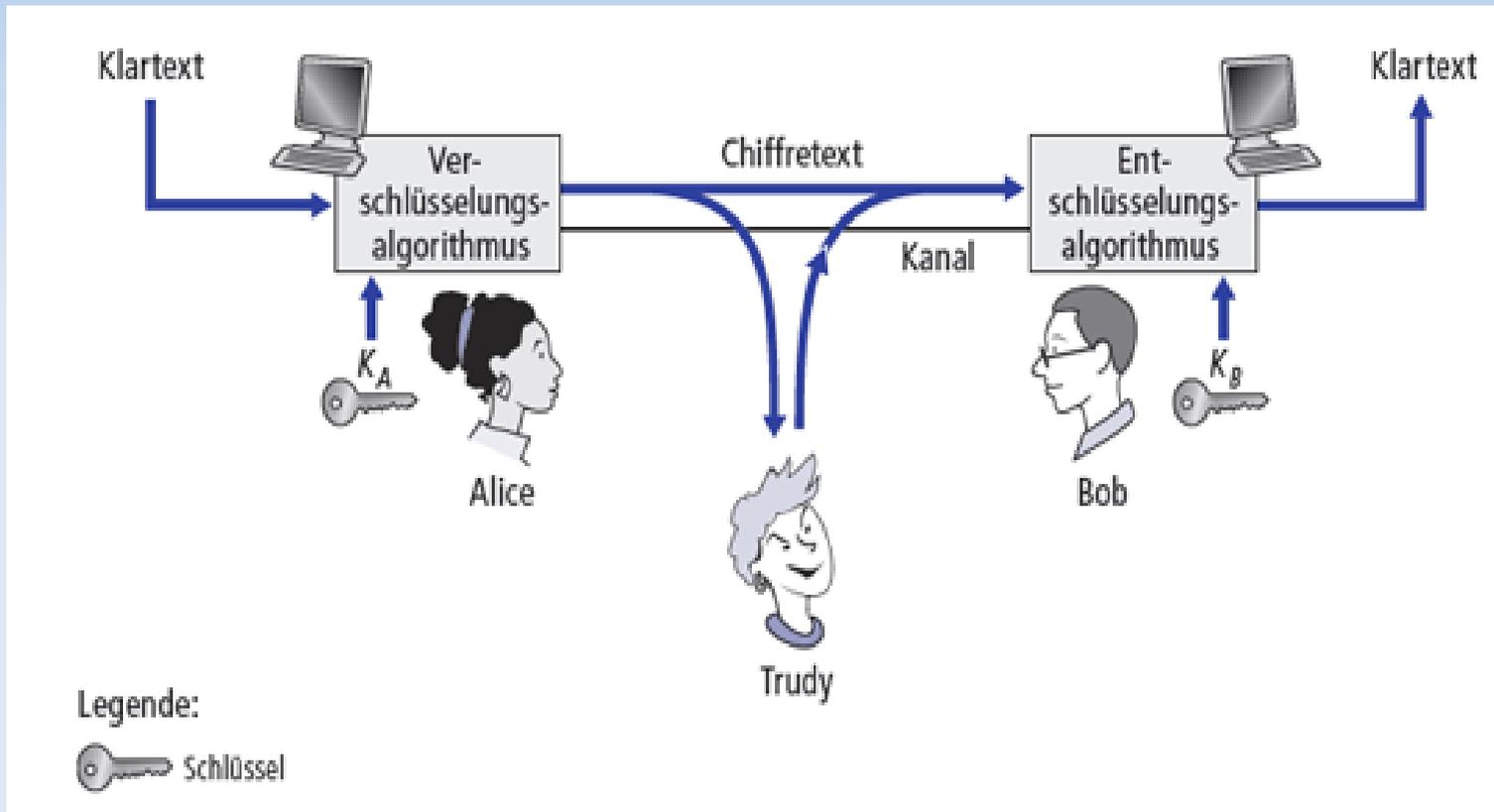


Fachbereich Medienproduktion

Herzlich willkommen zur Vorlesung im
Studienfach:

Grundlagen der Informatik

Kryptografische Komponenten



Quelle: Kurose-Ross, Computernetzwerke

Chiffre

Monoalphabetische Chiffre:

