Kryptografie und Digitale Signaturen im Bibliotheksumfeld

Ein Vortrag von Florian Seiffert für die Inetbib 2000 am 09.03.2000 von 14:00-14:30 in Dortmund.

Ich konzentriere mich in diesem Vortrag überwiegend auf E-Mails (elektronische Postkarten), die getroffenen Aussagen gelten aber analog für alle anderen elektronischen Dokumente (WWW-Seiten, PDF-Dateien, Word-Dateien, News, ...).

Florian Seiffert
13.03.2000

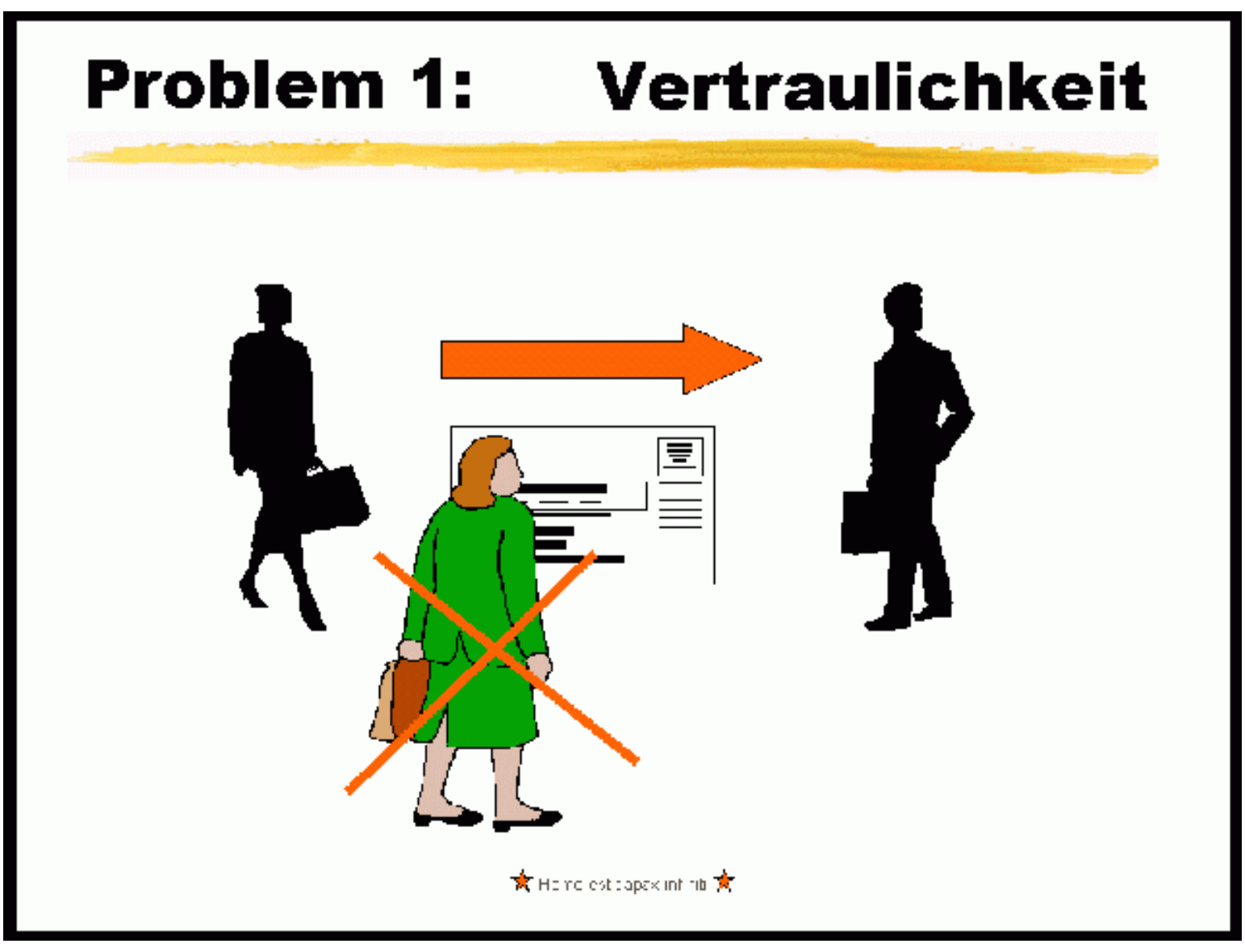
Einführung in das "Geheimnis" von Verschlüsselung und Digitalen Signaturen

Worum geht es?

Im Informationszeitalter, das nach allgemeiner Auffassung immer noch gerade beginnt, sind Daten und Informationen das wirtschaftlich wichtigste Gut. Um mit ihnen arbeiten zu können, sind sowohl die Authentizität und Integrität der Daten, also die gesicherte Erkenntnis, daß die vorliegenden Daten in genau dieser Form tatsächlich vom angegebenen Absender stammen, als auch die Geheimhaltung vertraulicher Daten unabdingbare technische Voraussetzungen. Gerade für Daten, die über das Internet verbreitet werden, ist beides normalerweise nicht gesichert. PGP schließt diese Lücke. Es verwendet moderne, gute Verfahren für digitale Unterschriften und für die Verschlüsselung vertraulicher Daten, auch ohne daß Sender und Empfänger irgendwelche weiteren Absprachen treffen müßten.
Die Tatsache, daß PGP bestens für den Einsatz durch Jedermann geeignet ist und im Gegensatz zu anderen Lösungen keinerlei zentrale Instanz voraussetzt, mit deren Glaubwürdigkeit das gesamte System steht und fällt, macht es zu einem wichtigen demokratischen Werkzeug, denn PGP gestattet dem mündigen Bürger, sein Grundrecht auf informationelle Selbstbestimmung selbst in die Hand zu nehmen, also selbst zu entscheiden, wer welche Informationen von ihm oder ihr verlangt. Da dies nicht von allen Entscheidungsträgern in Politik und Wirtschaft als unbedingt wünschenswert angesehen wird, sind Konflikte mit Regierungen gewissermaßen vorprogrammiert. Glücklicherweise ist die deutsche Bundesregierung kein solcher Konfliktgegner; in den USA sieht die Lage sehr viel weniger rosig aus. Diese Freiheit hat natürlich ihren Preis: Wie bei jedem Werkzeug, das dem einzelnen Endanwender viele Möglichkeiten bietet, lassen sich auch bei PGP durch Unkenntnis gravierende Fehler begehen. Im Gegensatz zu Tresoren, Bandschleifern, Briefumschlägen und Bildbearbeitungen ist es bei einem Verschlüsselungssystem aber für den Laien schwierig, die eigenen Fehler zu entdecken, bevor es zu spät ist. Daher möchte dieses Handbuch das nötige Wissen vermitteln, um PGP erfolgreich einzusetzen.

...

