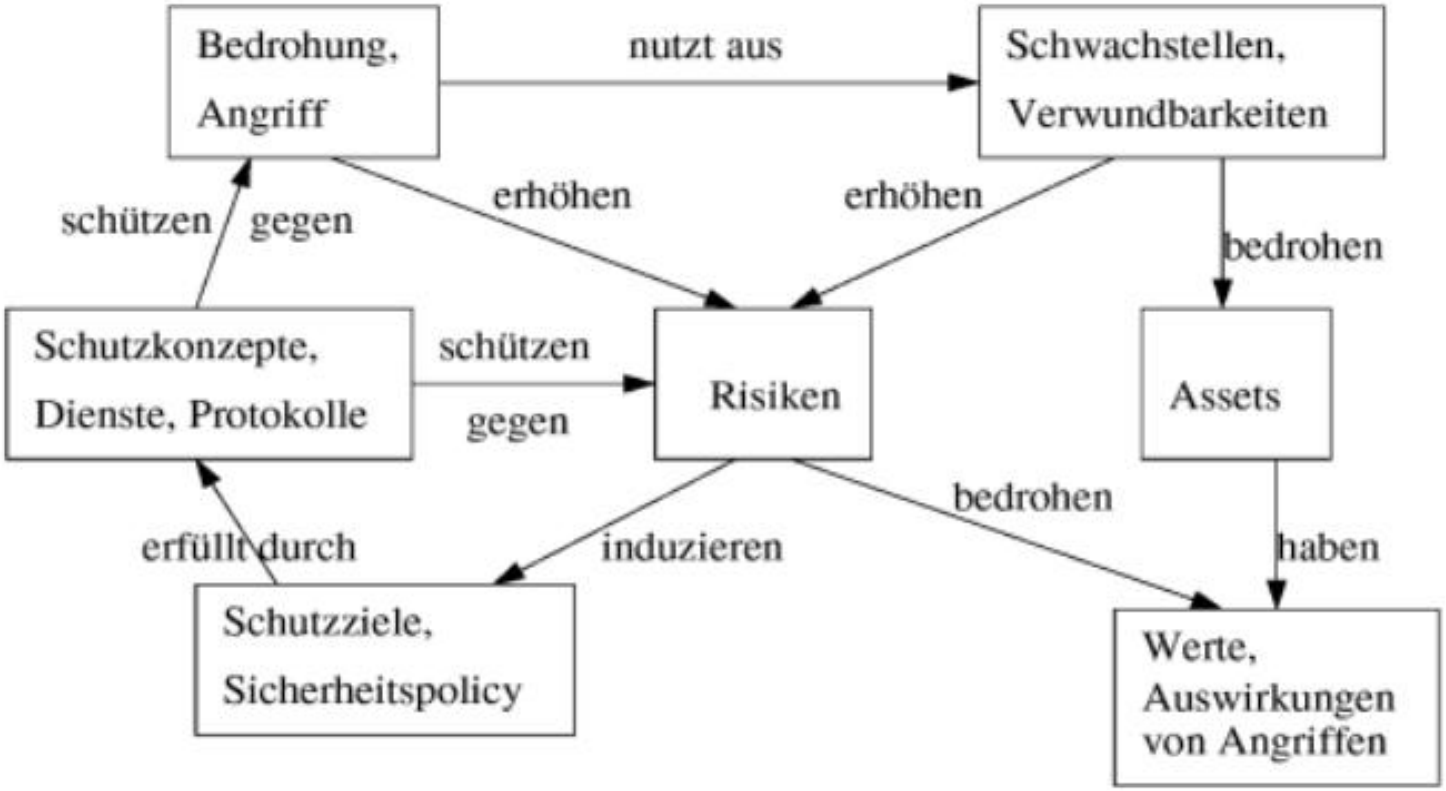
Kap. 6: IT-Sicherheit

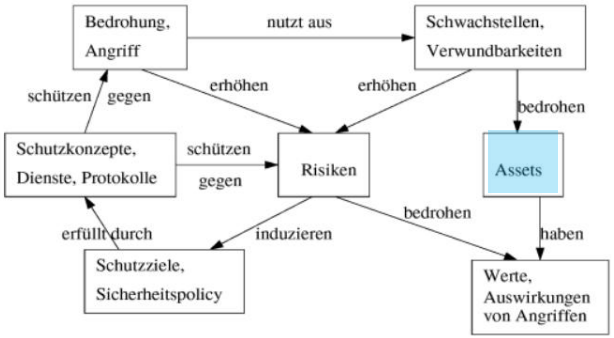
Was ist IT-Sicherheit?

- **Deutsch ist hier ungenau: Sicherheit - Security vs. Safety**
- **IT-Security**
  - The **protection of information assets** through the use of technology, processes, and training. (Microsoft)
  - Als Informationssicherheit bezeichnet man **Eigenschaften** von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die **Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen**. Informationssicherheit dient dem Schutz vor **Gefahren** bzw. **Bedrohungen**, der Vermeidung von wirtschaftlichen **Schäden** und der Minimierung von **Risiken**.. (Wikipedia)
- **Begegnet Bedrohungen von IT-Systemen**

Begriffe der IT-Sicherheit



Informationswerte (Information Assets)

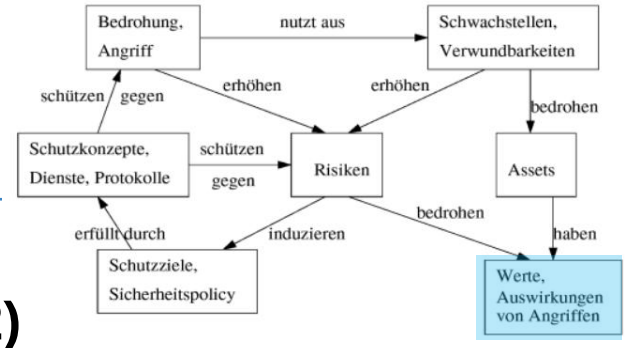


- **Def: Asset is any data, device, or other component of the environment that supports information-related activities. (Wikipedia)**

  - **Im engeren Sinne Werte, die für eine Organisation wichtig sind**
    - z.B. Datenbestände

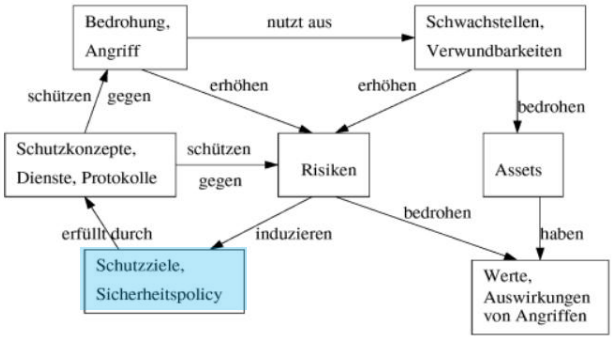
  - **Sind so entscheidend für eine Organisation, dass die Sicherheit dieser Werten (und damit die IT-Sicherheit) in Finanz-Richtlinien und Gesetzen gefordert werden.**
    - Basel II
    - Sarbanes-Oxley Act

Werte und Schäden



- **Klassifikation von Schäden (nach BSI 100-2)**
  - **normal**
    - Die Schadensauswirkungen sind begrenzt und überschaubar
  - **hoch**
    - Die Schadensauswirkungen können beträchtlich sein
  - **sehr hoch**
    - Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreich
- **Mögliche Schadensdimensionen**
  - **Leib und Leben, Sachschäden, Umweltschäden, finanzielle Schäden, Rufschäden**