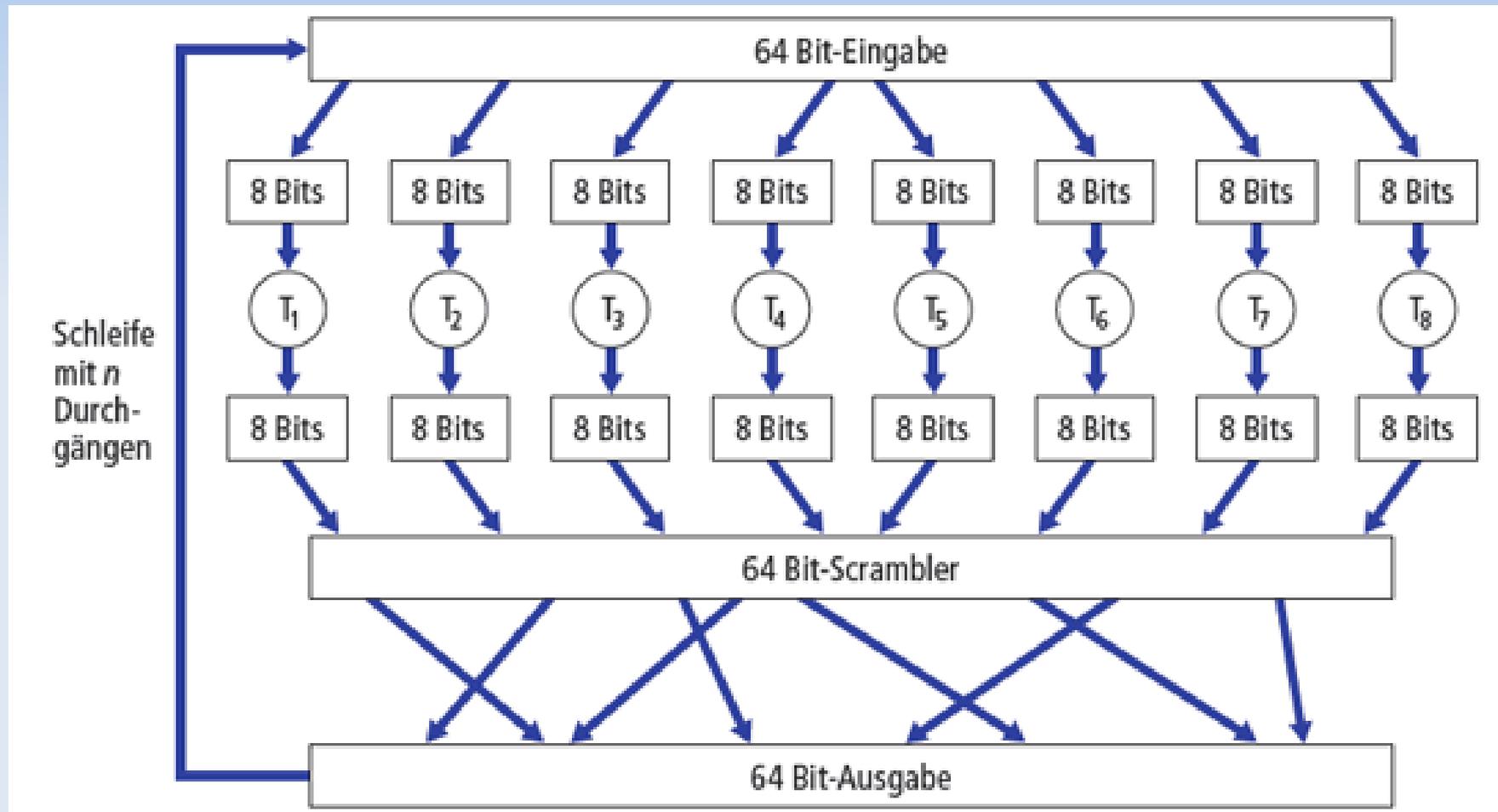
```
Buchstabe im Klartext:  a b c d e f g h i j k l m n o p q r s t u v w x y z
Buchstabe im Chiffretext: m n b v c x z a s d f g h j k l p o i u y t r e w q
```

