

# GNUPG

## HIGH LEVEL CRYPTOGRAPHY



**NO ONE** will spy on your e-mails anymore



**MEGA PROTECTION** for home and business



**100% FREE**, zero cost

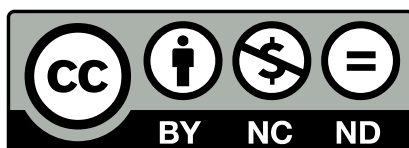
AND...  
JUST ONE WORD...

# PRIVACY

# Copyright

Except when otherwise stated, this document is licensed under the following license:

**Creative Commons**  
**Attribution-NonCommercial-NoDerivatives 4.0 International License**



That means you are free to:

- **Share** – copy and redistribute the material in any medium or format.

Under the following terms:

- **Attribution** – You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **NonCommercial** – You may not use the material for commercial purposes.
- **NoDerivatives** – If you remix, transform, or build upon the material, you may not distribute the modified material.

You can find more information about the license in the following link:

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

# Images copyright

## Icons and Logos

Below are listed the images used in this book that are licensed under different licenses than this book. If you use any of these images you must follow their respective license terms as well.

The table below contains an identification of the image, the pages they are used, the license they are subjected and a link to their original content and/or license terms.

Logo	Page(s) used	License	Link
Green shield	1	GNU GPL	<a href="#">LINK</a>
Red check mark	10, 11	GNU FDL v2.1 +	<a href="#">LINK</a>
NEW seal	14	CC BY ND	<a href="#">LINK</a>
Key	14, 15, 16, 17, 46, 48	Public Domain	<a href="#">LINK</a>
Male avatar	14, 15, 16, 17	CC BY	<a href="#">LINK</a>
Female avatar	14, 15, 16, 17	CC BY	<a href="#">LINK</a>
Verified seal	16	UNKNOWN	<a href="#">LINK</a>
Padlock	17	GNU GPL	<a href="#">LINK</a>
Mushroom	46	CC BY	<a href="#">LINK</a>
EFF logo	48	EFF Copyright's Policy	<a href="#">LINK</a>
GNU Project logo	48	GFDL v1.3 FAL v. 1.3 CC BY SA 2.0	<a href="#">LINK</a>
IETF logo	48	IETF Trade Mark Usage Guidelines	<a href="#">LINK</a>

## Screenshots

All screenshots used in this book are licensed under the same terms of the book.

# Table of Contents

<b>Introduction</b> .....	06
 <b>PART 1 – BASIC CONCEPTS</b> .....	07
<b>Chapter 1:</b> <a href="#">What is cryptography?</a> .....	08
<b>Chapter 2:</b> <a href="#">Why use cryptography?</a> .....	09
<b>Chapter 3:</b> <a href="#">How cryptography works?</a> .....	11
<b>3.1</b> <a href="#">Symmetric cryptography</a> .....	12
<b>3.2</b> <a href="#">Assymmetric or public key cryptography</a> .....	13
<b>Chapter 4:</b> <a href="#">Anatomy of a key</a> .....	17
<b>Chapter 5:</b> <a href="#">What is GnuPG?</a> .....	23
 <b>PART 2 – CONFIGURING AND USING PROGRAMS</b> .....	26
<b>GnuPG in six easy steps</b> .....	27
<b>Chapter 6:</b> <a href="#">Installing GnuPG</a> .....	28
<b>6.1</b> <a href="#">Microsoft Windows</a> .....	28
<b>6.2</b> <a href="#">*NIX systems</a> .....	35
<b>Chapter 7:</b> <a href="#">Creating a keypair</a> .....	37
<b>7.1</b> <a href="#">Text mode</a> .....	37
<b>7.2</b> <a href="#">Microsoft Windows</a> .....	41
<b>7.3</b> <a href="#">*NIX systems</a> .....	48
<b>Chapter 8:</b> <a href="#">Configuring Mozilla Thunderbird</a> .....	53
<b>8.1</b> <a href="#">Installation</a> .....	53
<b>8.2</b> <a href="#">Configure account</a> .....	58
<b>8.3</b> <a href="#">Configuring Enigmail</a> .....	62
<b>8.4</b> <a href="#">Testing messages and exchanging keys</a> .....	70
<b>8.5</b> <a href="#">Importing public key</a> .....	74
<b>8.6</b> <a href="#">Setting trust level</a> .....	78
<b>7.7</b> <a href="#">Setting rules</a> .....	80
 <b>PART 3 – OTHER RESOURCES OF GNUPG</b> .....	84
<b>Text mode (All systems)</b>	
<b>Chapter 9:</b> <a href="#">Revocation certificate</a> .....	85

