PCLinuxOS Magazine – 2013. november

Írta: YouCanToo



Mi is a Mailvelope? OpenPGP titkosítás webmailhez amit a Mailvelope integrál a webes levelező felületbe. A Mailvelope működik Chrome-mal és Firefox-szal (seaMonkey). A Mailvelope a következő webmail szolgáltatásokkal működik együtt:

Gmail™ GMX™ Outlook.com™ Yahoo!® Mail

Ebben a cikkben a Mailvelope-t Yahoo!® Mail-lel használjuk, Firefox-ban.

A Mailvelope a github oldalán található. (Szerk.: itt.)

Edit Verw Higtory Bookmarks Tools Help	⇔ v Uownload
GitHub This repository Search or type a command © Explore Features Enterprise Blog Sign up Sig	jn in
toberndo / mailvelope	¢ 65
Releases / Tags Prevelease Mailvelope 0.7.0b2	o O N
 ♦ v0 7.002 ♦ districts Set default key size for key generation on Firefox to 1024 ● mathetiges.chrome.zpp ● mathetiges.chrome.zpp ● Source code (zpp) 	m ≁ ⊡ ₽
Pre-reference Mailvelope 0.7.0b1 • statements • statements • statements	
mailvelope.chrome.zip mailvelope.throme.zip mailvelope.throme.zip Source code (zip) trs://sithub.com/tohen/demailvelope.threase.t/dwweloaddol 2 (b)2mailvelope.threase.t/	

Ha letöltötted, a Firefox-hoz úgy adod hozzá, hogy az **Eszközök** → **Kiegészítők**-höz mész. Ott kattints a kis csavarkulcs ikonra a kereső ablak mellett. Ezután válaszd a "Kiegészítő telepítése fájlból"-t.



Menj oda, ahová a mailvelope kiegészítőt letöltötted. Válaszd ki a mailvelope.firefox.xpi fájlt és kattints a "**Megnyitás**"-ra.

<u>P</u> laces	Name	Size Modified A
🛤 Search	🕞 mailvelope.firefox.xpi	1.9 MB 19:17
Recently Used		
💼 linuxguy		
Desktop		
🗒 File System		
🛅 Documents		
i Music		
🚞 Pictures		
🚞 Videos		
Downloads		

A kiegészítőt a Telepítés gombra kattintva telepítjük.



Most már bezárhatod a Kiegészítők ablakot. Megjegyzés: ennek a kiegészítőnek az indításához NEM KELL újraindítani a Firefox-ot.

A mailvelope használatához készítenünk kell egy titkosító kulcspárt. Ehhez kattints a lakat ikonra a Firefox képernyőjén jobbra lent. Ezután kattints a "Options"ra. (a következő olda-

lon, balra fönt)

PCLinuxOS Magazine



Új lap nyílik. Válaszd a "Generate Key"-t.

) 💿 le Edit View History Bookmarks	Mailvelope Opt	ions - Mozilla Firefox	elone/data/common/ii/ontions	ele (
CLOSmail - Login	me Print Sync Svr Mailvelope Options	nailvelope	•	Download
Mailvelope Options Doc	umentation About			©ŝq
KEY RING Display Keys Import Keys	Generate Key			
Generate Key SETTINGS General	Name	Full name of key owner		
Security Watch List	Email			
	Enter Passphrase	Advanced >>	Password is empty	
	Re-enter Passphrase			
		Submit Clear		
D 2012-2013 Mailvelope				v0.7.0b2
			() Q 100%	(unknow

Töltsd ki az üres részeket az adataiddal. Emlékezz, amikor jelszót választasz, olyat használj, amit nem lehet egyszerűen kitalálni és könnyen megjegyezhető. A lenti képernyőképen az Advanced (haladó) gombra rákattintottam. Nem kell semmit megváltoztatnod a haladó fül részénél.

