Hani Mebar, **Assignment 3**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
17/11/2022

h3 Public key

a) Read and summarize (with some bullet points)

€ Schneier 2015: Applied Cryptography:
Chapter 1: Foundations:
- 1.1 Terminology
- 1.6 Computer Algorithms
- 1.7 Large Numbers

Chapter 2 Protocol Building Blocks:
2.5 Communications Using Public-Key Cryptography: from start to end of "Hybrid Cryptosystems"
2.6 Digital Signatures:
- Digital Signature Trees [aka Merkle trees]
- Signing Documents with Public-Key Cryptography

b) Give two examples of public key cryptography (other than PGP). Explain how public keys are used here. (No hands-on tests required for this subtask)

c) Encrypt and sign a message. Then decrypt and verify it. Use PGP to encrypt and sign messages. (Do this hands on with a computer, and write the report while you're working).

d) Voluntary: Secrets with friends. Send a PGP message to your friend, and decrypt the reply.

e) Voluntary: Find the correct PGP key for Richard Stallman, the head of Free Software Foundation. Then find an incorrect, suspect or fake PGP key for Stallman. Why do you think one key is genuine and another is suspect?

f) Voluntary, programmers only: Cryptopals. Solve Set 1: Challenges 1-3. I highly recommend Cryptopals for learning to break cryptography.

Tips:

To encrypt with PGP, you can use GnuPG aka gpg (Linux: 'sudo apt-get install gpg', Windows gpg4win; I haven't tested the Windows version).

gpg --genkey; gpg --fingerprint; gpg --export --armor bob; gpg --import; gpg --encrypt --sign bob; gpg --decrypt;

To use PGP in your daily life, I recommend Thunderbird and Enigmail.

Answers

(a) Schneier Bullet points[i] (Schneier 2015, Chapter 1)

- **Plaintext:** A message, text, communication.

Hani Mebar, **Assignment 3**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
17/11/2022

- **Encryption**: a way to disguise a plaintext/message.
- **Ciphertext**: The disguised/encrypted plaintext/message
- **Cryptography:** The art and science of keeping messages secure
- **Cryptographers:** The people who practice cryptography
- **Cryptanalysts:** people who practice the art and science of breaking ciphertext
- **Cryptology**: The branch of mathematics encompassing both cryptography and cryptanalysis.
- **Cryptologists:** the people who practice cryptology
- Plaintext can be a stream of bits, text, or bitmap (voice, image etc) or simply binary data
- The encryption function *E*, operates on *M* to produce *C*
- In the reverse process, the decryption function *D* operates on *C* to produce *M*
- Mathematically: E(M)=C, D(C)=M, D(E(M))=M
- Cryptograhy needs to always ascertain its origin (**authentication**), ensure the message hasn't changed (**integrity**), be traceable (**non-repudiation**)
- **Cryptographic algorithm (a.k.a cipher)**, is the mathematical function used for encryption and decryption.
- **restricted** algorithm: Keeping the way the algorithm work as a secret. They are not good by today's standards as they have no quality control nor standardization protocols. They are used mainly in low security applications.
- To solve the inadequacy, we use a key. The range values of a key are called **keyspace**. Both encryption and decryption use this key.
- All of the security in these algorithms is based in the key (or keys); none is based in the details of the algorithm

Hani Mebar, **Assignment 3**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
17/11/2022