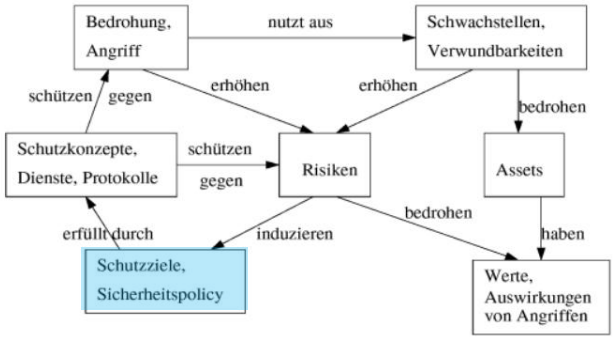
Schutzziele

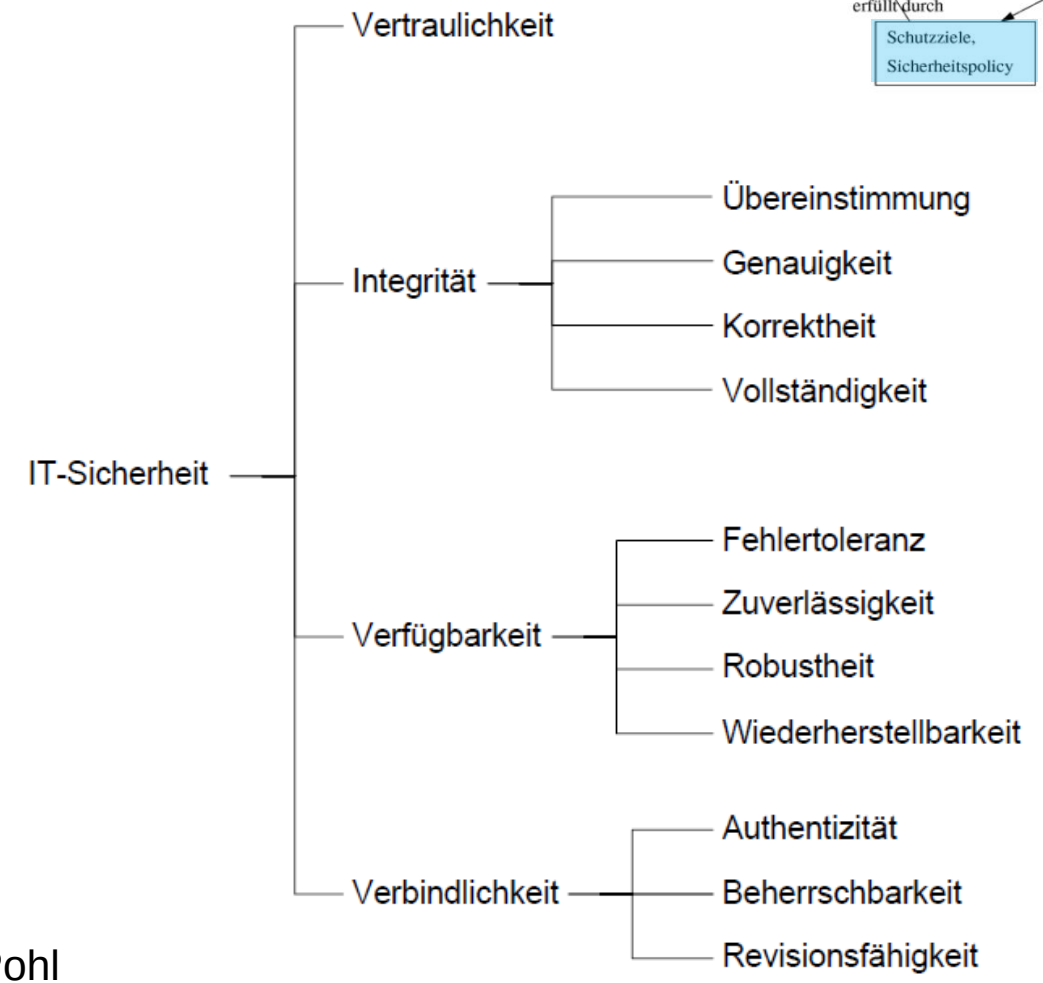


- **Vertraulichkeit (privacy)**
  - Es können nur Berechtigte Daten lesen.
- **Integrität (integrity)**
  - Daten können nicht ohne Berechtigung verändert werden.
- **Verfügbarkeit (availability)**
  - Ist der Rechner/Service erreichbar?
- **Verbindlichkeit (non repudiation)**
  - Es kann nachgewiesen werden, wer was gesendet (getan) hat.
- **Authentizität (authenticity)**
  - Es ist klar, mit wem man kommuniziert
- **Zugriffskontrolle/Autorisierung (autorisation, access control)**
  - Darf derjenige das, was er tun will?

- **Potentiell unabhängige Anforderungen!**

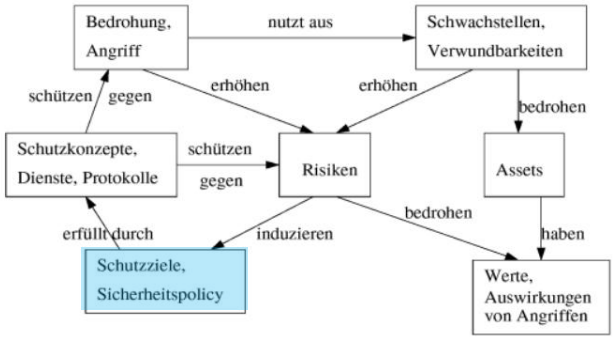
Weitere Klassifikation und abgeleitete Ziele





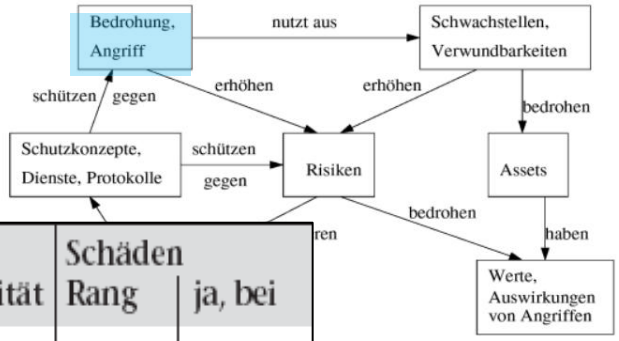
nach Prof. Hartmut Pohl

Sicherheitspolicy



- **Beinhaltet i.d.R.:**
  - Stellenwert der Informationssicherheit und Bedeutung der IT (Informationstechnologie) für die Aufgabenerfüllung
  - Benennung der Sicherheitsziele und Beschreibung der Sicherheitsstrategie
  - Beschreibung der Organisationsstruktur
  - Zusicherung, dass die Security Policy von der Leitungsebene durchgesetzt wird und Verstöße soweit möglich sanktioniert werden
  - Aussagen zur periodischem Überprüfung der Sicherheitsmaßnahmen
  - Aussagen zu Programmen zur Förderung der Informationssicherheit durch Schulungs- und Sensibilisierungsmaßnahmen (Erhalt und Förderung der Awareness)
  - Verantwortlichkeiten im Informationssicherheitsprozess

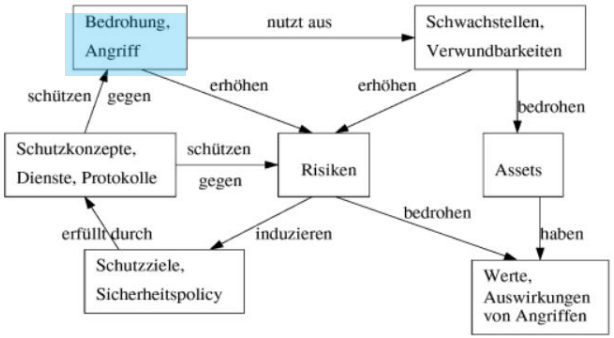
Allgemeine Bedrohungen von IT-Systemen



	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51%
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,34	1	2,80	1	54%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9%
Software-Mängel/-Defekte	4	0,57	5	0,96	3	43%
Hacking (Vandalismus, Probing, Missbrauch,...)	5	0,48	3	1,26	5	9%
Hardware-Mängel/-Defekte	6	0,40	8	0,32	4	38%
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15%
höhere Gewalt (Feuer, Wasser,...)	8	0,24	11	0,04	9	8%
Manipulation zum Zweck der Bereicherung	9	0,17	7	0,43	10	8%
Mängel der Dokumentation	10	0,15	10	0,20	6	17%
Sabotage (inkl. DoS)	11	0,12	6	0,55	11	8%
Sonstiges	12	0,03	12	0,00	12	3%

Quelle: http://www.kes.info/archiv/material/studie2006/

Mögliche Angriffe

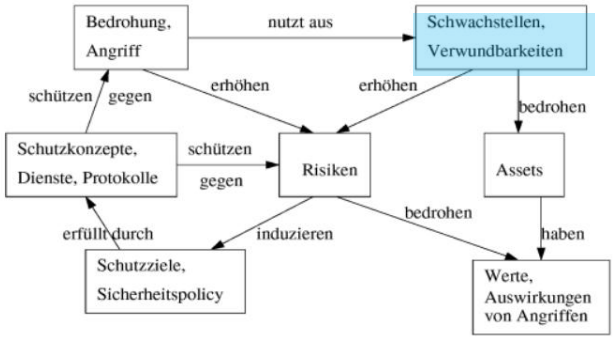


- **Maskierung (Masquerade)**
  - Jemand gibt sich als ein anderer aus
- **Abhören (Eavesdropping)**
  - Jemand liest Informationen, die nicht für ihn bestimmt sind
- **Zugriffsverletzung (Authorization Violation)**
  - Jemand benutzt einen Dienst oder eine Resource, die nicht für ihn bestimmt ist
- **Verlust oder Veränderung (übertragener) Information**
  - Daten werden verändert oder zerstört
- **Verleugnung der Kommunikation**
  - Jemand behauptet (fälschlicherweise) nicht der Verursacher von Kommunikation zu sein
- **Fälschen von Information**
  - Jemand erzeugt (verändert) Nachrichten im Namen anderer
- **Sabotage**
  - Jede Aktion, die die Verfügbarkeit oder das korrekte Funktionieren der Dienste oder des Systems reduziert

