What is PGP Encryption and How Does It Work?

Pretty Good Privacy (PGP) is an encryption system used for both sending encrypted emails and encrypting sensitive files. Since its invention back in 1991, PGP has become the de facto standard for email security.

- The popularity of PGP is based on two factors:
- The first is that the system was originally available as freeware, and so spread rapidly among users who wanted an extra level of security for their email messages.
- The second is that since PGP uses both symmetric encryption and public-key encryption, it allows users who have never met to send encrypted messages to each other without exchanging private encryption keys.

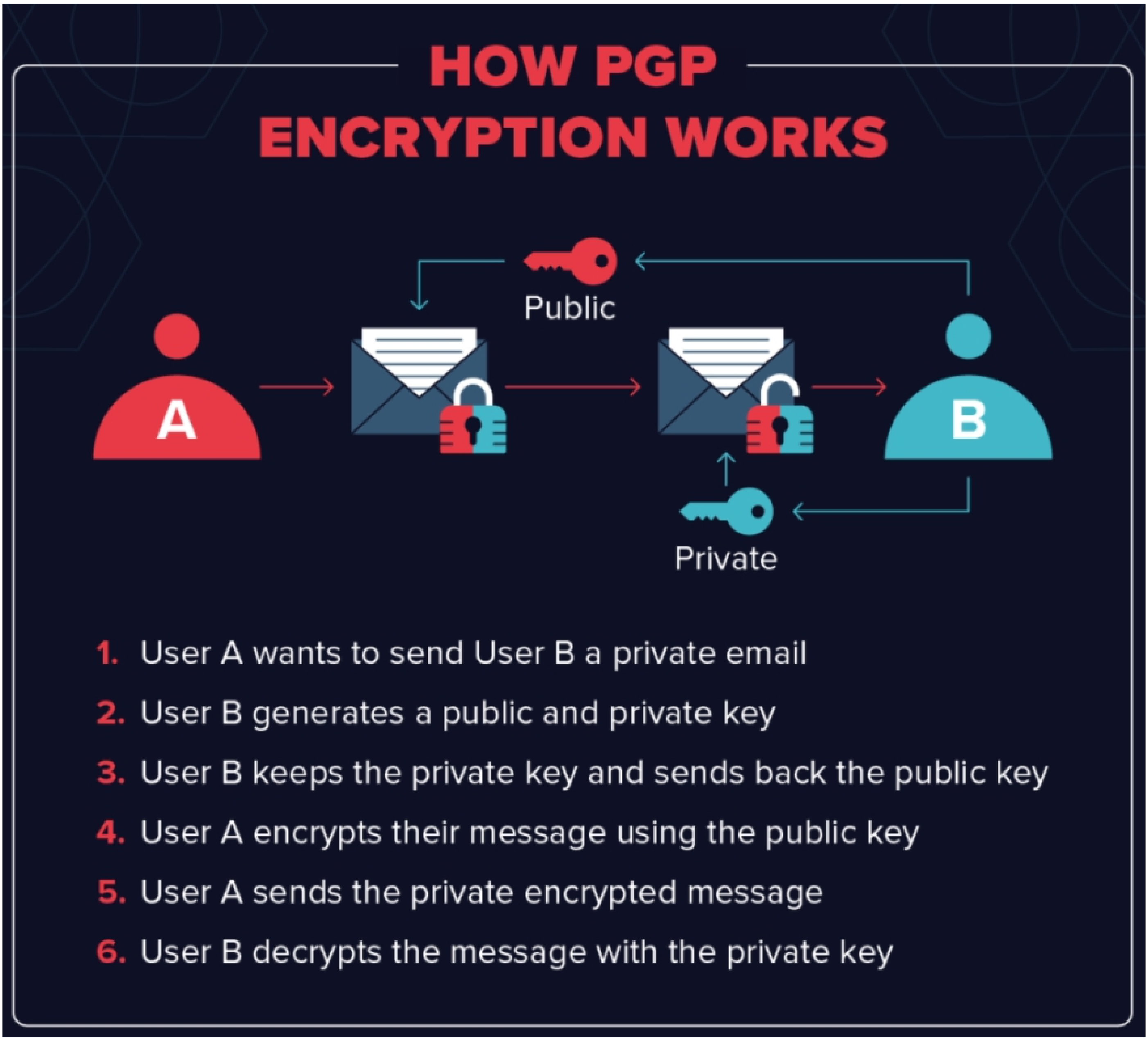
How Does PGP Encryption Work?