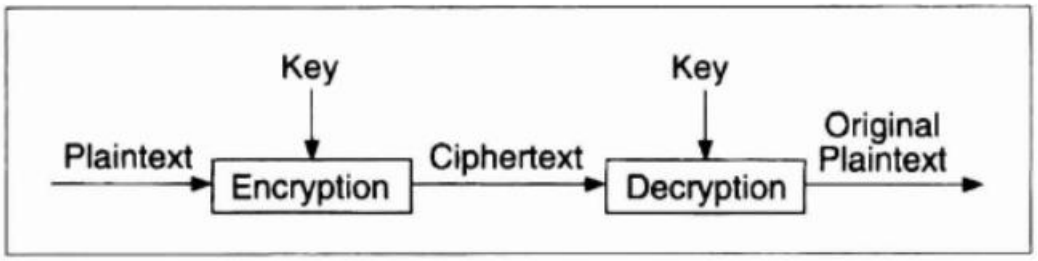
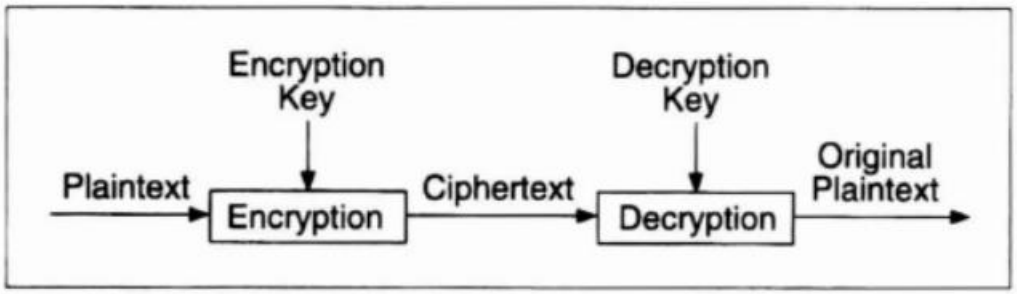


Figure 1.2 Encryption and decryption with a key.



- **cryptosystem** is an algorithm, plus all possible plaintexts, ciphertexts, and keys
- **Symmetric algorithms**: the encryption key can be calculated from the decryption key and vice versa. They require that the sender and receiver agree on a key before they can communicate securely. Has two categories:
    i. *Stream Algorithms/Ciphers:* operate on plaintext a single bit at a time.
    ii. *Block Algorithms/Ciphers*: operate on the plaintext in groups of bits
- **Public-key algorithms:** designed in a way that the key used for encryption is different from the key used for decryption
    i. **Public Key:** the encryption Key
    ii. **Private Key:** the decryption key
- **Compromise**: loss of a key through non-cryptanalytic means.
- **Attack:** what cryptanalysts try to do
- **There are many types of attacks:**
    i. **Ciphertext-only attack:** they have several messages encrypted with the same algorithm and try to break it.
    ii. **Known-plaintext attack** the cryptanalyst has access to the plaintext of those messages.
    iii. **Chosen-plaintext attack:** cryptanalyst chooses the plaintext that gets encrypted.

iv. **Adaptive-chosen-plaintext attack:** choose the plaintext that is encrypted, and can also modify his choice based on the results of previous encryption
v. **Chosen-ciphertext attack** can choose different ciphertexts to be decrypted and has access to the decrypted plaintext
vi. **Chosen-key attack** means that the cryptanalyst has some knowledge about the relationship between different keys
vii. **Rubber-hose cryptanalysis:** The cryptanalyst threatens, blackmails, or tortures someone until they give him the key

- Lars Knudsen classified these different categories of breaking an algorithm
  i. **Total Break**: A cryptanalyst finds the key, K, such that $D_K(C) = P$
  ii. **Global deduction** A cryptanalyst finds an alternate algorithm, A, equivalent to $D_K(C)$, without knowing K
  iii. **Instance Deduction**: A cryptanalyst finds the plaintext of an intercepted ciphertext
  iv. **Information deduction:** A cryptanalyst gains some information about the key or plaintext.
- Computer Algorithms come in various forms. Three common ones:
  i. DES (Data Encryption Standard): It is a symmetric algorithm; the same key is used for encryption and decryption
  ii. RSA (Rivest, Shamir and Adleman): can be used for both encryption and digital signatures (most popular public key alg)
  iii. DSA (Digital Signature Algorithm): only used for digital signatures.
- Large Numbers, refer to https://learning.oreilly.com/library/view/applied-cryptography-protocols/9780471117094/09_chapter01.html#ch1-sec020 chapter 1.7.
- **Public-Key Cryptography**[ii]**(**Schneier 2015, chapter 2.5**):** one of two keys, a public and a private one. It is hard to deduce the private key from the public key. Only the person with the private key can decrypt the message.
- **The private key:** The secret, or trapdoor, is the private key. With that secret, decryption is as easy as encryption.
- In the real world, public-key algorithms are not a substitute for symmetric algorithms. They are not used to encrypt messages; they are used to encrypt keys.
  i. Public-key algorithms are slow
  ii. Public-key cryptosystems are vulnerable to Chosen-plaintext attacks
- **Session-keys**: an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers[iii].
- **Hybrid Cryptosystem**: Session keys used with symmetric algorithms to secure a message.

