# H3 Public key

## Schneier 2015: Applied Cryptography: Foundations (Schneir 2015)

* 1.1 Terminology
  + Sender and Receiver: sending message without fear of intrusion
  + Message and Encryption: Disguising a plaintext to hide its substance to make it ciphertext and again back to plaintext, also named decryption.
  + ISO 7498-2 standard covers naming like encipher and decipher by the process of message and encryption

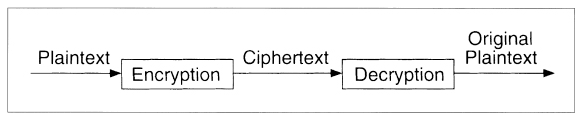


Figure 1. Encryption and Decryption

* Figure 1 kuva describes the process of Encryption and Decryption
* Authentication, integrity and Nonrepudiation must be added into the scope
  + Authentication must ensure the origin of sender to the receiver
  + Integrity must ensure that message has not been modified during the transit
  + Nonrepudiation ensures that the sender is who he/she is
* Algorithms and Keys: A cryptographic algorithm is a mathematical function which is also called cipher. Key ensures protection of the message process to make the function secure.
* Symmetric Algorithms: Two general types of key-based algorithms: symmetric and public-key.
* Cryptoanalysis: Recovering the plaintext to a message without key. It is also possible to recover a key.
* An attempted Cryptanalysis is an attack using different kind of mathematical functions, algorithms.

## Schneier 2015: Applied Cryptography: Foundations

* 1.6 Computer Algorithms
  + Three most common algorithms: DES, RSA and DSA.
  + DES is the most popular one. It is US. and international standard. DES uses same key for encryption and decryption and it’s called symmetric algorithm.
  + RSA is the most popular public algorithm, and it is used encryption and digital signatures.
  + DSA is also public-key algorithm for digital signatures.

## Schneier 2015: Applied Cryptography: Foundations

* 1.7 Large Numbers
  + Large numbers which describe different physical events. Regarding to the numbers in this book are used to described different things in cryptography.

## Schneier 2015: Applied Cryptography: Protocol Building Blocks (Schneir 2015)

* 2.5 Communications Using Public-Key Cryptography: from start to end of “Hybrid Cryptosystems”
  + Key of the symmetric algorithm safe is combination. Without combination it is not possible to open a document. Only using safecracking is possible to open it.
  + With public key encryption is possible. Private key makes decryption possible.
  + Mathematically the trap-door function makes decryption as easy as encryption.
  + Sender encrypts a message receivers public key and send it receiver. Receiver decrypts the message using receivers private key (Key pairs)
  + Symmetric cryptosystem
  + Hybrid Cryptosystems: Public-key algorithms are slow compering to symmetric algorithms. Public-key cryptosystems are vulnerable to chosen plaintext attacks.
* 2.6 Digital Signatures
  + Authentic signature which convinces documents recipient that document is signer signed
  + Unforgeable not reusable documents
  + Signatures can also be forged, altered and lifted to one paper to another
  + Signed signatures are also quite easy to forge. Snipping tool copy paste and computer files are easy to modify.
  + Digital signature trees make possible sign multiple documents at one time
  + Signing Documents with Public-Key Cryptography: Private or public key can be used to encrypt digital signature.
  + Cheating with digital signatures is fairly simple in certain cases.
  + Using one-way hash functions to sign save time fo long documents. Signing hash instead of a document make the process fast.
  + Using one-way hash function multiple signatures are easy to implement.

## b) Give two examples of public key cryptography:

SSL/TLS Encryption works over internet or a computer network encrypting sensitive data and transferring it to receiver. The SSL/TLS encryption works using both asymmetric and symmetric encryption in data-in-transit. A website needs a certificate to implement SSL/TLS connection. The certificate enables client and a server to securely send messages. The messages can be, for example, passwords, payment information etc.(F5) Public key is sent to client with server’s certificate. The client encrypts a session secret key with server’s public key and send it to back to the server.

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 2. SSL/TLS encryption and phases (F5)

Using SSH public key authentication to connect a remote server. Remote system must have SSH installed and, also computer connected to remote servers must have the SSH version installed. SSH Public authentication works on asymmetric cryptographic algorithm which generates a key pair, one public and one private. Public key must be transferred to the remote system either via log in using username and password or assigned administrator role on the remote system to be able to add the public key into the system. As previous things are valid the connection is possible establish with command line commands (University Information Technology Services 2021).

## c) Encrypt and sign a message. Then decrypt and verify it.

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 3. Check if gnupg is installed

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 4. Public and private key created

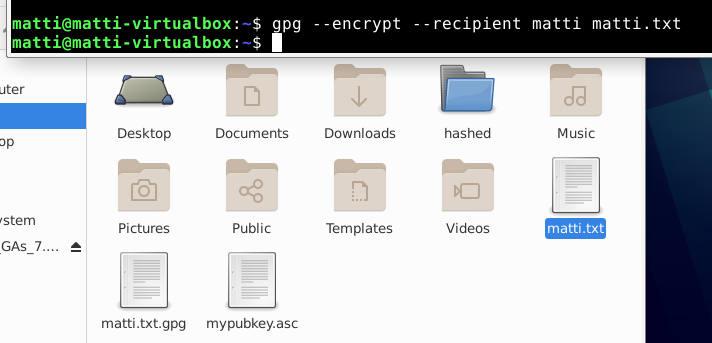


Figure 5. Encrypting file matti.txt

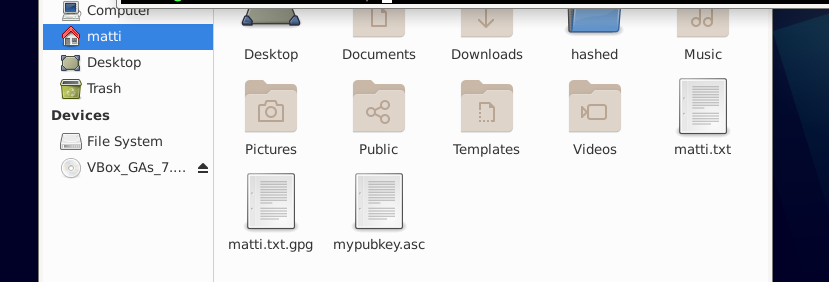


Figure 6. Matti.txt.gpg file exists im the current folder after the encryption

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 7. Signing file

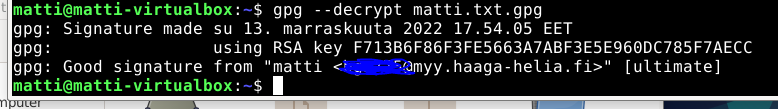


Figure 8 . Decrypting the file

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 9. Verifying signature

## Sources:

F5, SSL/TLS Encryption, <https://www.f5.com/services/resources/glossary/ssl-tls-encryption> Read: 13.11.2022

[PGP Encryption • Linux tutorial (pranabdas.github.io)](https://pranabdas.github.io/linux/pgp/)

Schneir 2015, OREILLY , Chapter 1: Foundations, <https://learning.oreilly.com/library/view/applied-cryptography-protocols/9781119096726/08_chap01.html#chap01> Read: 12.11.2022

Schneir 2015, OREILLY , Chapter 2: Protocol Builduing Blocks, [CHAPTER 2: Protocol Building Blocks | Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition (oreilly.com)](https://learning.oreilly.com/library/view/applied-cryptography-protocols/9781119096726/10_chap02.html#chap02) Read: 12.11.2022

University Information Technology Services, 2021, Set up SSH public key authentication to connect to a remote system, <https://kb.iu.edu/d/aews> Read: 13.11.2022