<b>Chapter 10:</b>	<a href="#">Encrypting and decrypting files</a>	89
<b>10.1</b>	<a href="#">Encrypting files</a>	89
<b>10.2</b>	<a href="#">Decrypting files</a>	90
<b>10.3</b>	<a href="#">Changing the output file name</a>	91
<b>10.4</b>	<a href="#">Choosing between multiple keys</a>	92
<b>Chapter 11:</b>	<a href="#">Signing and verifying files</a>	93
<b>11.1</b>	<a href="#">Making signatures</a>	93
<b>11.2</b>	<a href="#">Verifying signatures</a>	94
<b>11.3</b>	<a href="#">Extracting files from signed files</a>	95
<b>11.4</b>	<a href="#">Choosing between multiple keys</a>	95
<b>Chapter 12:</b>	<a href="#">Importing and exporting certificates</a>	96
<b>12.1</b>	<a href="#">Exporting certificates</a>	96
<b>12.1.1</b>	<a href="#">Exporting your public key</a>	96
<b>12.1.2</b>	<a href="#">Exporting your private key</a>	97
<b>12.1.3</b>	<a href="#">Exporting your whole keyring</a>	97
<b>12.2</b>	<a href="#">Importing keys and certificates</a>	98
<b>12.2.1</b>	<a href="#">Importing certificates from a file</a>	98
<b>12.2.2</b>	<a href="#">Importing certificates from key servers</a>	98
 <b>Graphical mode (Microsoft Windows)</b>		
<b>Chapter 13:</b>	<a href="#">Encrypting and signing files</a>	99
<b>Chapter 14:</b>	<a href="#">Decrypting files and verifying signatures</a>	107
<b>Chapter 15:</b>	<a href="#">Importing and exporting certificates</a>	111
<b>15.1</b>	<a href="#">Exporting your public key</a>	111
<b>15.2</b>	<a href="#">Exporting your private key</a>	113
<b>15.3</b>	<a href="#">Importing keys and certificates</a>	116
 <b>Graphical mode (*NIX systems)</b>		
<b>Chapter 16:</b>	<a href="#">Importing and exporting certificates</a>	119
<b>16.1</b>	<a href="#">Exporting your public key</a>	119
<b>16.2</b>	<a href="#">Exporting your private key</a>	121
<b>16.3</b>	<a href="#">Importing keys and certificates</a>	125
 <b>Chapter 17:</b>	<a href="#">Key servers</a>	127
 <b>PART 4 – FINAL CONSIDERATIONS</b>		
 <b>Chapter 18:</b>	<a href="#">Commands Reference List</a>	135
<b>Chapter 19:</b>	<a href="#">Bringing more people to GnuPG</a>	138
<b>Conclusion</b>		140

# Introduction

Welcome!

This guide was developed to help people understand what is cryptography, how it works and why they should use it. It deals primarily with e-mail cryptography, but there are also sections covering offline usage for local files.

Most people don't use cryptography simply because they don't know what it is, or they have erroneous ideas about it, such as being extremely complex, expensive and even outlawed. They are also not aware of the risks and dangers they face by not using it.

On the other side, the largest IT companies and e-mail providers also do not provide adequate information on this issue and resist implementing cryptography in their systems because it would increase their costs without giving them direct benefits.

We believe that cryptography is essential and necessary to maintain privacy and security of digital communications, and the more people adopt this technology, the more it becomes an indispensable item which will come together with every service.

This guide is destined to laypersons, so it is easy to understand and there is no need of prior advanced knowledge. You will learn how to install and configure all the necessary programs to have cryptography working in your system, and by the end you will be able to communicate with other people with maximum privacy and security.

We hope you enjoy it. Thanks for choosing this guide!

