Network Security (NetSec)

Summer 2015
Chapter 03: Application Level Security
Module 02: Email Security

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

Learning Objectives & Outline

SECURE MOBILE NETWORKING

Learning objectives

- Application level security has been designed in a number of protocols; the design of such protocols should be understood using (representative) examples.
- Comprehend email security using the example of PGP

- Outline
  (1) Securing Email is trivial; true or not?
  (2) Introduction to email security
  (3) Sender authentication and message integrity
  (4) Message confidentiality
  (5) Sender authentication, msg. integrity and confidentiality

Chapter 03, Module 02

Your Take on Email Security

What do you think about email security?

Your Take on Email Security

What do you think about email security?

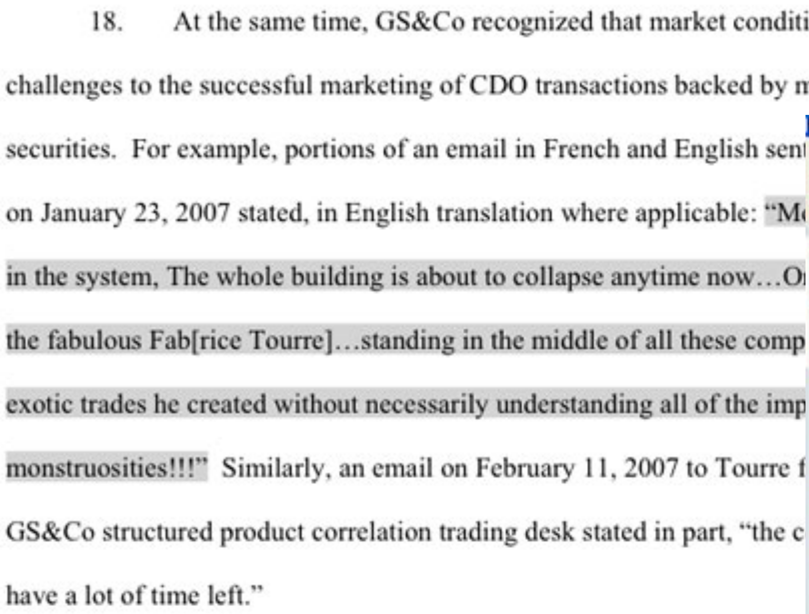

18. At the same time, GS&Co recognized that market conditions were presenting challenges to the successful marketing of CDO transactions backed by mortgage-related securities. For example, portions of an email in French and English sent on January 23, 2007 stated, in English translation where applicable: "M in the system, The whole building is about to collapse anytime now…O the fabulous Fab[rice Tourre]…standing in the middle of all these comp exotic trades he created without necessarily understanding all of the imp monstruosities!!!" Similarly, an email on February 11, 2007 to Tourre f GS&Co structured product correlation trading desk stated in part, "the c have a lot of time left."

