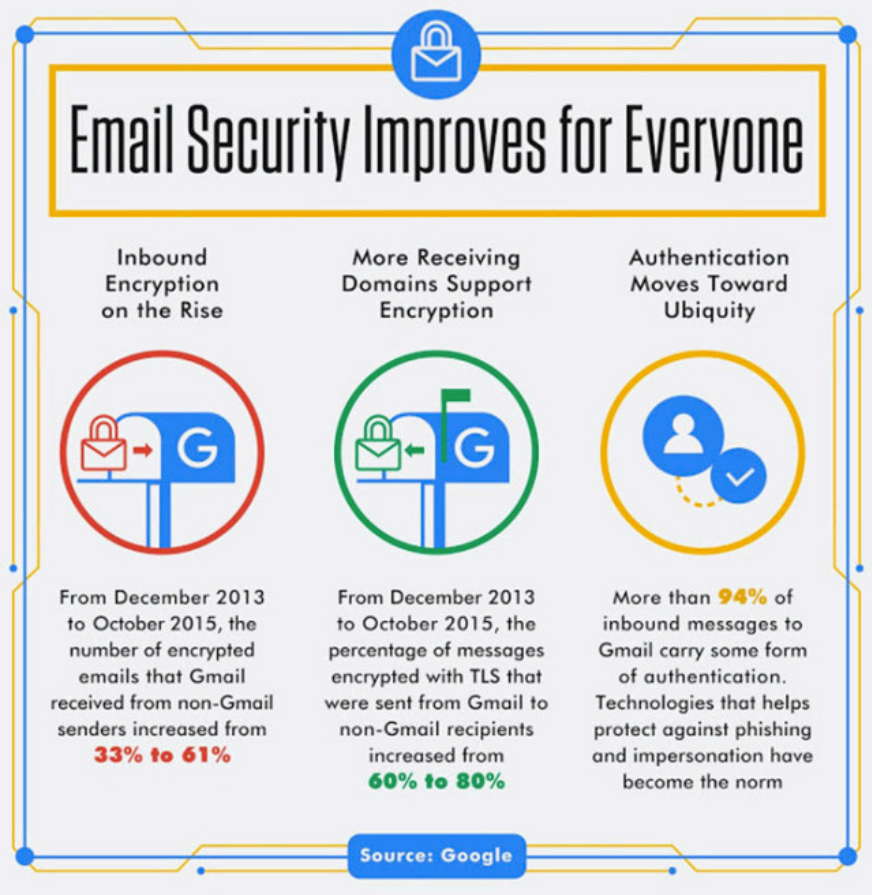
TD 4 Advanced Security: the mail

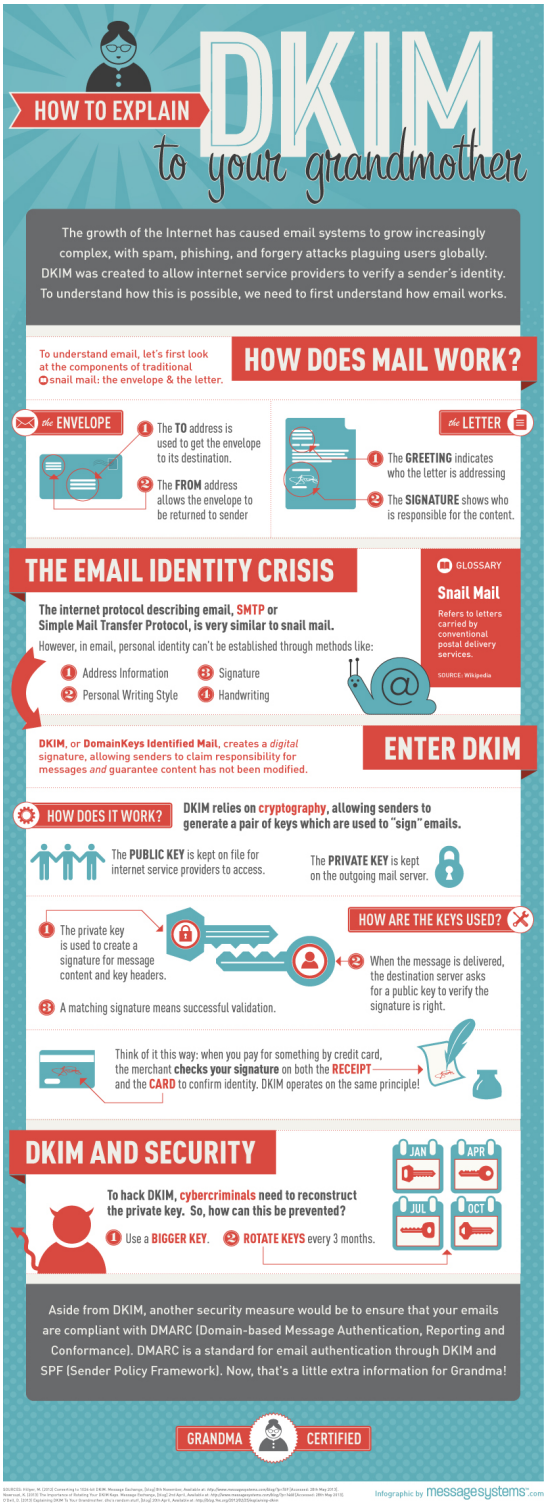
1 Is gmail secure?

Read the following figure and explain what you think about gmail's security:



2 Securing through DKIM

Read the next figure to have a quick overview of DKIM and search in the headers of your emails which ones respect the DKIM standard.



3 A short introduction to GnuPG

GnuPG (or GPG, for GNU Privacy Guard) implements the openPGP standard as defined in RFC 4880. It allows its users to send enciphered and signed messages. It thus provides respectively a confidentiality service as well as authentication and integrity services.
The goal of this lab is to use `gpg` basic CLI commands and to understand the difference between the trust chain provided by X.509 used by `openssl` and the one which is used by `gpg`. There are usable plugins (like `enigmail`) and it is currently fully integrated into the `thunderbird` mail client to ease its use. But it is interesting to understand how this tool can be used without a GUI.

3.1 Questions

For the following questions, you can refer to the documentation of `gnupg`. See for instance https://www.gnupg.org/howtos/en/GPGMiniHowto.html. Consider the `-armor` option to avoid character encoding problems. It is better to work by pairs or triple for exchanging messages.

(1) Create your keypair and a revocation certificate compatible with mail transmission.
(2) Send your public key to another user (by using mail or Discord).
(3) Import the received keys.
(4) Check your "keyring".
(5) When `gpg` knows other users' public keys, exchange messages.