۵	Mailvelope Opt	ions - Mozilla Firefox	
Elle Edit View History Bookmarks Tool Bookmarks Tool Book Forward Reload Stop Home	s Help (🕜 Oresource://j E () Print Sync	id1-ppxxh40gbjawna-at-jetpack/mailvelope/data/comm mailvelope	on/ui/options.html 🔗 🗸
🗌 PCLOSmail - Login 🛛 🕹 🦳 Ma	ilvelope Options 🛛 🔞	14	
Mailvelope Options Document KEY RING Display Keys	ation About		(BR)
ingolar Koys Generata Key SETTINGS General Security Watch List	Name	Youcantoo_Imuxguy Full name of key owner youcantoo_Imuxguy@webmail.com << Advanced	
	Algorithm Key size Expiration	RSA Image: Second	
	Enter Passphrase Re-enter Passphrase	Passwords :	natch
		Submt Clear	
0) 🔍 100% (unknown)

Ha minden rendben van, akkor kattints a "Submit" (elküld) gombra. A titkosítási kulcsaid elkészülnek. Dőlj hátra és lazíts, ez eltarthat néhány percig, vagy tovább.

Key gener	ation in prog	ress		
		i. ji		
			-	
			never 于	
		•••••)
		•••••		Pa
		Clear		

Ha minden rendben lefutott, egy "Success!" üzenetet kell látnod.

	Name	Youcantoo_linuxguy
		Full name of key owner
	Email	youcantoo_linuxguy@yahoo.com
		<< Advanced
	Algorithm	RSA
	Key size	1024 Dits
	Expiration	0 never
Enter Pa	assphrase	•••••
Re-enter Pa	assphrase	Passwords match
Success! Nev	v key genera	ted and imported into key ring

Gondoskodj arról, hogy titkosítási kulcsodról készüljön másolat, amit tégy el egy biztos helyre. Készítenünk kell egy publikus kulcsot is. Ez az a fájl, amit bárkinek, akinek titkosított üzenetet küldesz, megadsz. A publikus kulcs előállításához kattints a "Display Keys"-re képernyő balján.

Display Keys							
Import Keys	ey F	ting					
Generate Key	Export	•	Shov	v keys by type:	All		Ŧ
SETTINGS		Name	Email	Key ID	Creation		
Security	T1	Youcantoo_linuxguy	youcantoo_linuxguy	5DE8AD64	03.10.2013	× Delete	1
Watch List							

Rákattintva jelöld ki az újonnan készített titkosítási kulcsod sorát, majd kattints az "Export"-ra. Ezután a "Display public key"-re kattints.

۵ 🌚			Mailvelo	pe Optio	ns - Mozilla Firefox				90 0
<u>File Edit View</u> Hi	story <u>B</u> ookm	narks Tools Help	o 💿 🛞 🔞 res	ource://jid1	-ppxxh40gbjawna-at-j	etpack/mailvelo	pe/data/comm	non/ui/option	s.html 🗇 🕯
Back Forward R	eload Stop	Home Print	Sync pe Options	<mark>⊠</mark> ~ ma	ilvelope			*	Download
Mailvelope	Options	Documentation	About						@\$q
KEY RING Display Keys Import Keys		Key	/ Ring						
Generate Key		Ð	port -		Sho	w keys by type:	All		•
SETTINGS		D	isplay public key		Email	Key ID	Creation		
Security Watch List		D	end public key b Isplay private ke Isplay key pair	y mail y	youcantoo_linuxguy	5DE8AD64	03.10.2013	× Delete	
© 2012-2013 Mailvo	elope								v0.7.0b2

Gondoskodj arról, hogy a privát kulcsodat SOSE add ki. Ha mégis, akkor bárki, aki megszerezte, képes lesz elolvasni a küldött titkosított e-mail-jeidet.

BEGIN PGP PUBLIC KE	Y BLOCK			^
Version: Mailvelope v0.7.0b	2			
Comment: Email security by	Mailvelope - http://w	ww.mailvelope.com	1	
xo0EUk4tfgEEAJ+Er+BnI4S	ogAaBT1+UvXkg6g	sOTXnui5I SABsri	h8MphV	
TaT7suZ+OFdBRAr9004xc	rh1SvKvikKvzfOteNas	SMUslWaak10hVC	JFIUSr	
/i84iY+1zJzvKv3hs8vGZl0F	n6RX3DEU08JhzWb	HkxzEbWrsP16fK	JxvLsP0	
RIDABEBAAHNMVIvdWNh	bnRvb19saW51eGd1	eSA8eW91Y2Fud	G9vX2xpbnV4	
Z3V5QHlhaG9vLmNvbT7Ci	AQQAQgAEAUCUk4	t3AkQpQPluF3or	NQAAGbBA/0X	
YatPYGiD941Vel+mBgSFl	Icn9yDLom85scQsys	sZfcQjB3pAzdlusE	xfLdpzU	
TjvaxiW09emFwXf5C5h8lLj	eE4BIQWnXswvzbBlj	PzBlucr21ynm4V+	lov/F	
GyE7Fi5J544+Nb89g1c9O	kBLH3IxDXDFJoSGv	vJZKtdHxyd8Ng==		\mathbf{v}
=3+Yk				
Youcantoo linuxquv pub as	c Create file			

A publikus kulcs mentéséhez fájlként kattints a "Create file" gombra.



