



Berlin 15. April 2004

Veranstaltungsreihe eCOMM 2004

Thema: IT-Sicherheit / Kryptografie

Referent: Uwe Stache , berlin-one.de



Die Maßnahme



Bundesweites Netzwerk der Kompetenzzentren für den elektronischen Geschäftsverkehr

Laufzeit der 1. Phase:
01.05.1998 bis 30.04.2001

Laufzeit der 2. Phase:
01.05.2001 bis 30.04.2003

Weiterführung bis Ende 2005



Das Kompetenzzentrum eCOMM Berlin



Handwerkskammer Berlin



3



Aktivitäten von eCOMM Berlin

- **Beratungen und Informationen: über 670 Beratungen**
Tendenz: Von den Einstiegsberatungen hin zu anspruchsvollen Anfragen
- **Veranstaltungen: ca. 7000 Kontakte auf Veranstaltungen**
Tendenz: kleine Runden mit hohem Praxisbezug
- **Tagesgeschäft: Informationsrecherche und -aufbereitung,**
Tendenz: schnelle Verfügbarkeit von Informationen

4



Themen- und Branchenschwerpunkte

- eManagement
- eLogistik
- Beschaffung und Märkte
- Kundenbeziehung und Marketing
- Unternehmenskooperationen
- Netz- und Informationssicherheit (Recht)
- Elektronischer Geschäftsverkehr in der Touristikbranche
- Elektronischer Geschäftsverkehr im Handel
- Elektronischer Geschäftsverkehr bei den Freien Berufen

5



Nächste Veranstaltungen

- **27.04.2004** Elektronische Ausschreibung und Vergabe nach VOB im Land Berlin – Pilotprojekt eVergabe VOB der Senatsverwaltung für Stadtentwicklung
- **29.04.2004** Elektronische Beschaffung und elektronische Ausschreibung
- **13.05.2004** VOIP - Telefonieren im Internet
- **17. / 18.04.** D21- Kongress: Digitale Wirtschaft für KMU

6



Vielen Dank für Ihre Aufmerksamkeit

Michael Stamm
TSB Berlin GmbH
Ludwig Erhard Haus
Fasanenstraße 85
10623 Berlin



Telefon: (030) 46302-414
Fax: (030) 46302-444
Email: stamm@technologiestiftung-berlin.de

Internet: <http://www.ecomm-online.de>
<http://www.technologiestiftung-berlin.de>

7



Zur Person

Uwe Stache
Geschäftsführer SOC-Gruppe
berlin-one, Hosting-Provider



8



Kryptologie ?

- Kryptographie: Entwurf neuer Verfahren für die Informationssicherung
- – Symmetrische Verfahren: Kommunikationspartner haben ein gemeinsames Geheimnis
- – Asymmetrische (public-key) Verfahren: Kein *gemeinsames* Geheimnis notwendig
- Kryptoanalyse: Das Brechen von Verfahren (Entschlüsseln, Herausfinden von Schlüsseln aufgrund der erhältlichen Information)
- **Kryptologie** ist die Wissenschaft der algorithmischen Methoden zur Sicherung der Information

9

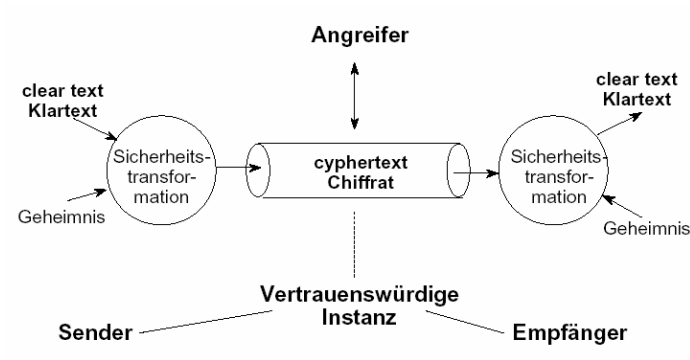


Geschichtlicher Abriss

- Ägypter, Perser, Griechen
- Cäsar: Cäsar-Code
- Frühmittelalter: verschlüsselte Runen (Stein in Rök, Schweden)
- ab 10. Jh: Klerus: Mythen, Latein
- ab 16. Jh: Politik, z.B. Maria Stuart
- 1. Weltkrieg: Telegramm von Zimmermann
- 2. Weltkrieg: U-Boot-Krieg, Enigma, Pearl Harbor
- 1948 Shannon's Informationstheorie
- 1974 Data Encryption Standard (DES)
- 1976 Public Key Cryptography (Diffie und Hellman)
- 1977 Digitale Unterschriften (Rivest, Shamir, Adleman)

