HTTPS / Asymetric Cryptography

- <u>Problematic :</u>

How to secure personal information during communications on the internet ?

Summary

- I What are the differences between HTTP and HTTPS ? (Pages 3-4)
- II What are the public and private keys? (Pages 5)
- III How are trusted third-parties useful and necessary to secure communications? (Pages 6-7)

I What are the differences between HTTP and HTTPS ?

- → HTTP = Hypertext Transfer Protocol
- → Used for structuring websites
- → Created by CERN in the 1980's
- → Allows clients and server to communicate
- → Data are not crypted
- → But problem of vulnerabilities

I What are the differences between HTTP and HTTPS ?

- HTTP<u>S</u> = Hypertext Transfer Protocol <u>Secure</u>
- → Created in 1994

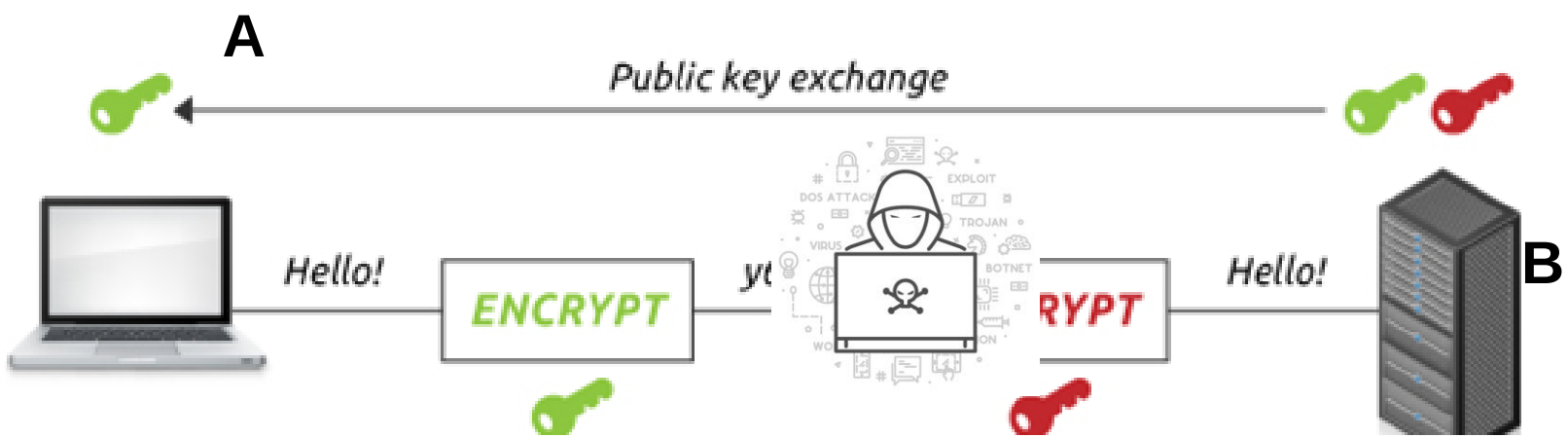
  -> S for “Secured”
- → Use the SSL/TLS Technology
- → Encrypted connexion

II What are the public and private keys?

→ Each speaker has <u>2 keys</u> :

- 1 public → encryption
- 1 private → decryption

→ It's different of symetric encryption methods because it's not the same key for encryption and decryption.



III How are trusted third-parties useful and necessary to secure communications?

→ Trusted third parties is a legal or a natural person who is authorized to set up electronic signatures from public keys.

→ There is 3 categories of trusted third-parties :

- certification authorities
- registration authorities
- certification authorities

→ ANSSI in France

III How are trusted third-parties useful and necessary to secure communications?

→ An electronic certificate containing the following informations :

- the identity of the owner of the public key
- a validity date for this key
- a signature

Conclusion

- See evolution of communications on the Internet
    -> HTTP -> HTTPS
    -> Asymmetrical Encryption
    -> Trusted Third Parties
    X Problem with quantum computers in the future

We are at your disposal for any questions relating to this presentation