PGP shares some features with other encryption systems you may have heard of, like Kerberos encryption (which is used to authenticate network users) and SSL encryption (which is used to secure websites).

At a basic level, PGP encryption uses a combination of two forms of encryption: symmetric key encryption, and public-key encryption.

At the highest level, this is how PGP encryption works:

- First, PGP **generates a random session key**. This key is a huge number that cannot be guessed, and is only used once.
- Next, **this session key is encrypted**. This is done using the public key of the intended recipient of the message. The public key is tied to a particular person's identity, and anyone can use it to send them a message.
- The **sender sends their encrypted PGP session key to the recipient**, and they are able to **decrypt it using their private key**. Using this session key, the recipient is now able to decrypt the actual message.



HOW PGP ENCRYPTION WORKS

1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

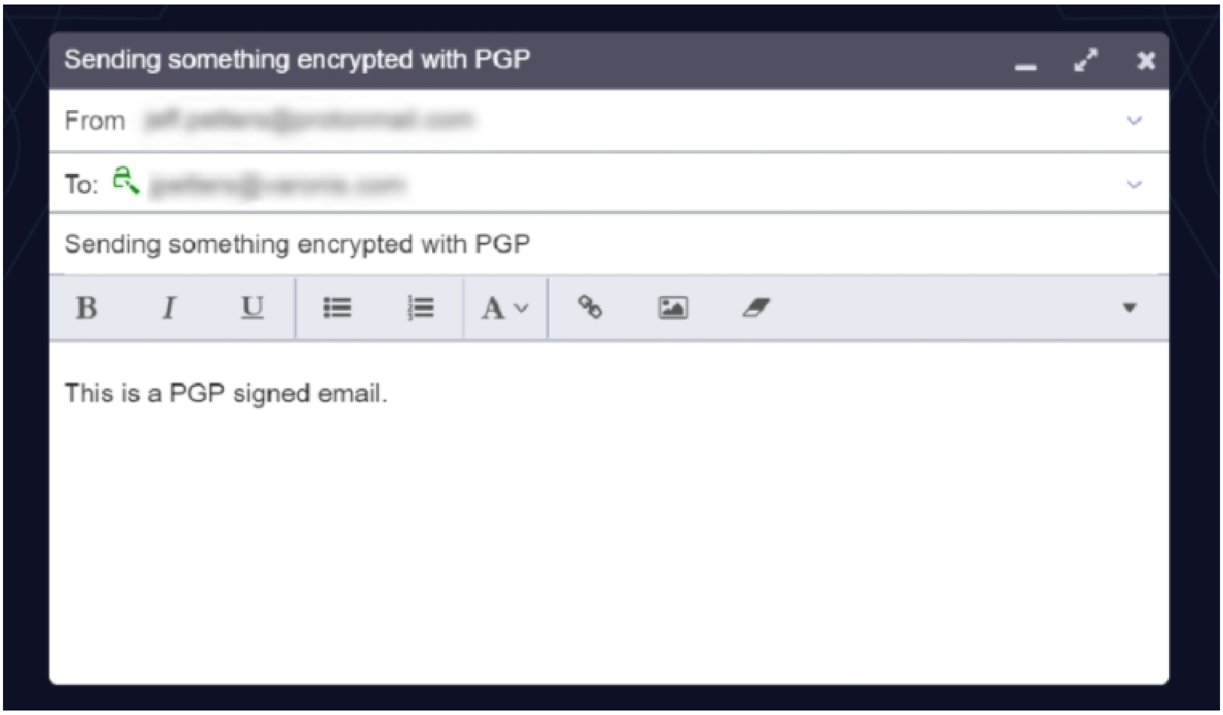
This might seem like a strange way to do things. Why would we encrypt the encryption key itself?

Well, the answer is pretty simple. Public key cryptography is much, much slower than symmetric encryption. Using symmetric encryption requires, though, that a sender share the encryption key with the recipient in plain text, and this would be insecure. So by encrypting the symmetric key using the (asymmetric) public-key system, PGP combines the efficiency of symmetric encryption with the security of public-key cryptography.

Example of PGP Encryption in Action

In practice, sending a message encrypted with PGP is simpler than the above explanation makes it sound. Let’s take a look at ProtonMail – as an example.