Polyalphabetische Chiffre:

```
Buchstabe im Klartext: 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
C1(k = 5):           f g h i j k l m n o p q r s t u v w x y z a b c d e
C2(k = 19):          t u v w x y z a b c d e f g h i j k l m n o p q r s
```

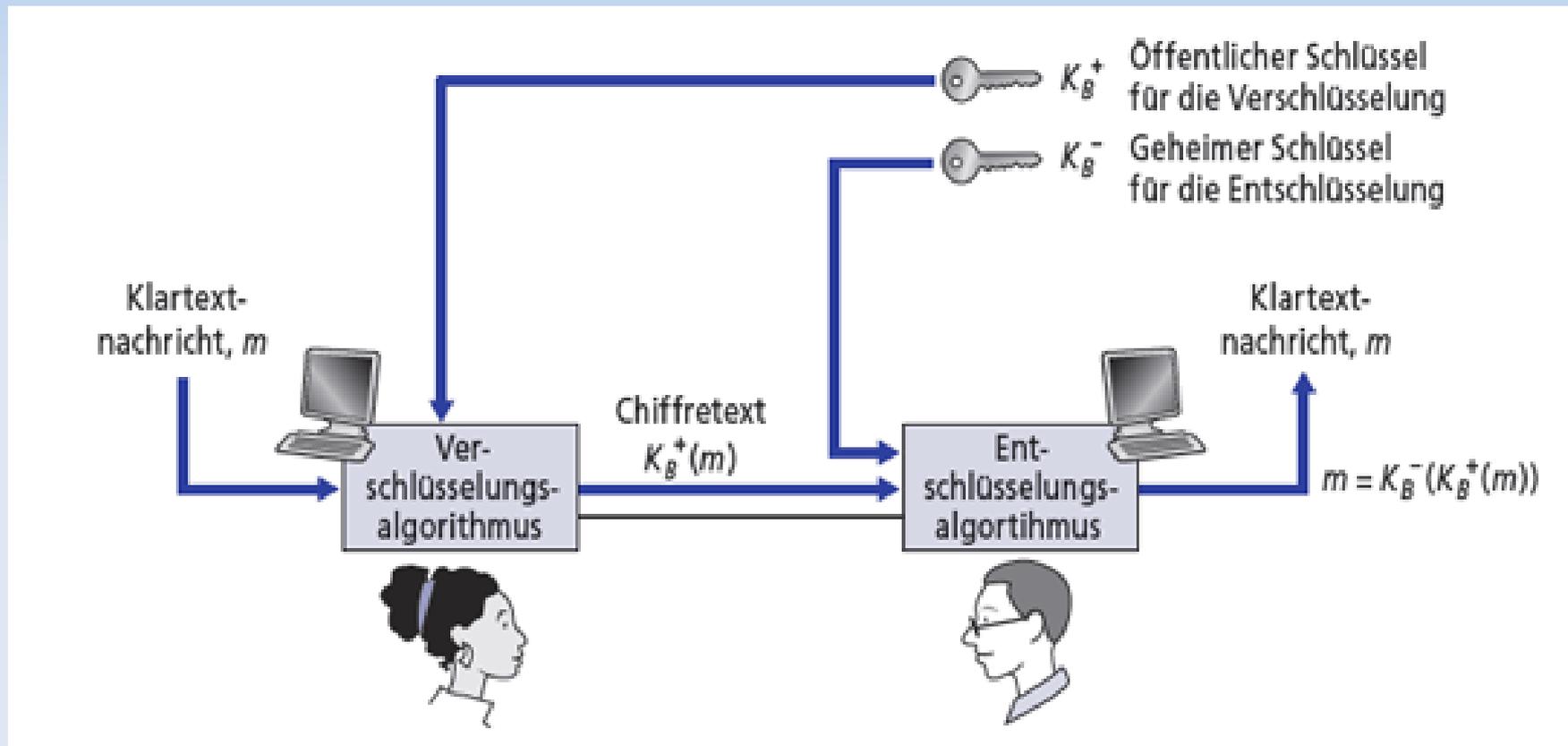
Quelle: Kurose-Ross, Computernetzwerke