Best regards,

The Golden Keys Team

<https://goldencontest.wordpress.com>

# PART 1

## BASIC CONCEPTS

***In this part you will learn:***

- *What is Cryptography*
- *Why use Cryptography*
- *How Cryptography works*
- *The Anatomy of a Key*
- *What is GnuPG*

**CHAPTER 1**

# What is cryptography?

Cryptography is the process of encoding and decoding information, messages and files using secret code with the purpose of offering privacy and security. This can be accomplished through machines, computer programs, or both.

Cryptography is always used when there is a need to transmit information in a secure way between two parts, ensuring that only the sender and the receiver will be able to decipher its original content. Anyone who tries to intercept it without authorization will only see a bunch of symbols and codes that makes no sense, and will not be able to decipher it.

Cryptography has existed for thousands of years, but for most part of its history it was considered a military tool, being used almost exclusively by governments and armies due to its high cost and complexity.

Things started to change with the emergence of personal computers and the internet. With the advent of those technologies, high level cryptography became affordable to the general public at the same time that the need for more secure systems was increasing.

Today cryptography is essential for many areas in our society and it is employed in a variety of systems including personal computing, mobile phones, banking systems, magnetic cards, ATM machines, electronic commerce, data storage, wireless devices, etc. However few users are aware of cryptography's presence in our life, and even fewer know how to use it or how it works internally.



**CHAPTER 2**

# Why use cryptography?

There are several reasons why you should always use cryptography on your personal and professional communications, they all come down to your privacy and security. Below we list 7 points so you can better understand the importance of this technology.

**E-mail is extremely insecure**

E-mail is one of the most insecure systems ever simply because it was not designed to be secure. Messages travel through many machines, networks and even countries, and they can be intercepted in many different ways by anyone who has access to them. By default their contents (text, images and attachments) are transmitted without any security at all.

**You are constantly being monitored**

E-mail providers (such as Hotmail, Gmail, Yahoo) store all your sent and received messages for indeterminate time – possibly forever – even after you have erased them from the trash bin or terminated your account. They do it for two reasons: to sell you more services and advertisements, and to collaborate with government surveillance programs.

The registers of your e-mail communications may be – and often are – stored in machines located in countries different than yours, and once they are in another jurisdiction they are subjected to that nation's laws and there is virtually nothing you can do to claim the right to privacy you may have in your country. This may happen even if you have never been in those countries.

**It can be used at home or in business**

Cryptography can be used at home or in business and it works with a wide variety of devices such as personal computers, mobile phones, tablet computers, workstations, servers, complex network infrastructures and others.

It can be used for personal communications with family and friends, to store sensitive information, to backup sensitive information, to encrypt the whole disk, to send and receive files, to provide a secure channel to access one's machine, among other uses.

**It increases your credibility**

When you offer a secure means for people to communicate with you it demonstrates how much you value and worry about their privacy and security. This is especially true in business where there is often a high volume of sensitive information being exchanged, but it also applies to personal relationships.

**You convince more people to use it**

To send and receive encrypted messages requires that others you communicate with also use cryptography, so if you start using it you will naturally tell other people about it. Given the advantages and benefits of using cryptography, many of them will eventually embrace it, and it is easier to start doing something when others they know are already doing.

Another advantage is that it is possible to use cryptography and still communicate with people who don't use it. The communication will be unencrypted of course, but at least you don't have to limit yourself to only one group of people.