ProtonMail natively supports PGP, and all you have to do to encrypt your email is to select Sign Mail. You will see a padlock icon on the subject line of their emails. The email will look like this (the email addresses have been blurred for privacy reasons):



Sending something encrypted with PGP

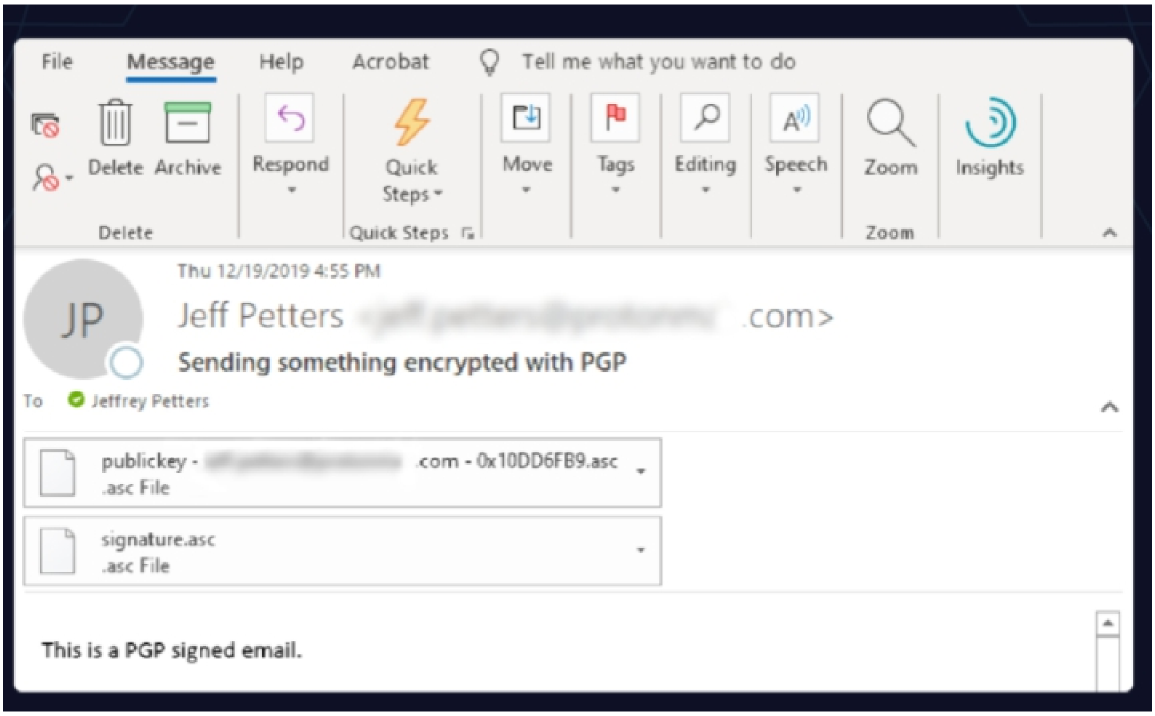
From [redacted]

To: [redacted]

Sending something encrypted with PGP

This is a PGP signed email.

ProtonMail – like most email clients that offer PGP – hides all of the complexity of the encryption and decryption of the message. If you are communicating to users outside of ProtonMail, you need to send them your public key first.