Blockchiffre



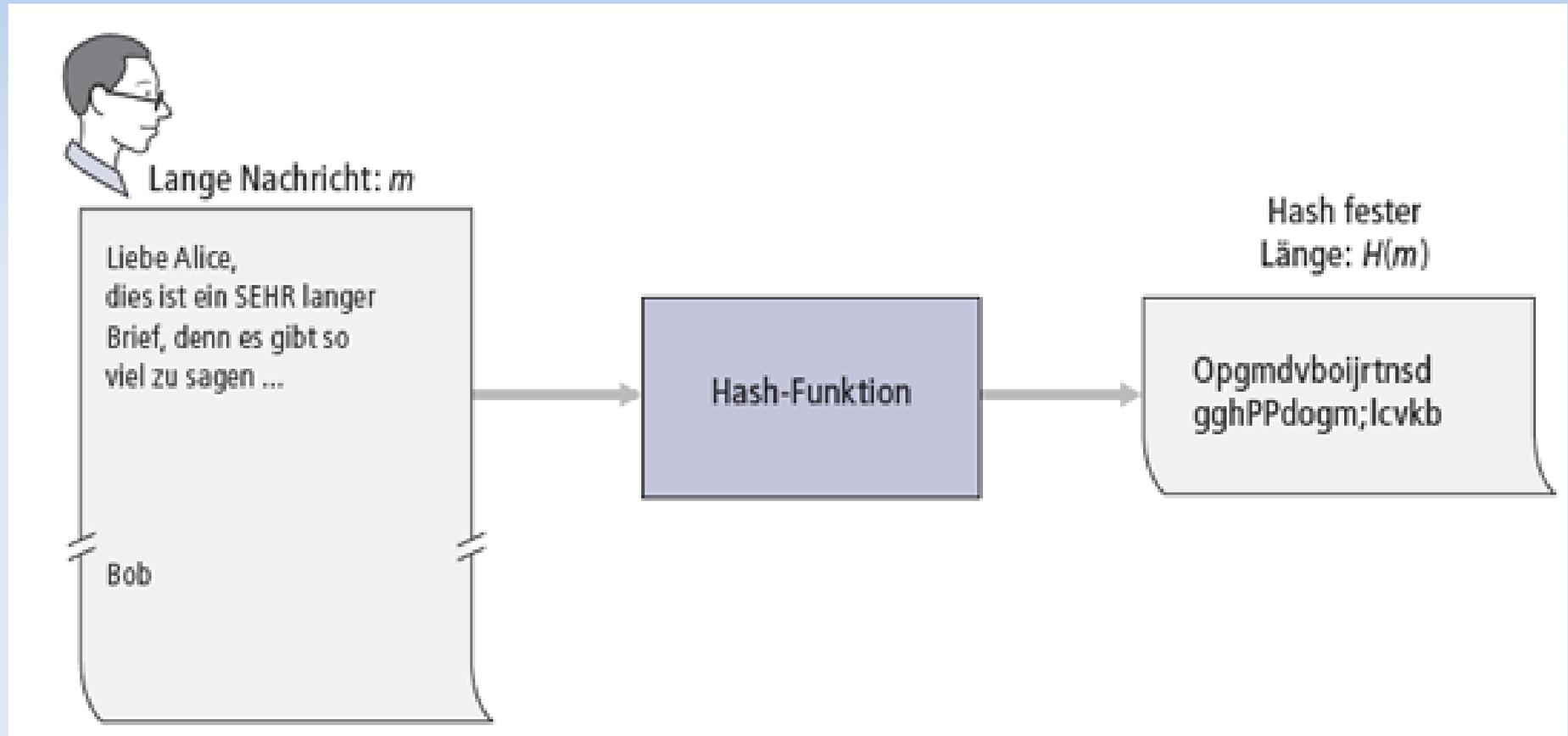
Quelle: Kurose-Ross, Computernetzwerke

Public Key Kryptografie



Quelle: Kurose-Ross, Computernetzwerke

Hash Funktion

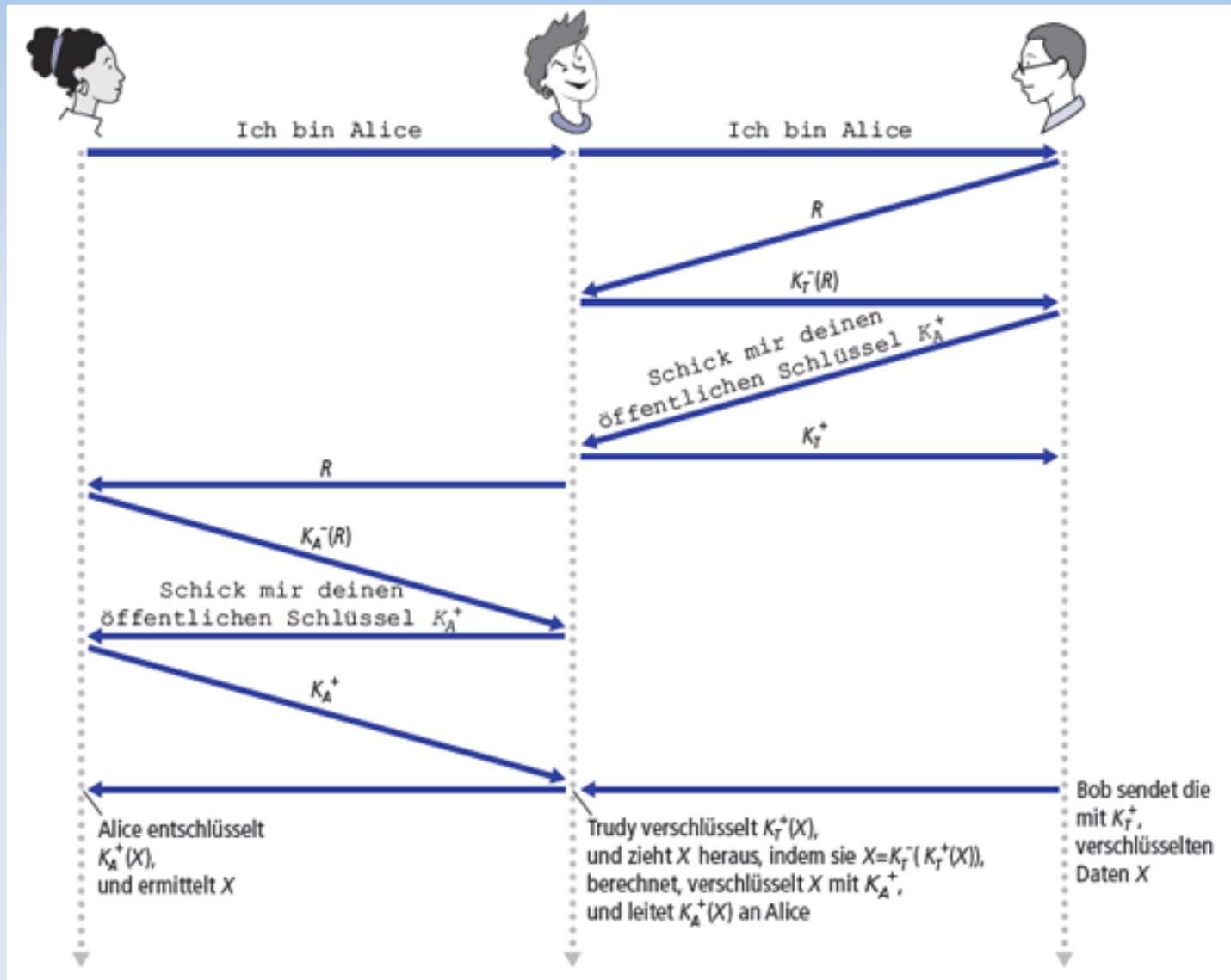


Quelle: Kurose-Ross, Computernetzwerke

Fragen



Man-in-the-Middle-Attack

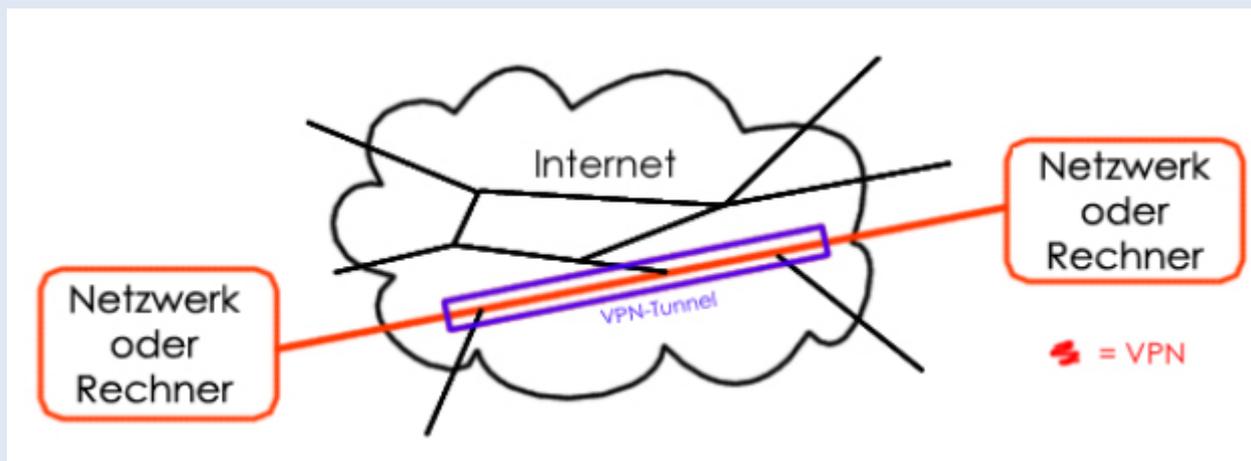


Fragen



VPN

- VPN = virtuelles privates Netzwerk
- Eine Verbindung von Netzwerken oder Endgeräten verschiedener Standorte mittels öffentlicher Kommunikationsnetze zu einem in sich geschlossenen Gesamtnetz wird als VPN bezeichnet
- In diesem Gesamtnetz ist die „sichere“ Nutzung von gemeinsamen Diensten möglich