**It's free**

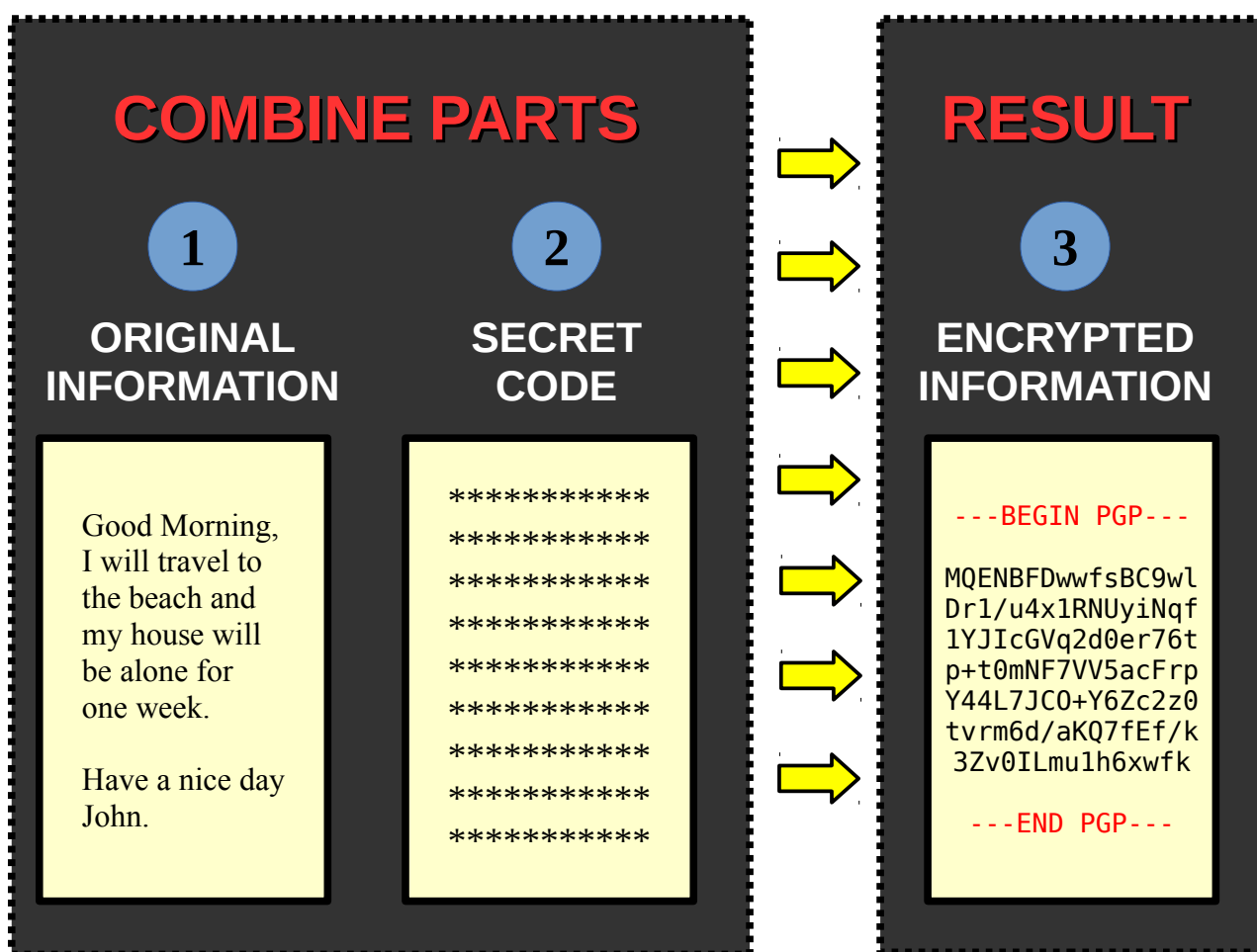
There are many types of cryptography systems for different needs with varying prices. The system we present to you in this book, GnuPG, is 100% free both in terms of price and in freedom to use it. You can set it up in any environment you want without having to pay for licenses, royalties, fees or require any type of authorization, and the program is powerful enough to be used in a single computer and in the infrastructure of a multinational corporation.

**Your privacy**

Last but not least, your e-mail communications are private and they should remain private. It doesn't matter if you send a message telling about a new restaurant in the city, your credit card number with the password (yes, people do it), or a picture of yourself naked (yes, people do it A LOT), it is not of anyone else's business and it is up to you to ensure your privacy remains private.

**CHAPTER 3****How cryptography works?**

The basic idea is to **shuffle** the original information with the secret code, resulting in the encrypted information. The power, strength and security of encryption lies exactly in how these parts are shuffled. The diagram below illustrates this process:



That's it, your message is now encrypted and ready to be sent. For the person to be able to decrypt it he will need to possess the secret code, which will be covered in the next section.

Now let's see the two main types of encryption methods: symmetric and asymmetric.

## 3.1 Symmetric Cryptography

Symmetric cryptography is the simplest of all and you probably have used it many times. The word symmetric means “equal”, which means that to encode and decode a file the password is the same.

