Secure email?

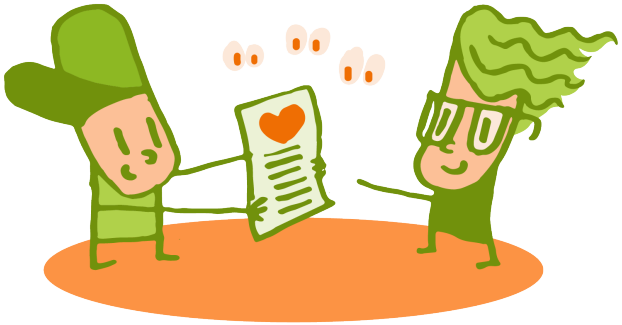
Guide for users

[INDEX]

Contents

1 SECURE EMAIL?

Mail, unlike the web, travels unprotected over the internet. We can protect our messages from modifications that alter our messages (signing) or protect them so that they can only be decrypted by the recipient of our message (encrypt).



[INDEX]

2 ENCRYPTION CONCEPTS (CRYPTOGRAPHY)

Key (key): a text which can contain all kinds of characters. Using a cryptographic algorithm, you can transform another text (encrypt or decrypt). Who knows the key determines who can encrypt or decrypt and who cannot.

Encryption algorithm (encryption): the procedure that transforms information from a readable format, plaintext, into an unreadable format, ciphertext. The operations are called **encrypt** and **decrypt**.

If the algorithm is **symmetric**, sharing the key allows a message encrypted with the key to be decrypted using the same key. In the key metaphor, all copies of a key can open and close boxes (ciphertext) that contain the readable (unencrypted) text.

If the algorithm is **asymmetric**, two **complementary keys** are needed: what one encrypts can be decrypted by the other. When generated, if one is made public and the other is not, they are called the **public key and the private (secret) key**. In the key metaphor, we have a **private key** and publicly available **open padlocks**. Anyone can lock a box containing readable text to generate encrypted text. The padlock can only be opened (decrypted) by the person who has the private key, which must not be shared with anyone (secret).

Therefore, **our private key should never be shared with anyone**, which is why it is also called a secret key, because we give you the ability to use that key on your own. **We always have to**

What is an algorithm?

In mathematics, logic, computer science, and related disciplines, an algorithm is a defined, unambiguous, ordered, finite set of instructions or rules that typically allows one to solve a problem, perform a computation, process data, and perform other tasks or activities.

In everyday life, algorithms are frequently used to solve specific problems. Some examples are user manuals, which show algorithms to use a device or the instructions a worker receives from his employer. Some examples in mathematics are the multiplication algorithm, the division algorithm to calculate the product, and the quotient of two numbers.

Wikipedia - https://en.wikipedia.org/wiki/Algorithm

share our public key because no one can send us messages if it is not made public. Metaphorically, we have to give away open padlocks so that our private key can open them.

Summary function: any function used to calculate from data of arbitrary length a result of fixed size. For example, the remainder of division by 100 (modulo 100) always generates a result between 0 and 99 for integers with any number of digits: the modulus is a compact representation of an integer. Furthermore, a good summary function should be fast to compute and difficult to reverse (i.e., find matching entries from a summary).

The **public key fingerprint** is a short sequence of bytes that identifies a longer public key. It is the result of a hash function of the public key.

For example:

The key for leandro@pangea.org is 4096 bytes long, and its fingerprint (or digest) is:

3987 0457 1F85 B6D9 6551 D827 260C 3E8C 8E9E CEC6

3

MESSAGE PROTECTION

Sign: make it easier for anyone to verify the integrity of a message (content) and its authenticity (sender), **adding** a value to the text that allows **verifying** that the set has not changed.

Encrypt: allow only one person to read it (extract the readable message from an encrypted message), **substituting** the readable text for an encrypted one.

For example, if Ann wants to send a message to Blanca:

Sign:

Ann can prepare her message: her address (identity) and the text to send. The message is passed through a digest function, and the result is encrypted with your private key. This is the signature, which is added to the message.

Therefore, Blanca and any other person will be able to read the text and will also be able to verify its integrity: she can apply the digest function to it and decipher the signature. If both digests match, the message has not been altered.

Therefore, **we sign** our messages with **our private key** (not with the recipient's, since it is our signature).

[INDEX]

Encrypt:

Ann wants to send a message that only Blanca can read. Ann looks up Blanca's public key and encrypts the message, which replaces the readable text. If no one but Blanca has her private key, only Blanca can decrypt it.

