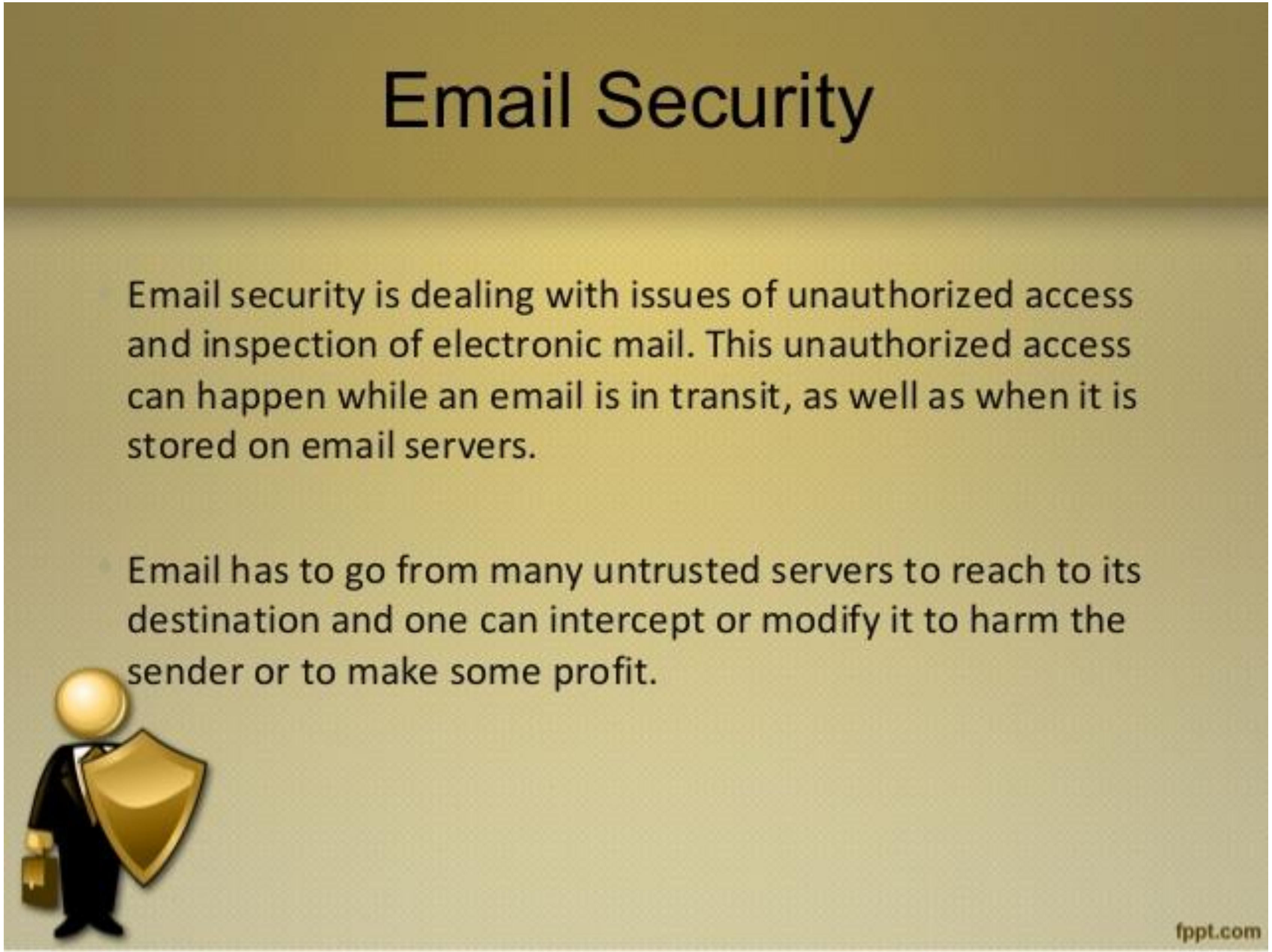
Email Security

Need of an hour ☺



Email Security

- Email security is dealing with issues of unauthorized access and inspection of electronic mail. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers.

- Email has to go from many untrusted servers to reach to its destination and one can intercept or modify it to harm the sender or to make some profit.

CIA for Email (Yeah! Again CIA ☺)

- Confidentiality: Email should be only viewed by the person it is intended to.
- Integrity: Original content should be received by the receiver.
- Availability: Receiver should be able to access the mail any time he requires.

Steps to secure our Emails

- Security at sender’s side
- Security at Receiver’s side
- Secure transmission of emails

Security at sender’s side

❑ Can be implemented by non-technical person

❑ Use incognito mode while sending mails

❑ Avoid using public computers

Security at receiver's side

- ❑ Avoid downloading attachments from unknown sender's
- ❑ Check Email Headers to verify identity of sender

Secure Transmission of Emails

- ✓ PGP (**P**retty **G**ood **P**rivacy)
- ✓ S/MIME

(**S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtension)