The most basic example is when you save a file with password. It doesn't matter if you save it for yourself or for others, the password to open it is always the same.

Symmetric cryptography is faster, simpler and more economic than asymmetric cryptography because it does less mathematical calculations, which in turn uses less machine resources (e.g.: electricity). It is also more compatible with other systems and it is very secure.

However its main problem lies not in strength, but in the *transmission* of the secret code. When you send an encrypted file to another person you also have to send the password so the person can open it, and symmetric cryptography does not provide any means to send the password in a secure way.

You cannot send the encrypted file through e-mail and the password wrote in the message body because that is too obvious and risky. You could send the password by phone, SMS or letter, but these methods are also insecure and could be easily intercepted. You could deliver the password personally, but this is very inconvenient and sometimes inviable.

So how do you do it? As you see the major problem of symmetric cryptography is to transmit the password in a convenient and secure way. If the password is compromised, anyone can access the file and even modify it.

Another disadvantage is that if you use a password, you automatically know it, and others could coerce you to reveal it, as in the customs, through a law order or under interrogation.

It is because of these reasons that symmetric cryptography is recommended for local files that stay stored locally (such as backup copies) or files to be transfered through physical media.

## 3.2 Asymmetric or public key cryptography

Asymmetric cryptography, also known as public key cryptography, was created to solve the problem of transmitting the secret code that symmetric cryptography poses.

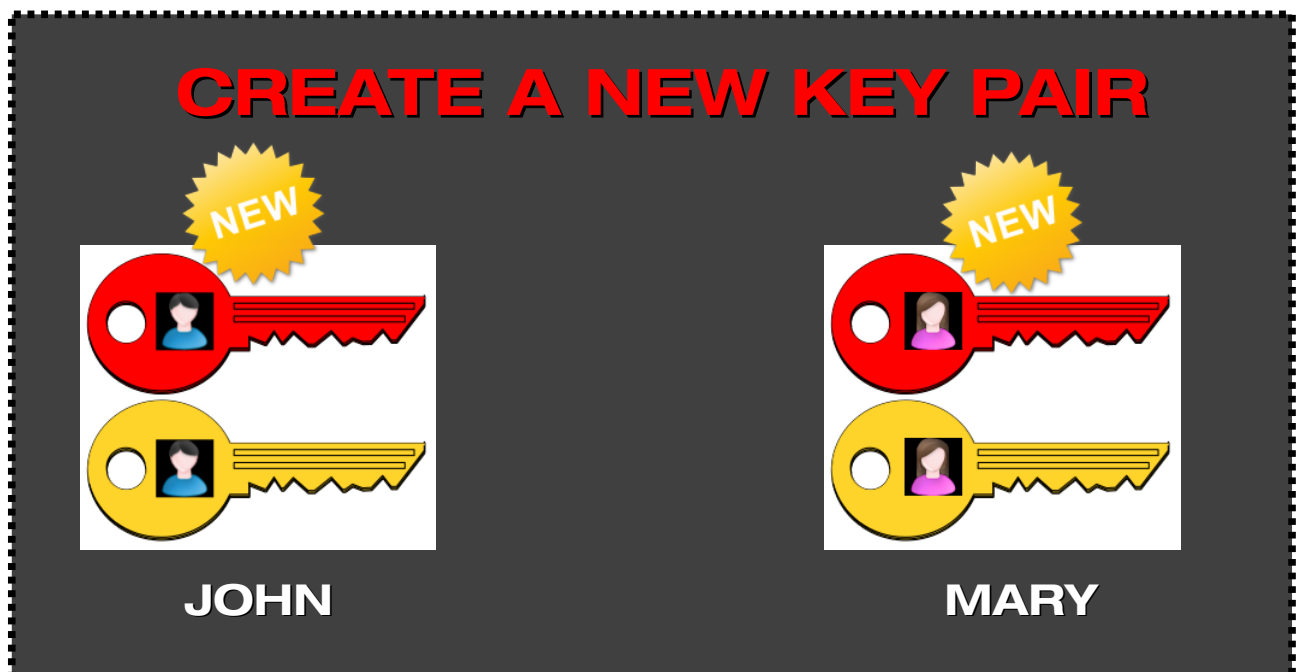
Simply speaking, in public key cryptography instead of using a single code equal for all, it is used **a code with two parts**: your part and the other person's part. This way only her will be able to decrypt the information you send to her. If someone intercept this information along the way he will not be able to do anything because he does not have the necessary part of the code.