Therefore, we **encrypt** our messages with the **recipient's public key**.

3.1 How to publish our public key?

We can **publish it** on a public key server (associated with our email address). We may also include our public key in any message we send or include a link to a public server where you are or to our personal web page.

We can always send a signed message to anyone: we just have to say something and sign it with our private key.

In contrast, to send an encrypted message to someone, we have to get their public key to encrypt it with their key. That way, only he can read it. Not even we can.

[INDEX]

4 SECURE EMAIL?

Unlike the web, which has mostly moved from HTTP to HTTPS (encryption), the email transport (SMTP) is not usually encrypted; there is no guarantee. If mail transport cannot be guaranteed, it is time to protect the messages: ensure integrity (content), ensure authenticity (sender), and ensure confidentiality (only the recipient can read it).

To have integrity and authenticity, we must sign (a digest) with our key and add it to the message. Anyone can verify the integrity and authenticity of a signed message using the sender's public key.

To achieve confidentiality, we have to encrypt our message with the recipient's public key, which only she can decrypt (if she and only she has her private key).

4.1 Methods

- The key pair is given to us by an authority: it gives us our private key and publishes the other. This is the case of S/MIME.
- The key pair is generated by us: individual. We generate the pair of keys, keeping one private and publishing the other. This is the case with OpenPGP.

[INDEX]

- If we do not have an authority that provides us with the key management service (S/MIME), we have to generate them ourselves (OpenPGP).

4.2 Recommended tools

Thunderbird for PC.

K-9 Mail and OpenKeychain for mobile (Android).

Flowcrypt and Mailvelope for webmail clients like Gmail on PC.

5 IN PRACTICE

5.1 Installation and configuration

If we have an email account configured in Thunderbird on our PC, we only have to generate our key pair[1]. We have to publish the public key[2] and carefully store the private one on our PC, protected by a password. It is recommended to use a password manager like KeepassXC to avoid forgetting one more password since you don't have to reuse them.

Suppose we have the same email account configured in our mobile's "K-9 mail" application and the OpenKeychain application installed (Android). In that case, we only have to export our key pair to a file, transfer it to the mobile, import it into OpenKeychain and tell K-9 that we want to use “end-to-end encryption” for our email account to enable OpenPGP, and choose our key on OpenKeychain.

1 Tools → Account Settings → End-to-End Encryption → Add Key… → Create a new OpenPGP key
2 Tools → Account Settings → End-to-End Encryption → [X] Add my public key when adding an OpenPGP digital signature

[INDEX]

5.2 Tests

If I am Ann@pangea.org, I can generate an email message for Blanca and activate the signature in options[3]. When sending it, you can ask us for the password that protects our private key. It will add a signature and send it.

When Blanca receives it, she will see in her mail application that Ann@pangea.org signs the message. She will also see Anna's public key or a part of it (the public key fingerprint). With that, she could use or find Ann's public key and send her an encrypted message.

If Ann has never communicated with Blanca, she does not have her public key yet. She can find it on some key server on the Internet from your email address (although we will not be sure if Ann has published it) or if Ann has it on her personal web page. If we know her, we can ask Ann directly for her fingerprint. That way, we will be safer. It can also be passed on to us by someone who knows both of you (but signed so as not to lose trust) or through intermediaries who know each other (a network of trust) and have exchanged them carefully. We should not trust a signature that comes to us by email made with a public key that we do not know because another person may have sent it to confuse us and pretend that it comes from Blanca (the mail transport does not check much).

This explanation is intended for us to know how to make email more secure: integrity of the content, the authenticity of the sender and confidentiality of the content for the recipient.

3 Thunderbird: In the new message window: Security → Digitally sign this message
K-9 Android: Click on the three vertical dots on the top right and choose to activate PGP-signing-only mode . An icon appears next to my sender address indicating signature, not encryption

[INDEX]

5.3 Programs

Thunderbird

https://www.thunderbird.net/

K-9 Mail Android[4]

https://k9mail.app

OpenKeychain Android

https://www.openkeychain.org

Mailvelope

https://www.mailvelope.com/en/

Flowcrypt

https://flowcrypt.com

Keepassxc

https://keepassxc.org

4 Recommended on F-Droid, like many other free software applications for Android: https://f-droid.org

www.pangea.org
Plaça Eusebi Güell 6-7
Edifici Vertex, planta 0
08034 Barcelona
Tel: +34 934015664
Email: suport@pangea.org

WITH THE SUPPORT OF:

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Pangea
.org
< INTERNET
ÈTIC I SOLIDARI >

[INDEX]