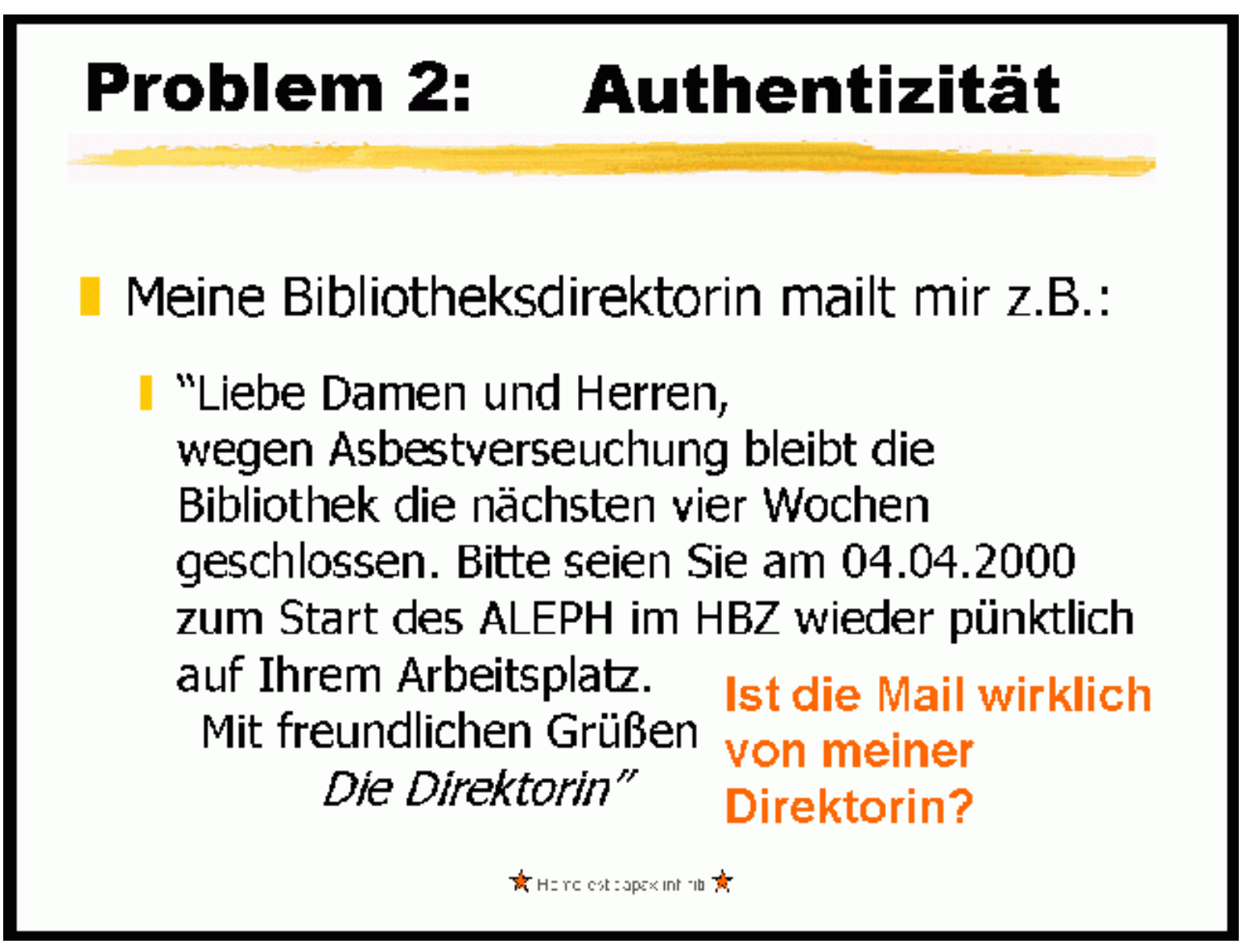
Stecken Sie Ihre Datenpostkarten zukünftig in Briefumschläge. Denn ohne PGP versandten Sie bisher keine E-Mails sondern lediglich E-Cards. Allerdings können wir Ihnen nicht alle Mühe abnehmen. Auch Sie müssen sich ein wenig plagen, PGP und die Verschlüsselung mit Öffentlichem und Privatem Schlüsseln zu verstehen. Es gibt keine Sicherheit mit "Klick&Go". Falsch verstandene und fahrlässig verwendete Verschlüsselung kann den Unsicherheitsgrad noch um den Faktor erhöhen, dass Sie sich nun sicher glauben, aber dennoch ausspioniert werden (Zitiert nach: http://www.foebud.org/pgp/auflage4/html-dateien/pgp.html).



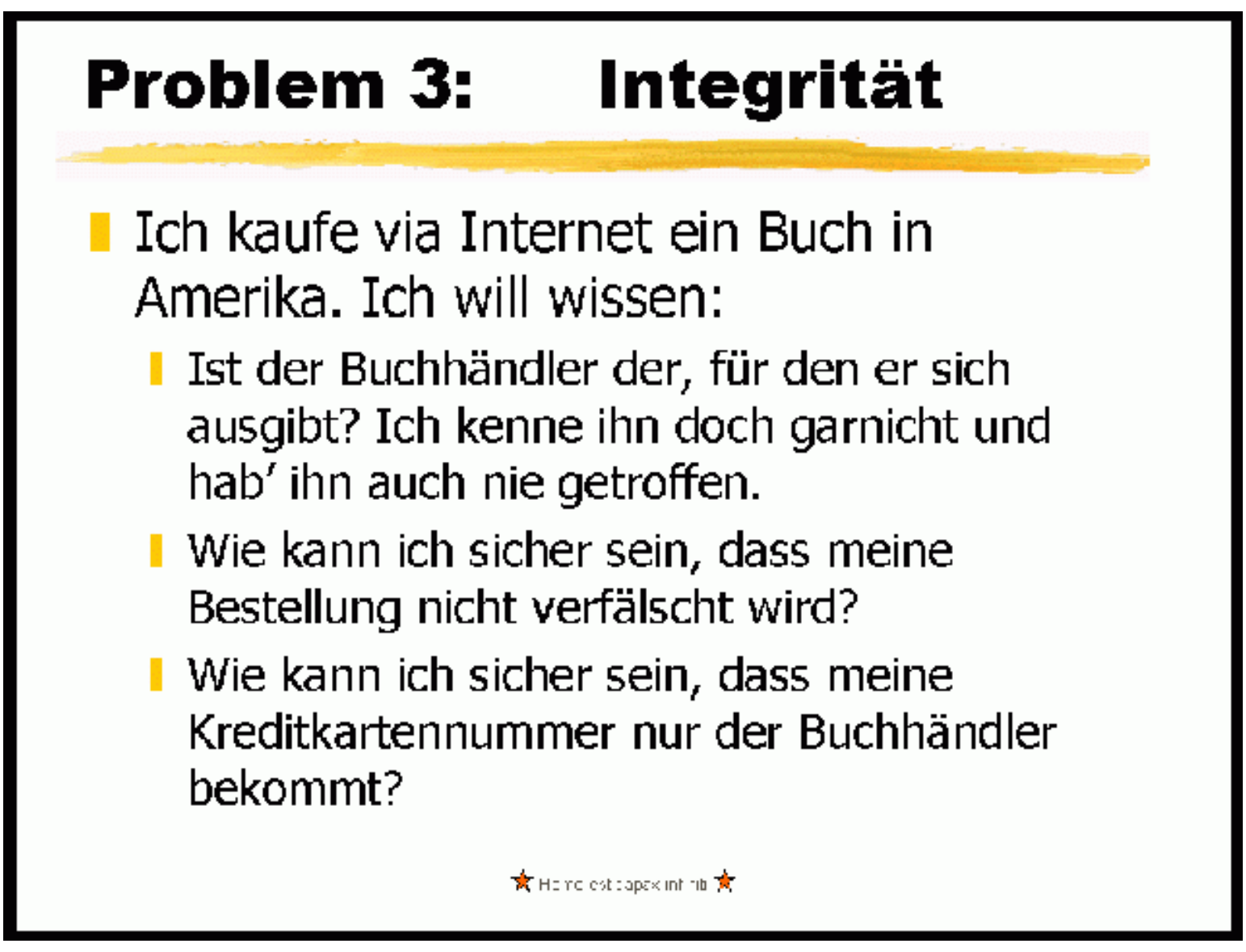
Stellen Sie sich vor, Sie möchten eine elektronische Postkarte (E-Mail) an Ihren Freund schicken und möchten nicht, dass die "Vermieterin", die Briefträgerin oder eine Systemadministratorin den Inhalt der Postkarte mitliest. Es geht also um **Vertraulichkeit**.