PGP

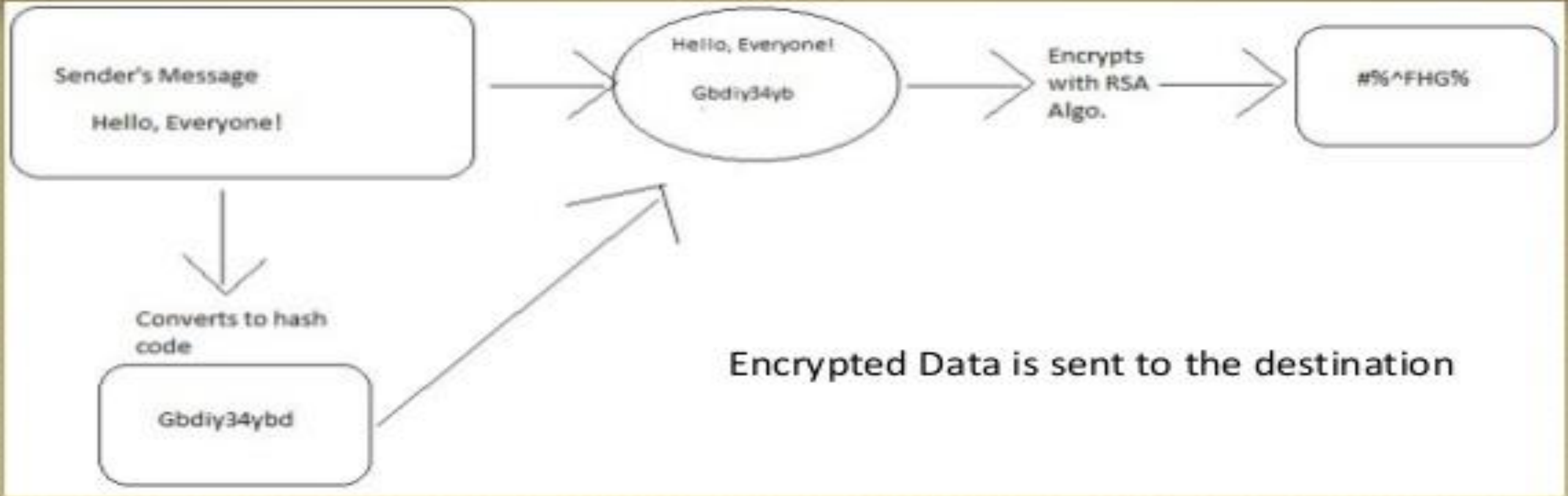
- Pretty Good Privacy
- PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
- Available free worldwide
- Based on extremely secure algorithm
- Not developed by governmental organization

fppt.com

PGP: Services

- ✓ Authentication
- ✓ Confidentiality
- ✓ Compression
- ✓ Email Compatibility
- ✓ Segmentation

PGP: Authentication



Sender's Message

Hello, Everyone!

Converts to hash code

Gbdiy34ybd

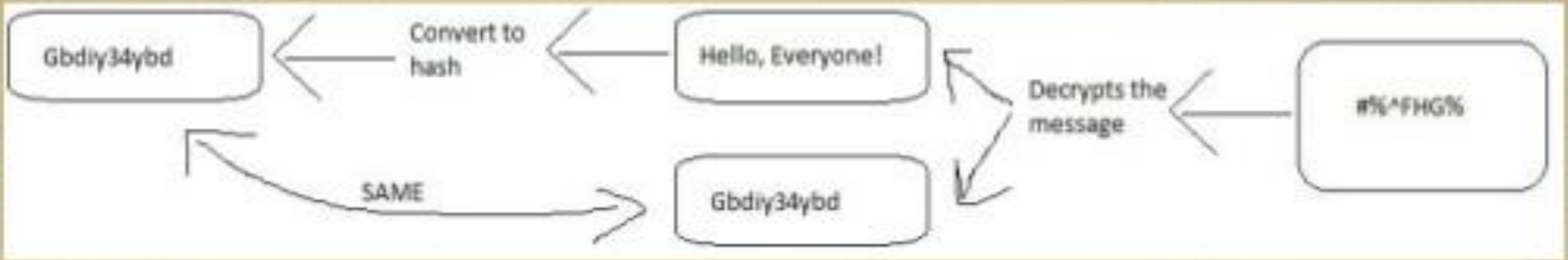
Hello, Everyone!

Gbdiy34yb

Encrypts with RSA Algo.

#%^FHG%

Encrypted Data is sent to the destination



#%^FHG%

Decrypts the message

Hello, Everyone!