These “parts” are actually called keys, which are public and private. The example below illustrates this more easily:

Let's imagine that John wants to send an encrypted file to Mary using public key cryptography. Here are the steps they have to follow to accomplish this:

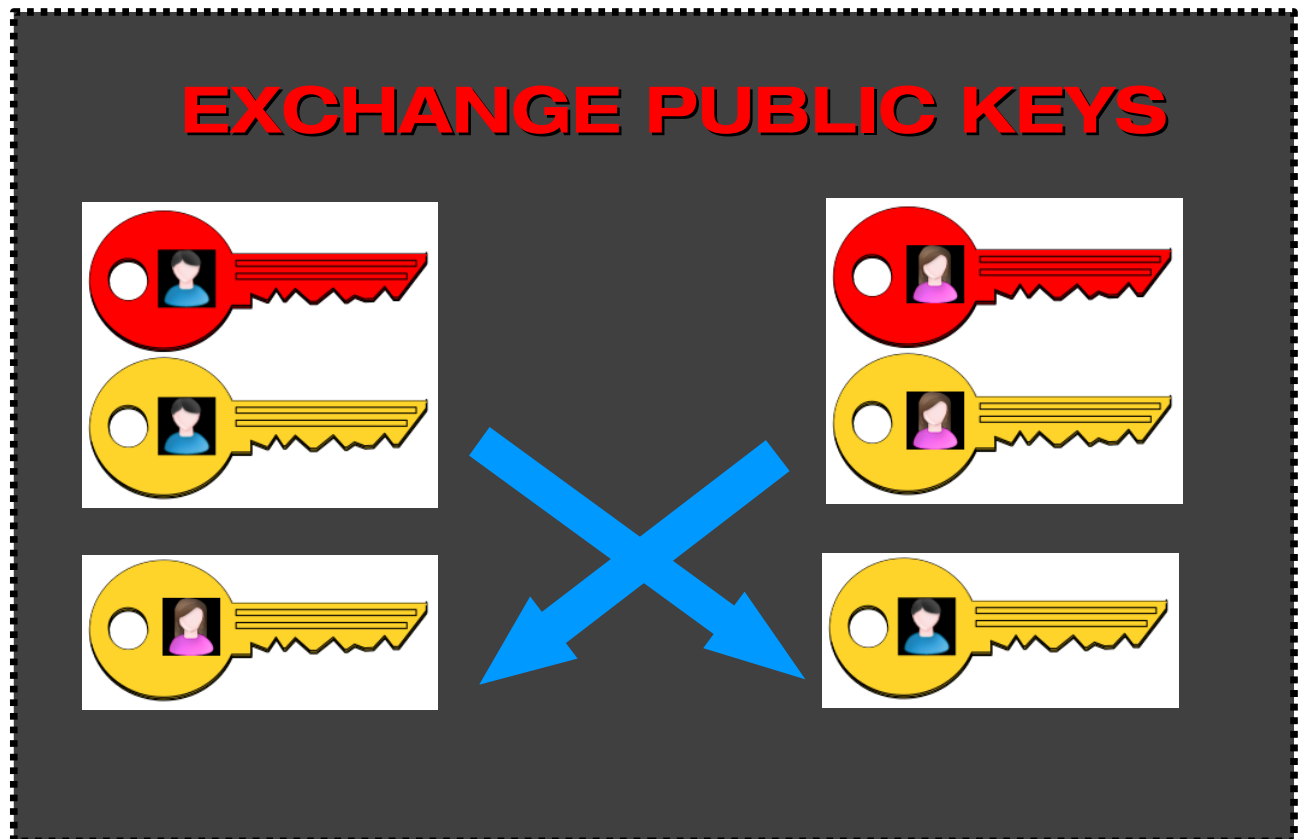
### 1 - Create a key pair

First each one of them creates a key pair containing a private key (red) and a public key (yellow). This step is covered with details on chapter 6.