Ein Fall aus dem Leben:
Die Freeware 'Send It' von 'Delphi-Total' zur Verwaltung von E-Mails verschickte heimlich von jeder E-Mail eine Kopie an die Programmautoren. "Eine Verletzung des Briefgeheimnisses liegt nicht vor, weil eine E-Mail kein verschlossenes Schriftstück ist. Und das Ausspähen von Daten ist nur strafbar, wenn der Täter eine besondere Zugangssicherng überwindet." sagt Rechtsanwalt Stefan Jaeger dazu [6].

Was ist zu tun?



Sie bekommen obige Mail von Ihrer Direktorin. Es stellt sich die Frage: Ist sie authentisch? Wie kann ich gerade bei E-Mails sicher sein, daß sie wirklich von der genannten Absendeadresse stammen?



Wie kann ich bei E-Mails sicher sein, dass sie z.B. zusätzlich auch noch unverfälscht sind?

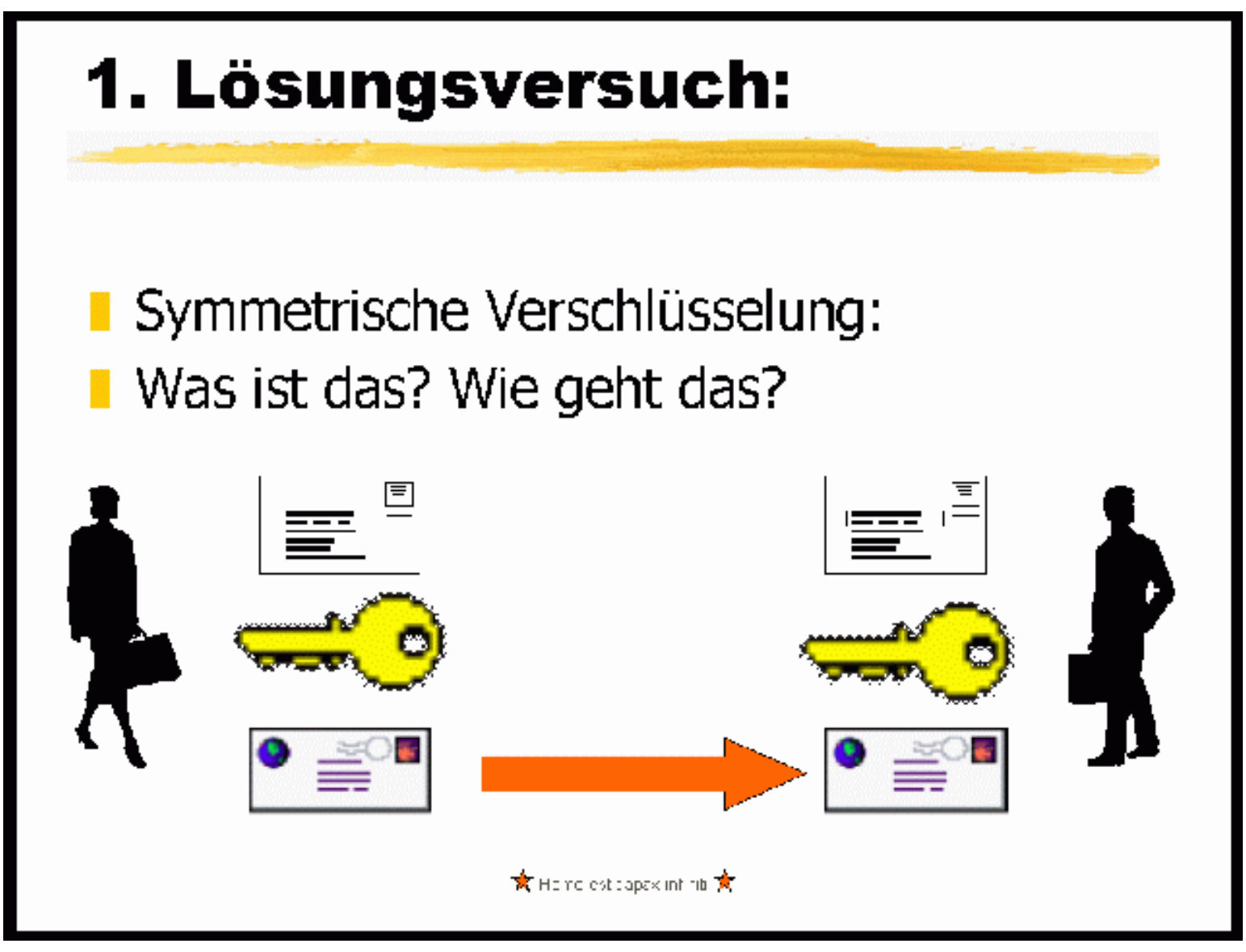
Die drei Beispiele machen somit deutlich, dass wir im Internet Kommunikation brauchen, wo

- Vertraulichkeit
- Authentizität
- Integrität

gesichert sind.