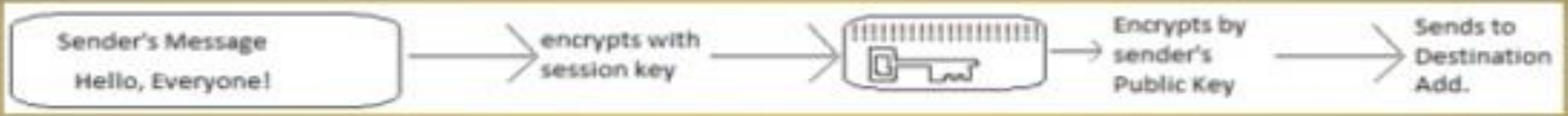
Gbdiy34ybd

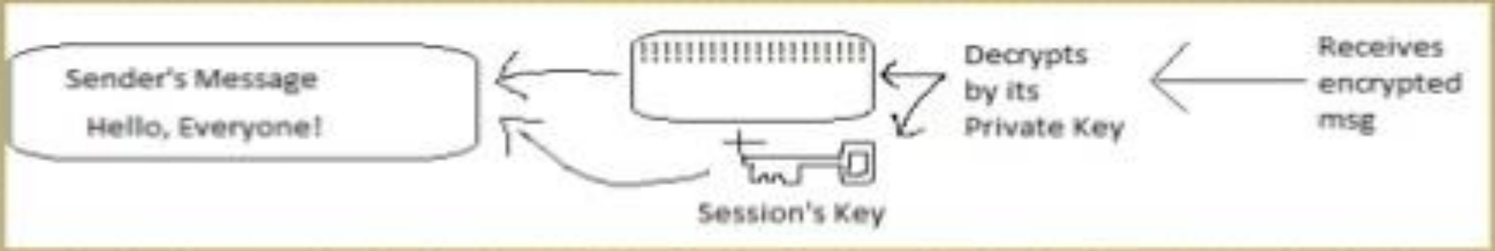
Convert to hash

Gbdiy34ybd

SAME

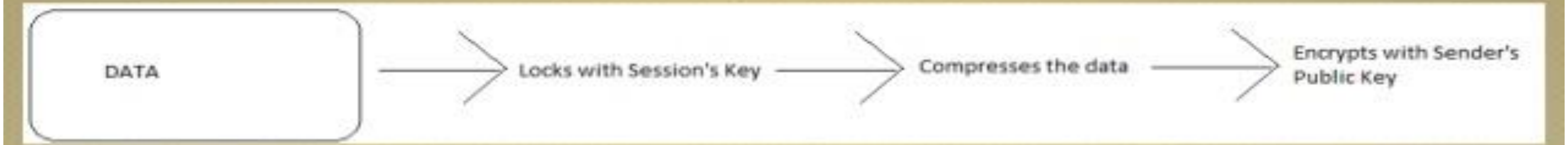
PGP: Confidentiality


Sender's Message
Hello, Everyone!
encrypts with session key
Encrypts by sender's Public Key
Sends to Destination Add.



PGP: Compression

- Compresses the data before encrypting
- Compression is done after signing (Locking with session key)
- Use ZIP Compression Algorithm



PGP: Email Compatibility

- Binary Data is obtained after applying PGP
- Converted to ASCII to able to send it over mail
- Uses Radix64 Algorithm for conversion

NOTE: PGP divides big emails in smaller sizes just before sending. (Segmentation)

S/MIME

- Secure / Multipurpose Internet Mail Extensions
- S/MIME is standard for exchanging secure mails with the help of encryption
- Previously, Mails were supposed to carry text only
- S/MIME provides support for varying content
- Supported by major email programs like Outlook, Netscape