Thu 12/19/2019 4:55 PM

Jeff Petters <[redacted].com>

Sending something encrypted with PGP

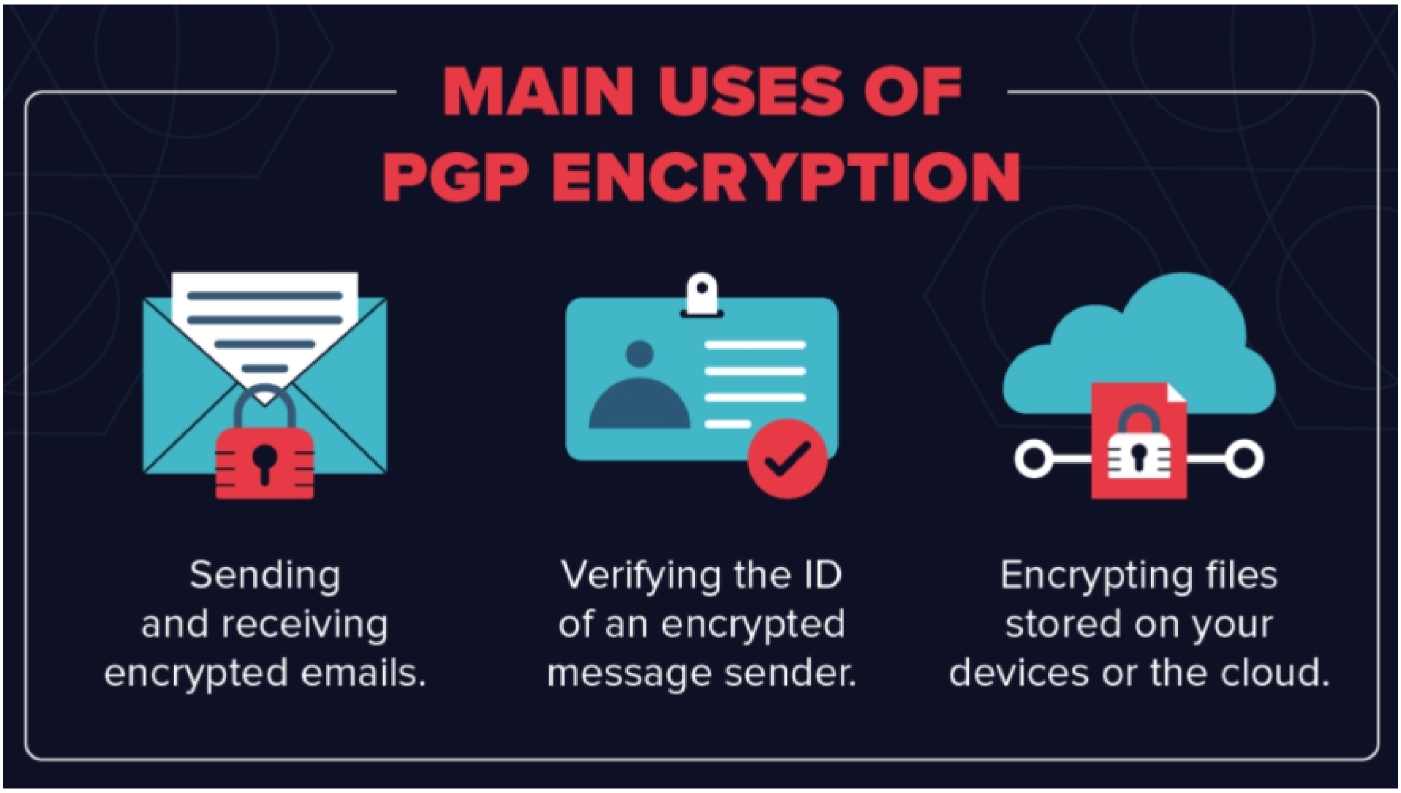
To Jeffrey Petters

publickey - [redacted].com - 0x10DD6FB9.asc
.asc File

signature.asc
.asc File

This is a PGP signed email.

Uses of PGP Encryption


MAIN USES OF PGP ENCRYPTION
Sending and receiving encrypted emails.
Verifying the ID of an encrypted message sender.
Encrypting files stored on your devices or the cloud.

There are, essentially, three main uses of PGP:

- Sending and receiving encrypted emails.
- Verifying the identity of the person who has sent you this message.
- Encrypting files stored on your devices or in the cloud.

Of these three uses, the first – sending secure email – is by far the dominant application of PGP. But let's take a brief look at all three

Encrypting Emails:

As in the example above, most people use PGP to send encrypted emails. In the early years of PGP, it was mainly used by activists, journalists, and other people who deal with sensitive information. The PGP system was originally designed, in fact, by a peace and political activist named Paul Zimmerman, who recently joined Startpage, one of the most popular private search engines.

Today, the popularity of PGP has grown significantly. As more users have realized just how much information corporations and their governments are collecting on them, huge numbers of people now use the standard to keep their private information private.

Digital Signature Verification:

A related use of PGP is that it can be used for email verification. If a journalist is unsure about the identity of a person sending them a message, for instance, they can use a Digital Signature alongside PGP to verify this.

Digital signatures work by using an algorithm to combine the sender's key with the data they are sending. This generates a "hash function," another algorithm that can convert a message to a block of data of fixed size. This is then encrypted using the sender's private key.