Florian Seiffert
13.03.2000

1. Lösungsversuch: Symmetrische Verschlüsselung

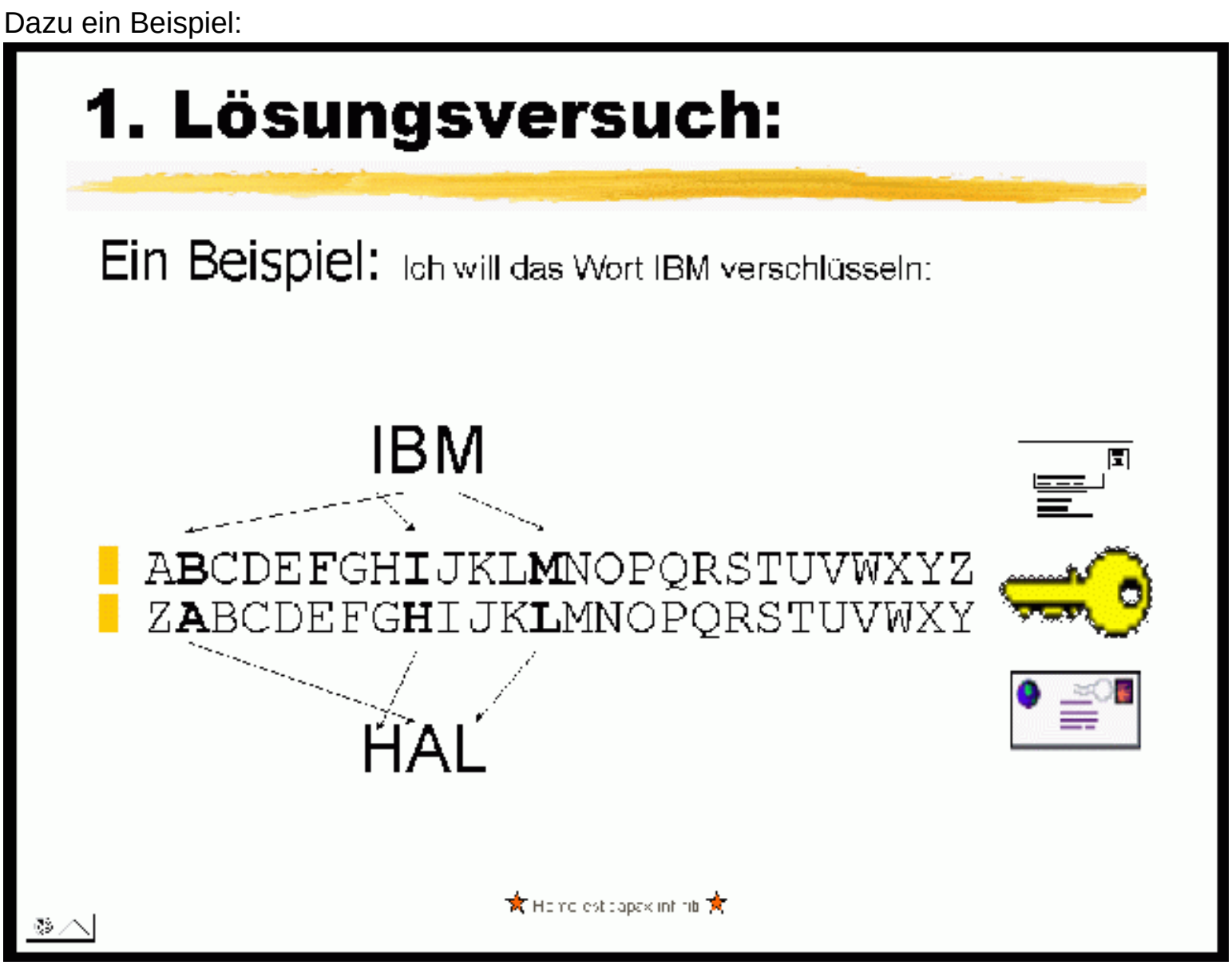


Versuchen wir den drei Problemen mit symmetrischer Verschlüsselung beizukommen.

- Sie schreiben eine Postkarte (E-Mail)
- Sie verschlüsseln die E-Mail, machen aus der Postkarte somit
- einen elektronischen Brief.
- Sie übermitteln den elektronischen Brief zu Ihrem Freund.
- Dieser nimmt den elektronischen Brief
- entschlüsselt den Brief durch Rückwärtsanwendung der von Ihnen benutzten Verschlüsselung.
- Er erhält somit wieder die ursprüngliche Postkarte. Soweit, so gut.

Da der Schlüssel zum Ver- und Entschlüsseln identisch sind, heißt die Methode: Symmetrisch. (Wenn es nicht auch asymmetrische Verschlüsselung gäbe, müssten wir das hier nicht besonders erwähnen.)

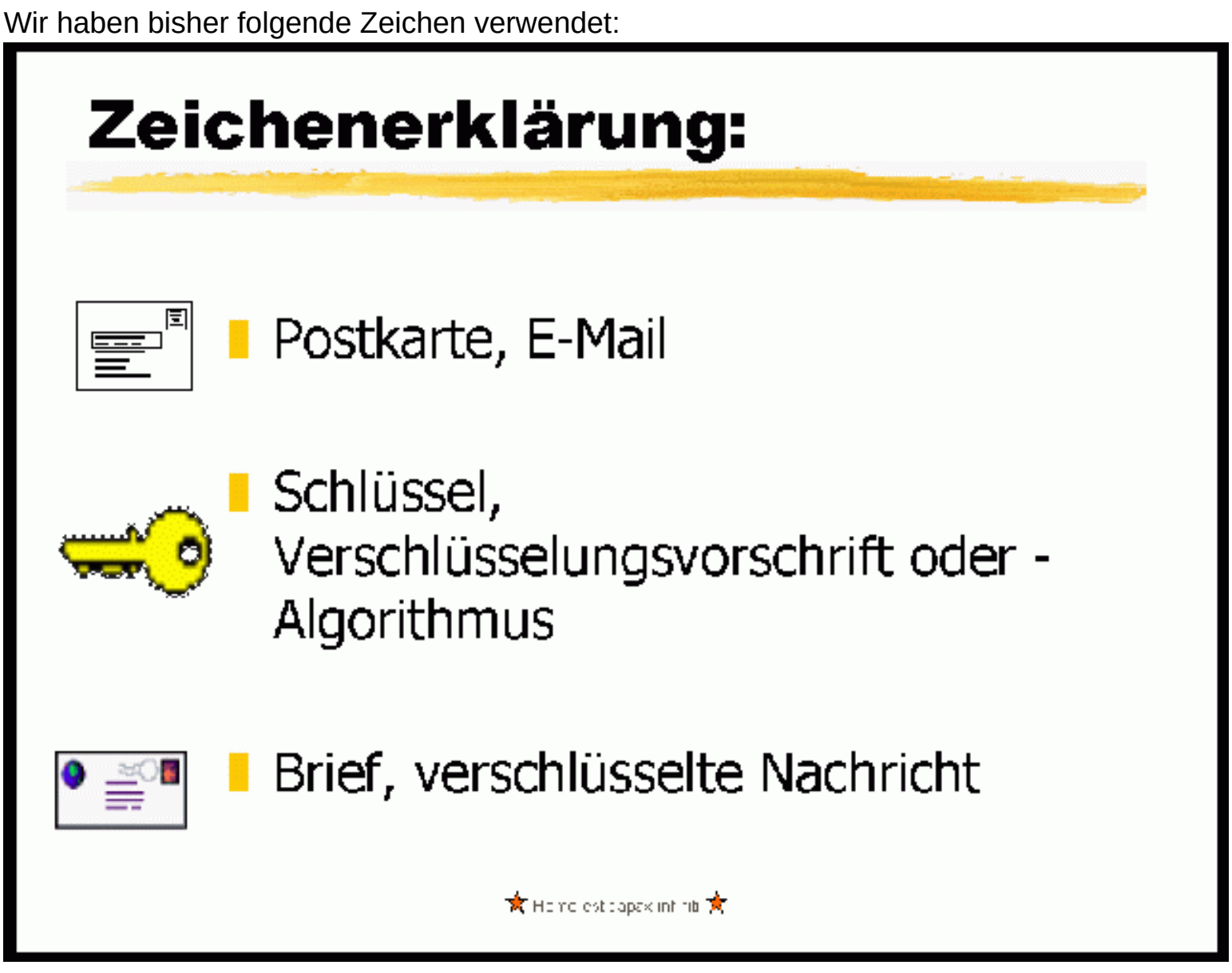
Dazu ein Beispiel:



