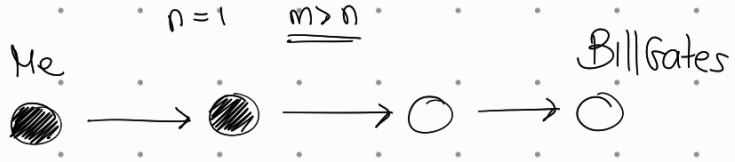
1 PGP Certificates

1. PGP confidence graph. You have just received an electronic mail signed by somebody called Bill Gates. Unfortunately you have never exchanged any key with Bill. His key, though, is signed by Luc Tucru and the key of Luc is signed by a person whom you completely trust (and $n = 1$). What can you say about the validity of Bill's key ?
2. What is the fundamental difference in the confidence architecture between PKIX and PGP ?

(1)

The PGP graph may be as follows:



The key of BillGates does not have enough syns on it to be considered trustworthy

(2)

The fundamental difference is that in PKIX the trust is based on a hierarchy where the CA is capable of certifying identities and so we rely fully on it. With PGP the trust has to be built and spread by propagation.

2 GNU Privacy Guard (GPG)

2.1 GPG keys

1. With gpg it is possible to export a public key, a private key, but also a private *subkey*. What could be the usage of a subkey?
2. To cipher some data, I use different PGP keys, one for my professional e-mails, one for my personal e-mails. These two keys are mutually signed. Discuss some advantages and drawbacks of this method.
3. A signing subkey of an OpenPGP key must certify its master key. Why?
4. What is the interest of having a signing subkey when the master key can already sign?

2.2 GPG Packets

5. To export or create a public key, what is the minimum number of packets to provide so that it is functional?
6. In terms of packets, what has to be done in order to revoke an OpenPGP key?
7. When an OpenPGP has expired, which packet stores this information?

2.3 Message sizes

8. ~~Compare the sizes of a clear message and of the same message ciphered with OpenPGP.~~
9. What if the original message is already ciphered?

2.4 GPG revocation

10. How do you take back a PGP key from the PGP servers?
11. Why is it recommended to create a revocation certificate as soon as a PGP key is created?
12. What should be done with a revocation certificate when a key has been compromised?
13. My key has been compromised on October 1st, 2023. I do not need to publish a revocation certificate since it will expire on November 10th, 2023. What do you think of this line of thoughts?
14. My ciphering subkey expires sooner than my OpenPGP master key. Is this interesting?
15. My ciphering subkey expires later than my OpenPGP master key. Is this interesting?

2.1 GPG keys

(1) The concept of subkeys comes handy in various domains. Having the possibility of generating multiple subkeys can allow us to:

→ Separate their usage and capabilities

→ Protect our masterkey by limiting its exposure and usage

→ Ease of keyrotation

(2) It is a good practice to separate the two domains and if one of the two is compromised it will not expose the other. However, it may be difficult to manage..

hard

(3) Because there must be a link between the two and it may use to move into the chain of trust and transfer it

④ Giving the possibility to sign to the subkey may allow to reduce the exposure and to

2.2 GPG Packets

⑤ We will need 3 packets in total:

- Public key packet
- User ID packet
- Signature packet

⑥ To revoke an openPGP packet we have to create and publish a "Revocation signature packet"

→ Generate a "RSP"
→ This packet is attached to the public key packets
→ Distribute the revoked key

⑦ This information is stored in a pgg packet called "key expiration time subpacket".

2.3 Message size

⑧ Clear Message → Size of the input
Ciphered Message → This size includes the original message content (possibly compressed), plus encryption overhead, PGP packet structure and possible ASCII armor

⑨ The encryption phase would apply to any message even if the input itself is already encrypted

2.9 GPG revocation

(10) This process involves post a revocation certificate to the server where the key is hosted.

(11) This is because in case the private key gets compromised we always have the possibility of revoking it.

(12) It should be retrived from the secure place where we store it and posted and published so that the other users will no longer host that key.

(13) This means that there is a time window in which anyone that has my key (private key has been compromised) can impersonate my identity.

3 PGP Deployment

Alice, manager of a bureau of the Terical company, must regularly send an activity report to the quality manager of the company. In order to fulfil this requirement, the quality manager recommend to all his bureau managers to use PGP and sign and crypt all the data.
Alice therefore installs PGP and generates an asymmetric key pair for signature and enciphering. She stores this pair solely on her computer's hard disk.

