Einführung in die Datensicherheit

Dr. Lorenz Müller

BFH, HTI

Datensicherheit und Kryptologie

Grundbegriffe

1.1. Information und Daten

1.2. Datenübertragung im Kanalmodell

1.3. Sicherheit im IT System

1.4. Bedrohungen, Angriffe

Risiken und Schutz

2.1. Risikoanalyse

2.2. Sicherheitspolitik und Sicherheitskonzept

2.3. Sicherheitsmassnahmen

Logische Sicherheitsmassnahmen

3.1. Elemente des Sicherheitssystems

3.2. Logische Datenschutztechnologie, Angriffe

3.3. Quantenkryptographie

3.4. Steganographie

Kryptologie

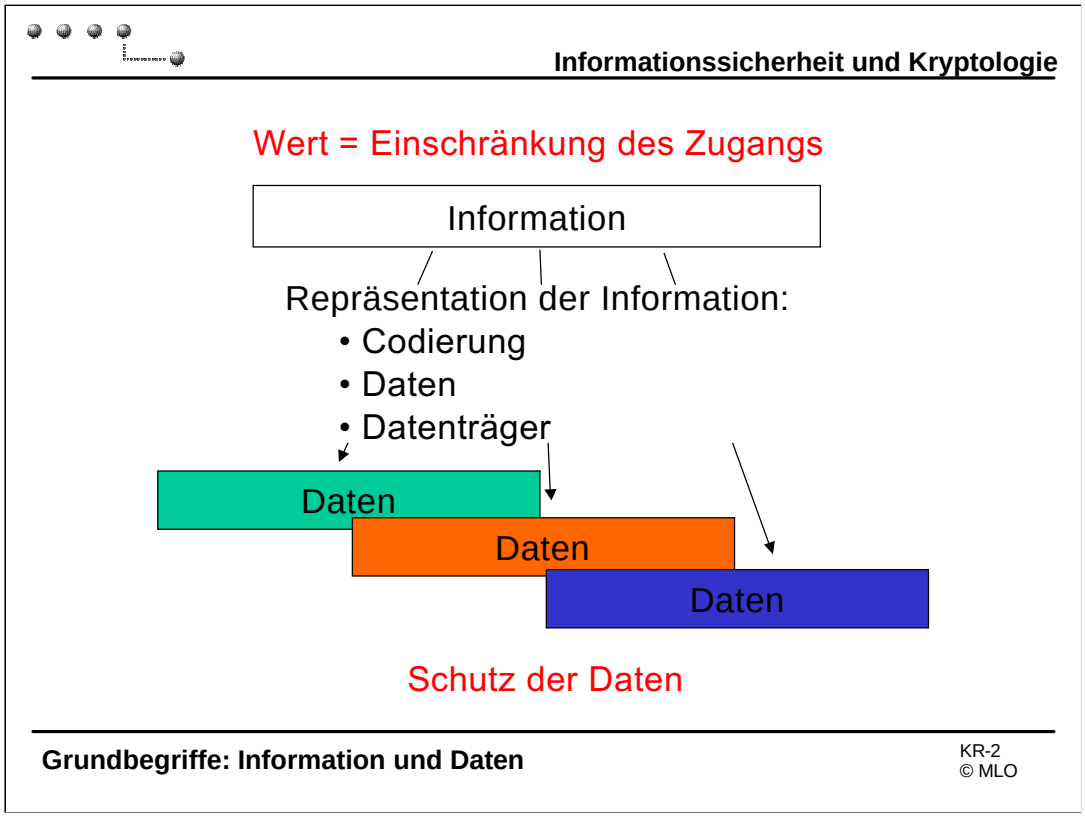
4.1. Grundbegriffe

4.2. Definition eines Kryptosystems

4.3. Kategorien von Kryptosystemen

4.4. Betriebsmoden

4.5 Kryptoanalyse und Angriffe



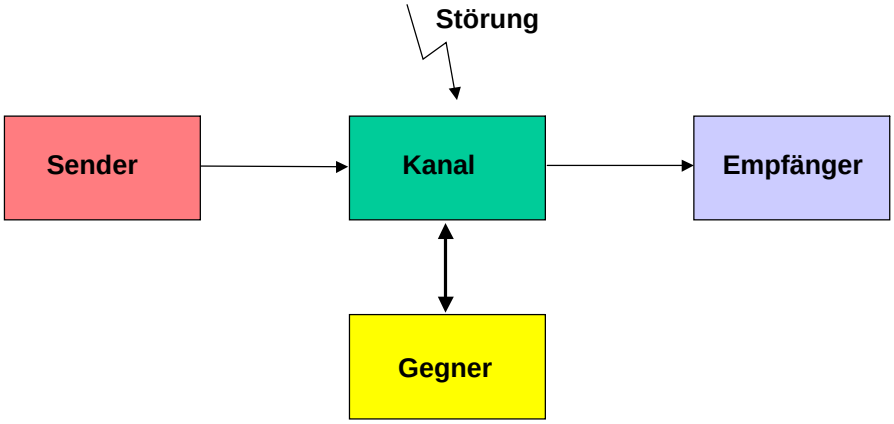
Aufnahme und Weitergabe von Information kann man ohne Zweifel zu den menschlichen Grundbedürfnissen zählen.

