

GPG in Linux

Chari Karipidis
2TinG

May 16, 2012

Contents

1	Introductie	3
2	GPG	3
2.1	Geschiedenis	3
2.2	Wat is GPG?	4
2.3	Frontend GPG programma's	4
3	Belangrijke woorden	4

1 Introductie

In dit document wordt het gebruik van GPG(GnuPG) nader verklaard.

Benadering De geschiedenis, werking en uitvoer wordt uitgewerkt in Sectie 2 GPG.

Sectie 3 Belangrijke woorden, geeft een overzicht van belangrijke woorden in het document.

2 GPG

2.1 Geschiedenis

Er is altijd wel een probleem met boodschappen verzenden en ontvangen, zonder dat men deze kunnen onderscheppen en lezen. Hier zijn handige uitvindingen voor ontworpen, die helpen bij dit probleem.

Scytale In de tijd van de romeinen had men een manier nodig om berichten te versturen naar geallieerde troepen. Verzender en ontvanger waren in het bezit van een 'Scytale' van ieder dezelfde grootte. Dit voorwerp was een soort van cilinder. Hier werd een riem over gewikkeld en een boodschap op geschreven.

Bij het verwijderen van de riem, was deze tekst onleesbaar zonder behulp van de Scytale. De letters waren namelijk door mekaar. Bij ontvangst van de riem bij de troepen, wikkelden ze de riem over de Scytale die zij bezitten en was het zo mogelijk, de boodschap te lezen.

Dit was een soort van encryptie. Ervoor zorgen dat een onderschepper, de boodschap niet kan lezen.

Caesar methode Een andere encryptie-methode was de Caesar methode. Deze bestond uit een zin hervormen m.b.v. het alfabet. Dit klinkt natuurlijk zeer logisch. Het alfabet wordt namelijk gebruikt om zinnen te schrijven.

Maar na het schrijven van de nodige boodschap, wordt er een 'sleutel' gekozen. Deze sleutel is afgesproken cijfer tussen 1 en 26, tussen beide partijen.

Belangrijk is dat de cijfers overeenkomen met een letter uit het alfabet. Als het gekozen cijfer, 6 is. Wordt het alfabet 6 maal naar links verschoven. A

wordt dan F en B wordt dan G, enz...

De ontvanger krijgt dan een wirwar van letters en kan deze ontcijferen door het alfabet terug te vormen voor het 6 maal naar rechts te verschuiven.

2.2 Wat is GPG?

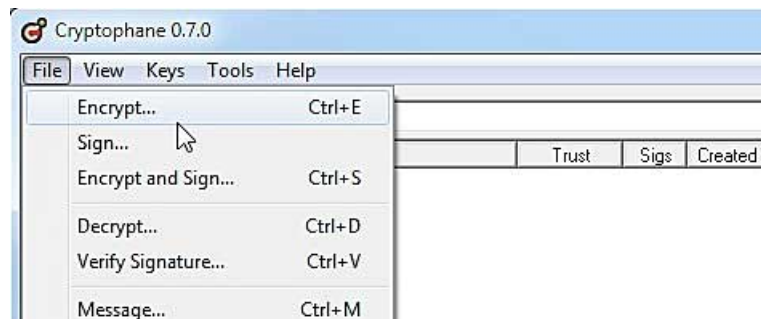
GPG of GnuPG staat voor; Gnu Privacy Guard. Zoals de naam al voorstelt, is het om de privacy van gebruikers te beschermen. Dit doormiddel van encryptie van boodschappen die verzonden moeten worden zoals mails, data encrypteren, 'sleutelhangers', enz...

GnuPG is een commando voor de terminal, maar er zijn dergelijke frontend programma's om deze in een gui te kunnen gebruiken. Te zien in Subsectie 2.3

2.3 Frontend GPG programma's

Cryptophane	Een applicatie voor Windows.
Gajim	Een Jabber client voor GNOME.
GnuPG Shell	Een cross-platform, grafische Frontend voor GnuPG.
GPA	De standaard Frontend voor GPG.
KGpg	GnuPG voor KDE.
Seahorse	GnuPG voor GNOME.
Wija	Een cross-platform jabber client (MacOsX, Linux, Windows).
XAP	Applicati paneel en Bestandsmanager.

Cryptophane Deze wordt gebruikt om te encrypteren, decrypteren, handtekenen, beheer van sleutelhanger en een command-line interface voor GnuPG.



/ tabellen / figuren / lijst van tabellen / lijst van figuren

3 Belangrijke woorden

weergave van moeilijke woorden in tabelvorm