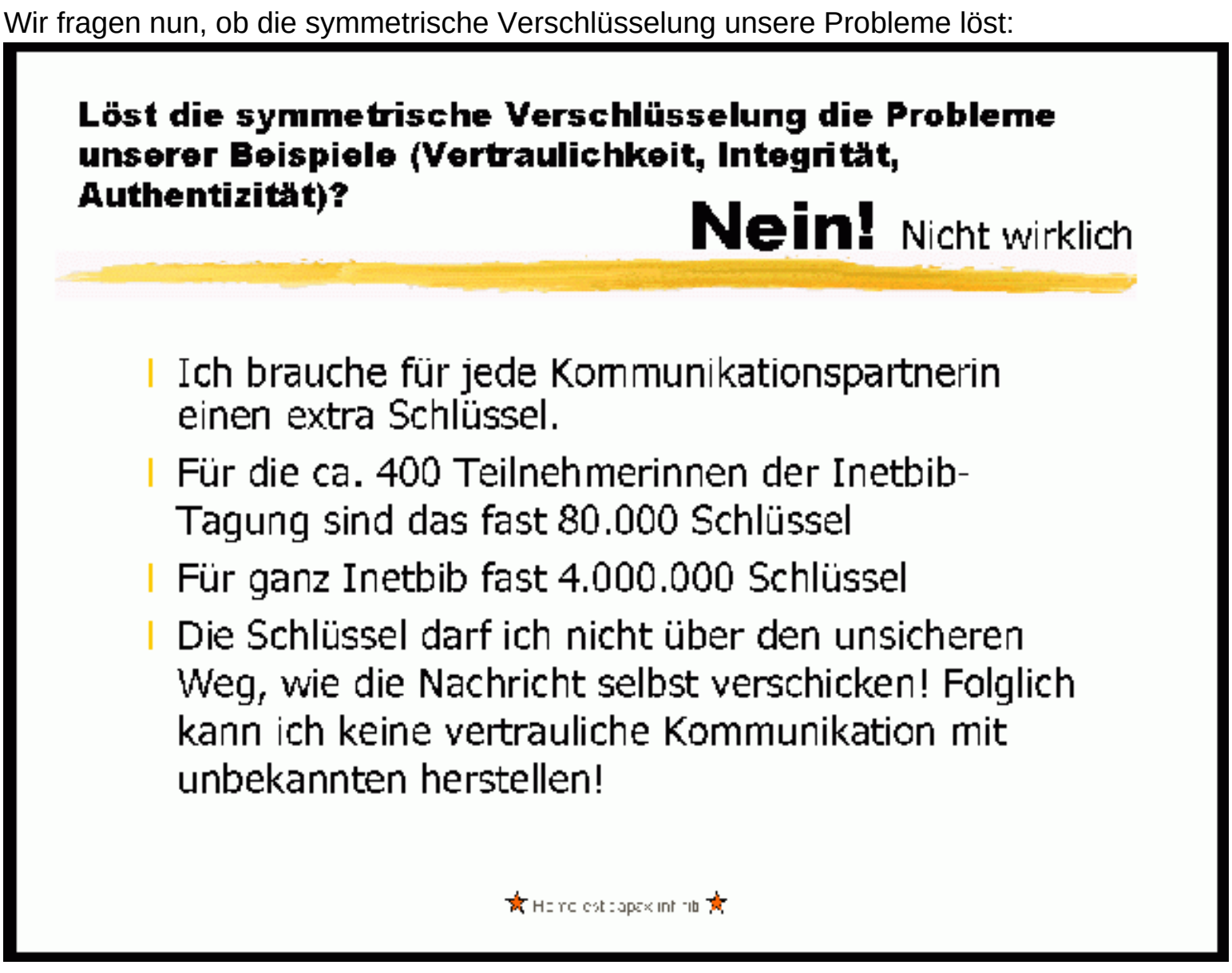
Wir wollen das Wort IBM verschlüsseln. Wir wählen als Beispiel ein sehr einfaches Verschlüsselungsverfahren. Wir verschlüsseln durch Verschieben der Buchstaben im Alphabet um eine Position. Aus I wird H, aus B wird A, aus M wird L. Aus der elektronischen Postkarte (E-Mail), wird so ein elektronischer Brief!

Julius Caesar verwendet ein solches Verfahren, wobei alle 7 Zeichen das Alphabet um eine weitere Position weitergeschoben wurde.

Wir haben bisher folgende Zeichen verwendet:



Wir fragen nun, ob die symmetrische Verschlüsselung unsere Probleme löst:

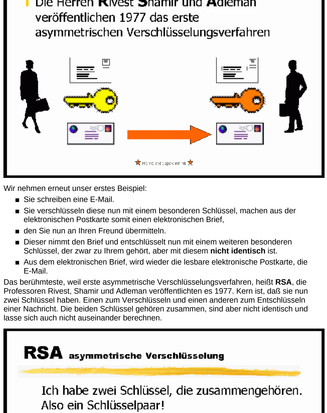


- Kommunikation im Internet, die Vertraulichkeit, Integrität und Authentizität sicherstellt, läßt sich mit symmetrischer Verschlüsselung erreichen, was wir hier nicht weiter vertiefen.
- Durch die Zahl der Schlüssel, die ich brauche, um vertrauliche Kommunikation herzustellen und durch das Problem, dass ich mit Unbekannten (wir denken an den Buchhändler in Amerika) keinen gesicherte Schlüssel austauschen kann, löst symmetrische Verschlüsselung unsere Probleme nicht wirklich.

Wir probieren also was anderes!

Florian Seiffert
13.03.2000

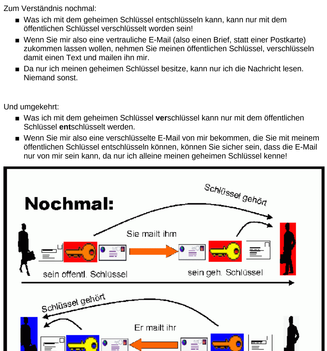
2. Lösungsversuch: Asymmetrische Verschlüsselung



Wir nehmen erneut unser erstes Beispiel:

- Sie schreiben eine E-Mail.
- Sie verschlüsseln diese nun mit einem besonderen Schlüssel, machen aus der elektronischen Postkarte somit einen elektronischen Brief,
- den Sie nun an Ihren Freund übermitteln.
- Dieser nimmt den Brief und entschlüsselt nun mit einem weiteren besonderen Schlüssel, der zwar zu Ihrem gehört, aber mit diesem **nicht identisch** ist.
- Aus dem elektronischen Brief, wird wieder die lesbare elektronische Postkarte, die E-Mail.

Das berühmteste, weil erste asymmetrische Verschlüsselungsverfahren, heißt **RSA**, die Professoren Rivest, Shamir und Adleman veröffentlichten es 1977. Kern ist, daß sie nun zwei Schlüssel haben. Einen zum Verschlüsseln und einen anderen zum Entschlüsseln einer Nachricht. Die beiden Schlüssel gehören zusammen, sind aber nicht identisch und lasse sich auch nicht auseinander berechnen.



Wichtig ist, dass Sie Ihren geheimen Schlüssel geheim halten, denn er wird so wertvoll werden, wie Ihre Unterschrift!

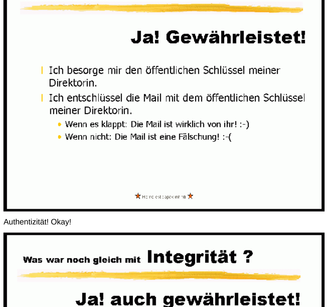
Zum Verständnis nochmal:

- Was ich mit dem geheimen Schlüssel entschlüsseln kann, kann nur mit dem öffentlichen Schlüssel verschlüsselt worden sein!
- Wenn Sie mir also eine vertrauliche E-Mail (also einen Brief, statt einer Postkarte) zukommen lassen wollen, nehmen Sie meinen öffentlichen Schlüssel, verschlüssein damit einen Text und mailen ihn mir.
- Da nur ich meinen geheimen Schlüssel besitze, kann nur ich die Nachricht lesen. Niemand sonst.