S/MIME: Signed Mail

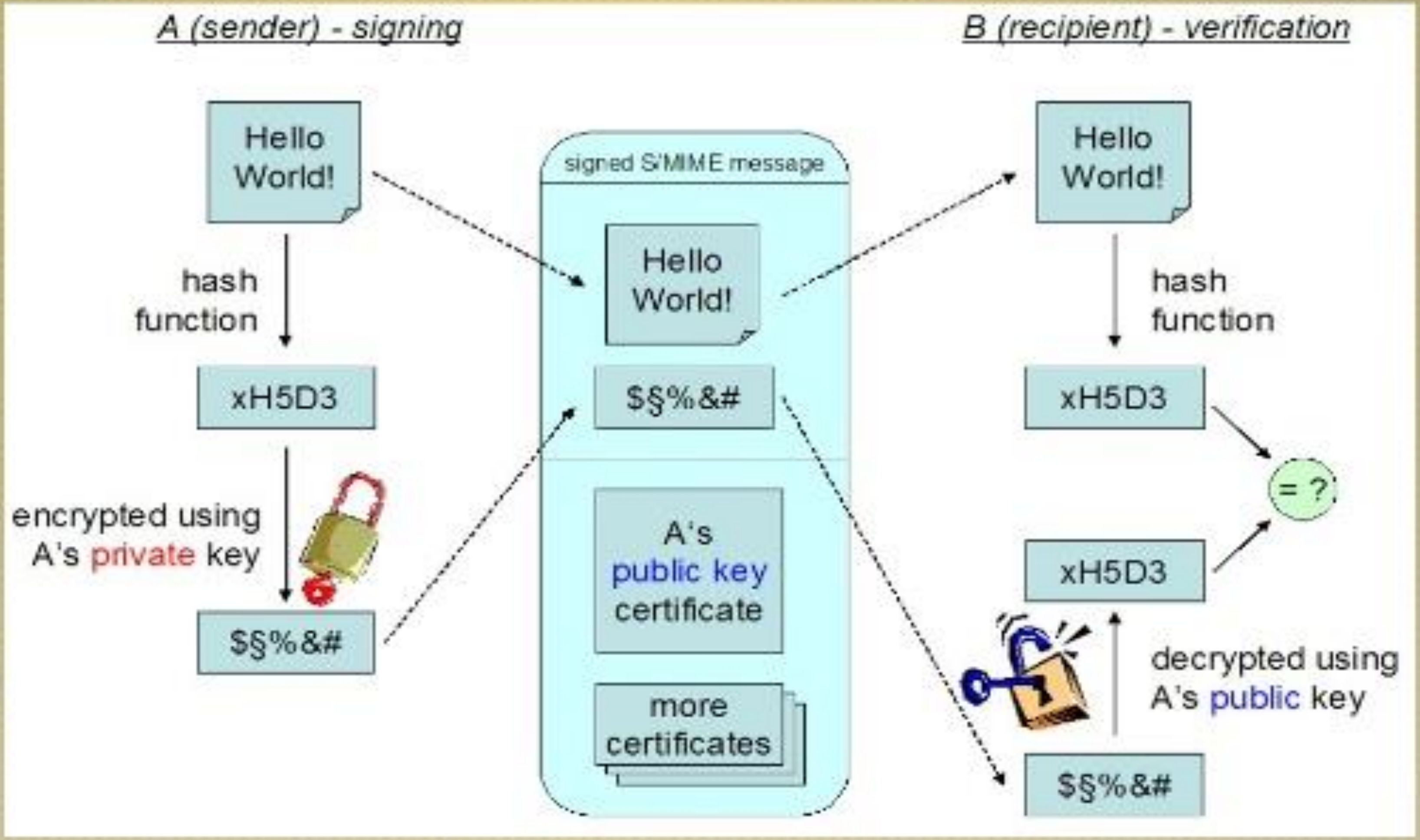
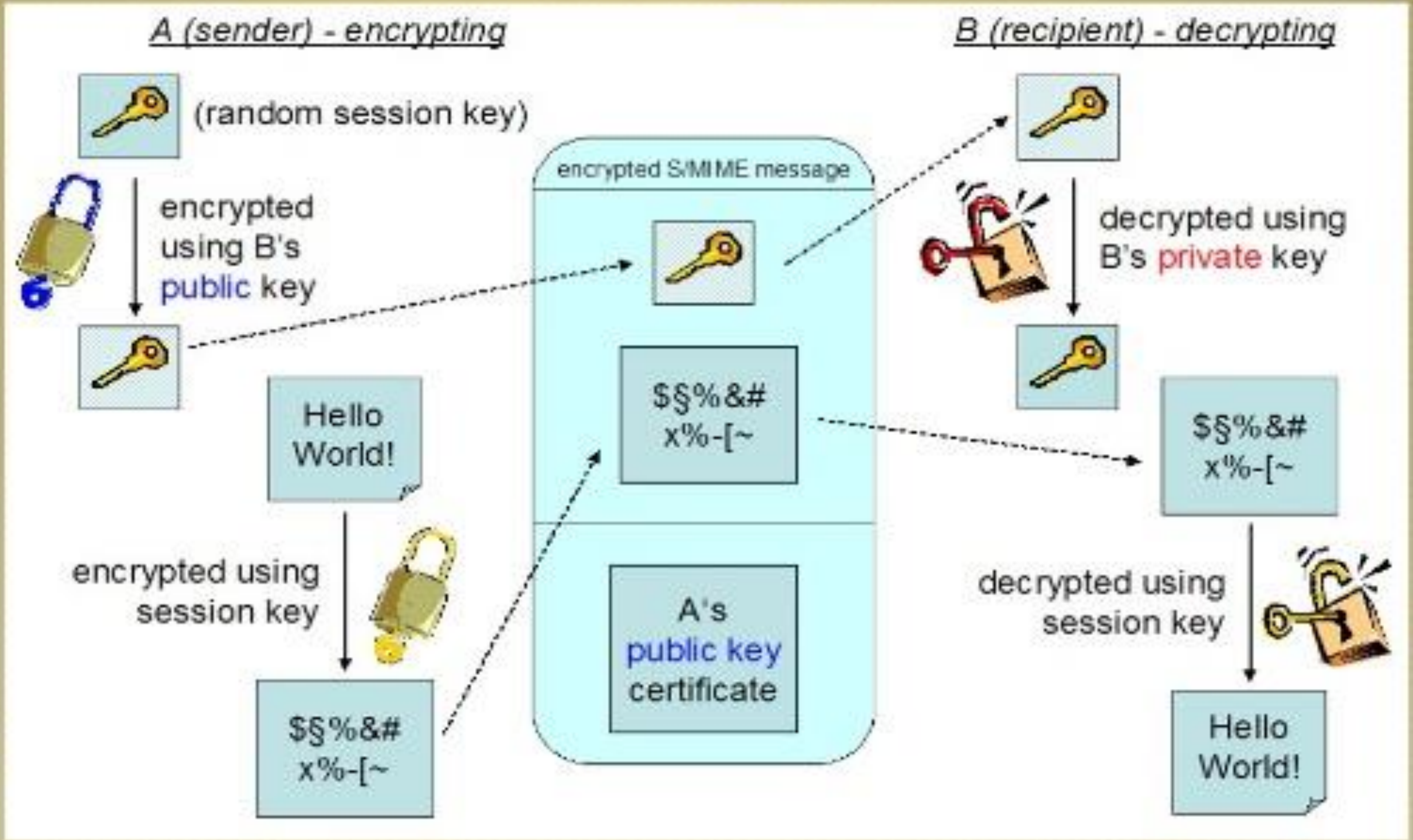


Image copied from internet (Not the complete PPT :P)

S/MIME: Encrypted Mail



A (sender) - encrypting

(random session key)

encrypted using B's public key

Hello World!

encrypted using session key

$§%&# x%-[~

encrypted S/MIME message

$§%&# x%-[~

A's public key certificate

B (recipient) - decrypting

decrypted using B's private key

$§%&# x%-[~

decrypted using session key

Hello World!