## 2 - Exchange public keys

Each one of them sends a copy of their public key to the other, since the purpose of the public key is to give it to others. There are several ways to do it, the most common is to send it via e-mail (discussed in chapter 8.4), but it is also possible to publish the key in a key server, in a personal website, or deliver it through physical media (such as a CD-ROM).

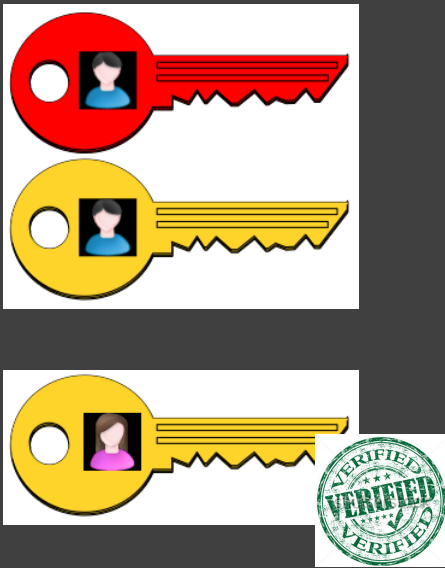


### 3 - Verify the received key


Now each one of them possesses their own key pair and a copy of the other person's public key. They must verify the other's public key to confirm they received it correctly. This is the most important step because it ensures that the key they received was not twisted or modified along the way.

Verifying is a simple process: every key comes with a number (a digital fingerprint) and all they have to do is to check this number with the sender to ensure it is correct.

## VERIFY PUBLIC KEYS



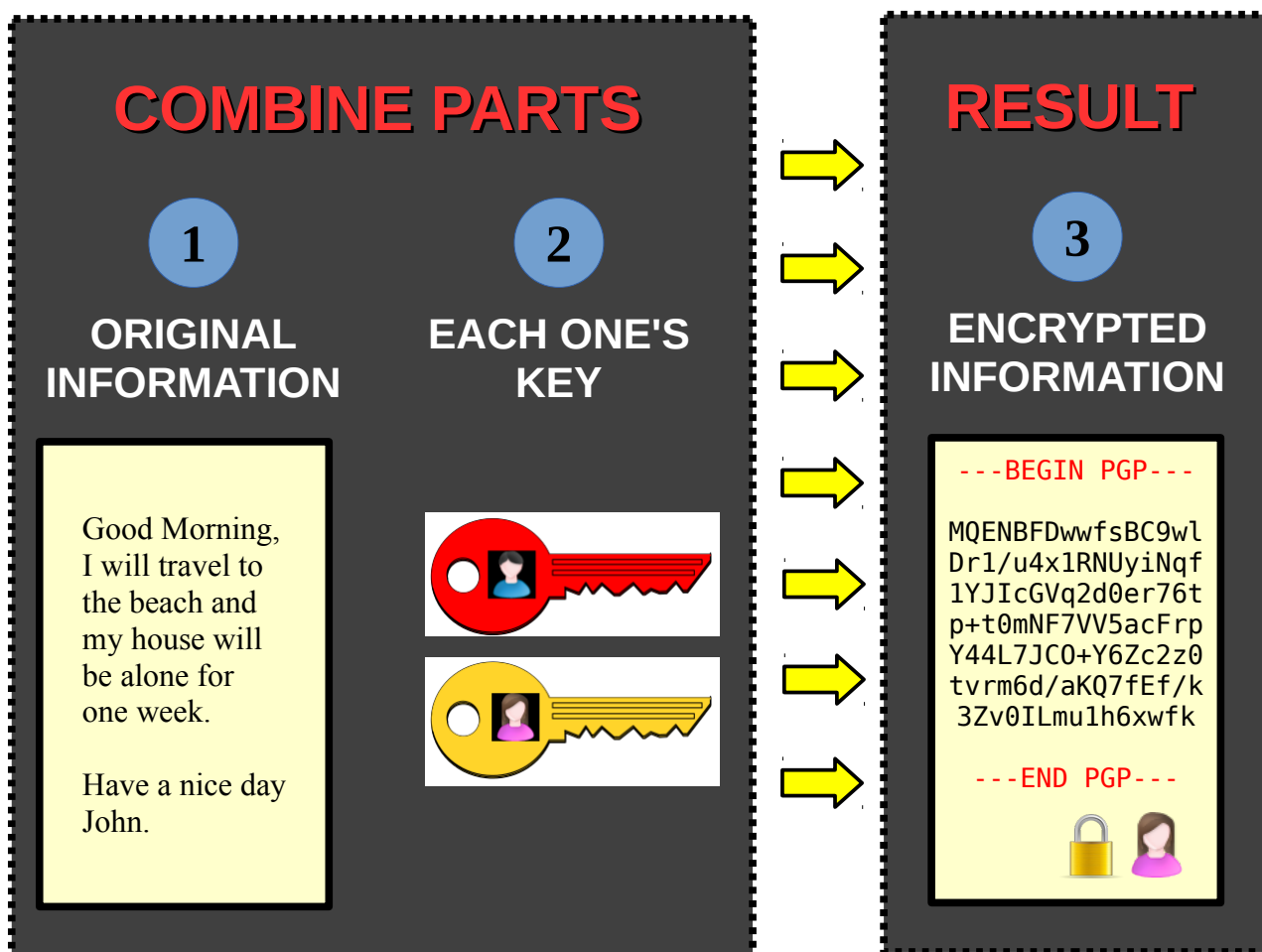
**JOHN says:**  
“I've checked this key's fingerprint with Mary and she confirmed the same number, so the key is correct.”



