Lecture Notes

Security on the Internet

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

Winter 2008

28.10.08
SOFT 1

eMail

Goal:

- communication, discussion
- speed
- send information, share it
- send text messages
  (NOT entire DVDs!)
- make it easier, it's faster
  it's cheaper
- less paper
- connect geographically distributed parties
- notification
- independent of sender's & recipient's location

Format:

- pure text, electronic
- formatted: Header
  <blank line>
  Body

Thunderbird
Ctrl+U

Outlook
→ ? Pull to desktop and open the file
→ Properties give Headers

Special header lines:

From: <sender>

eg: From: Michael Nüsken <nuesken@bit....>

To: <recipient>

Subject: <subject>

Date: <sending date>

More:

Received: ~~~ } inserted by mail servers
Return-Path:
Cc:
Bcc: ← like a Cc: but must deleted before delivery.
X-Spam...
Priority:
... encoding info...
Message-ID: ...
... format info... (is it text or HTML or multipart...)
Reply-To: ...
... confirmation...

Before all that is one Line starting 'From_'
eg: From_ nuesken@bit.uni-bonn.de date

Transport of eMail?

Security?

Goals:

encryption

Confidentiality, Privacy
„Only Bob can read the email."

signature

Authenticity
Bob knows that it was Alice who sent the mail.

Integrity
The text wasn't changed underway.

Message flow confidentiality
Even the existence of the message stays 'secret'.

Non-repudiation
Alice cannot deny that she sent the mail. In other words, Bob can prove to Charlie that the mail is from Alice

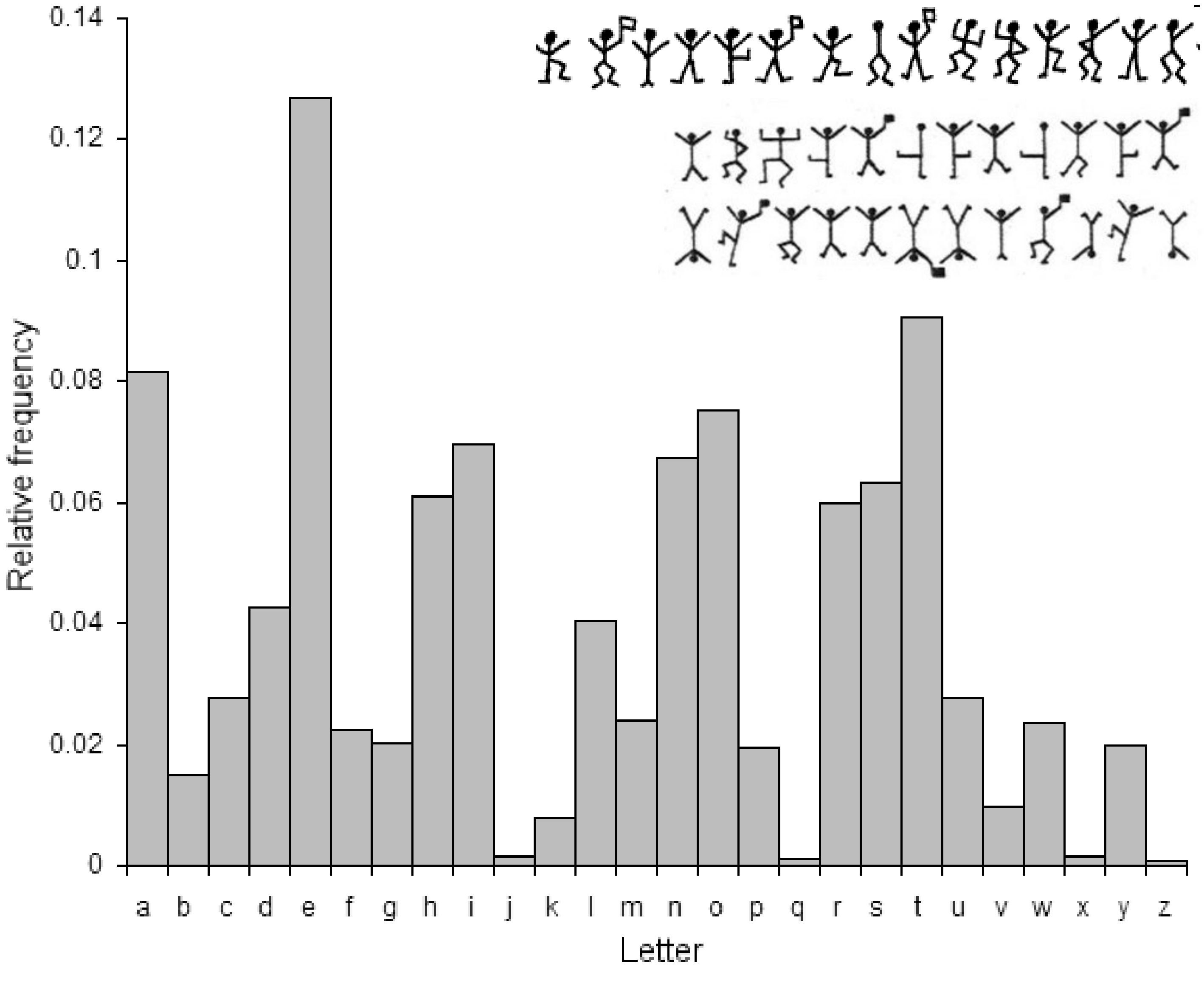
(Accessibility, Reliability)