- Why signatures are viewed as important[iv] (Schneier 2015, chapter 2.6):
    i. Provides proof of authenticity.
    ii. Each signature is unique to the individual
    iii. Cannot be forged
    iv. Cannot be reused
    v. Cannot change or alter the signed document
    vi. Cannot be denied
- All the above can actually be undone/faked – when it comes to real-life tangible signatures. But not when it comes to digital signature.
- Digital signatures almost work in reverse order of an encrypted public-key. The basic protocol is that the author encrypts a document with their private key, the author sends the encrypted document to a receiver, and the receiver decrypts it with the author's public key thus confirming the authenticity of the sender.
- Digital signatures include timestamps; the data and time of the signature get attached to the message which solves the issue of reusing an old signature (like, say, when cashing a cheque).
- one-way hash function: a code or hash of a whole document that is 'signed' rather than signing a large document. Speed is increased dramatically.
    i. signature can be kept separate from the document
    ii. recipient's storage requirements for the document and signature are much smaller
    iii. Can be archived without storing the content
- **digital signature:** The bit string attached to the document when signed.
- **Multiple signatures:** instead of each person signing the document, one person signs the document, and the other people sign the person's signature.

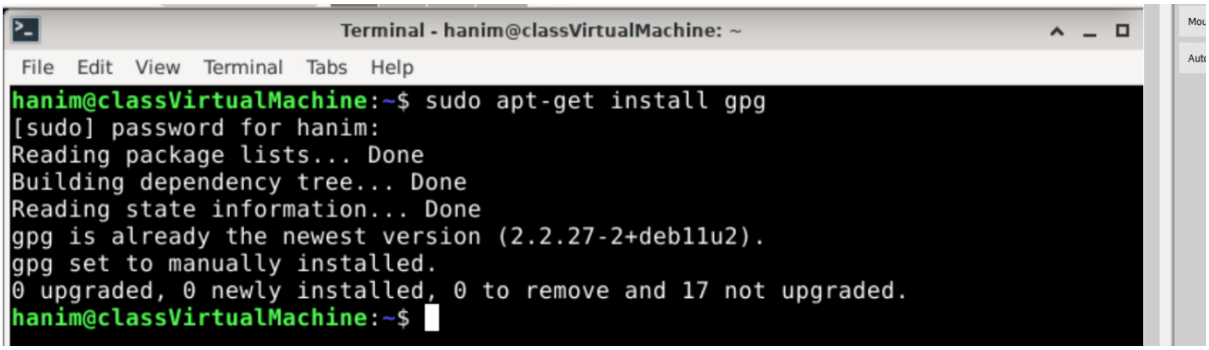
(b) Two Examples of Public-Key Cryptogrpahy other than PGP could be **RSA (Rivest, Shamir and Adleman)**, and **DES (Data Encryption Standard**).

- A use case for RSA could be digital signatures where one would need a one-way hash key specific to a set of documents. But RSA is considered flawed because it can be hacked through brute force attachs.
- DES is not used so much other than on non-classified sites or computers where access the data, even if private, is enough to keep basic hackers away.