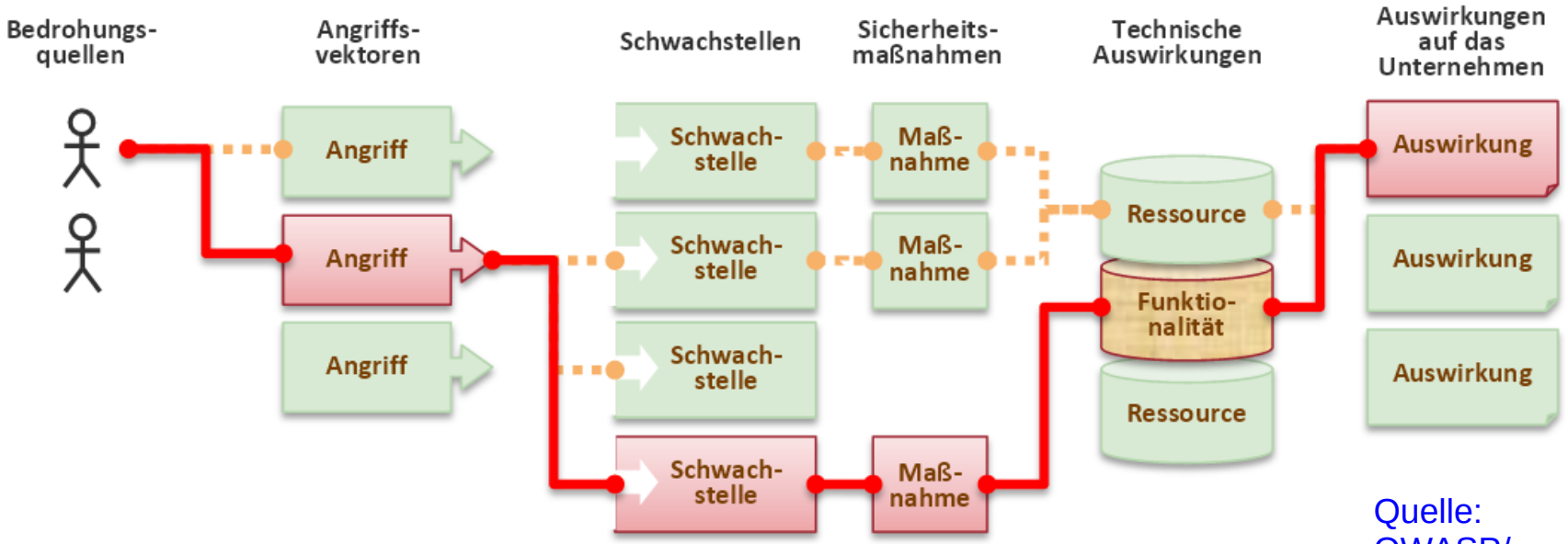
Angriffe vs. Ziele

Sicherheits-ziele	Bedrohungen						
	Mas-kierung	Abhören	Zugriffs-ver-letzung	Verlust oder Verän-derung (über-tragener) information	Verleug-nung der Kommuni-kation	Fäl-schen von Infor-mation	Sabotage (z.B. Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x		x	
Verantwort-lichkeit	x		x		x	x	
Verfügbarkeit	x		x	x			x
Zugriffs-kontrolle	x		x			x	

Schwachstellen, Verwundbarkeiten

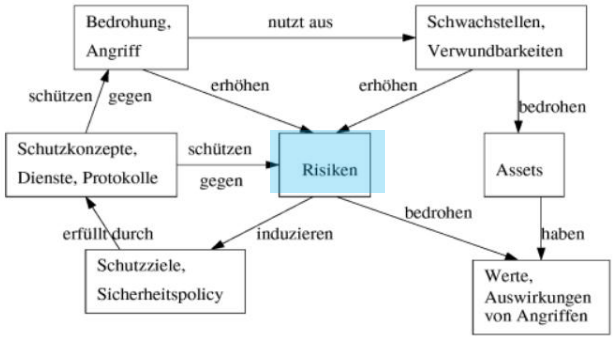


- Eine **Schwachstelle** (weakness) ist eine Stelle, an der ein System verwundbar werden kann. (Eckert 2015)
- Eine **Verwundbarkeit** (vulnerability) ist eine Schwachstelle, über die eine Sicherheitsmaßnahme umgangen, getäuscht oder modifiziert werden kann. (Eckert 2015)



Quelle: OWASP/

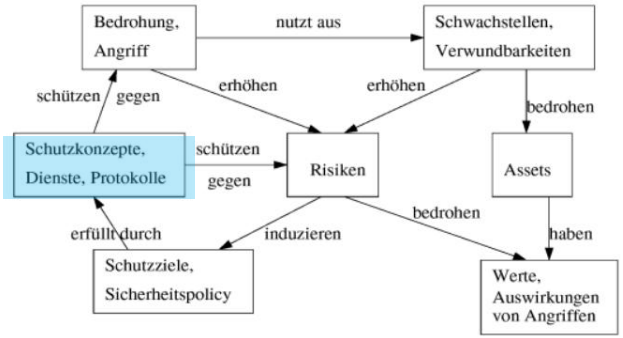
Risiko



- **Es gibt viele Bedrohungen**
  - **Alle zu betrachten ist zu teuer**
  - **Bestimmung der Aufwand/Nutzen-Relation!**
  - **Bestimmung des Risikos zur Prioritäten-Setzung**

- **Größen in einer Risikoanalyse**

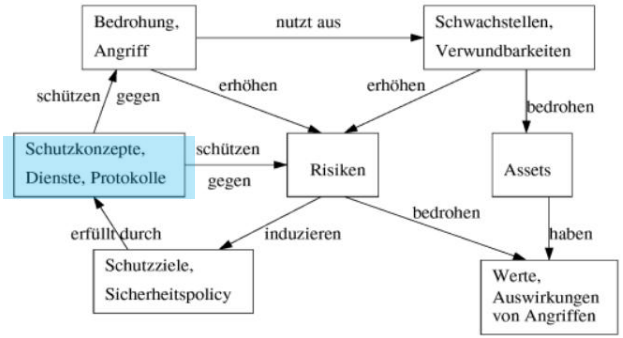
Sicherheitsmaßnahmen



- **Arten von Maßnahmen**
  - **Technisch**
  - **Organisatorisch**

- **Maßnahmen im Lebenszyklus eines Angriffs**
  - **Präventive Maßnahmen**
    - Zur Einhaltung der Sicherheitsziele
  - **Detektierende Maßnahmen**
    - Zum Erkennen von unerwünschten Sicherheitsereignissen, bei denen die präventiven Maßnahmen unzureichend waren
  - **Reaktive Maßnahmen**
    - Zum Wiederherstellung des Soll-Zustands nach dem Erkennen von Sicherheitsereignissen

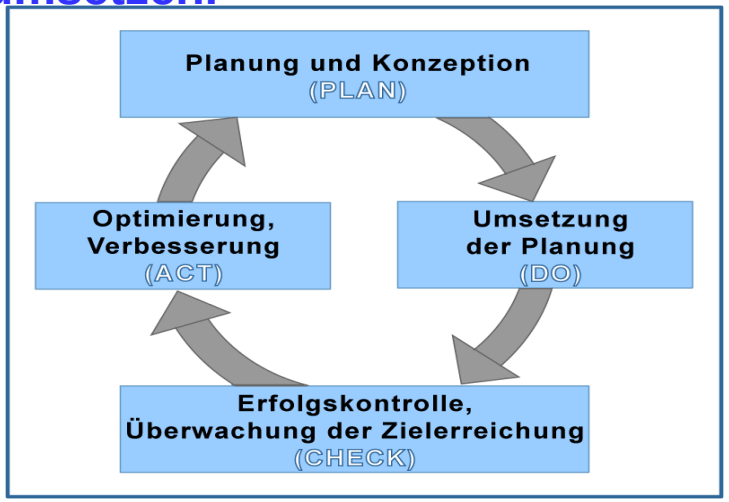
Beispiele von Sicherheitsmaßnahmen



Maßnahmen	präventiv	detektierend	reaktiv
organisatorisch	Schulungen, Passwort-Richtlinie, Password-Reset-Prozess	Log-File Audit	Security Incident Response Prozess
technisch	Kryptographischen Mechanismen (Verschlüsselung, MAC, Authentifizierung), Firewall, Virenscanner	Intrusion Detektion System	Automatische Rekonfiguration