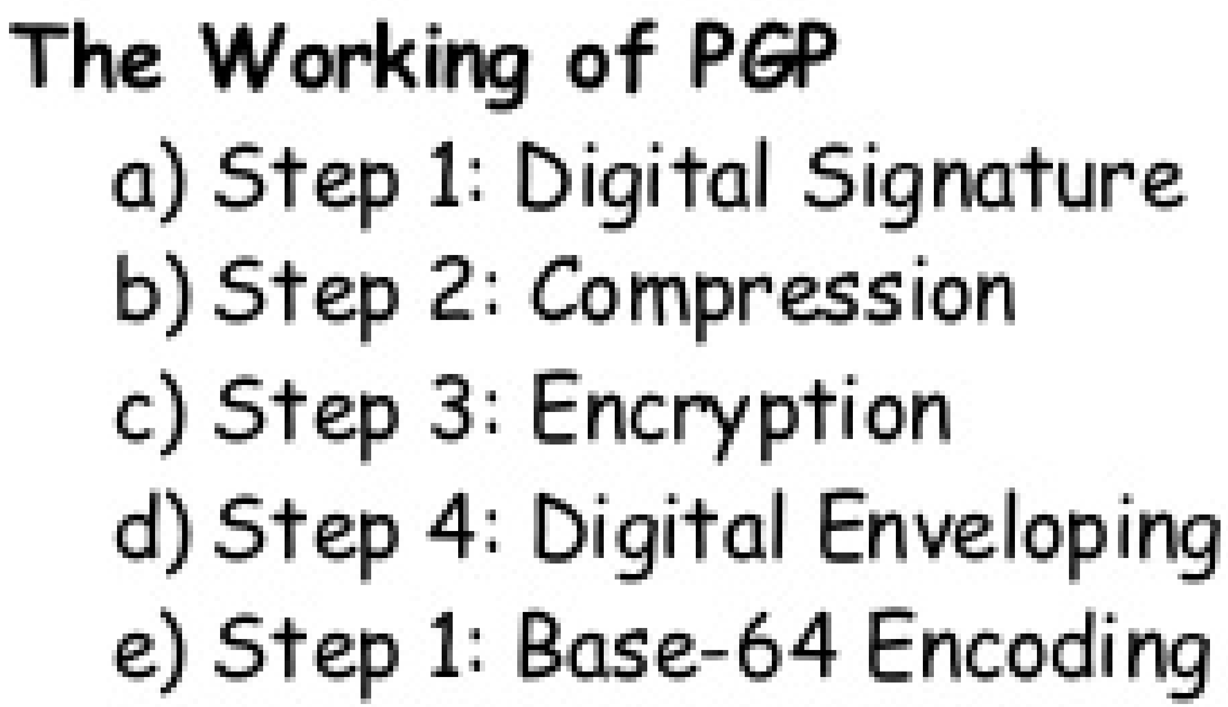
Image copied from internet (Not the complete PPT :P)

S/MIME: Functions

- ❑ Enveloped Data : Encrypted content and Associated keys
- ❑ Signed Data : Encoded message + Signed digest
- ❑ Clear-signed data : Clear text message + Encoded signed digest
- ❑ Signed & Enveloped Data : Nesting of signed & encrypted entities

“E-mail Security Protocol

Pretty Good Privacy (PGP)



The Working of PGP

a) Step 1: Digital Signature

b) Step 2: Compression

c) Step 3: Encryption

d) Step 4: Digital Enveloping

e) Step 1: Base-64 Encoding

Introduction

Phil Zimmerman is the father of the **Pretty Good Privacy (PGP)** protocol. The most significant aspects of PGP are that it supports the basic requirements of cryptography, is quite simple to use, and is completely free. Including its source code and documentation.

Moreover, for those organizations that require support, a low-cost commercial version of PGP is available from an organization called **Viacrypt** (now *Network Associates*). PGP has become extremely popular and is far more widely used, as compare to PEM. The E-mail cryptographic support offered by PGP is shown below:

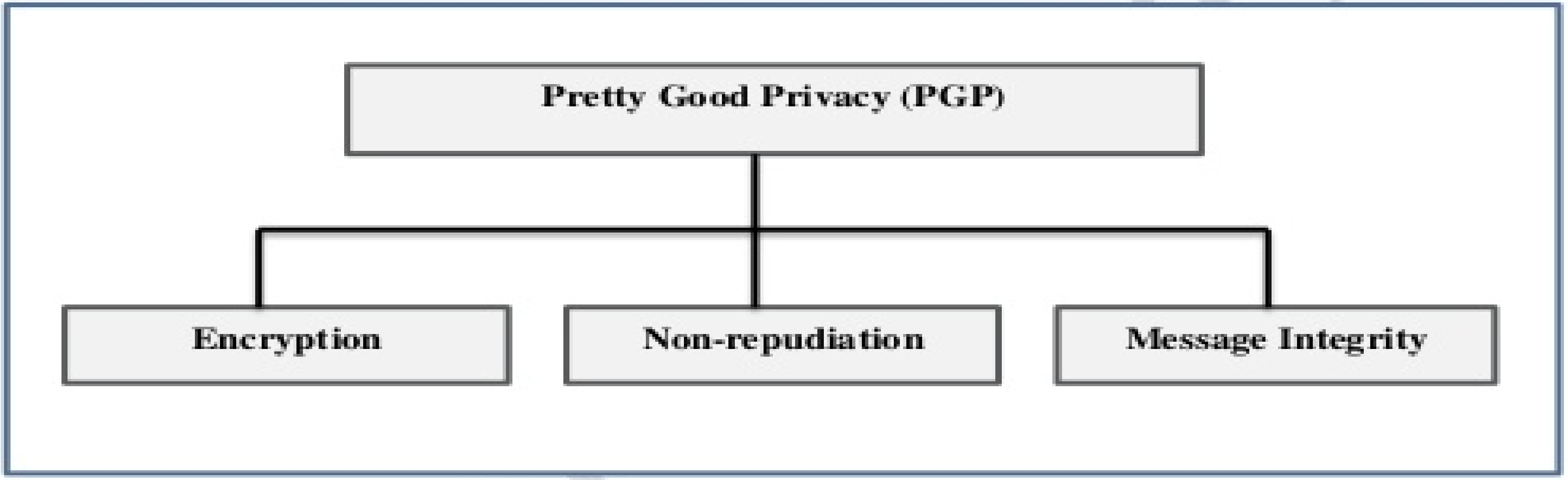


Fig: - Security Features offered by PGP

1 The Working of PGP

In PGP, the sender of the message needs to include the identifiers of the algorithm used in the message, along with the value of the keys. The broad-level steps of PGP are illustrated in the fig. as shown, PGP starts with a digital signature, which is followed by compression, then by encryption, then by digital enveloping and finally, by Base-64 encoding.