Proof of submission
Proof of delivery
Anonymity

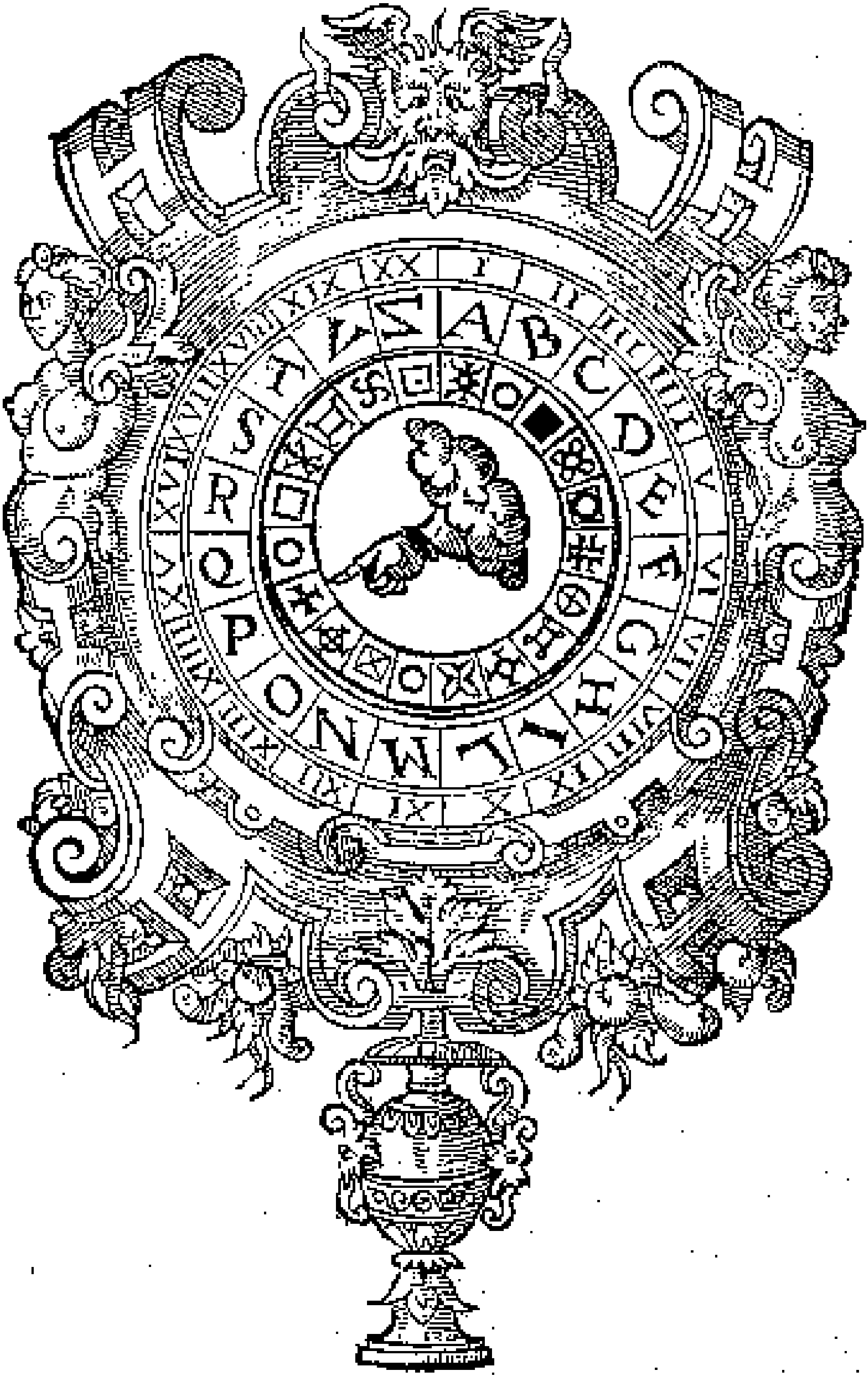
```
Return-Path: <08ws-soti-admin@bit.uni-bonn.de>
X-Original-To: nuesken@math.upb.de
Delivered-To: nuesken@math.upb.de
[...]
Received: by postfix.iai.uni-bonn.de (Postfix, from userid 13020)
        id 94C365C834; Mon,  3 Nov 2008 21:10:04 +0100 (MET)
X-Sieve: cmu-sieve 2.0
X-IAI-Env-From: <08ws-soti-admin@bit.uni-bonn.de> : [131.220.8.1]
Received: from uran.iai.uni-bonn.de (uran.iai.uni-bonn.de [131.220.8.1])
        by postfix.iai.uni-bonn.de (Postfix) with ESMTP
        id 97F4F5C829; Mon,  3 Nov 2008 21:10:03 +0100 (MET)
        (envelope-from 08ws-soti-admin@bit.uni-bonn.de)
        (envelope-to VARIOUS) (2)
        (internal use: ta=0, tu=1, te=0, am=-, au=-)
Delivered-To: 08ws-soti@alias.informatik.uni-bonn.de
X-IAI-Env-From: <first.family@uni-bonn.de> : [80.136.68.129]
Received: from [192.168.178.46] (p50884481.dip.t-dialin.net [80.136.68.129])
        by postfix.iai.uni-bonn.de (Postfix) with ESMTP
        id A1CCC5C829; Mon,  3 Nov 2008 21:09:55 +0100 (MET)
        (envelope-from first.family@uni-bonn.de)
        (envelope-to VARIOUS) (2)
        (internal use: ta=1, tu=1, te=1, am=P, au=first.family)
Message-ID: <490F5A8B.6000205@informatik.uni-bonn.de>
Date: Mon, 03 Nov 2008 21:09:47 +0100
From: First Family <first.family@uni-bonn.de>
Reply-To: first.family@uni-bonn.de
User-Agent: Thunderbird 2.0.0.17 (Windows/20080914)
MIME-Version: 1.0
To: 08ws-soti@bit.uni-bonn.de
Subject: [08ws-soti] 1234567
X-Enigmail-Version: 0.95.7
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