Sicherheit als Prozess

- **Sicherheit ist kein Zustand, sondern ein Prozess**
  - **d.h. Sicherheit unterliegt einer kontinuierlichen Dynamik**
    - (z. B. durch Änderungen im Bedrohungs- und Gefährdungsbild, in Gesetzen oder durch den technischen Fortschritt)
- **Sicherheit muss aktiv gemanagen, aufrecht erhalten und kontinuierlich verbessert werden**
  - **IT-Systemeinführung planen**
  - **IT-Sicherheitsmaßnahmen definieren und umsetzen.**
  - **Erfolgskontrolle regelmäßig durchführen**
  - **Schwachpunkte oder Verbesserungs-möglichkeiten finden**
  - **Maßnahmen verbessern**
    - (Änderungen planen und umsetzen)
  - **IT-Sicherheitsaspekte bei Außerbetriebnahme berücksichtigen**



ISMS - Information Security Management System

- **Komponenten:**
  - **Management-Prinzipien**
  - **Ressourcen**
  - **Mitarbeiter**
  - **IT-Sicherheitsprozess**
    - IT-Sicherheitsleitlinie (einschl. IT-Sicherheitsziele und -strategie)
    - IT-Sicherheitskonzept

- **Standards**
  - **ISO/IEC 27000**
    - Zertifizierungen nach ISO/IEC 27001 möglich für:
    - Organisationen (seit 2005)
    - Personen (seit 2010)
  - **BSI-Standard 100 (kompatibel ISO/IEC 27001, früher “IT-Grundschutz”)**

Sicherheitsziele

- **Integrität (integrity)**
  - Daten können nicht ohne Berechtigung verändert werden.
- **Vertraulichkeit (privacy)**
  - Es können nur Berechtigte Daten lesen.
- **Verantwortlichkeit/Authentifikation (authentication)**
  - Jeder weiß, mit wem er kommuniziert.
- **Zugriffskontrolle/Autorisierung (autorisation, access control)**
  - Darf derjenige das, was er tun will?
- **Verfügbarkeit (availability)**
  - Ist der Rechner/Service erreichbar?
- **Unabstreitbarkeit (non-repudiation)**
  - Kann nachgewiesen werden, dass jemand etwas getan hat?
- **Potentiell unabhängige Anforderungen!**

Angriffe

- **Maskierung (Masquerade)**
  - Jemand gibt sich als ein anderer aus
- **Abhören (Eavesdropping)**
  - Jemand liest Informationen, die nicht für ihn bestimmt sind
- **Zugriffsverletzung (Authorization Violation)**
  - Jemand benutzt einen Dienst oder eine Resource, die nicht für ihn bestimmt ist
- **Verlust oder Veränderung (übertragener) Information**
  - Daten werden verändert oder zerstört
- **Verleugnung der Kommunikation**
  - Jemand behauptet (fälschlicherweise) nicht der Verursacher von Kommunikation zu sein
- **Fälschen von Information**
  - Jemand erzeugt (verändert) Nachrichten im Namen anderer
- **Sabotage**
  - Jede Aktion, die die Verfügbarkeit oder das korrekte Funktionieren der Dienste oder des Systems reduziert

Angriffe auf Ziele

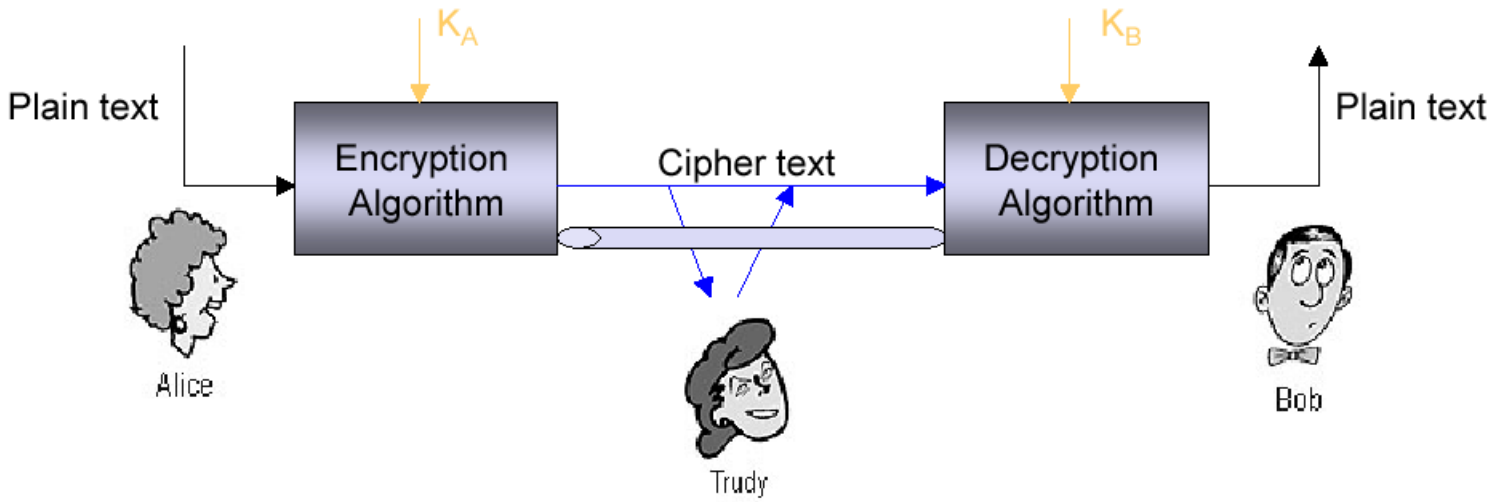
Sicherheits-ziele	Bedrohungen						
	Mas-kierung	Abhören	Zugriffs-ver-letzung	Verlust oder Verän-derung (über-tragener) information	Verleug-nung der Kommuni-kation	Fäl-schen von Infor-mation	Sabotage (z.B. Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x		x	
Verantwort-lichkeit	x		x		x	x	
Verfügbarkeit	x		x	x			x
Zugriffs-kontrolle	x		x			x	

Sicherheitsmechanismen

- **Überwiegend mit kryptographischen Mechanismen:**
  - Authentisierung
    - von Systemen/Benutzern (entity authentication)
    - von Datenpaketen (data origin authentication)
  - Integritätssicherung **(integrity protection)**
  - Verschlüsselung **(encryption)**
  - Schlüsselmanagement **(key exchange)**
  - **…**
- **Ohne kryptographische Mechanismen:**
  - Zugriffskontrolle **(access control)**
  - Policy-Management
  - Einbruchserkennung **(intrusion detection)**
  - **…**

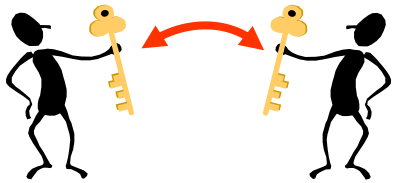
Prinzipien der Kryptographie

- **Prinzip**
  - Sender verschlüsselt Daten so, dass ein Intruder die übertragene Information nicht erkennen kann.
  - Empfänger ist in der Lage, die Daten zu lesen.
- **Komponenten**



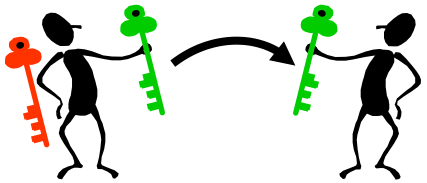
Kryptographie-Verfahren

Symmetrische Kryptographie



- **Instanzen besitzen gemeinsamen geheimen Schlüssel.**
- Vorteile**:**
  - **geringer Rechenaufwand**
  - **kurze Schlüssel**
- Nachteile**:**
  - **Schlüsselaustausch schwierig**
  - **keine Verbindlichkeit**

Asymmetrische Kryptographie (Public-Key-Kryptographie)



- Schlüsselpaar aus privatem und öffentlichem Schlüssel
- Vorteile:
  - öffentliche Schlüssel sind relativ leicht verteilbar
  - Verbindlichkeit möglich
- Nachteile:
  - hoher Rechenaufwand
  - längere Schlüssel

Beispiele – Symmetrische Verschlüsselung

ältere ENIGMA (ab 1918)