Image source: http://businessinsider.com

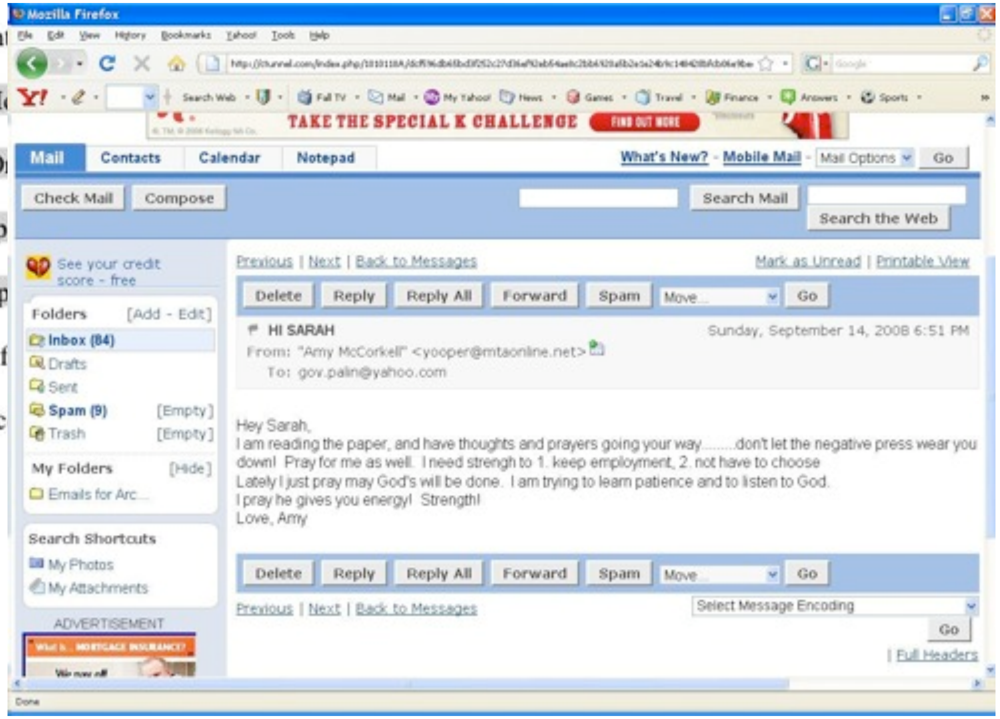


Image source: http://www.heise.de/tp/r4/artikel/28/28744/1.html

Introduction to Email Security

Email is one of the most widely used network services; essentially file transfer, except:

- has diversity (character sets, headers, …)
- not a transparent channel (text-based, 8 bit data, CRLF)
- often across realms

Can you think of other characteristics that might be special?

- Sender & receiver are not present at same time (store-and-forward)
- Distribution list -> where to perform explosion of list

Email Security as of Today

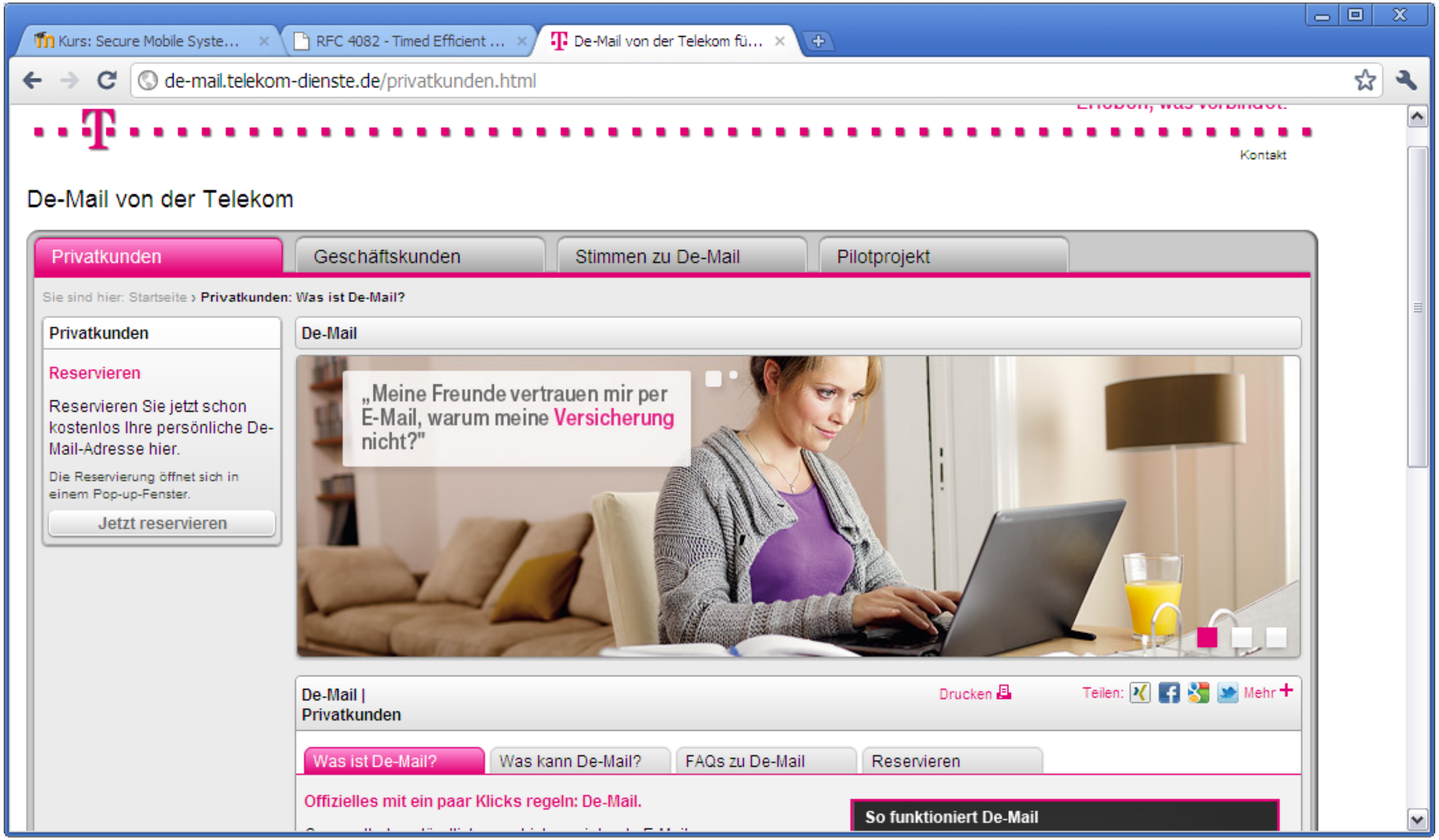
While we use SSL for web transactions regularly (and hence feel secure), in 2014, most of the email message contents are not secured in transit

- May be inspected either in transit
- Or by suitably privileged users on destination system
- Need to worry about sniffing, modifying, end-user masquerading, replaying

Goal should be rather

- Protection from disclosure
- Protection from modification
- Protection of authentication of sender of message
- Protection from denial by sender
- ...