**MARY says:**  
“I've checked this key's fingerprint with John and he confirmed the same number, so the key is correct.”

## 4 - Encrypt a file and send it

To encrypt a file to another person John just chooses the file he wants to send and the file will be encrypted exclusively to that person.



The original message is combined with the sender's private key (John's) and the receiver's public key (Mary's), resulting in an encrypted file that only the receiver (Mary) can decrypt.

Now the resulting file can be sent to Mary through any means (such as e-mail) because only her can decrypt it, because to do it she needs her private key and the sender's public key.



## CHAPTER 4

# Anatomy of a key

A key pair consists of a public key and a private key. The public key is the key that you distribute to others, and the private key is the key that you keep with yourself. Keys are basically a stream of text that contains all the necessary information that identify them. Here we provide text and graphical representations of keys. Keys are always stored in key rings.

Keys can realize up to 4 different operations:

- Sign and Verify (S)
- Encrypt and Decrypt (E)
- Certify (C)
- Authenticate (A)

In this book we cover the first two operations, which are discussed with more details in their respective chapters.

The example below illustrates the basic information contained in a key pair. The private key is the red one, and the public key is the yellow one.

## 4.1 – A key pair

Here you can see a key pair containing a private key and a public key.

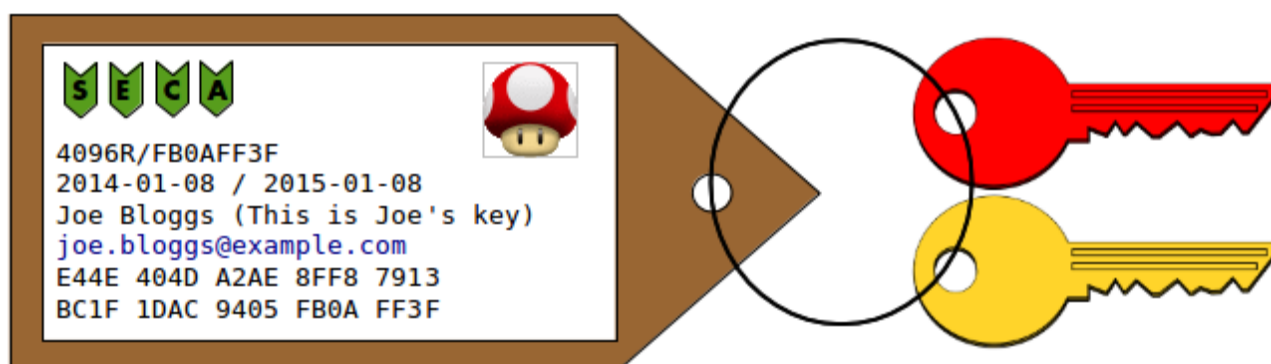


Figure 1: Information contained in a key pair

## Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below