Ezután kattints a "Download Key" hivatkozásra. A megnyíló ablakban legyen a "Save File" kijelölve és kattints az "OK"-ra. Jegyezd meg, hogy a nyílt kulcsodat hová mentetted, mert később szükséged lesz rá.

Egy utolsó dolog. Kattints a "General" hivatkozásra a bal oldali menüben és győződj meg arról, hogy a Primary Private (elsődleges saját) kulcs van használatban. Ha üres, vagy a kulcs rossz, használd a le nyilat és válaszd a megfelelő "Private key"-t. Ha kiválasztottad a megfelelőt, kattints a Save-re.

General	
Mail Compose Editor Type Primary Private Key	Rich Text Editor Plain Text Inuxguy <youc (allows="" add="" aways="" decrypt="" key="" list="" mails)<="" of="" primary="" recipients.="" sent="" th="" to=""></youc>
Please reload your mail provider tab (F5) to make	te these settings take effect.
Save Cancel	

Mindenképpen frissítsd (Firefox-ban F5) a levelező kiszolgálód honlapját.

Most próbáljuk ki, hogy tudunk-e írni és küldeni titkosított e-mailt. Mivel Yahoo-t használok, a mail.yahoo.com-ot nyitom meg a böngészőmben, a fiókomba belépéshez. Ha már beléptél a fiókba kattints a "Levélírás"-ra. Töltsd ki a "Címzett" és "Tárgy" mezőket, ahogy szoktad. (jobbra, fönt)

Most kattints a kis "papír és ceruza" ikonra a szerkesztő ablakban. (jobbra, középen)

Ezzel megnyílik egy szerkesztő ablak, ahol megírjuk a titkosítandó e-mail-ünket. (jobbra)

Ha befejezted az e-mail-ed szerkesztését, kattints a sárga lakatra a szerkesztő ablak jobb sarkában. Ezzel egy kis ablak nyílik meg. (köv. lap, balra, fönt)







Kattints a "Transfer" (továbbítás) gombra. Ez megjeleníti a titkosított e-mailt. (következő lap, balra lent)

PCLinuxOS Magazine

) 💿	resource://jid1-ppxxh40gbjawna-at-jetpack - Mozilla Firefox	\odot	8
Compo	se Mail	@\$q	1
This is a tes	David Moore < linuxguv@ domain .net>		
	Encrypt for:		
	Delete		
	Ok Cancel S HTML S Text		
			/ .
	Cancel	Transfer	



Compos	se Mail				@\$q
BEGIN F	GP MESSAGE-				
Version: Maily	elope v0.7.0b2				
Comment: Er	mail security by N	Mailvelope - http:	//www.mailvelope	.com	
IND MARZOLI				PDDCar ATaMb	aD.
	SDKKVW9AQI9G	-OldUbD1/ml	QUORINJAE0904V		ar
			ANPWIZE/VKQI4I	15X4+11K8KA3	
			TAIC90E3IIJ4KyV		07/
Ac2n/24ilab7	CoNakTGTI foEt				02/
4551 y54 j1dD7	Celva 70 LICFL	a/czDtCAcrYiv/8	Dfnu6muEvAifNvE		
					~
TINUMARIXQUI	VIILENGAC53T	R41L49/4//100	euDDyeJ+5CHOF		

Most visszatérünk a Yahoo szerkesztő ablakához és láthatóvá válik a titkosított üzenet.



Most kattints a "Send"-re az e-mail elküldéséhez.

A példámban, az egyik teszt fiókomból küldtem emailt. Először importálnom kellett a nyilvános kulcsomat, amit korábban a Thunderbird-höz mentettem el. Egyszerűen kettőt kattintottam a kulcs fájlon és megadtam, hogy a Kpgp-ben nyissa meg, és automatikusan importálta a kulcsot. A Kpgp már telepítve van a PCLinuxOS-ben.

