваряне на всички досегашни допълнителни менюта.



Фиг. 7.3. Избор на фраза при генериране на ключа

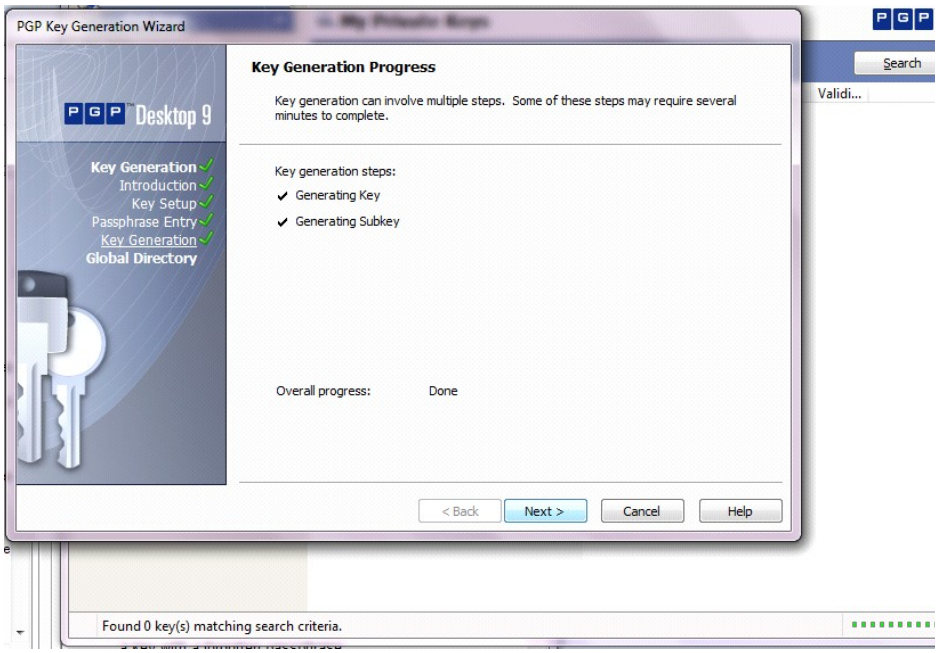


Фиг. 7.4. Пореден етап от генерирането на ключа

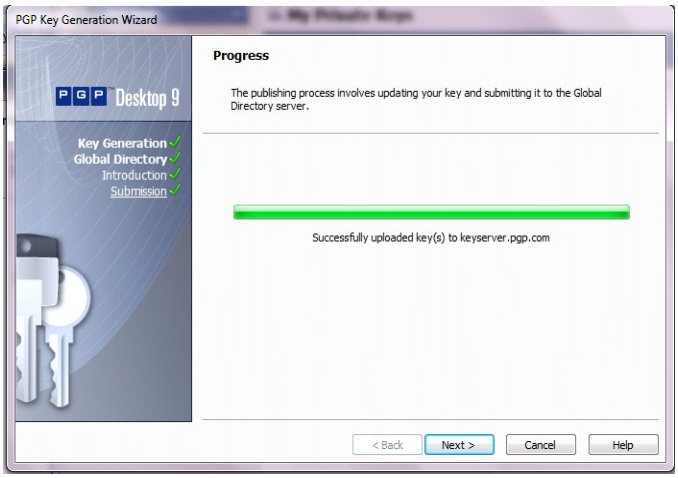
В новопоявилия се прозорец се въвежда фразата-парола, която ще предотвратява достъп до частния ключ, който се генерира.

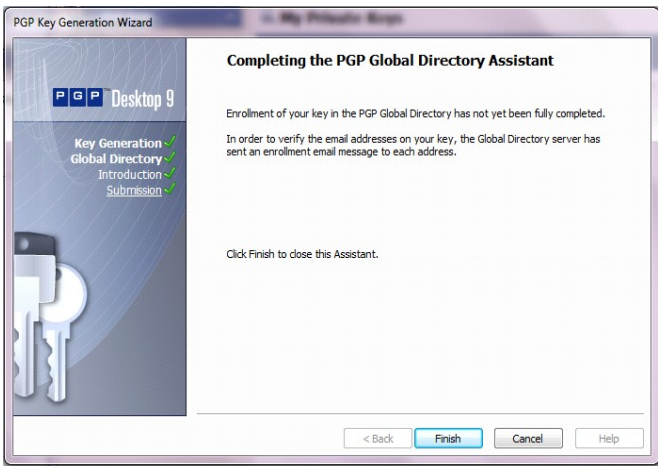
След натискане на Tab, ще се появи поле за потвърждаване Confirmation field, където ще трябва да се въведе фразата-парола.

Избира се Next, за да започне процеса по генериране на нов keypair (Фиг. 7.5.). Процесът може да отнеме няколко минути.



Фиг. 7.5. Създаване на нова двойка ключове при генерирането на ключ





Фиг. 7.6. Генериране на ключа

След създаването на keypair, трябва да се предостави публичния ключ на тези, до които се изпраща съобщението. Има няколко начина за доставяне на публичния ключ.

Публичният ключ се прави явен (например PGP Global Directory) или се разпространява чрез имейл, социална мрежа или флаш памет.

4. Заключение

Досега не е известен метод за разбиване на PGP криптирането. По-ранните версии имат някои теоретични уязвимости, затова е препоръчително да се използват по-новите версии. За разлика от други системи и протоколи за защита, като протокола SSL, който осигурява единствено защита на данни при предаване по мрежа, криптирането с PGP осигурява защита и при съхранение на данни за по-дълъг период, например в компакт дисковете [2].

- Криптографската сигурност на PGP зависи от предположението, че използваните алгоритми са устойчиви при директен криптоанализ с наличната компютърна техника. Практически в системата се използват алгоритми, за които досега не са открити слабости от гледна точка на криптоанализа.

- Всеки, който иска да прочете съобщения, криптирани с PGP, би могъл да използва така наречения Rubber-hose cryptanalysis (кражба на криптографските секрети или вземането им със сила) или да инсталира някаква форма на “троянски кон” или keystroke logging software/hardware върху тази част на компютъра, на който са съобщенията, за да изтегли криптиращите ключове и техните пароли. FBI вече са използвали такива атаки срещу PGP. На практика тези атаки са приложими срещу всеки софтуер за криптиране [2].

GNU Privacy Guard (GnuPG, GPG) е “free open source”, създаден като алтернатива на PGP. GnuPG е съобразен с RFC 4880, т.е. текущите IETF стандарти и спецификации на OpenPGP.

- Новите версии на PGP са съвместими с GnuPG и други системи, съобразени с OpenPGP;

- GPG е част от проекта GNU software project на Фондацията за свободен софтуер (Free Software Foundation), който е

финансиран от германското правителство. Системата е реализирана при условията на версия 3 на GNU General Public License, така че GPG е свободен софтуер (free software) [2].

Източници:

1. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html
2. http://pgp.en.softonic.com/download
3. http://techs-mobile.blogspot.com/2010/03/pgp-smime.html
4. http://www.capital.bg/vestnikut/kapital_net/2001/03/24/207948_kriptografiiata_-_kljuchut_kum_elektronniia_podpis/
5. http://www.pgpi.org/doc/pgpintro/
6. https://www.philzimmermann.com/BG/background/background.html
7. PGP Desktop Help