# Email titkosítása Thunderbird-ben

## PCLinuxOS Magazine – 2013. november

### Írta: YouCanToo

A "big brother" és mások mellett, akik egyre jobban kutakodnak a személyes életünkben, hogyan nyerhetnénk vissza valamennyit a magánéletünkből?



Egyik módja az e-mail-jeink titkosítása és a többiek felvilágosítása, hogy miért kell hasonlóképpen cselekedniük. A cikk bemutatja, hogyan állítsd be a Thunderbird-öt (Linux, Windows és Mac OS X – 32, vagy 64 bit) GnuPG-t és enigmail kiegészítőt használva.

Kiindulásképpen nyissuk meg a Thunderbird-öt. Amikor nyitva van, kattintsunk az "**Eszközök** → **Kiegészítők**"-re. A keresőablakban keressünk az "enigmail"-re. Válaszd ki és kattints a telepítésre.

i>		erigmail ~ تلو	
		Név Utoljára frissitve TLe	jobb egyezés
🔍 Keresés	Ker	esés: 🗉 Saját kiegészítők 📧 Elérhető kiegészítők	
📥 Kiegészítők letöltése		Enigmail 1.6 OpenPSP message encryption and authentication for Thurderbird and SeaMorkey. <u>Toylob</u>	2013-10-2
🚓 Kiterjesztések		X-notifier (for Gmail,Hotmail,Yahoo,AOL) 3.3.9	2013-10-2
🗿 Mercielenés	~	Notifier for gmail, yahoo, hotmail, aol and more webmails.X-notifier(aka WebMa Tovibbe	H Telepítés
. megjelenes		Mail Merge 3.6.0	2013-10-1
Bővítmények		Mass Mail and Personal Mail Towabb	🖬 Telepítés
🔯 Nyelvek	2	Mail Redirect 0.7.8	2013-10-2
	-	Allow to redirect (a.k.a. "bounce") mail messages to other recipients Toxibb	🖬 Telepítés
		MailHops 0.8.2	2012-10-2
		MailHops maps the route an email took to get to you. Displaying the senders I <u>Tovibb</u>	Telepítés
		EditEmailSubject 2.0.3	2013-04-0
		This module allows you to change email subjects <u>Towabb</u>	Telepítés
	29	Display Mail User Agent 1.6.9	2012-07-1
		Displays icon for user agent of received mails. Tovable	Telepités
	÷	Mailbox Alert 0.16.4 Mailbox Alert allows you to specify, for each separate mail folder, a message, s Toxibb	2013-11-1 Telepítés
		Az összes (56) eredmény megjelenítése	

Amikor letelepült, kattints az "újraindítás most"-ra. Ezzel a Thunderbird újraindul az új Enigmail kiegészítővel. Megjegyzés: az Enigmai kiegészítő csak Thunderbird-del, IceDove-val és Seamonkey-val működik.



A Thunderbird újraindulása után észre kell venned az új, "OpenPGP" elemet a felső sorban. Kattints az "OpenPGP"-re és válaszd ki a "Beállítás varázsló"-t