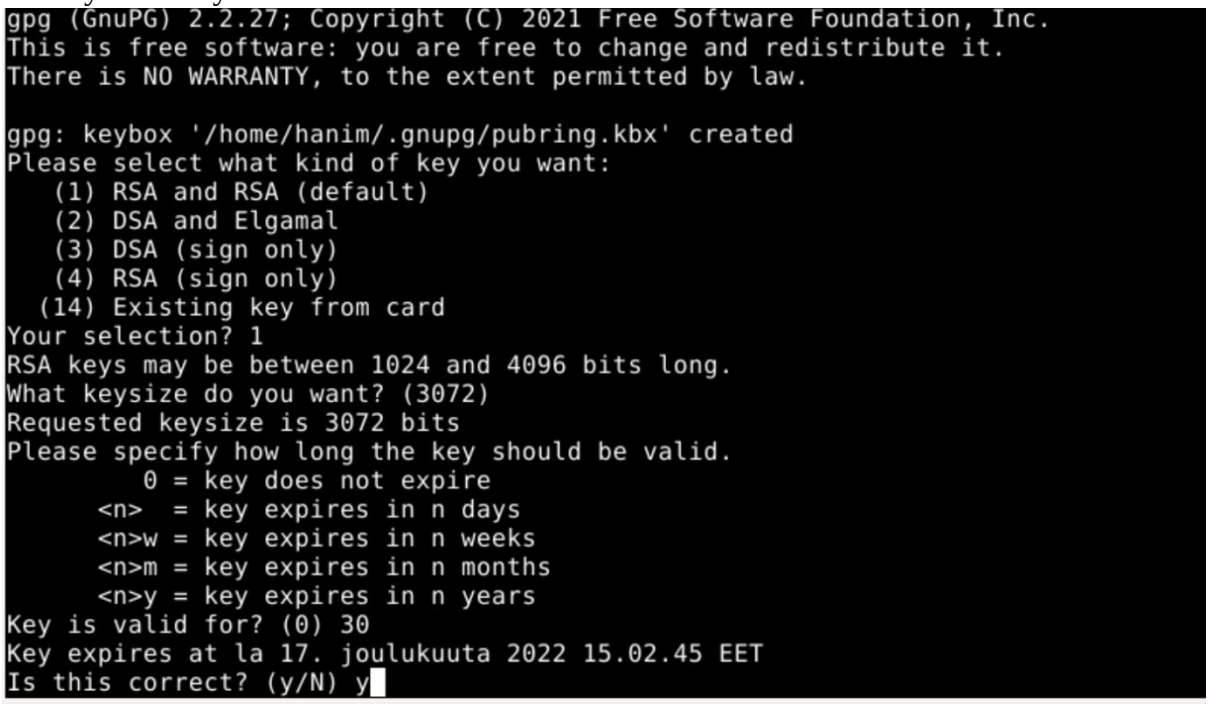
(c) Encrypting a message on GnuPGP in Linux

- Got the PGP software installed

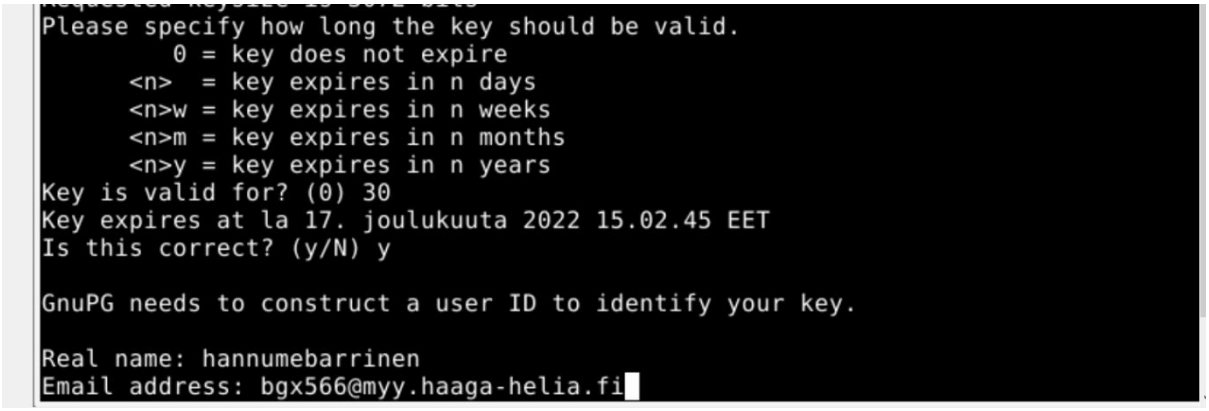
Hani Mebar, **Assignment 3**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
17/11/2022