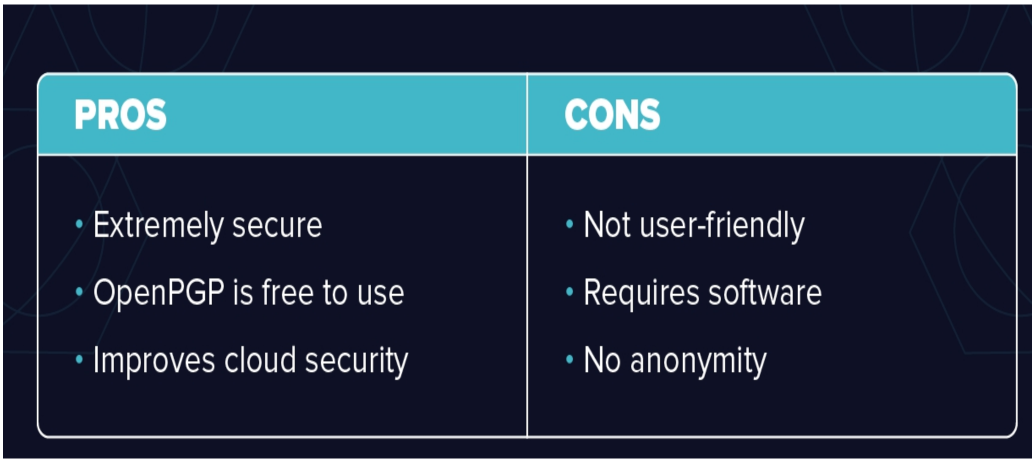
The recipient of the message can then decrypt this data using the sender's public key. If even one character of the message has been changed in transit, the recipient will know. This can indicate either the sender is not who they say they are, that they have tried to fake a Digital Signature, or that the message has been tampered with.

Encrypting Files:

A third use of PGP is to encrypt files. Because the algorithm used by PGP – normally the RSA algorithm – is essentially unbreakable, PGP offers a highly secure way of encrypting files at rest, especially when used alongside a Threat Detection and Response Solution. In fact, this algorithm is so secure that it has even been used in high-profile malware such as the CryptoLocker malware.

Back in 2010, Symantec acquired PGP Corp., which held the rights for the PGP system. Since then, Symantec has become the dominant vendor of PGP file-encryption software through such products as Symantec Encryption Desktop and Symantec Encryption Desktop Storage. This software offers PGP encryption for all your files, whilst also hiding the complexities of encryption and decryption processes.

Do I Need Pretty Good Privacy Encryption?



PROS	CONS
• Extremely secure • OpenPGP is free to use • Improves cloud security	• Not user-friendly • Requires software • No anonymity

Whether you need to use PGP encryption will depend on how secure you want your communications (or files) to be. As with any privacy or security software, using PGP requires that you do a little more work when sending and receiving messages, but can also dramatically improve the resilience of your systems to attack.

Let’s take a closer look.

Pros of PGP Encryption:

The major pro of PGP encryption is that it is essentially unbreakable. That’s why it is still used by journalists and activists, and why it is often regarded as the best way of improving cloud security. In short, it is essentially impossible for anyone – be they a hacker or even the NSA – to break PGP encryption.

Though there have been some news stories that point out security flaws in some implementations of PGP, such as the Efail vulnerability, it’s important to recognize that PGP itself is still very secure.

Cons of PGP Encryption:

The biggest con of PGP encryption is that it is not that user-friendly. This is changing – thanks to off-the-shelf solutions that we will come to shortly – but using PGP can add significant extra work and time to your daily schedule. In addition, those using the system need to be aware of how it works, in case they introduce security holes by using it incorrectly. This means that businesses considering a move to PGP will need to provide training.

For that reason, many businesses might want to consider alternatives. There are encrypted messaging apps like Signal, for instance, that offer encryption that is more straightforward to use. In terms of storing data, anonymisation can be a good alternative to encryption and can be a more efficient use of resources.

Finally, you should be aware that PGP encrypts your messages, but it doesn’t make you anonymous. Unlike anonymous browsers using proxy servers or working through a VPN to hide your true location, emails sent through PGP can be traced to a sender and recipient. Their subject lines are not encrypted either, so you shouldn’t put any sensitive information there.