🖄 Beérkezett üzenete 👌 🍓 Kiegész	Visszafejtett üzenet mentése						•
Letőltés 👻 📝 Új üzenet 🌻 Cseveg	Beállítások OpenPGP Kulcskezelő		Visszafejtés 📣	Gy	orsszűrő		≡
🛎 Local Folders	open of Bacherero	•	Feladó	•	Dátum v	Méret	1.03
🖄 Beérkezett üzenetek	<u>S</u> úgó	5	KütyüBazár hu	0	2013-11-0	8.6	KB ^
Piszkozatok	Beállítás Tündér		HIX GURU	0	2013-11-0	17.0	кв
🛽 Sablonok	Az Enigmail néviegye		HIX GURU	0	2013-11-0	11.0	кв
📕 Elküldött elemek	FWG: FWG: EQV KIS		Török Árpád	0	2013-11-0	4.5	кв
Þ 튆 Archívum	*** HIX GURU ***	0	HIX GURU	0	2013-11-1	13.3	кв
🛅 Törölt elemek	Fwd: Fwd: FW: Idái	0	Török Árpád	0	2013-11-1	9,8	кв
🖄 Postázandó üzenetek		0	David Pocsi	0	2013-11-1	6.7	кв
🚞 Adi	*** HIX GURU ***	0	HIX GURU	0	2013-11-1	12.7	кв
AEGON	Beépíthető készül	0	Bemutatótere	0	2013-11-1	291	кв
🚞 Âgyf©lkapu	Csatlakozzon kárm	0	Aegon Biztosító	0	2013-11-1	122	кв
Barsony	*** HIX GURU ***	0	HIX GURU	0	2013-11-1	12.9	кв
🛅 Birinyi	Fwd: FW: naaagyo	0	Török Árpád	0	2013-11-1	75.5	кв
🛅 Csaszar	🗇 🖉 🛛 Fwd: FW: Fwd: Akt	0	Török Árpád	0	2013-11-1	4.1	мв
🗢 🛅 David	Fwd: Fw: Vicces	0	Török Árpád	0	2013-11-1	5.1	кв
UPC							
🛅 Digi							
🛅 ELMŰ							
ESET Antispam							
マ 🛅 Full Circle							
Togadott							
🛅 Küldött							
🛅 Guru							
🛅 ING							
🚞 Kubuntu							
🚞 Linux							
🚞 Margareta 👘							
🚞 Markiel							
🛅 МКВ							
MMEX							
🛅 Mozilla							
Nordtelekom							
🗢 🛅 janu							
E Forgadatt							
royauott							

#### Most végigmegyünk a lépések zömén.

Q.C.	<b>(</b>	OpenPGP Beállítás Tündér
Oper	nPGP Beál	lítás Tündér első lépése
	A követke nyújt segí beállításol megválasz végrehajto	ző néhány lépés a kezdő OpenPGP használók számára tséget az első lépésekben, illetve a kezdeti knál. A képernyőn kérdések jelennek meg, amelyek odását követően, a beállítások automatikusan ódnak.
	El kívánja	indítani a Beállítás Tündért?
	• Igen, sz	eretném ha a Tündér segítene a beállításokban
	Unem, In	kabb sajat magam antom be a programot
		Ø Mégse → Tová

Az alapbeállításokat használjuk itt. Kattints a Next-re.

9	OpenPGP Beállítás Tündér 🛛 📀 🗞 😵
<b>Aláí</b> Kime	<b>rás</b> enő üzenetek aláírása
	OpenPGP lehetőséget biztosít a levelek digitális aláírására. Ez ahhoz hasonló, mint amikor egy levelet aláírunk, csak itt digitális formában történik. Ez alapján ellenőrizhető, hogy a levél valóban a feladótól érkezett-e. Biztonsági szempontból ajánlott bekapcsolni, hogy minden kimenő levél aláírásra kerüljön.
	Kéri a kimenő üzenetek alapértelmezés szerinti aláírását?
	<ul> <li>Igen, az összes kimenő üzenet aláírása</li> </ul>
	. Nem, címzettek szerinti szabályokat készít azoknak, akiknek szóló üzeneteket alá kell írni
	ØMégse

NEM AKARJUK az összes e-mailt aláíratni, tehát válasszuk a "No"-t, majd **Next**.

### Email titkosítása Thunderbird-ben

Itt engedélyezzük a programbeállítónak, hogy végrehajtsa a kellő változtatásokat a Thunderbird beállításaiban, ezért válaszd az "Igen"-t. Rákattintottam a "Részletek" gombra, hogy meggyőződjem, a "Ne hozzon létre html üzeneteket" be van-e jelölve. Kattints OK-ra. A részletek ablak bezáródik. Most kattints a "**Next**"-re.

Beállítások E-mail beállítások megváltoztatá Ez a Tündér megváltoztath róla, hogy az e-mail üzenet Az alkalmazandó beállításo változás, hogy az üzenetíra	sa az OpenPGP megbízhatóbb működésének érdekében atja a postafiók beállításait. Kérem bizonyosodjon meg tek alárísa és titkosítása jól működik ezen a számítógépen. k elősorban technikai jellegűek, az egyetelne észrevehető ás alapértelmezett formátuma síma szöveg lesz.
Szeretne változtatni néhár megbizhatóbban működjör • Igen Részletek, Köszönöm, nem kére	y alapértelmezett beállításon, hogy az OpenPGP a számítógépén? Beállítások • • • • • • • • • • • • • • • • • • •
	<ul> <li></li></ul>
	⊘Mégse

Most elkészítjük az OpenPGP-kulcsunkat. Legyen a "Szeretnék készíteni egy új kulcspárt…" sor kijelölve. Ha már van kulcspárod és használni akarod, akkor válaszd a másik lehetőséget, a létező kulcsok importálására. Ha a kijelölés rendben, kattints a "**Next**"-re.