De-Mail Anyone?



Possible features ...

Possible features

- confidentiality (privacy)
- authentication
- integrity
- non-repudiation
- plausible deniability
- proof of submission
- proof of delivery

More possible features

- message flow confidentiality
- anonymity
- containment; mark msgs, filter
- self-destruct
- message sequence integrity
- preventing post or back dating
- auditing, accounting

How do you do it

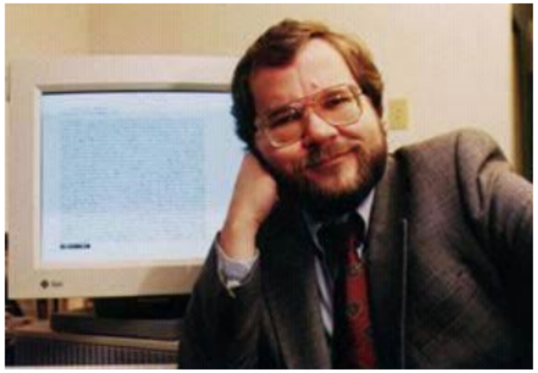
- In light of sniffing, masquerading, ...

PGP – Phil Zimmermann

SEMO SECURE MOBILE NETWORKING

> **"If privacy is outlawed, only outlaws will have privacy"**

Philip Zimmermann



Why I Wrote PGP

Part of the Original 1991 PGP User's Guide (updated in 1999)

"Whatever you do will be insignificant, but it is very important that you do it."

–Mahatma Gandhi.

It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance. Or you may be communicating with a political dissident in a repressive country. Whatever it is, you don't want your private electronic mail (email) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.

The right to privacy is spread implicitly throughout the Bill of Rights. But when the United States Constitution was framed, the Founding Fathers saw no need to explicitly spell out the right to a private conversation. That would have been silly. Two hundred years ago, all conversations were private. If someone else was within earshot, you could just go out behind the barn and have your conversation there. No one could listen in without your knowledge. The right to a private conversation was a natural right, not just in a philosophical sense, but in a law-of-physics sense, given the technology of the time.

But with the coming of the information age, starting with the invention of the telephone, all that has changed. Now most of our conversations are conducted electronically. This allows our most intimate conversations to be exposed without our knowledge. Cellular phone calls may be monitored by anyone with a radio. Electronic mail, sent across the Internet, is no more secure than cellular phone calls. Email is rapidly replacing postal mail, becoming the norm for everyone, not the novelty it was in the past.

Source: http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Secure smartphone communication: http://blog.cryptographyengineering.com/2014/03/here-come-encryption-apps.html

Pretty Good Privacy (PGP)

Widely used confidentiality and authentication service for securing electronic mail and other file storage applications

- developed by Phil Zimmermann
- selected best available crypto algorithms at the time
- integrated into a single program
- available on Unix, PC, Mac systems
- originally free, now have commercial versions available also
- was neither controlled by government nor standards organization
  - rather considered “subversive”, Zimmermann was subject of three year federal investigation (for allegedly breaking the Arms Export Control Act)

Consists of five services:

- (1) authentication, (2) confidentiality
- (3) compression, (4) e-mail compatibility, (5) segmentation

Pretty Good Privacy (PGP)