Ran the program to create a key. Selected the default, chose a 3072 bit keysize, gave it a validity of 30 days

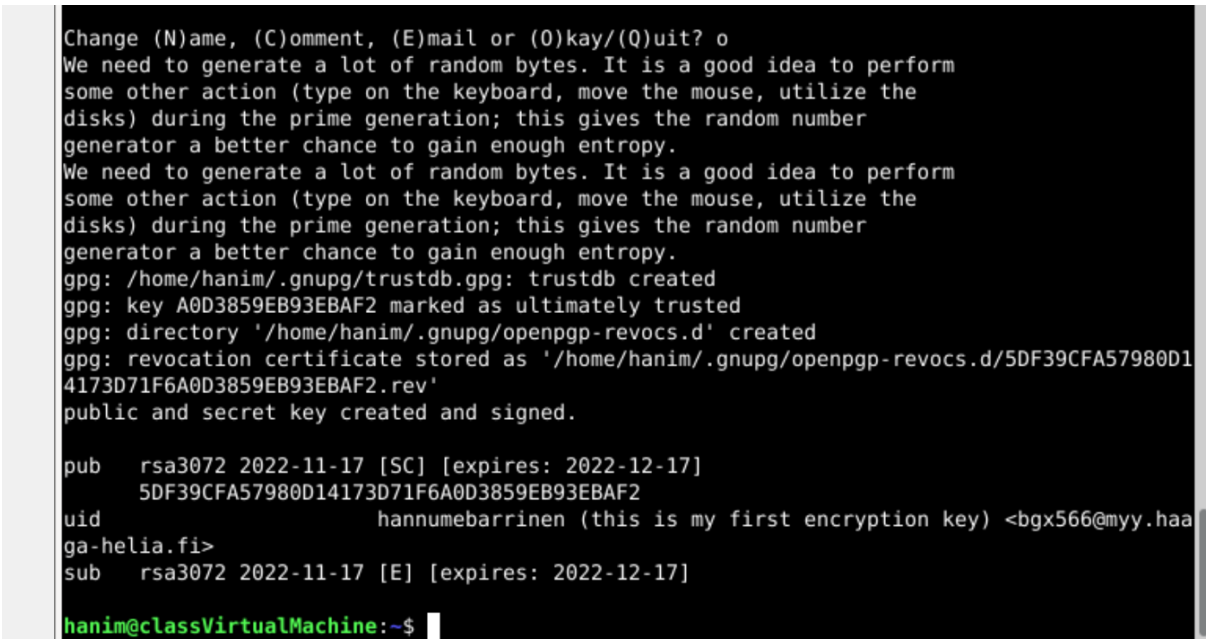


Created an identity for my key, used my haaga helia email and fake name.



Hani Mebar, **Assignment 3**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
17/11/2022

Made a passphrase to secure the message



Didn’t know how to retrieve it afterwards and my session timed out and had no idea how to go back to it. ☹️

v

[i] Schneier, Bruce, 2015; Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition; Accessed E-book, 16/11/2022.
[ii] Schneier, Bruce, 2015; Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition; Accessed E-book, 16/11/2022.
[iii] Tech target contributor 2022, URL: https://www.techtarget.com/searchsecurity/definition/session-key. Accessed 17/11/2022
[iv] Schneier, Bruce, 2015; Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition; Accessed E-book, 16/11/2022
[v] p@55phr@5E