A kulcsod elkészítésének első lépése, hogy beállítasz egy jelszót. Olyat válassz, amire emlékezni fogsz, de nem található ki egykönnyen. Amikor beírtad a jelszót, kattints a "**Next**"-re.

Most lehetőségünk van átnézni, hogy miket fogunk használni a következőkben. Ismét "**Next**".

Ha már a varázsló elkészítette a kulcsaidat, feldob egy ablakot, amivel készíthetsz egy visszavonási tanusítványt. Az tanusítvány elkészítése javasolt. Kattints a "Tanusítvány elkészítése"-re.

A fájlkezelő nyílik meg, lehetővé téve, hogy



kiválaszd, hová mentse a visszavonási tanusítványt. Ha kiválasztottad a mentés helyét, kattints a **men-tés**-re. Egy ablak bekéri a korábban kitalált jelszót.

pinentry-qt4	$\odot$	۲
You need a passphrase to unlock the secret k "David Moore <linuxguy@ "<br="" domainname.com="">2048-bit RSA key, ID 5AC9A1F4, created 2013</linuxguy@>	ey for u 3-10-01	ser:
Passphrase ******		
<u>K</u>	Cance	el

Amikor beírtad a jelszavadat, kattints az **OK**-ra. A varázsló bezár és a Thunderbird-ben találod magad.

Most meg kell néznünk, hogy minden úgy működik, ahogy kell.

Kattints az "Új üzenet" fülre, e-mail készítéséhez. Az írás párbeszédablakban kattints az **OpenPGP** fülre. Ellenőrizd az **aláírás** és **titkosítás** négyzeteket.

4			iras: (nincs targy)	
<u>F</u> ájl S <u>z</u> erkesztés <u>N</u> ézet <u>B</u> eáll	ítások	OpenPGP <u>E</u> szközök	<u>S</u> úgó	
🔟 Küldés 🛛 🍄 Helvesírás 🗸	Ø Mel	✓ Üzenet <u>a</u> láírása	Ctrl+Shift+S	
		✓ Üzene <u>t</u> titkosítása	Ctrl+Shift+P	
Fel <u>a</u> dó:	Török	PGP/MIME e-mail fo	ormátum <u>h</u> asználata a levélben	
Clinzett:	<u> </u>	OpenPGP Kulcskeze	elő	
		Titkosítás visszavo	nása	
		📄 Sajá <u>t</u> nyilvános kul	cs csatolása	
<u>T</u> árgy:		Súgó		

Most készítsd el az e-mail-edet, ahogy szoktad.

<b>a</b>	Írás: Thunderbird titkosítás ellenőrzése
<u>F</u> ájl S <u>z</u> erkesztés <u>N</u> ézet <u>B</u> eállí	tások <u>O</u> penPGP <u>E</u> szközők <u>S</u> úgó
🔣 Küldés 🛛 👋 Helyesírás 🗸 🍘	🖉 Melléklet 🔻 🔒 OpenPGP 👻 🔷 S/MIME 👻 🔚 Mentés 👻
Fel <u>a</u> dó:	Török Árpád
Címzett:	8
<u>T</u> árgy:	Thunderbird titkositas ellenorzese
A titkosítás működik-e, vagy sem	
A titkositas mukooik-e, vagy sem	

Amikor kész vagy az e-mail írásával, menj tovább és kattints a **Küldés**-re. Ekkor kérdezni fogja, hogy melyik tanúsítványt akarod használni. Legyen a megfelelő tanúsítvány kiválasztva és utána **OK**.

<u> </u>	PGP-k	ulcsválasztás				00
Címzett nem érvén valami@freemail.hu	yes, megbízható v	agy nem talá	ható			
Válassza ki a címze	tteket a titkosítá	shoz				
Postafiók / Felha	sználói azonosító		Megb	Lejá	Kulcsa	: m :
🗹 Török Árpád <		>	teljesen	. 2018-1	. 687D34FC	
Levél titkosítatlan k	cüldése					
Kulcslista frissítése	Hiányzó kulcsok ir	mportálása				
Szabályok létrehozás	a a címzettekhez			🔗 Mégs	se 🖌 🖌 🗸	ж

Még egyszer kérheti újra a titkosítási kulcsodat az email elküldése előtt. Ennél a pontnál látod a rendes szövegedet eltűnni és a titkosított üzenetet feltűnni. Ez a rész nagyon gyorsan lezajlik.