(6) Decipher the encrypted mails you received.
(7) Answer the mails by a signed but not encrypted message (to make it easier to read, use the `-clearsign` option to avoid compression).
(8) Check the integrity of the message and the authenticity of the signature. Since the signatures are not certified, you should get a warning.
(9) To have a better verification of the signatures, we decide to sign a key to provide certification (option `-edit-key`).
(10) Check again the integrity and the authenticity of the previous message to see if the previous warning disappeared.
(11) Send back to the sender his certified public key that can be next forwarded to other users.
(12) Next, send to another user a signed and encrypted message and wait for such a message in your inbox.
(13) Upon reception of a signed and enciphered message, read and verify it.
(14) How can you send an encrypted and signed message to two different users? Which trust is granted by this third user joining the pair?

There are several key servers which publish public keys of the users like https://keys.openpgp.org. These servers can record your public key and you can make requests to retrieve a key. Try to get the public key linked to my email address and to find which PKC I used for signing and encrypting.

4 Feedback

Write a (very) short report of this lab directly in an encrypted mail. Explain the main differences between S/MIME and PGP. I should be able to read your mail from my client (meaning as an inline GPG encrypted mail and not as a PGP/MIME attachment). Just to be sure I can read your answers, also send the report as a plaintext. The deadline is October 29, 2021.