Und umgekehrt:

- Was ich mit dem geheimen Schlüssel **ver**schlüssel kann nur mit dem öffentlichen Schlüssel **ent**schlüsselt werden.
- Wenn Sie mir also eine verschlüsselte E-Mail von mir bekommen, die Sie mit meinem öffentlichen Schlüssel entschlüsseln können, können Sie sicher sein, dass die E-Mail nur von mir sein kann, da nur ich alleine meinen geheimen Schlüssel kenne!

Wir fragen nun nochmal nach den drei Anfangsproblemen:



Vertraulichkeit! Okay!

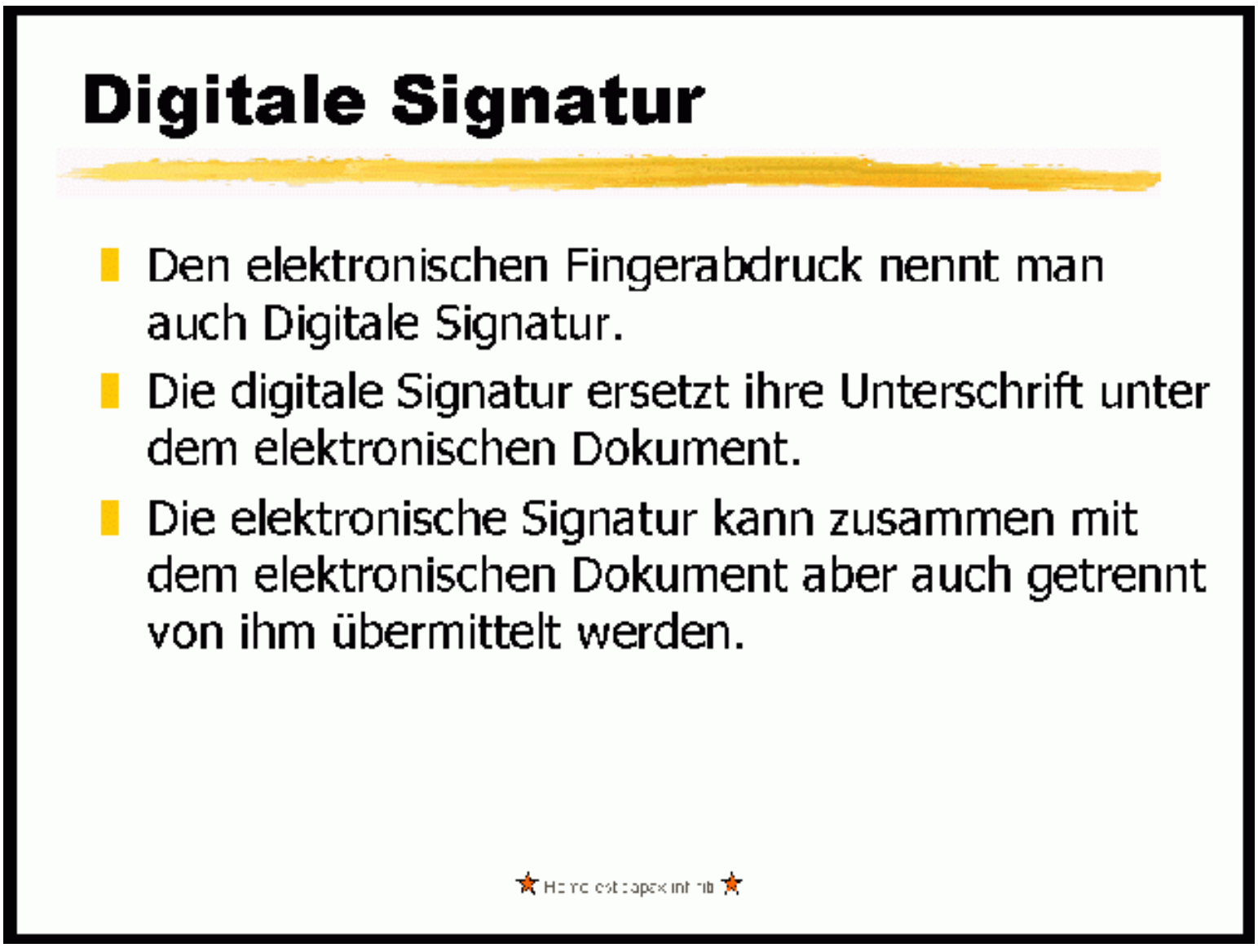
Authentizität! Okay!

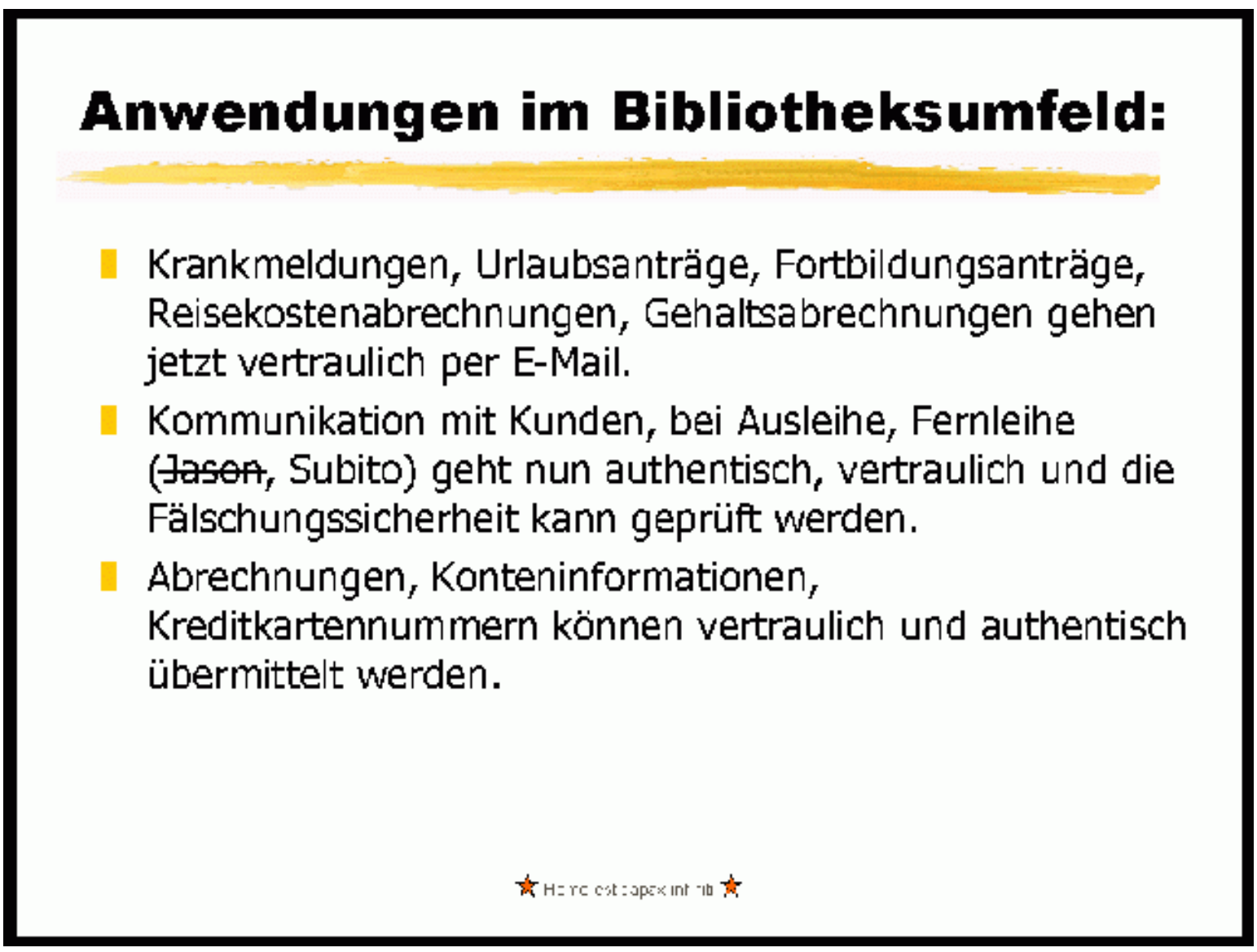
Integrität! Okay!