1. How to prevent anybody to read Alice's private key ?
2. Give the precise steps, in the PGP model, required for both Alice and her quality manager, before being able to surely exchange data by e-mail.
3. We now suppose that these steps have been fulfilled. Alice wants to send her report. She crypts this file but forgets to sign it. To her great surprise PGP does not ask her any password, why ?

1/2

4. Asymmetric ciphers are usually slower than symmetric ciphers. Therefore PGP does not use directly asymmetric ciphers to crypt data. Explain how PGP could work ?
5. Detail this procedure if the quality manager sends the same e-mail to several bureau managers.
6. Alice is pleased with PGP. She even wants to use it to crypt her backups on her hard disk: she crypts her directory with PGP and then stores the obtained file only on an external device (usb key, flash card). What could go bad if her hard disk fails ?
7. The quality manager is not so happy with the PGP procedure and wants to rather use a web-accessible service using HTTPS. What is the security protocol on which HTTPS is based on ?
8. The quality manager has obtained an X-509 certificate for his web site. what is the goal of this certificate ?
9. What are the main components of a X-509 certificate ?
10. When Alice will connect on the web site, her browser checks the validity of the given certificate. What will be the key used by the browser ? How has it obtained this key ?

4 Attack on the key identifier

With a PGP key identifier on only 32 bits, there would be only 2^{32} distinct identifiers. Thus, describe an attack allowing to modify the public key of a given identifier for instance: 0xDEADBEEF.

With only 2^{32} key we may have the possibility to bruteforce the key.
We have to create different packages with different fields used to calculate the key finger print.

5 PGP Signatures

1. What are the main components of an electronic certificate ?
2. What is the trust model of a public-key architecture using PGP and how does that works (in other words, why and how is it possible to trust a PGP certificate)?
3. How many packets at least compose a PGP certificate and what are their types?
4. From which packet(s), and therefore from which data, is computed a PGP Key ID (or PGP Key fingerprint)?
5. In which packet(s) are found the data about creation and expiration date of a PGP public-key?
6. In a PKIX architecture (PKI for X.509) or in a PGP architecture, is it possible to modify the validity period of a certificate and why? Detail the 4 possible cases (PKIX/PGP and reduction/extension of validity).
7. For a PGP architecture, detail the procedure(s) allowing to modify the validity period of a certificate.
8. When modifying the validity period of a PGP certificate, reduction or extension, can a non-up-to-date user be in a *fail-safe* mode?
9. For a PGP architecture, is it possible to modify the validity period of a signature? Detail both cases (reduction/extension) and the associated procedure(s).

Skipping (1) (2) (3) since answer same as Exercise 2

(4) It is computed from the PGP key ID material, specifically it is computed starting from the entire public key packet (which includes the public key algorithm, key creation time, key itself)

(5) creation date → public key packet
expiration date → signature packet

(6) Both of them allow for modification since there may be the need of changing it due to problems like private key compromised.

	REDUCING	EXTENDING	
PKIX	YES	NO	→ The certificate is immutable
PGP	YES	YES	→ New self-signature with longer validity

and the associated procedure(s).

6 Cypherpunk

Cypherpunk (Type I) is a system used for sending anonymous messages. It uses the OpenPGP format for its messages. To send an anonymous message to Bob, Alice prepares an email, `Message`, which recipient is Bob. Then she ciphers it for the public key of the cypherpunk server number 1: $C_1 = E_{K_{pub1}}(K_1)||AES_{K_1}(Bob||Message)$. Alice can then send this ciphered message to server 1; the server is then responsible of deciphering the message and then sending it to the recipient.
Alice may also decide to use the system to cover her tracks even more: she constructs a new e-mail containing the message C_1 and the recipient is now the server number 1. She then re-ciphers this e-mail for the cypherpunk server number 2 and relays the message, etc.
At each new step, the cipher is converted to base64.

1. Explicit all the public keys that Alice needs to produce her message.
2. What is the role of PGP in the overall security of the anonymity system ?
3. This protocol is officially obsolete. Indeed, and if an attacker can listen to all the communications of cypherpunk servers, she can trace messages, at least in parts. Discuss possible counter-measures.