10

Modell eines Kommunikationskanals



11

Historische Verschlüsselungen

Cäsar-Verschlüsselung

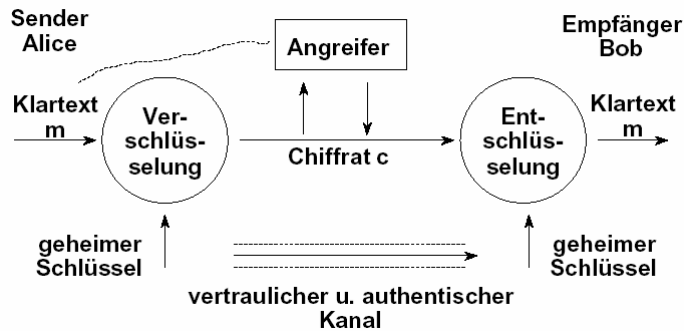
A ↯ F
B ↯ G
C ↯ H
D ↯ I
...
X ↯ C
Y ↯ D
Z ↯ E

Alphabetische Substitution

A ↯ X
B ↯ R
C ↯ S
D ↯ L
...
X ↯ W
Y ↯ I
Z ↯ M

12

Symmetrische Verschlüsselung



13

Überprüfung von Authentizität und Integrität

Prüfung der Echtheit von Information, Systembenutzern, Prozessen, Personen, Gegenständen aller Art

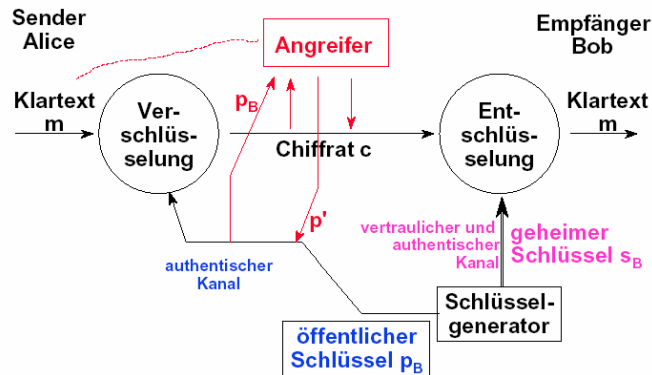
Bei einem symmetrischen Verfahren: Erfolgreiches Entschlüsseln impliziert Kenntnis des Schlüssels durch den Absender, somit ist die Nachricht authentisch und wurde nicht verändert.

Aber: Wie erkenne ich, dass ich erfolgreich entschlüsseln konnte?

- ✗ Aufgrund des Formates des Klartexts (deutscher Text, Windows-Programm): *implizite Redundanz*.
- ✗ Durch die Überprüfung eines Authentifikators, Message Integrity Code (MIC) oder Message Authentication Code (MAC): *explizite Redundanz*.

14

Asymmetrisches Verschlüsselungsverfahren



15

Diffie-Hellman: Prinzip ist ganz einfach

Benötigte Mathematik:

- *Modulare Arithmetik* - das Rechnen mit Resten: $R_n(a)$ ist der Rest r (zwischen 0 und $n-1$) bei einer ganzzahligen Division $a \text{ DIV } n = (q, r)$, so dass $a = q \cdot n + r$
- Andere Schreibweise: $a = r \pmod{n}$
- *Modulares Exponentieren*: $R_n(a^3) = R_n(a \cdot R_n(a^2))$
- *Primzahlen* sind positive Zahlen ≥ 2 , die nur durch 1 und durch sich selbst teilbar sind.
- Eine Zahl g ist dann ein primitives Element modulo einer Primzahl p , wenn die Sequenz $R_p(g^0), R_p(g^1), R_p(g^2), \dots$ alle Zahlen zwischen 1 und $p-1$ enthält.
 - 2, 6, 7, 8 sind primitive Elemente modulo 11

16