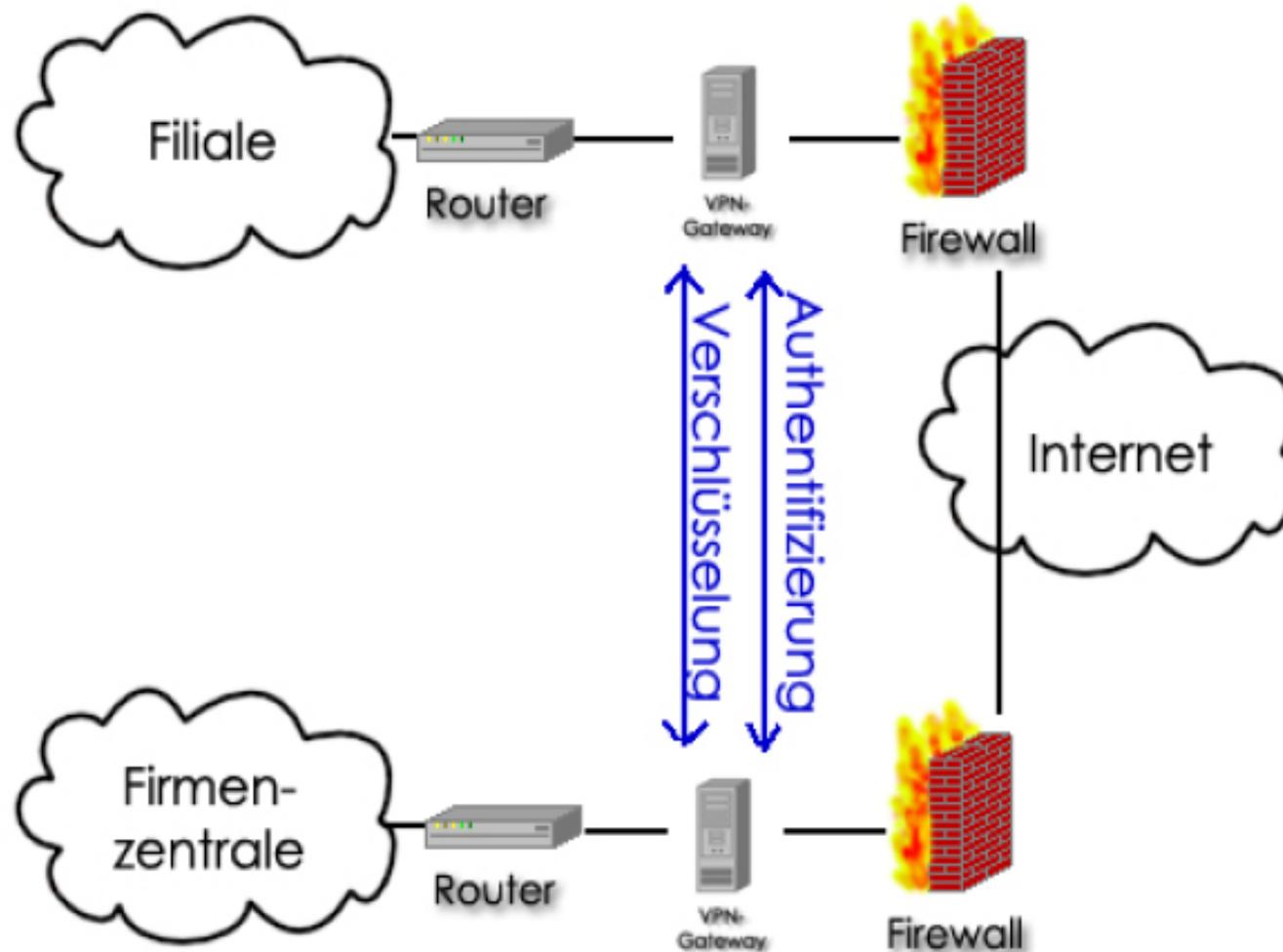


Anforderungen in Bezug auf die Netzwerksicherheit

- Verschlüsselung der Daten
 - Identifizierung und Authentifizierung
 - Zugriffsberechtigung
 - Datenintegrität
 - Angriffssicherheit
-
- *Virtuell*, weil durch Verbindung mittels öffentlicher Kommunikationsplattformen keine physikalische Verbindung erforderlich ist
 - *Privat*, weil die Kommunikationspartner an die Verbindung den Anspruch haben, dass sie gesichert ist, so dass kein unbefugter Dritter die Kommunikation beeinflussen kann