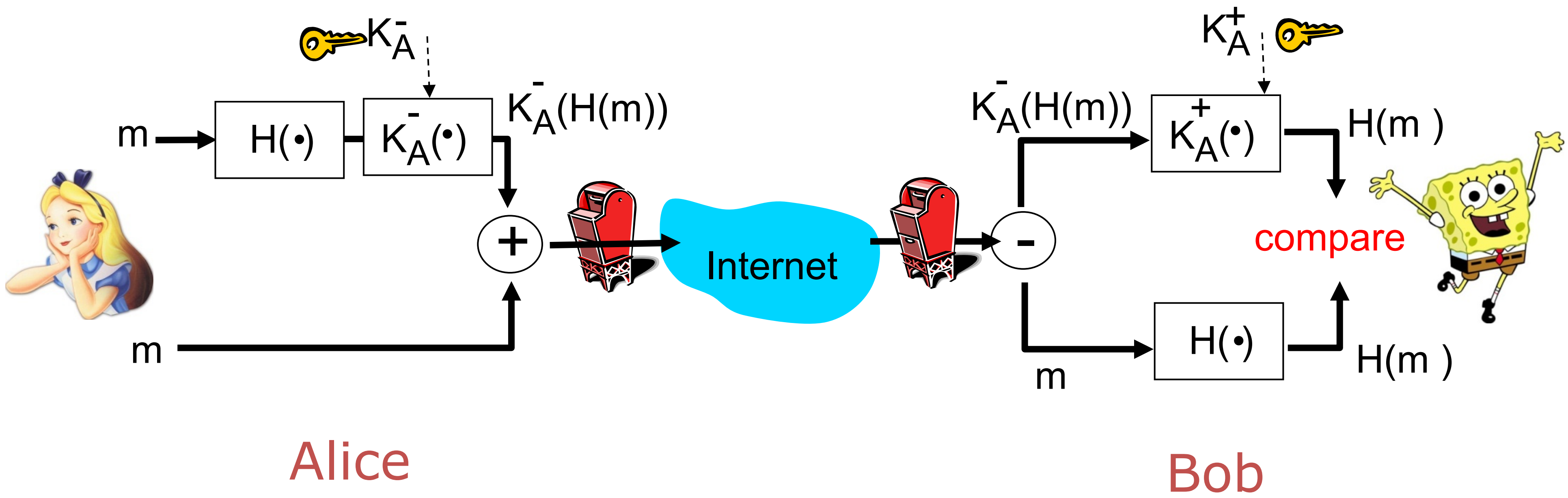
How to combine these five services?

- (1) authentication, (2) confidentiality
- (3) compression, (4) e-mail compatibility, (5) segmentation

Sender Authentication and Message Integrity

Alice wants to provide sender authentication message integrity

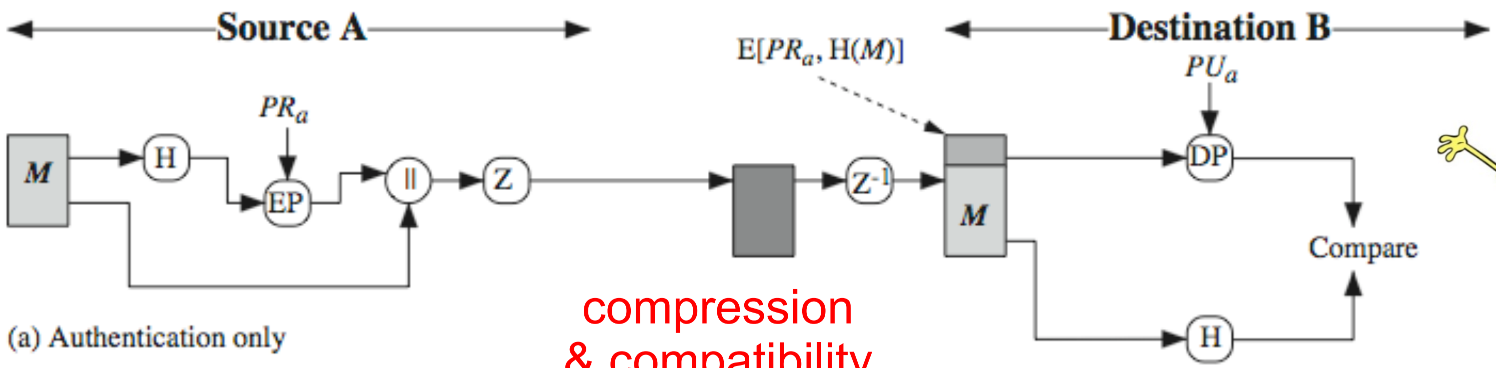
- Alice digitally signs message
- Sends both message (in the clear) and digital signature



[Image sources: Alice: visitgwinnett.wordpress.com, Bob: chicagonow.com]

Sender Authentication and Msg. Integrity: PGP Operation

1. Sender creates a message
2. SHA-1/SHA-2 used to generate 160-bit hash code of message
3. Hash code is encrypted with RSA using the sender's private key, and result is attached to message
4. Receiver uses RSA or DSS with sender's public key to decrypt and recover hash code
5. Receiver generates hash code for message, compares with decrypted hash code; if match, message is accepted authentic



(a) Authentication only

compression
& compatibility

Image Source: Stallings

Design Decisions
Authentication and Integrity

Public key?