Ezután én ellenőriztem az e-mail fiókomat, ahová elküldtem a titkosított üzenetemet. Igen, megérkezett az üzenet.

🖞 Letöltés 👻 📝 Új üzenet 📃 Csev	vegés 🛄 Cín	njegyzék 🕐 Címke v 🕼 Visszafejtés 🏟 Gyorsszűrő	
Local Folders	1 * @	Tárgy	
Piszkozatok		*** HIX GURU *** #5517	
Templates		[unu-kezdo] Skype out 2x	
Elküldött elemek		[moznia_nu] meetya/ munderbird + levelszemet kezeles	
Archivum		ke: [uhu-kezdo] X ujrakoniguralasparancssorbor	
Törölt elemek		fund-kezdőj kyet sebesseg konacozasa	
🖄 Postázandó üzenetek		Re: [mozilia_nu] Thunderbird + levelszemet kezeles	
Adi		[mozilia_hu] muhderbird + levelszenlet kezeles	
AEGON			
Agyf©lkapu			
Barsony			
Birinyi			
Csaszar			
🗢 🛅 David			
UPC			
🛅 Digi			
🛅 ELMŰ			
ESET Antispam			
🗢 🛅 Full Circle			
Fogadott			
🛅 Küldött			
🛅 Guru			
ING .			



Miért néz így ki, nem tudom elolvasni? Az ok az üzenet fejlécében olvasható: "titkos kulcs kell az üzenet kibontásához". Úgy tűnik, nem küldtem el a publikus kulcsomat. A kulcsot több úton is elküldhetem.

- 1. elküldöm az e-mail-lel.
- 2. a kulcsot fájlba exportálom és elküldöm.
- 3. exportálom egy kulcskiszolgáló szerverre.

Most az e-mail-lel együtt küldöm. Tehát menjünk vissza és küldjünk egy másik e-mailt, de ez alkalommal gondoskodom a publikus kulcs csatolásáról.

Készítek még egy e-mailt. Most, az OpenPGP fülre kattintva, nem csak az üzenet **aláírását** és **titkosítását** választom, hanem a "**Saját nyílvános kulcs csatolása**"-t opciót is. A Küldés-re kattintva egy párbeszéd nyílik, kérdezve hogyan akarod a csatolmányt (a nyilvános kulcsodat) kezelni. Válaszd az alapbeállítást. Utána **OK**.

🔊 💿 💿 OpenPGP kérdés 💿 💿 💿
Az üzenet mellékleteket tartalmaz. Hogyan szeretné titkosítani/aláírni?
<ul> <li>Üzenettörzs titkosítása/aláírása, de a mellékleteké nem</li> </ul>
A mellékleteket egyenként titkosítása, majd az üzenetet beágyazott PGP-vel küldése
Az egész üzenet titkosításra/aláírásra, és PGP/MIME formátumban küldése
Megjegyzés: PGP/MIME formátum csak néhány levelezőprogramban használható. Windows alatt csak a Mozilla/Thunderbird, Sylpheed, Pegasus és Mulberry támogatja ezt a szabványt; Linux/UNIX és Mac OS X legjobban elterjedt levelezőprogramjai támogatják. Ha nem biztos benne, válassza a második lehetőséget.
Ezentúl a kiválasztott művelet legyen alkalmazva a mellékletekre.
Ø Mégse ✔ OK

A jelszó bekérése után az e-mailt elküldi. Ismét megnézem a másik fiókomat, hogy lássam, mit kaptam. Siker. A Thunderbird megkapta és kibontotta az elküldött e-mailt. Most már sikerült mind küldenem, mind fogadnom titkosított e-mailt.

Most, a világod kicsiny zuga valamivel jobban rejtett a kíváncsi szemektől, hála a Thunderbird-nek, a GnuPG-nek és az Enigmail kiterjesztésnek.

Az Enigmail kiegészítőről további dokumentumokat olvashatsz az Enigmail honlapján.

## Email titkosítása Thunderbird-ben



0