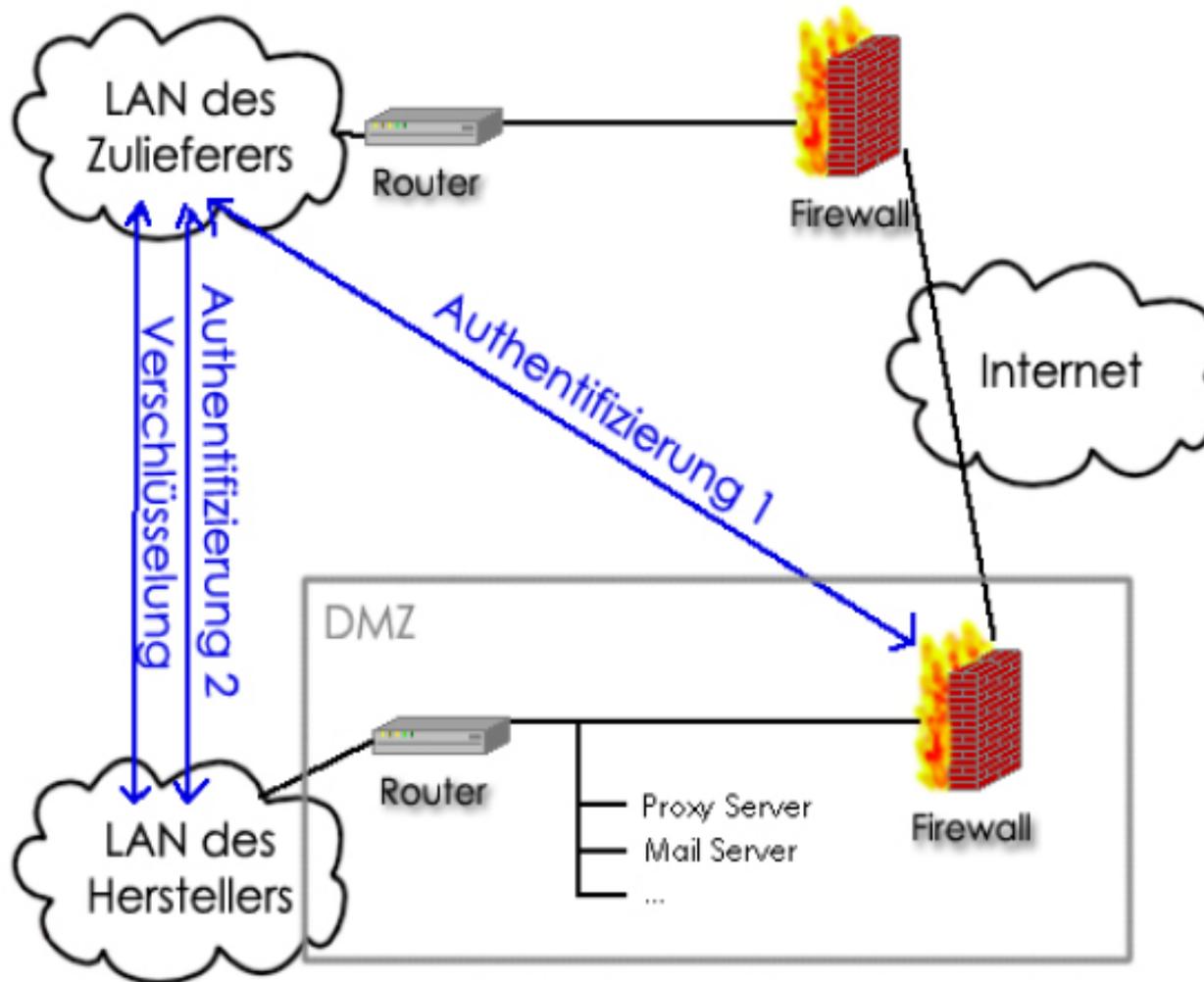
VPN Site-To-Site

Intranet-VPN (Site-To-Site):



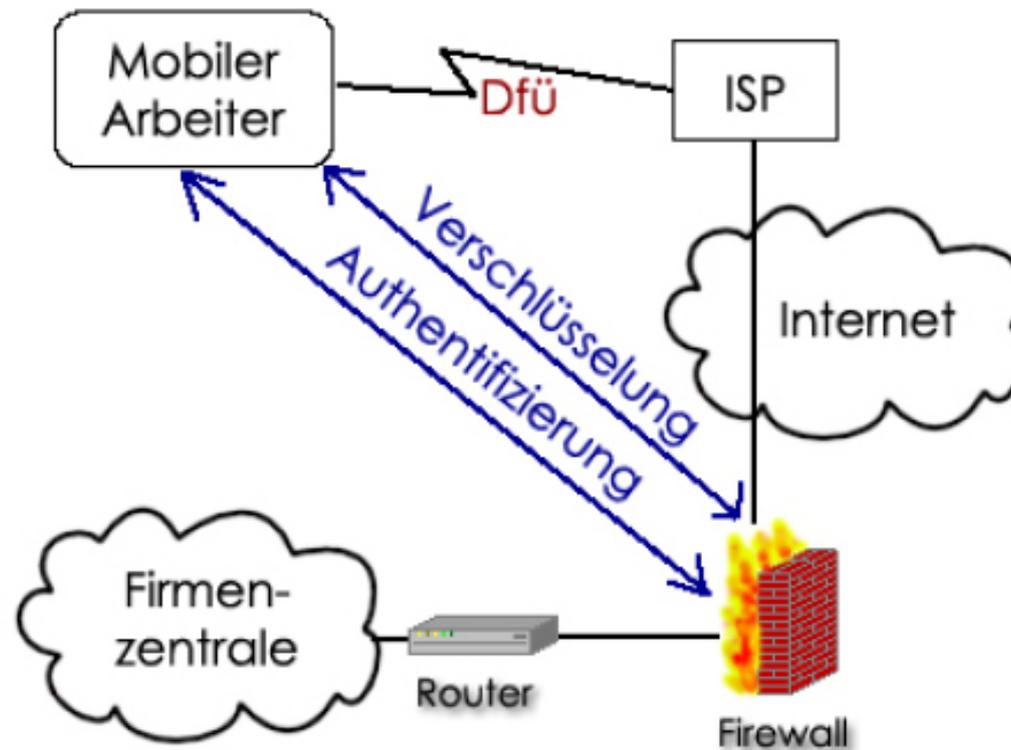
VPN End-To-End

Extranet-VPN (End-To-End):



Remote-Access-VPN

Remote-Access-VPN (End-To-Site):



Vielen Dank für Ihre Aufmerksamkeit!