- Implementation straightforward

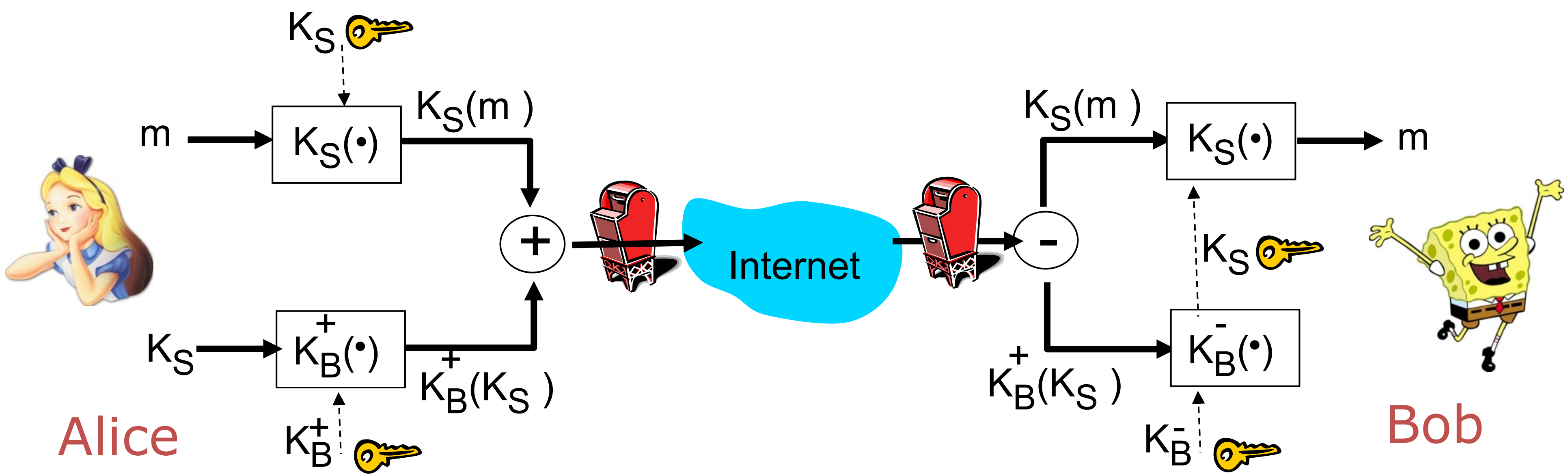
Secret key?

- Various possibilities
  - Keyed hash (HMAC) with per-user shared secret
  - MD encrypted with the shared secret
  - What about taking a per-message secret S, and doing any of the above using S?

Question: Why digital signatures for authentication? Why not a MAC?

Message Confidentiality

Alice wants to send confidential e-mail, m, to Bob.

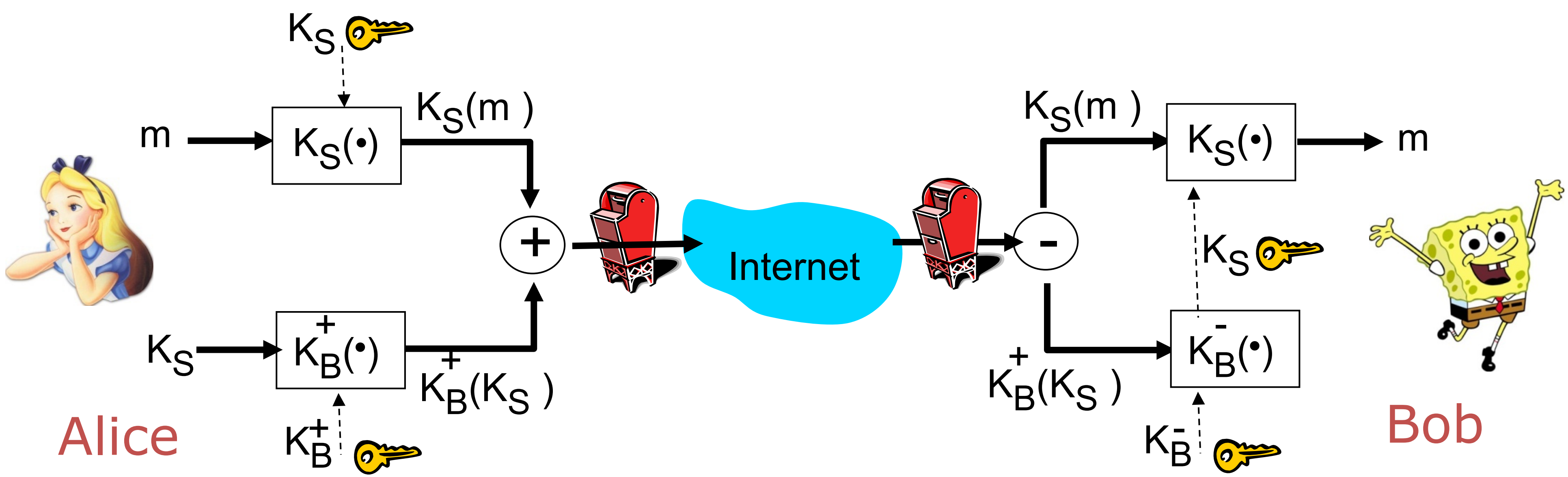


Alice:

- generates random *symmetric* key, K_S.
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

Message Confidentiality

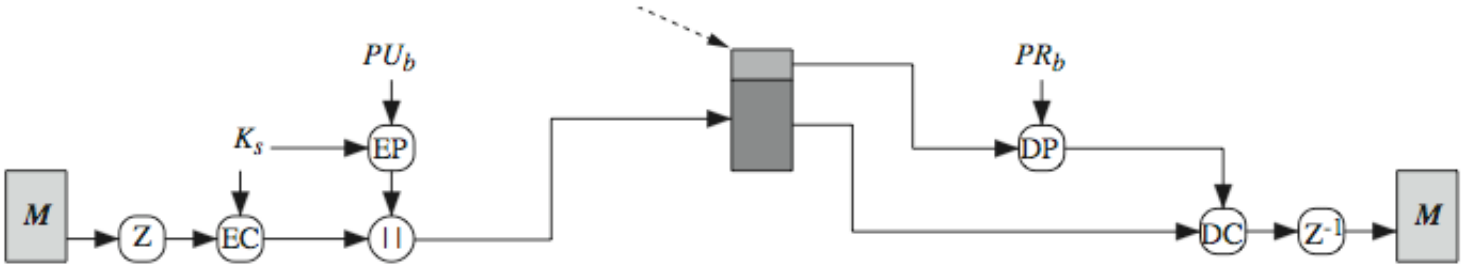
Alice wants to send confidential e-mail, m, to Bob



Bob:
- uses private key to obtain K_S
- uses K_S to decrypt $K_S(m)$

Message Confidentiality: PGP Operation

1. Sender generates message and random 128-bit number to be used as session key for this message only
2. Message is encrypted, using AES / CAST-138 / IDEA / 3DES with session key (and CFB)
3. Session key is encrypted using RSA with recipient's public key, then attached to message
4. Receiver uses RSA with its private key to decrypt and recover session key
5. Session key is used to decrypt message