Ergebnis (Hurra!):

Wir haben also mit der asymmetrischen Verschlüsselung eine Methode der Kommunikation gefunden, bei der Authentisch, Vertraulich und Integrität sichergestellt sind.

Digitale Signatur





Ist das denn nun ganz so einfach, wie es sich hier anhört?

- Bei Verschlüsselung und digitalen Signaturen, gibt es (wie so oft) kein "Klick and Go"!
- Sie müssen sich die Mühe machen, die Vorgänge bei der asymmetrischen Verschlüsselung zu verstehen und zu durchschauen!
- Sie können die Ver- und Entschlüsselung Ihrer E-Mails nicht ohne Gefahr Ihrem Sekretariat überlassen!

Lesen Sie dazu auch: Digitale Signatur und ihre juristische Bedeutung

---

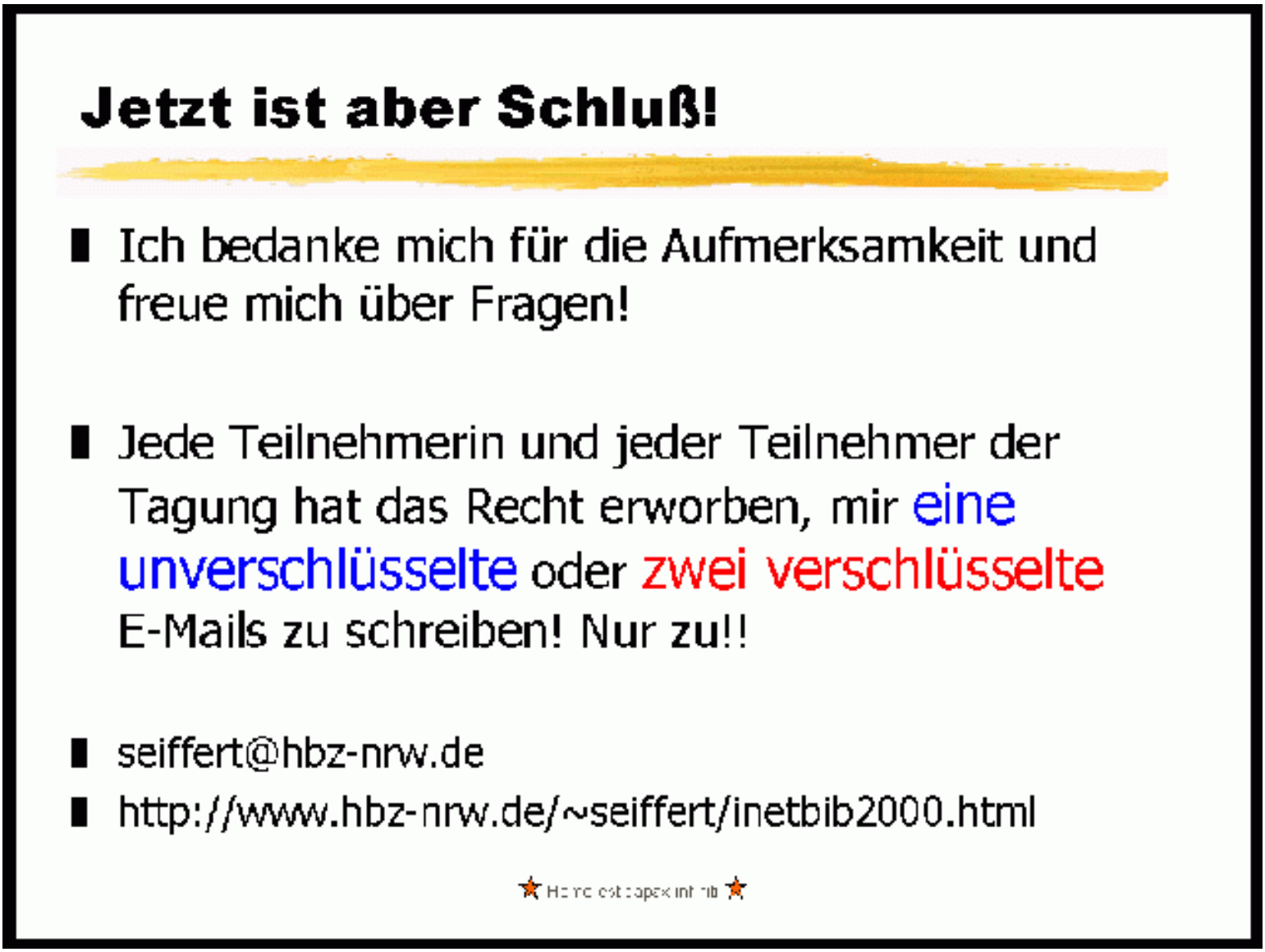
Florian Seiffert
13.03.2000

Pretty good Privacy: PGP

- Es gibt mit PGP ("Pretty good Privacy" = "recht gute Privatshäre") ein Freeware-Programm, welches die Handhabung der asymmetrischen Verschlüsselung sehr erleichtert.
- Die Landesbeauftragte für den Datenschutz in Nordrhein-Westfalen empfiehlt für die E-Mail-Verschlüsselung PGP! Lesen Sie dazu die sehr gute Broschüre, die kostenlos mit CD zu haben ist.