Vierwalzen-ENIGMA
(Marineausführung, ab 1942)

Voraussetzung

- **Notwendige Voraussetzung für sichere Verschlüsselung:**
  - **Durchprobieren der Schlüssel muss aussichtslos sein**

- **Beispiel: Klartextangriff mit Spezialrechner bei bekanntem symmetrischen Verfahren, 10^{10} Schlüssel pro Sekunde**

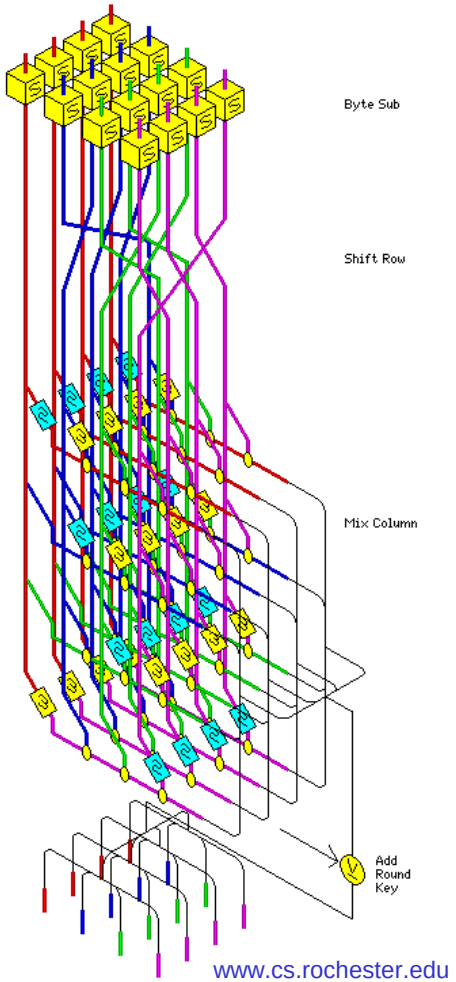
Schlüsselgröße	*benötigte Zeit*	*Qualität*
40 Bits	100 Sekunden	schlecht
56 Bits	10 Tage	schwach
64 Bits	30 Jahre	mäßig
128 Bits	10^{20} Jahre	gut
256 Bits	10^{60} Jahre	sehr gut

Kryptoanalyse

- **Ziel:**
  - Code knacken
  - Schlüssel und Klartext herausfinden
- **Ansätze:**
  - Entschlüsselungsangriff – wenn nur Geheimtext vorliegt
  - Klartextangriff – wenn zusätzlich Teile des Klartextes vorliegen
- **Notwendige Voraussetzung:**
  - Sprache der Nachricht muss bekannt sein !

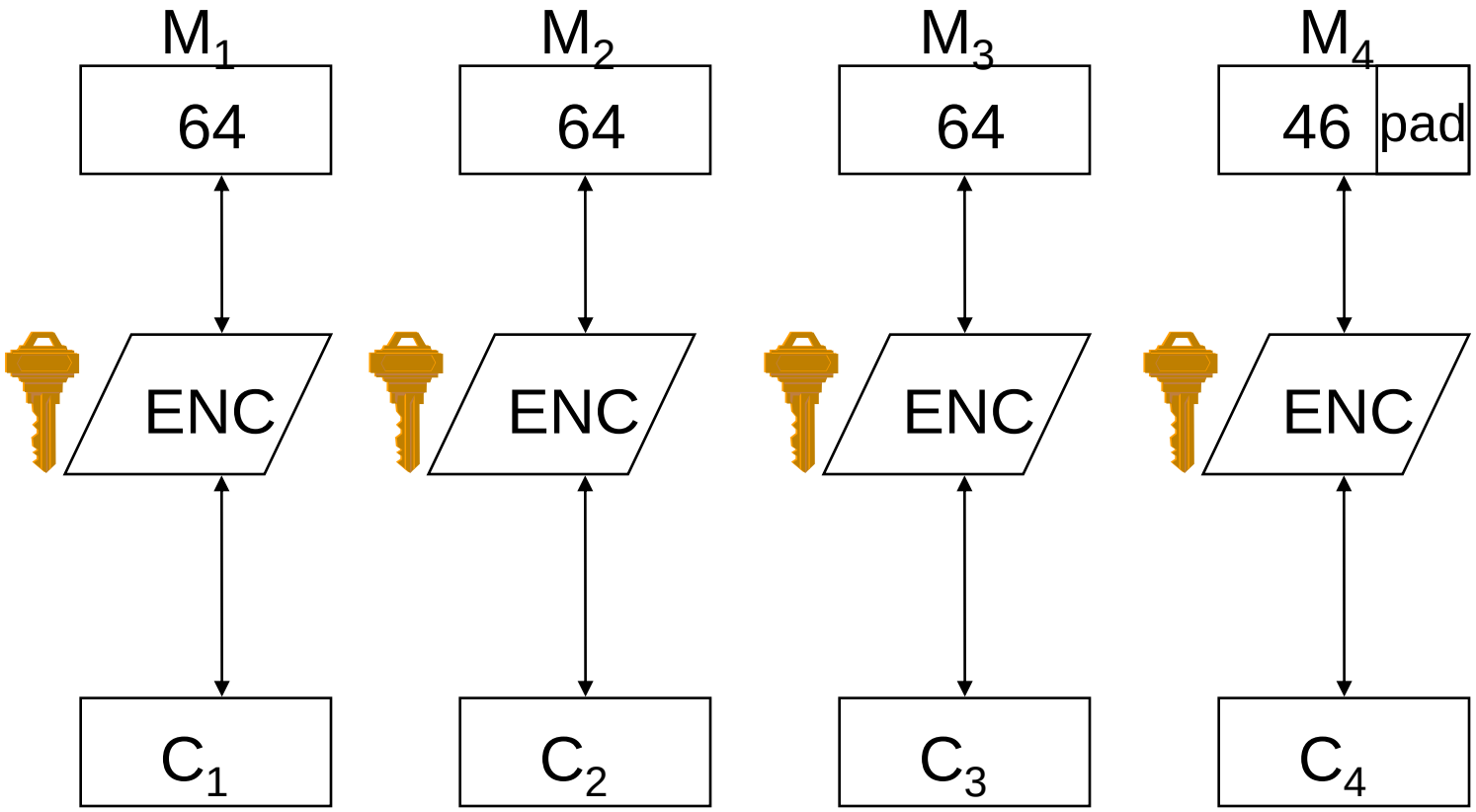
AES - Advanced Encryption Standard

- **Heute DAS symmetrische Verschlüsselungsverfahren**
  - Standardisiert seit 2001
  - Das Verfahren ist bekannt, der Schlüssel ist geheim
  - Schlüssellängen von 128, 192 und 256 Bit
  - Blockchiffrierung: 64-bit-Blöcke
  - Mehrstufiges Verfahren mit Transpositionen und Substitutionen
  - Schnelle Realisierung auch in Software möglich
  - Hardware-Realisierung ebenfalls möglich
  - Weitere Informationen unter http://csrc.nist.gov/encryption/aes/