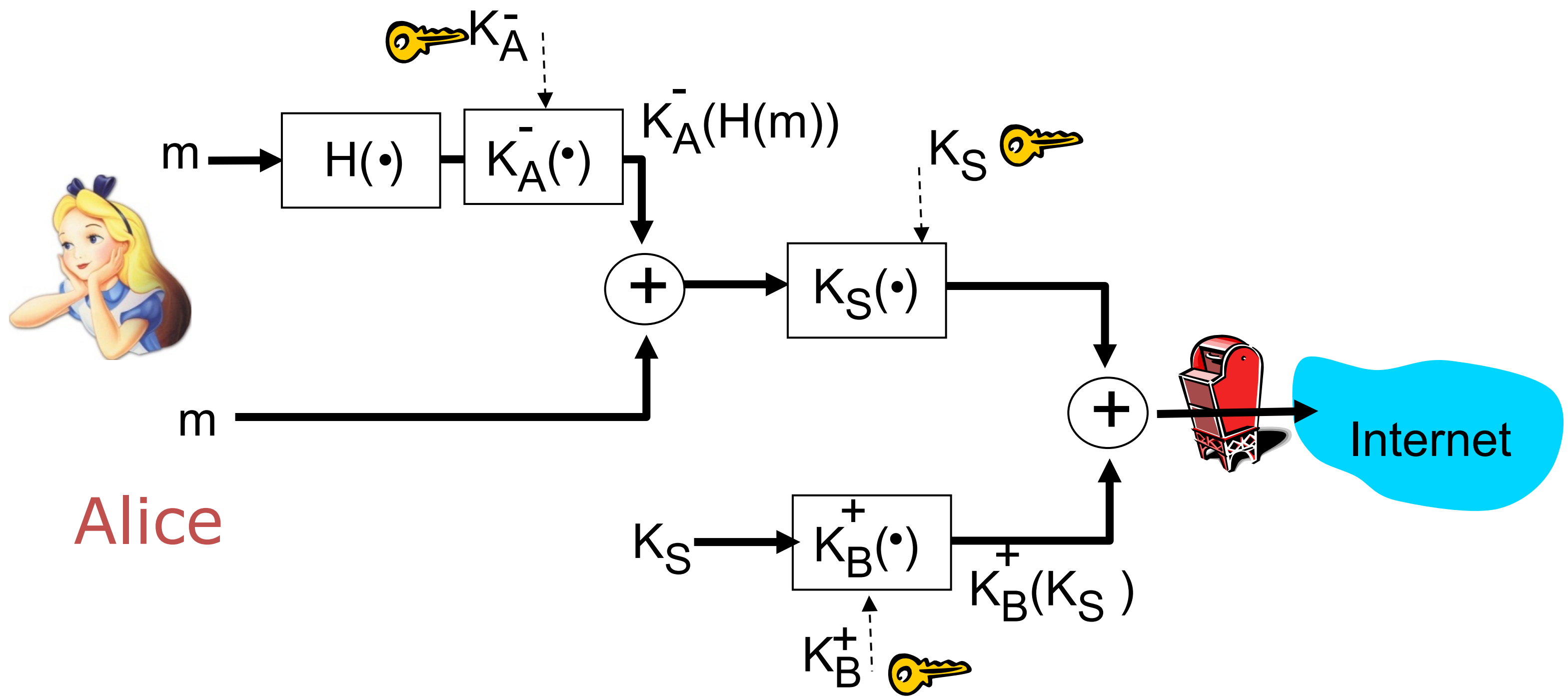


(b) Confidentiality only

Image Source: Stallings

Msg. Integrity, Confidentiality and Sender Authentication

Alice wants to provide sender authentication, message confidentiality and message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric (session) key

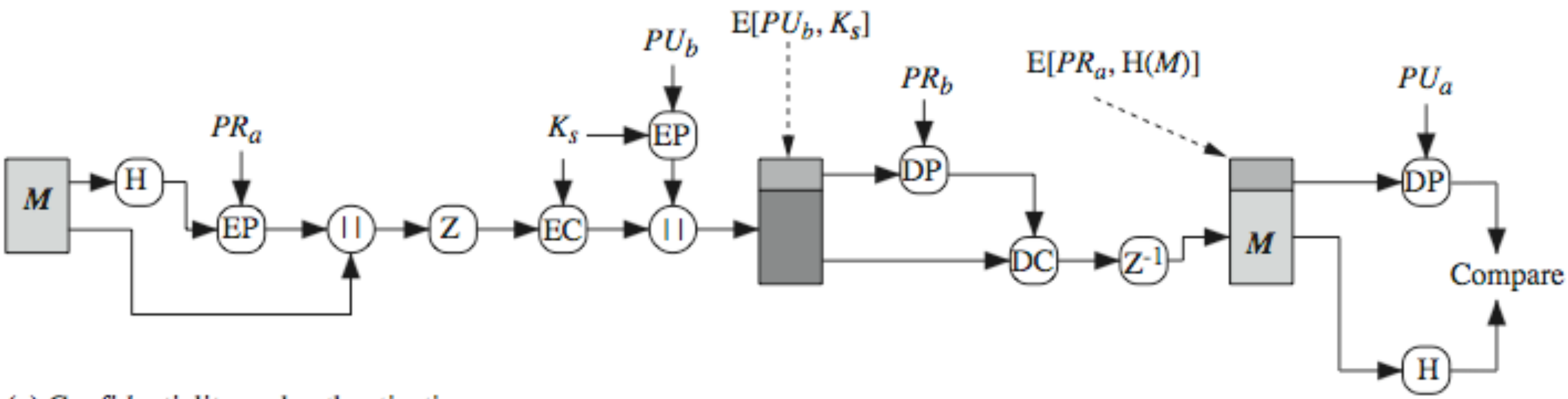
Msg. Integrity, Confidentiality and Sender Authentication: PGP Operation

Can use both services on same message

- Create signature & attach to message
- Encrypt both message & signature
- Attach RSA/ElGamal encrypted session key

By default PGP compresses msg. after signing before encrypting

- Placement of the compression algorithm is critical: why?



(c) Confidentiality and authentication

Image Source: Stallings

Other Security Goals?

Non-repudiation and plausible deniability

Public key crypto:

- Non-repudiation easy
- Plausible deniability hard

Secret key crypto:

- Vice versa

If you are interested to dig deeper:

- How to achieve plausible deniability with public key crypto?
- How to achieve non-repudiation with secret key crypto?
- How to achieve proof of submission/delivery

PGP Operation: Email Compatibility & Segmentation

SEEMOO SECURE MOBILE NETWORKING

When using PGP will have binary data to send (encrypted message, etc.)