Sender: 08ws-soti-admin@bit.uni-bonn.de
Errors-To: 08ws-soti-admin@bit.uni-bonn.de
X-BeenThere: 08ws-soti@bit.uni-bonn.de
X-Mailman-Version: 2.0.4
Precedence: bulk
[...List-Stuff...]
X-Virus-Scanned: by mailscan-system at math.uni-paderborn.de
X-Spam-Status: No, hits=0.2 tagged_above=-999.0 required=4.0 tests=AWL,
        BAYES_00, DNS_FROM_SECURITYSAGE, SPF_PASS, SUBJ_HAS_UNIQ_ID,
        UNIQUE_WORDS
X-Spam-Level:

-----BEGIN PGP MESSAGE-----
Charset: UTF-8
Version: GnuPG v1.4.9 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

hQIOA8SRdzc1IdlqEAf/VqwMFWs1Y2rqD0AQgBjJAyVWshp6TnEFutXOEloM4q4z
CVtNAium3o2+6R3bToYgx7NIetmiQWsRm7o5QWmIeDKu6zu2ogvn275ik71vBAKk
0/M+IfUl2WSjpmYDZm62R2iAjwlQy6BbLbPeGXJ/AICm65mgajUT/mum8PA8ako6
EezCwYpbS3A0V0xHopKWDWtc9iUBaIsGR9xLozvcVyXXWMCJSV/BAHewoTFD8U57
vnMU0oSp/j8VjI+kp6koY86MJoNplcUUYG5j+IHnuJpfpIbxs2c5cNwYLKFuvZrV
RpnjoDq/61ATmssidZEw5mF4/utOG913ftKoCdXpGAf9Fzul4wPGUFOzcATLX4Ef
Q+I+x60keFC4K+mIwefsZHdhbT/XtilkeoFCtaHtvwWaqTuaSfxRnlaJshQzwHxL
[...]
aHvqZs9s5+264Q0yUgB8i7AVq6d64JL8lg1h3vKEcDdFFUbSlgEYjsQ0zFI4UK0i
H+xRNHEYaC8UN1EYbulOlx1MZxz3VQ8bneX7cWmuYggkYDM0XUWfX6OP3CKoCWoU
0mZbZWGzH+Il2nzeRO9/TOtHfF5enDO2yuEF3Fr6flFDjlsZIFDq4jdrZy6ucMuO
o2AR6QwuWJQO37KIiJg1ngcfA+SO+Mbdg803wuMH3ORVMNc1ejo5DYRlxw==
=suKP
-----END PGP MESSAGE-----
_______________________________________________
08ws-SotI mailing list
08ws-SotI@bit.uni-bonn.de
https://mailbox.iai.uni-bonn.de/mailman/listinfo.cgi/08ws-soti
```



Relative frequency
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
a b c d e f g h i j k l m n o p q r s t u v w x y z
Letter



One of Giovanni Battista Porta's cipher disks