PGP allows for three security options when sending an email message. These options are.

- Signature (steps 1 and 2)
- Signature and Base-64 encoding (Steps 1, 2 and 3)
- Signature, Encryption, Enveloping, and Base064 encoding (Steps 1 to 5)

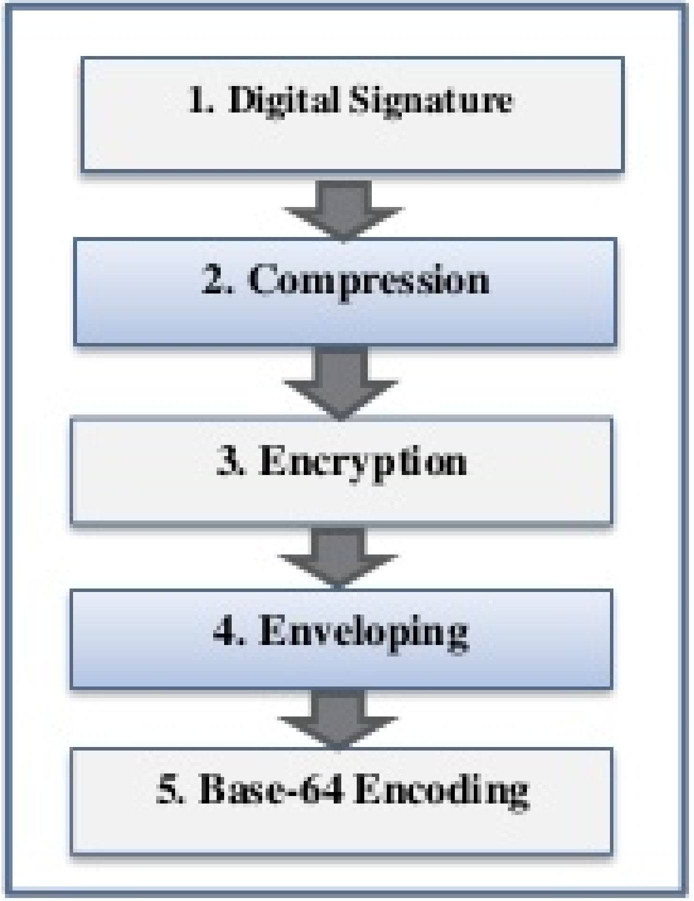


Fig: *PGP operation*

Step 1: Digital Signature

We had earlier discussed about the digital signature in the Step 1 of Privacy Enhance Mail protocol.

Step 2: Compression

This is additional step in PGP. Here, the input message as well as the digital signature are compressed together to reduce the size of final message that will be transmitted. For this, the famous ZIP program is used. ZIP is based on **Lempel-Ziv-algorithm**.

The *Lempel-Ziv-algorithm* looks for repeated strings or words, and stores them in a variable. It then replaces the actual occurrence of the repeated word or string with a pointer to the crossponding variable. Since a pointer requires only a few bits of memory as compare to original string, this this method reduces in the data being compressed.

Step 3: Encryption

In this step the compressed output of stem 2 (*the compression from of the original email and digital signature together*) are encrypted with a symmetric key. For this, generally the IDEA algorithm in CFB mode is used. We have already discussed this process in PEM (Privacy Enhance Mail) protocol.

Step 4: Digital Enveloping

In this case symmetric key used for encryption in step 3 is now encrypted with receiver public key. The output of stem 3 and step 4 together forms a digital envelope. This is shown in below figure:

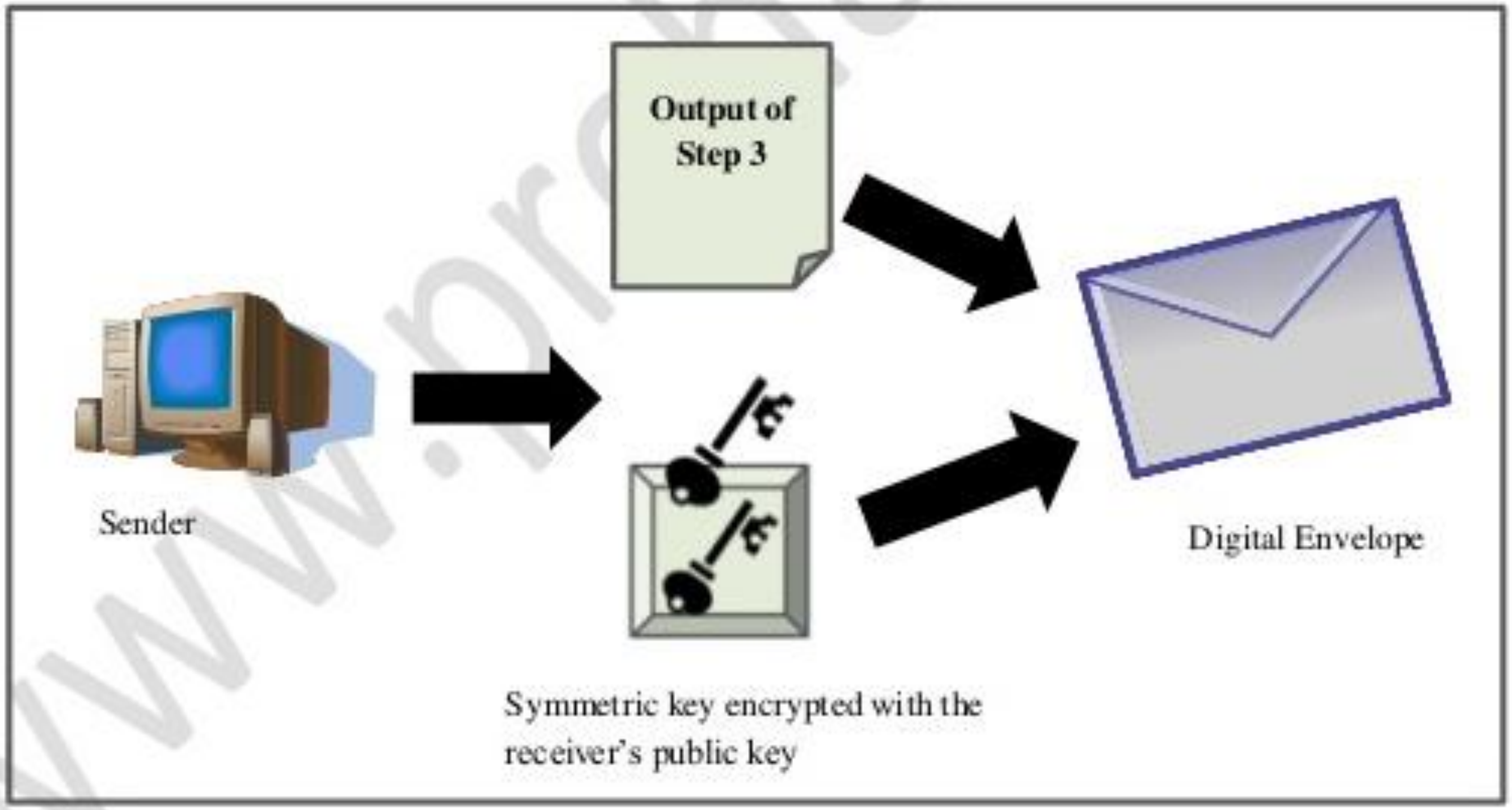


Fig: - Formation of Digital Envelope

Step 5: Base-64 encoding

The output of step 4 is Base-64 encoded; we have already discussed the process of this encoding in PEM (Privacy Enhance Mail) protocol.

2.2 PGP Algorithms

PGP supports a number of algorithms. The most common of them are listed below:

Algorithm type	**Description**
Asymmetric Key	RSA (Encryption and signing, Encryption only, Signing only)
	DSS (Signing only)
Message Digest	MD5, SHA-1, RIPE-MD
Encryption	IDEA, DES-3, AES

Table: - PGP Algorithms

PRETTY GOOD PRIVACY

(PGP)

SECURITY FOR ELECTRONIC EMAIL

PGP

- There are two main schemes which are especially designed to provide confidentiality and authentication for electronic mail systems. These are:

- PGP(Pretty Good Privacy)

- S/MIME(Secure/Multipurpose Internet Mail Extension)

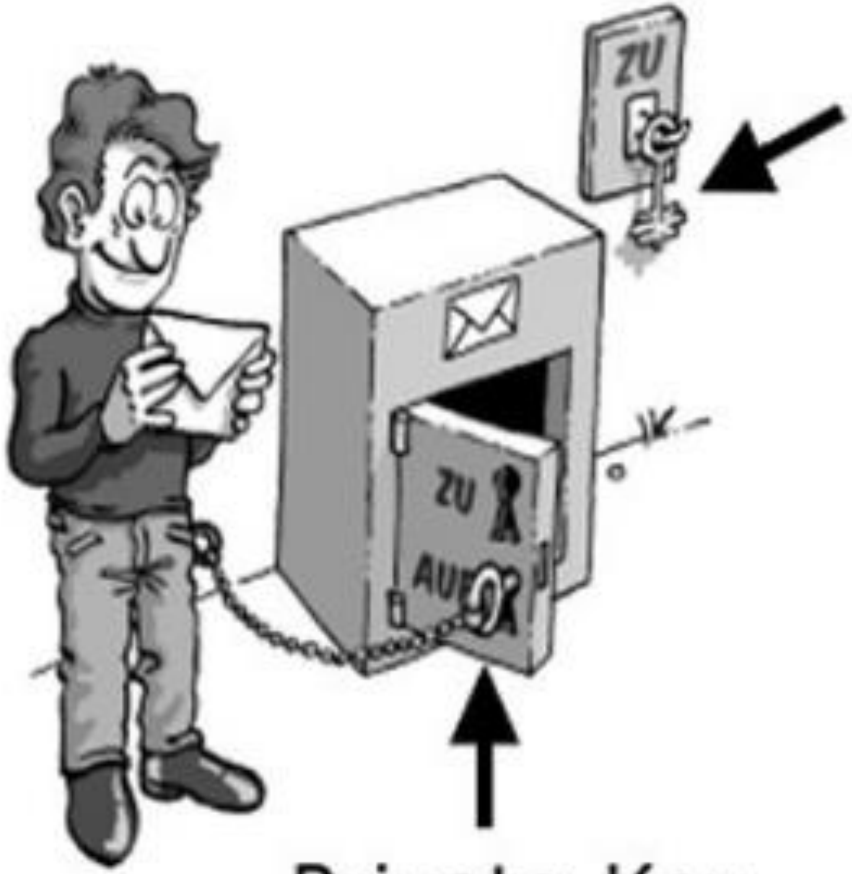
INTRODUCTION OF PGP

- Developed by Phil Zimmerman in 1995.
- Documentation and source code is freely available.
- The package is independent of operating system and processor.