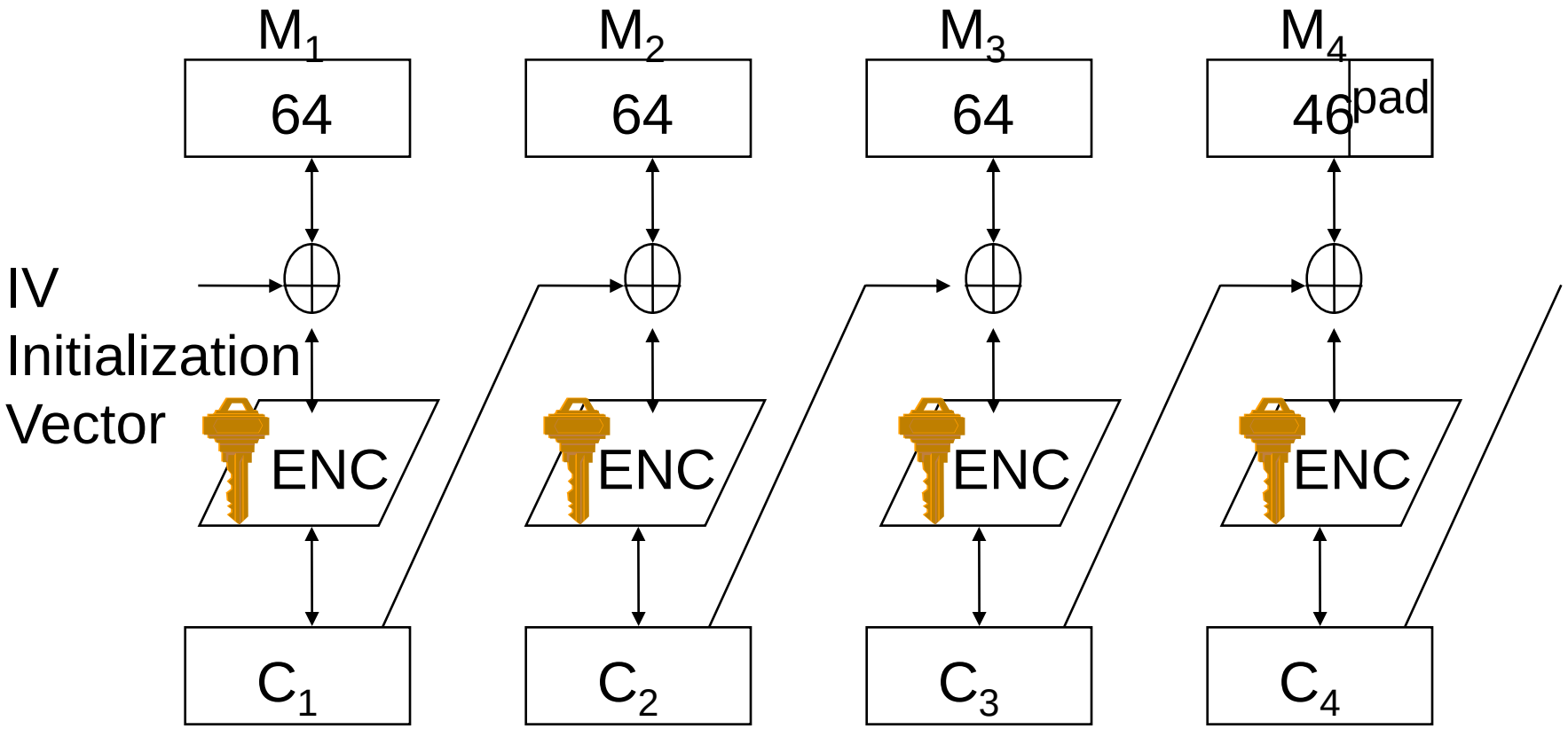
www.cs.rochester.edu

Electronic Code Book (ECB)
Elementare Blockverschlüsselung



- **Zwei Nachteile:**
  - Wiederholungen von Klartextblöcken im Geheimtext erkennbar
  - Wiedereinspielen zuvor abgefangener Blöcke verletzt Authentizität

Cipher Block Chaining (CBC)



- **benutzt die Blockverschlüsselung für eine Stromverschlüsselung mit Rückkoppelung**
  - **(M1 = M3) führt kaum zu (C1 = C3)**

Vor- und Nachteile der symm. Verschlüsselung

Pros:

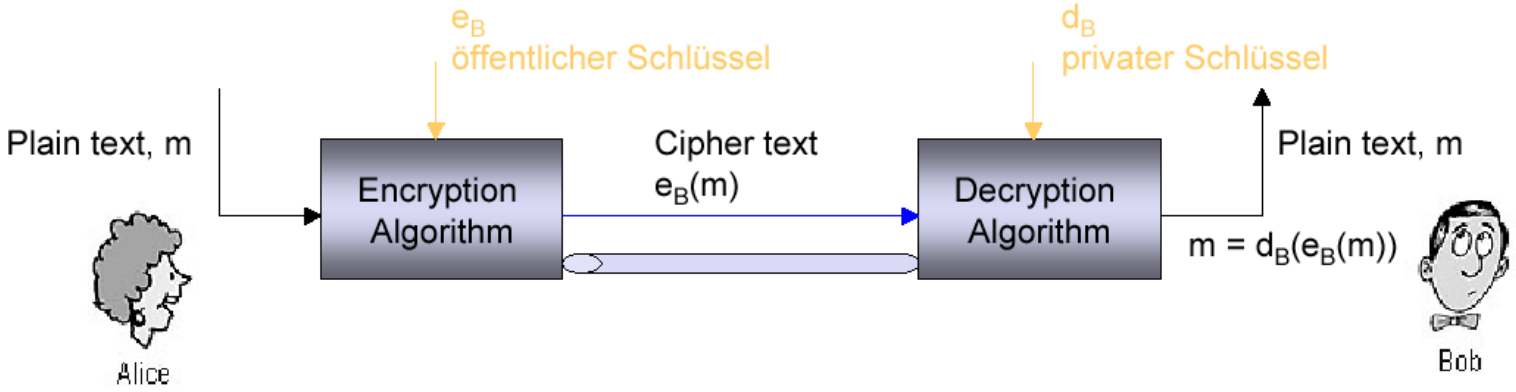
- Effiziente Verschlüsselung
- Kurze Schlüssel
- Große Erfahrung mit den Algorithmen

Cons:

- Sichere Verteilung der Schlüssel.
- Viele Schlüsselpaare in einem großen Netzwerk
- Ggf. eine „Trusted Thrid Party“ TTP erforderlich

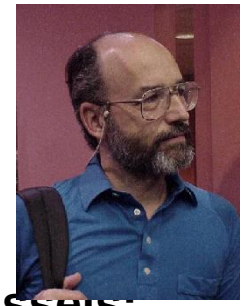
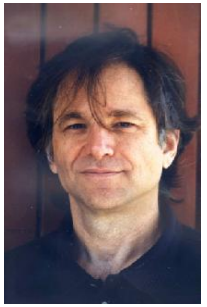
Asymmetrische Kryptographie

- **Kommunikationspartner können sicher kommunizieren, ohne einen gemeinsamen geheimen Schlüssel zu benötigen**
  - **Es gibt einen öffentlich bekannten Schlüssel und einen privaten Schlüssel**
  - **Grundlage: Die Berechnung des privaten Schlüssels auf Grundlagen des öffentlichen Schlüssels und des Verschlüsselungsalgorithmus ist praktisch nicht möglich.**
- **Vorteil**
  - **Es müssen keine geheimen Schlüssel verteilt werden**
- **Schema**



Der RSA-Algorithmus (1)

- **Entworfen von Ron Rivest, Adi Shamir und Len Adleman**

- **Auswahl des privaten und öffentlichen Schlüssels:**
  - **Auswahl zweier großer Primzahlen p und q**
    - 768 bit für private Nutzung empfohlen von RSA Laboratories
    - 1024 bit für Nutzung innerhalb einer Firma
  - **Berechne n = p * q und z = (p- 1) * (q- 1)**
  - **Wähle eine Zahl e < z, die außer 1 keinen gemeinsamen Faktor mit z hat**
  - **Finde d, so dass ed-1 durch z dividierbar ist**
    - d wird so gewählt, dass ed/ z = 1
    - Modulo-Operation
  - **Öffentlicher Schlüssel: (n, e), Privater Schlüssel: (n, d)**

Vor- und Nachteile der asymm. Verschlüsselung

Pros:

- Nur der private Schlüssel muss geheim gehalten werden
- Schlüsselmanagement erfordert nur Vertrauen in die Funktion der TTP (Trusted Third Party)
- Langlebige Schlüssel

Cons:

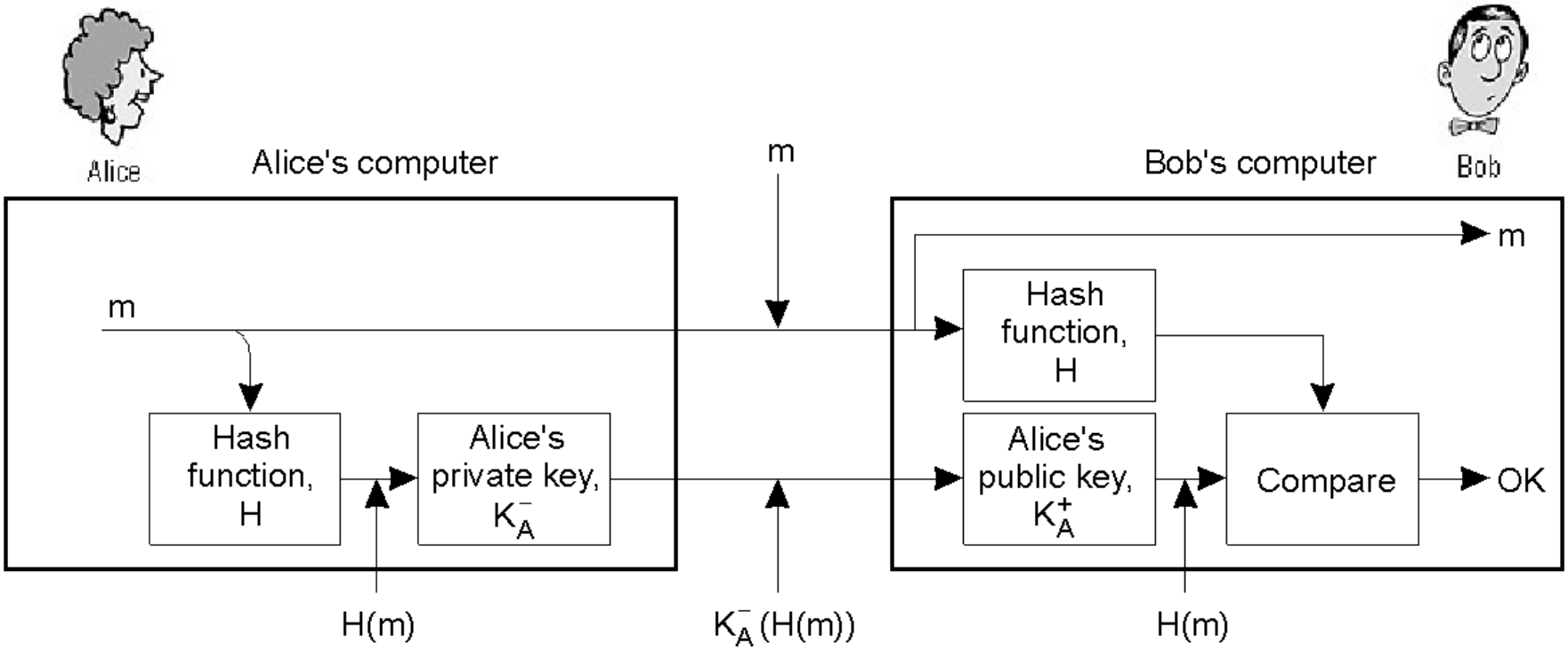
- Geringer Durchsatz
  - Faktor 1000 und mehr gegenüber symm. Kryptographie
- Lange Schlüssel
- Sicherheit beruht auf wenigen mathematischen Prinzipien
- Beschränkte Erfahrung

Folgerung

- Asymmetrische (Public Key) Verschlüsselung für
  - Schlüsselmanagement
  - Digitale Signaturen
  - Authentifizierung
- Symmetrische (Shared Secret Key) Verschlüsselung für
  - Effiziente Verschlüsselung von großen Datenmengen

➔ Man benutzt asymmetrische Verfahren um einen Schlüssel für die anschließende symmetrische Verschlüsselung auszuhandeln

Digital Signaturen



- **Digital Signatur mit einem Public-Key Verfahren und einer Hash-Funktion**

Message Digest

- **Ziel**
  - Einfach zu berechnende digitale Signatur fester Länge (Fingerabdruck)
- **Beispiel**
  - SHA-2 (2002 NIST, 256 – 512 bit)
  - SHA-3 (2012 NIST, 224 – 512 bit)
- **Vorgehensweise**
  - Anwenden der Hashfunktion H auf Nachricht m
    - Message Digest: H(m)
- **Eigenschaften von Hashfunktionen**
  - Many-to-One
  - Ergebnis fester Länge
  - Bei gegebenem Message Digest x ist es praktisch unmöglich, H so zu ermitteln, dass H(m) = x
  - Es ist praktisch unmöglich, zwei Nachrichten m und m‘ zu finden, so dass H(m)= H(m´) (*Kollision,* Verfahren für SHA-1 zz. bei 2^{69} Versuche)

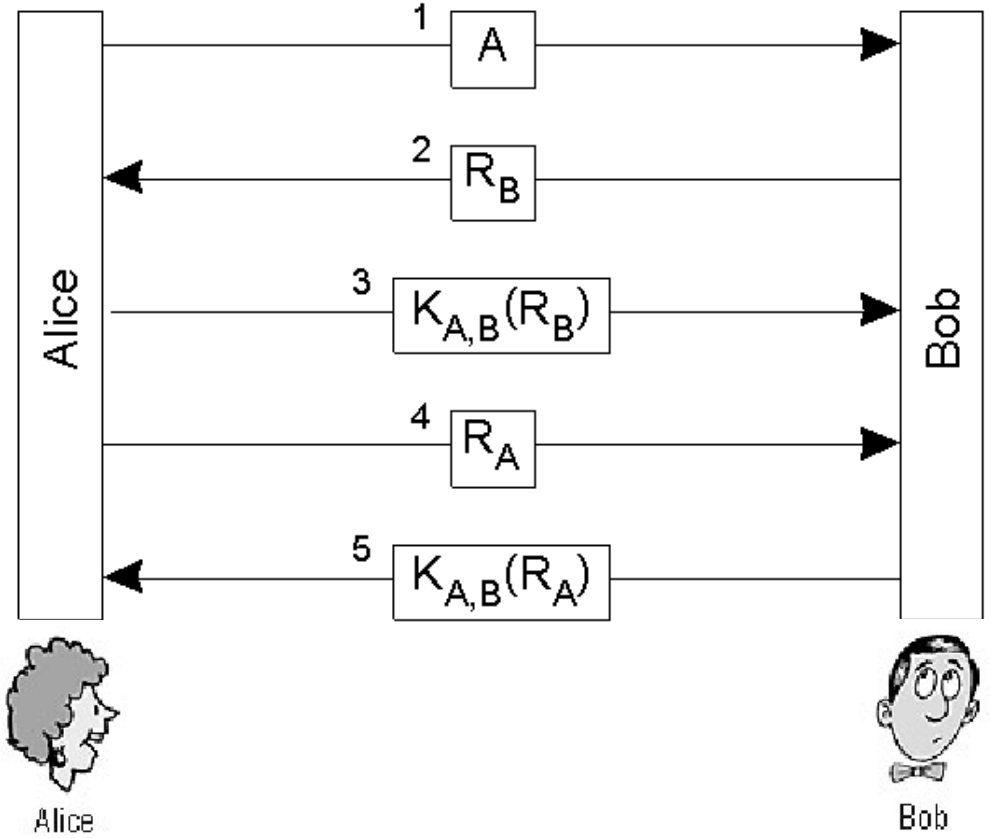
Authentifizierung und Authentisierung

- **Authentifizierung (engl. authentication)**
  - Vorgang der Überprüfung der Identität eines Gegenübers
- **Authentisierung**
  - Vorgang des Nachweises der eigenen Identität. Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Diensten

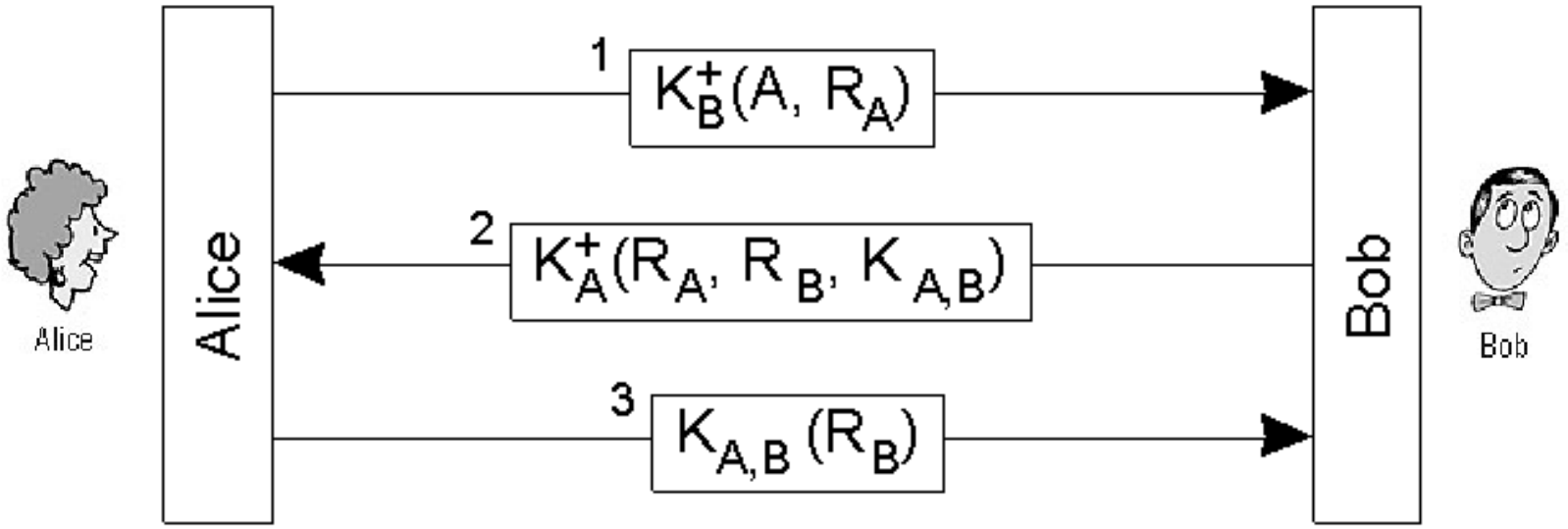
- **Zwischen Nutzern und/oder Maschinen**
  - Identität einer Maschine
    - IP-Addresse, Hostname, UID, … ?