- However email was designed only text
- Hence PGP must encode raw binar data into printable ASCII characte

Uses radix-64 algorithm

- maps 3 bytes to 4 printable chars (essentially base-64)
- also appends a CRC

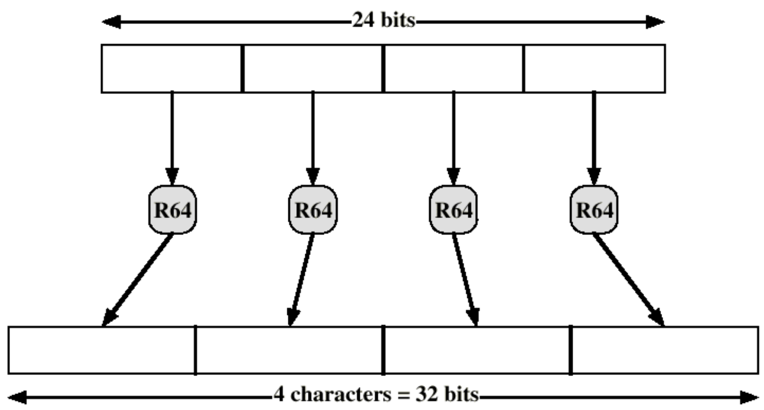
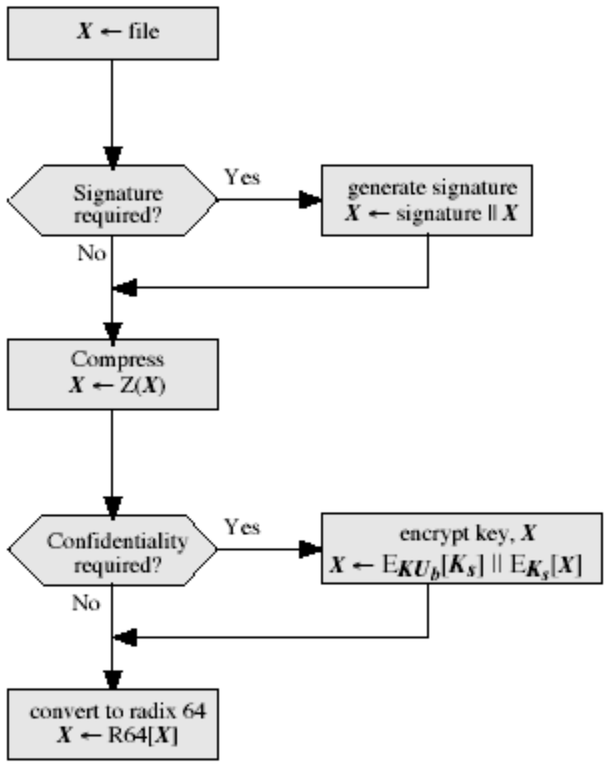


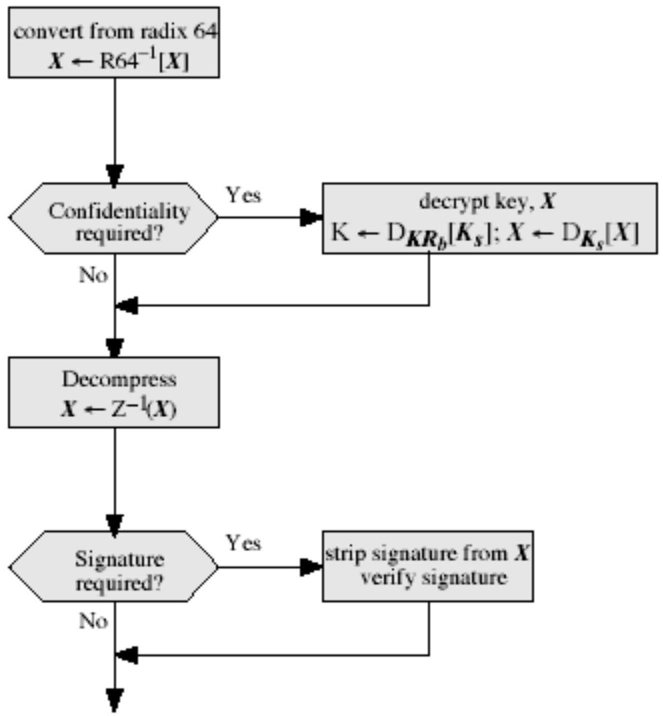
Figure 5.11 Printable Encoding of Binary Data into Radix-64 Format

Segmentation: divides email into blocks of size that can be handled by email-system

PGP Operation: Summary



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Some slides courtesy of G. Schäfer (TU Ilmenau) with changes of J. Schmitt (TU Kaiserslautern) and myself incorporated
- Some other slides courtesy of R. Perlman, S. Kent, K. Ross, Y. Chen, W. Stallings (and partners); changes of myself incorporated

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6
- [Stallings2014] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2014, ISBN: 978-0-136-10805-4
- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

Copyright Notice

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de