Florian Seiffert
13.03.2000

Jetzt ist aber Schluß

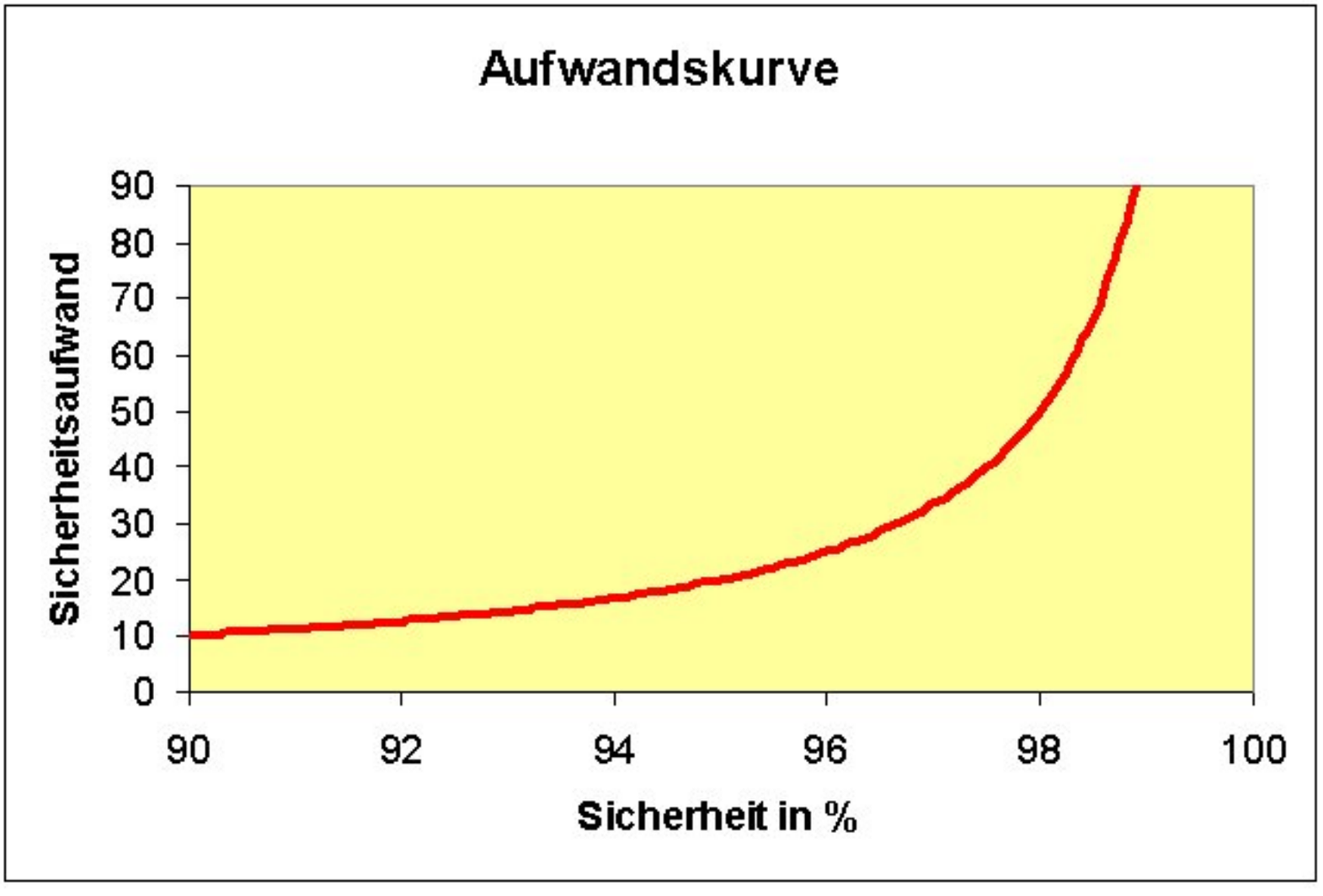


Der Vortrag (nur 20 Minuten Zeit) endet hier. Zum Thema Sicherheit noch ein paar weiterführende Hinweise.

Florian Seiffert
13.03.2000

100 prozentige Sicherheit?

Bedauerlicherweise ist es nicht möglich 100 prozentige Sicherheit zu erlangen. "Klick&Go" gibt es bei Sicherheit schon garnicht. Den Aufwand (in Geld, Mühe, Begreifen, ...), den Sie leisten müssen, steigt mit dem Maß an Sicherheit, welches Sie brauchen oder verlangen!



Dies führt uns zu dieser berühmten Aufwandskurve. Sie gilt sehr allgemein. Z.B. wenn es um den Aufwand geht, ein Dokument von Tippfehlern zu befreien oder wenn es darum geht, ihren Computer sicher vor Viren oder Datenspionen zu machen. Der Weg von 90% zu 95%, kostet so viel, wie der von 95% zu 97%. 100% ist häufig nicht möglich, der Aufwand wird unendlich.
Wenn Sie also die Kosten (oder Aufwand) einer Sicherheitslösung in Beziehung setzen, zu der Wichtigkeit eines Schutzes, werden Sie fast immer einen Kompromiß schließen müssen, der bei vertretbaren Kosten ein akzeptables Maß an Sicherheit erreicht! Es lohnt sich, dies zu bedenken.

Florian Seiffert
13.03.2000

Literatur / Quellen / Links

Literatur:

1. c't 3/2000 S. 26. RSA-Konferenz: Von Verschlüsselung bis Biometrie.
2. c't 3/2000 S. 110. Chiffriermaschinen des 20. Jahrhunderts.
3. c't Krypto-Kampagne PGP Key Certification Authority und c't startet Krypto-Kampagne
4. Deutsche Anleitung zu PGP von Kai Raven.
5. http://www.zerberus.de/pgp/pgp.pdf
6. c't 3/2000 S.64 Send It: Programmierer lasen E-Mails mit.
7. Rechtsanwalt Dr. Stefan Ernst aus Freiburg im Breisgau: Digitale Signatur un dihre juristische Bedeutung
   In: RRZK Kompass, Nr.84, 31.01.2000, Mitteilungen des Zentrums für Angewandte Informatik der Universität zu Köln.
8. E-Mails ... aber sicher! Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Postfach 200444, 40102 Düsseldorf, Telefon (0221) 384240, EMail: datenschutz@mail.lfd.nrw.de. Internet: http://www.lfd.nrw.de

Ein paar Abkürzungen zum Thema:

- **ADK**, Additional Decryption Keys, Zusazschlüssel bei PGP 5.0 u. 6.0, die z.B. Firmen das Mitlesen verschlüsselter EMails ihrer Mitarbeiter ermöglichen. (s. c't 23/98)
- **CMR**, Company Key Recovery. Dient dazu verschlüsselte Nachrichten durch das (automatische) mitverschlüsseln für Firmen- oder Regierungskeys für diese mitlesbar zu machen.
- **GAK**, Government Access to Keys, Erzwungener regierungsseitiger Zugriff auf private verschlüsselte Kommunikation
- **IPSEC**, IP Security. Standard zur gesicherten Übertragung von TCP/IP
- **KRA**, Key Recovery Alliance, www.kra.org (s. c't 22/1998)
- **MD5**, Message Digest Algorithm 5. 128bit-Hash-Algorithmus (Verfahren zur Generierung einer Textprüfsumme.), der in der ältesten PGP-Version eingebaut war. Er wurde 1996 von Hans Dobbertin "geknackt".
- **NSA**, National Security Agency. US-Amerikanische Behörde, Initiator des globalem Abhörsystems ECHELON. (s. c't 5/98). Gilt als die geheimnisvollste Geheimdienstbehörde der Welt.
- **PGP**, Pretty Good Privacy, Im Internet weit verbreitete Verschlüsselungssoftware. Ursprünglich geschrieben von Phil Zimmermann. 1991 erstmals veröffentlicht.
- **PKCS**, Public Key Cryptography Standards, Verschlüsselungsprotokoll, welches auch in SSL verwendung findet.
- **PKI**, Public-Key-Infrastruktur, Infrastruktur für das Management von öffentlichen (und dazugehörigen pivaten) Schlüsseln. i'x 2/2000.
- **RSA**, Rivest Shamir Adleman. Das erste und berühmteste asymmetrische Verschlüsselungsverfahren. 1977 erstmals veröffentlicht.
- **SKIP**, Simple Key Management for Internet Protocols, Teil des IPSEC Standards.
