Microsoft Office Outlook PGP Add-in

Group 37

Instituto Superior Tecnico

December 15, 2013

Overview
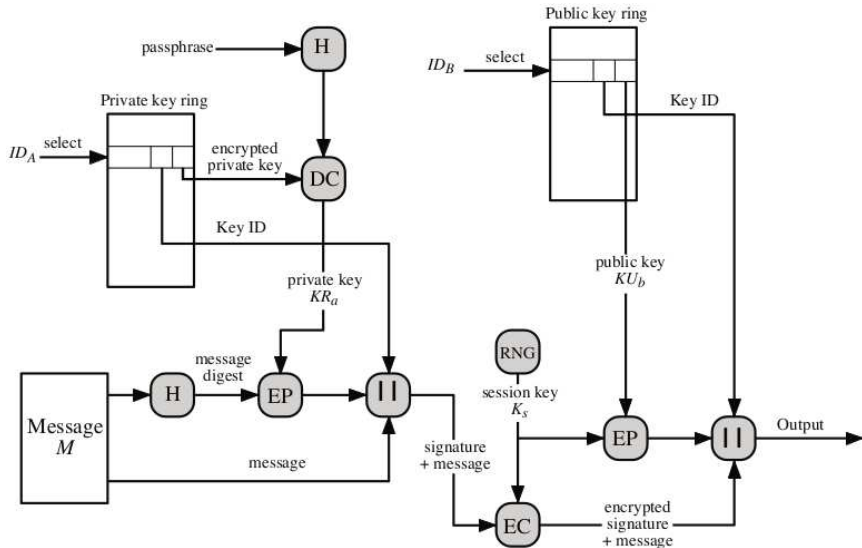
OpenPGP

- PGP, GnuPG, OpenPGP
- Used for:
    - Digital Signature (DSS/SHA or RSA/SHA)
    - Message Encryption(CAST-128, IDEA, 3-DES with RSA)
    - Compression
    - Compatibility (Radix-64 conversion)
- 1998, IETF WG, RFC 4880
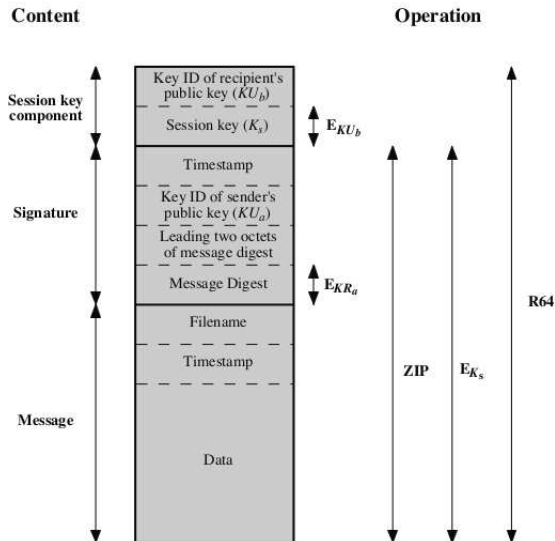- interoperability
- legal issues

How it works

1. 4 key types: passphrase, session-key, private key, public key
2. Public and private key rings
3. Passphrase encrypts private key ring
4. Every user can have a public-private key pair

How it works

How it works

Content

Operation

Session key component

Signature

Message

Key ID of recipient's public key (KU_b)

Session key (K_s)

E_{KU_b}

Timestamp

Key ID of sender's public key (KU_a)

Leading two octets of message digest

Message Digest

E_{KR_a}

Filename

Timestamp

Data

ZIP

E_{K_s}

R64

Design

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Implementation

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table: Table caption

Theorem

Theorem (Mass–energy equivalence)

$E = mc^2$

Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2012].

John Smith (2012)
Title of the publication
Journal Name 12(3), 45 – 678.

Demo