Authentifizierung mit Secret Keys

- **Ziel**
  - Bob möchte, dass Alice Ihre Identität beweist
- **Protokoll mit Shared Secret Key**
  - Nonce: Zufallszahl (R), die der Benutzer eines Protokolls nur einmal benutzt
  - Alice sagt „I am Alice“.
  - Bob sendet Nonce R, der von Alice verschlüsselt zurück gesendet wird.
  - Anschließend umgekehrt
- **Challenge-Response**
  - Häufig genutztes Verfahren



Authentifizierung mit Public Key Verfahren (1)



- Basierend auf R_A und R_B kann nun ein Session-Key für eine nachfolgende symmetrische Verschlüsselung bestimmt werden
- Angewendetes Verfahren bei
  - SSL, HTTPS, TLS, SSH, …

Authentifizierung mit Public Key Verfahren (2)

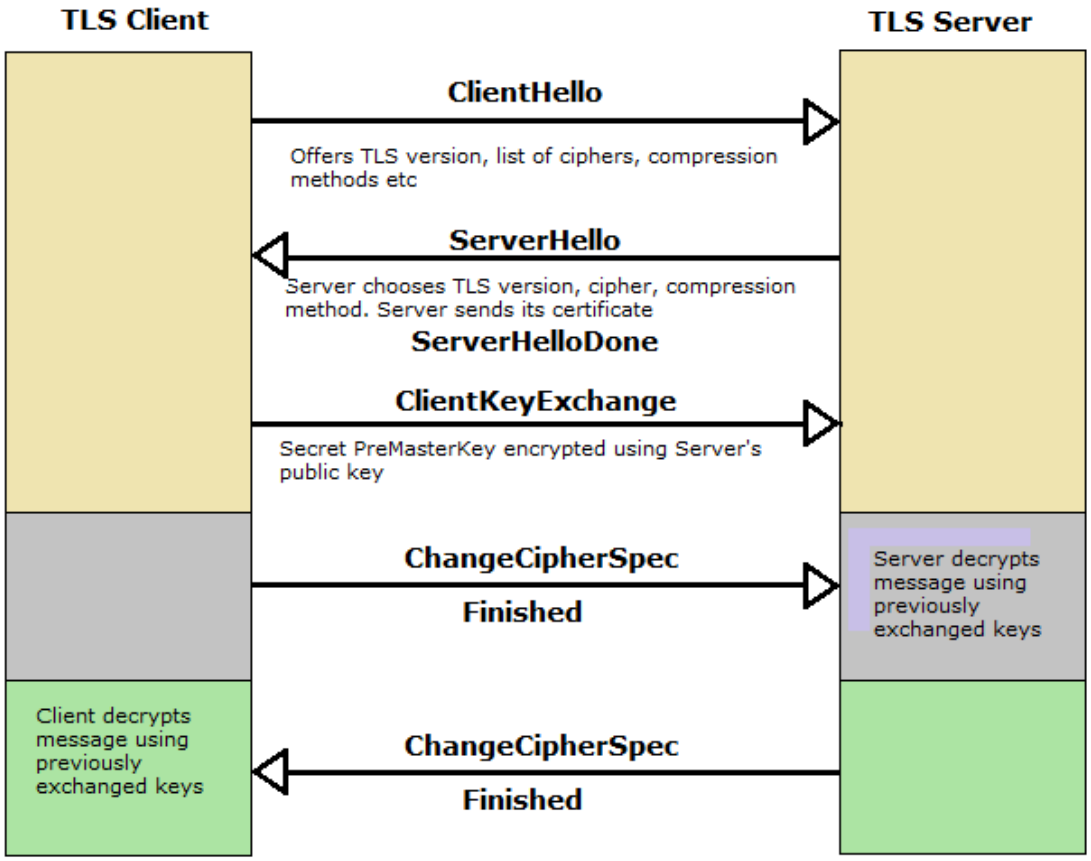
- **Problem:**
  - **Wie kann man sicher sein, dass man den richtigen Public Key kennt?**
  - **Veröffentlichung (z.B. auf der Web-Site) ist ganz gut, aber nicht wirklich sicher**

- **2 Ansätze**
  - **Web-of-Trust: Nutzer bestätigen sich Peer-2-Peer die Gültigkeit von Schlüsseln**
    - Beispiel: PGP
    - Probleme: Skalierung und benötigtes Verständnis beim Nutzer
  - **Public Key Infrastructure (PKI): Eine Hierarchie von trusted „Certification Authorities“ bestätigt zentral die Gültigkeit von Public Keys (Zertifikate)**

Mechanismen in Protokollen (1)

- **HTTPS (HTTP secure): „sicherer“ Web-Zugriff**
  - **Authentifizierung des Servers mittels Zertifikat**
    - Meist authentifiziert sich der Client auf Anwendungsebene (mit Passw.)
    - Optional auch: Authentifizierung des Clients mittels Zertifikat
  - **Verschlüsselung der übertragenen Daten mittels sym. Verschlüsselung**
  - **Übertragung über TCP-Port 443 (statt 80 für HTTP)**
  - **Nutzt SSL/TLS, ähnlich z.B. WLAN mit PEAP**
- **S/MIME: signierte und/oder verschlüsselte Email**
  - **Signierte Email mittels Zertifikat des Senders (s.o.)**
  - **Verschlüsselte Email mittels Zertifikat des Empfängers**
    - Verschlüsselt mit Public Key des Empfängers
    - Nur er kann das mit seinem Private Key wieder entschlüsseln
    - Daten werden wieder mit sym. Verschlüsselung verschlüsselt
      - Nur der sym. Schlüssel wird im „Envelope“ asym. verschlüsselt

Mechanismen in Protokollen (2): Ablauf TLS (Transport Layer Security)



- **Eine Kernkomponente: Firewall**
  - **Verbindung zwischen „sicherem“ und „unsicherem“ Netz**
  - **Regelt und überwacht gesamten Datenverkehr**
  - **Oder besser: zwischen verschiedenen Sicherheits-Domänen**
    - Können auch innerhalb einer Organisation sein
    - z.B. zwischen WLAN und Festnetz, zwischen Produktion und Verwaltung, etc.

- **Besteht meist aus mehreren Komponenten**
  - **Packet Filter**
  - **Application Gateways (z.B. Web-Proxy)**
  - **ggf. Intrusion Detection System (IDS)**
  - **ggf. VPN-Gateway**

Web Proxy

- **Für ausgehenden Web-Verkehr von internen Browsern**
- **Aufgaben eines Web-Proxies:**
  - **Zwischenspeicher (Cache)**
    - gestellte Anfragen zu statischen Inhalten bzw. deren Ergebnis werden gespeichert
  - **Security-Scanner**
    - Scannen von Inhalten nach Schadcode
  - **Zensur/Zugriffssteuerung**
    - Sperren oder Protokollieren von bestimmten Webzugriffen
    - ggf. nutzerabhängig
    - Auch z.B. Ausfiltern von Werbung
  - **SSL-Terminierung**
    - Aufbrechen einer SSL-Verbindung (terminiert), um auch deren Inhalte auf Schadcode zu überprüfen
    - weitere Verschlüsselung zum Client (Browser) mit Proxy-Zertifikat, Problem: Benutzer sieht das Originalzertifikat nicht mehr

Firewalls

- **Ungelöste Probleme**
  - Eingeschränkter Zugriff auf erwünschte Dienste
  - Evtl. Durchsatzprobleme
- **Firewalls helfen nicht gegen**
  - schlechte Passwörter
  - Social Engineering
  - physisches Eindringen
  - 'Angriffe von Innen'
  - 'Hintertüren' (z.B. Modems)
  - Viren und Mail Bomben

- **Auch im eigentlichen Einsatzgebiet kein vollkommener Schutz - Beispiele:**
  - Programm- und Konfigurationsfehler auf der Firewall
  - Denial of Service Angriffe
  - Schwierige, aber notwendige Anwendungsprotokolle
- **Daher**
  - Abwägen von Schutz gegen Kosten