A Thunderbird-ben a "Get mail" (letöltés) gombra kattintottam és láss csodát, kaptam egy üzenetet a Yahoo fiókomtól.

Amikor az új üzenetre kattintottam, rövid ideig a felbukkanó titkosított, később a visszafejtett tényleges üzenetet láttam. (jobbra, fönt)

Megpróbálok válaszolni a titkosított üzenetre. Ezért a "Replay" (válasz) gombra kattintottam, megírtam a választ, lenyomtam a "Send"-et. (jobbra, középen)

Néztem, ahogy a program titkosította a válaszomat és elküldte. A folyamat nagyon gyorsan játszódik le.

Visszalépve a Yahoo fiókomba, rákattintottam a

			_							
Get Mail 👻 📝	Write	Chat	Addre	ess Book	🚫 Tag 🗸	🕼 Decrypt	A Quick Filt	er		=
linuxguyoor	re.net	🛠 Quid	k Filter:		300		Filter the	se messages	<ctrl+< td=""><td>Shift+K></td></ctrl+<>	Shift+K>
Sent		1 * 0	si Subje	ct		00	From		Date	× 0.
📅 Trash		2 B	sav w	hat		0	David Moore	0	09:49 F	РМ
Local Folders			test	encrypted	email	•	David Moore		10:47 6	РМ
ा Trash 襘 Outbox		OpenPG	P Decryp	ted messa	age	• Reply	+ Forward	Rechive	é lunk	Details ✓
			Dana							
		Subject	test en	crypted e	email				6	10:47 PM
		Reply to	David Mo	ore 😭					_	-
		т.	Math						Othe	er Actions v
		10	men						oun	
) Gle Edit ⊻iew C Send V Send From: - To:	Options elling ~ David M & youc	Ope <u>n</u> PG Ø Atta loore <lir antoo_lin</lir 	Write P <u>T</u> ools ach v muxguy@f muxguy@y	e: Re: tes <u>H</u> elp OpenPC indmoore.l ahoo.com	st encrypte SP v 🔒 S/ net> linuxg	ed email MIME 🗸 🔚	Save V			
<u>S</u> ubject:	Re: tes	t encryp	ted email					-		
On 10/03/2013 10:- > This is a encryp > I got your encryp:	47 PM, D ption em	avid Moon ail test l Yea	re wrote: from Yaho ah	00						

frissítés gombra és csodák csodájára kaptam egy válaszüzenetet.

🗹 Compose –	Ē.	Delete 🕴 🔶	*	+	Move -	😵 Spam –	
Inbox (1)	合樂	American Air	. The	New Am	erican is A	Sponsored	
Drafts		SORT BY DATE					
Sent		David Moore	🛧 Re: t	est encr	rypted email	11:08 PM	î î

Az üzenetre kattintva egy titkosított üzenet fogadott. (következő lap, balra, fönt)

Az egérmutatót az ablakba húzva látod, hogy kulcsra változik. A "lakat"-tal jelölt ablakban bárhová kattintva a kulcs ikonnal, a "Key unlock" ablak nyílik meg és kérni fogja a jelszót. Beírás után az "OK"-t kell nyomni.

Kis ideig dolgozik, majd megjelenik az üzenetem.



Gratulálok, most már képes vagy küldeni és fogadni titkosított e-mail-eket a Yahoo!® Mail-től.

Does your computer run slow?

Are you tired of all the "Blue Screens of Death" computer crashes?



Are viruses, adware, malware & spyware slowing you down?

Get your PC back to good health TODAY!





Re: test encrypted email

Key unlock

User ID:

Key ID:

Password:

Key unlock

User ID:

Key ID:

Password:

0

from David Moore to you

resource://jid1-ppxxh40gbjawna-at-jetpack - Mozilla Firefox

linuxguy <youcantoo_linuxguy@yahoo.com>

Remember passwords for this session

resource://jid1-ppxxh40gbjawna-at-jetpack - Mozilla Firefox

linuxguy <youcantoo_linuxguy@yahoo.com>

Remember passwords for this session

45B39EF30F311912

.....

45B39EF30F311912

Please enter.

11:08 PM

1hN4H

NaYUB a/X4r E.ZvBGi2t W9YVqYgh MPXhiM

E4WWu

7MO

@\$q

Cancel

Cancel

@\$q

 \odot

 \odot \odot \otimes