- PGP does not rely on the "establishment" and it's popularity and use have grown extensively since 1995.
- PGP combines the best available cryptographic algorithms to achieve secure e-mail communication.
- It is assumed that all users are using public key cryptography and have generated a private/public key pair.

PRETTY GOOD PRIVACY

- PGP is a remarkable phenomenon that provides confidentiality, authentication, and compression for email and data storage.
- Its building blocks are made of the best available cryptographic algorithms: RSA, DSS, Diffie-Hellman.
- It is independent of operating system and processor.
- It has a small set of easy-to-use commands



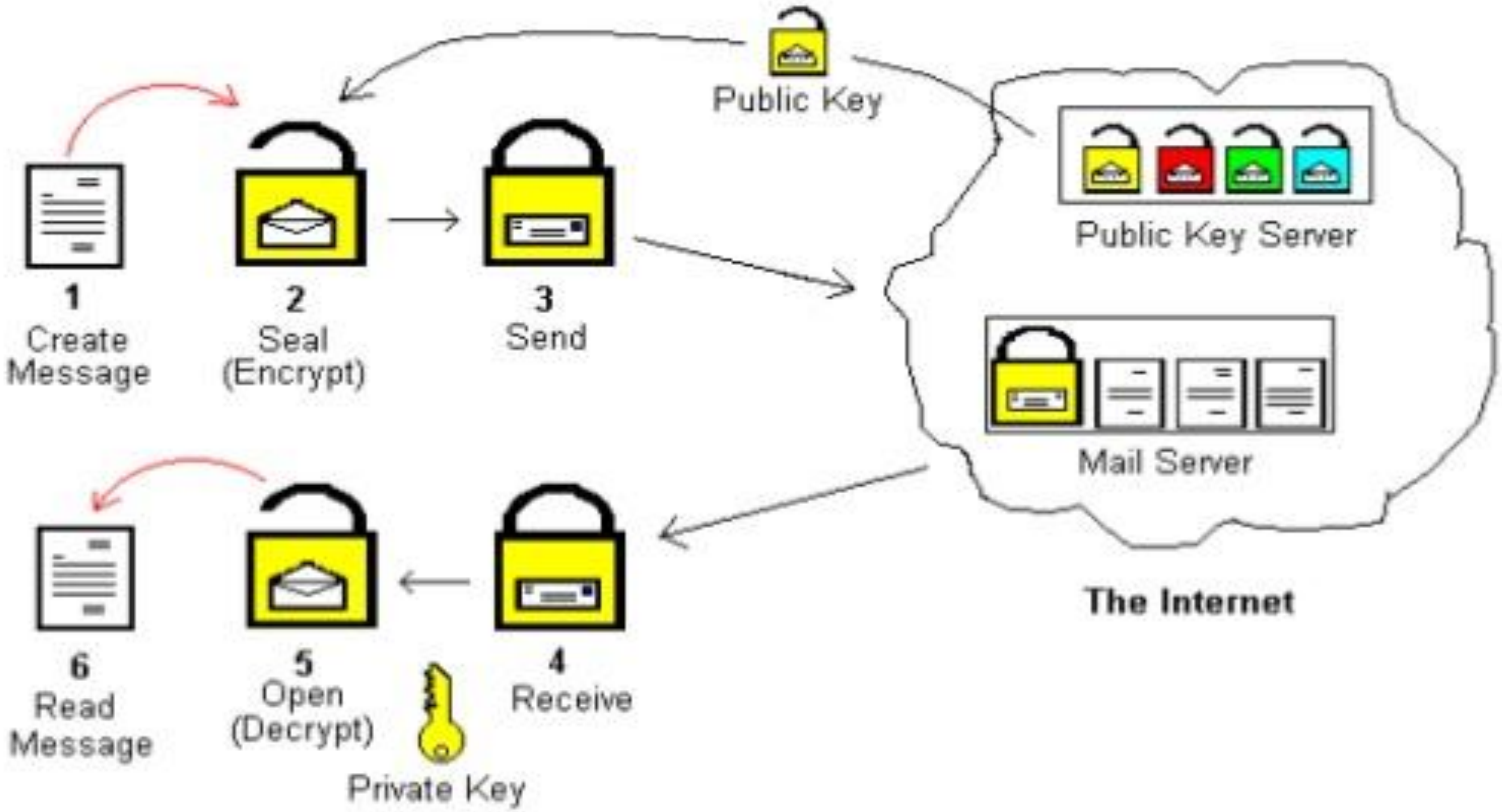
Public-Key

Private-Key

WHY USE PGP?

- Security
- Flexibility
- It's Free!
- Worldwide Strength and Compatibility

WORKING OF PGP



Design

- Compatibility
- Confidentiality
- Digital signatures
- Web of trust
- Certificates
- Security quality

ADVANTAGES OF PGP

- Your valuable information is always protected, others cannot view it, and it cannot be stolen over the Internet
- No compatibility problems - works with any email application that you or your recipients are using
- Verification of the sender of information ensures you are not being spoofed by a third party
- Absolute assurity that the information you send or receive has not been modified in transit
- Your secure mail and text cannot be infiltrated by hackers or infected and mis-used by email attacks

DISADVANTAGES OF PGP

- ADMINISTERING CONFLICTING VERSIONS
- COMPATIBILITY ISSUES
- COMPLEXITY
- NO RECOVERY

CONCLUSIONS

- Because PGP is freely available via the Internet, and has a fully compatible low-cost commercial version it is now widely used.
- It has a wide range of applicability from corporations to individuals who wish to communicate worldwide securely over the Internet and other networks.
- It is not controlled by any government which makes it attractive to many.