Parallel zur Entwicklung einer Kultur oder Zivilisation steigt der Stellenwert des Informationsbesitzes, der letztlich für die Struktur und Differenzierung in einer Gesellschaft verantwortlich ist.

Informationsbesitz ist ein wichtiges Machtmittel und die Information selbst deshalb seit alters her ein schützenswertes Gut. Besitzer von Informationen können Einzelpersonen, Gruppen, Sippen, Unternehmen, Kartelle, gesellschaftliche Klassen, Nationen und Bündnisse von Nationen sein.

Information ist ein abstraktes Konzept. Brauchbar wird sie erst durch eine geeignete Repräsentation. Diese umfasst eine Codierungskonvention (Sprache, Alphabet, Codes: Syntax), die Darstellung der Information (Daten: Semantik) und Datenträger.
Die gleiche Information kann dabei in vielfacher Form als Daten dargestellt werden. Der Wert der Information wird auf die Daten projeziert und diese müssen deshalb als Gesamtheit geschützt werden.

Datenübertragung im Kanalmodell



Zeitlich: Datenspeicherung Räumlich: Datenvermittlung

Grundbegriffe: Datenübertragung im Kanalmodell KR-3 © MLO

Information ist ein handelbares Gut
Ihren wahren Wert erhält die Information erst, wenn sie der Besitzer einem Kommunikationspartner, der die Information braucht, zur Verfügung stellen kann. Dies geschieht durch eine Uebertragung von Daten, die die gewünschte Information enthalten.
Die Information verliert jedoch ihren Wert, wenn sie den Kreis der Besitzenden unkontrolliert verlässt oder von aussen verändert werden kann.

Informationsträger sind Daten
Informationsträger sind Daten. Sie sind ein handelbares Gut, haben einen eigenständigen Wert und müssen deshalb vor Verlust oder Eingriffen geschützt werden. Beim Handel mit Informationen werden Daten übertragen.

Unter Datenübertragung versteht man

zeitliche **Datenspeicherung** und

räumliche **Datenvermittlung**

Sicherheit im Kanalmodell der Datenübertragung
Der Prozess der Datenübertragung wir durch das Kanalmodell mit

Sender
Uebertragungskanal
Empfänger

dargestellt.
Gefährdet ist die Information bei der Datenübertragung durch natürliche Störungen und durch Einwirkungen Dritter.

Ablauf der Datenübertragung
Der schrittweise Ablauf einer Datenübertragung von Sender zu Empfänger wird als **Protokoll** bezeichnet

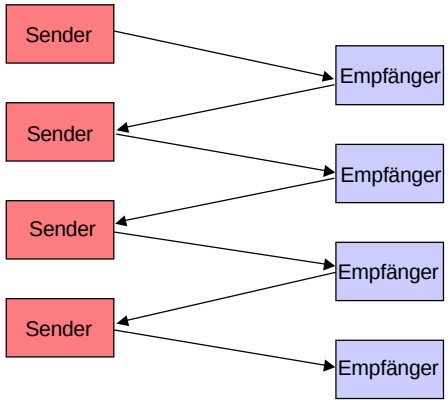
In der Terminologie der sicheren Datenübertragung personifiziert man die Protokollteilnehmer oft:

Sender	**Empfänger**	**Gegner**
Alice	*Bob*	*Eve, Mallory*

weitere Akteure in einem Protokoll können sein

Vertrauensperson
Trent
Überwacher
Walter

- Protokollschritte



Beispiel eines Protokolls

Digitale Unterschrift mit einem public key System

(a) Alice erzeugt einen Hash des Dokumentes **h(m)**

(b) Sie verschlüsselt **h** mit ihrem privaten Schlüssel und erhält **h'**

(c) Sie sendet das Dokument **m**, **h'** und **h**

(d) Bob entschlüsselt **h'** mit Alices öffent. Schlüssel und erhält **h''** . Er kontrolliert ob

h'' = h

Wenn ja, ist die Unterschrift gültig

Protokoll

Ein Protokoll ist eine Reihe von Schritten, die zwei oder mehrere Parteien unternehmen, um eine bestimmte Aufgabe auszuführen.

Eigenschaften

• Alle im Protokoll beteiligten Parteien müssen das Protokoll mit allen verlangten Schritten zum voraus kennen

• Alle Parteien müssen bereit sein den Protokollschritten zu folgen

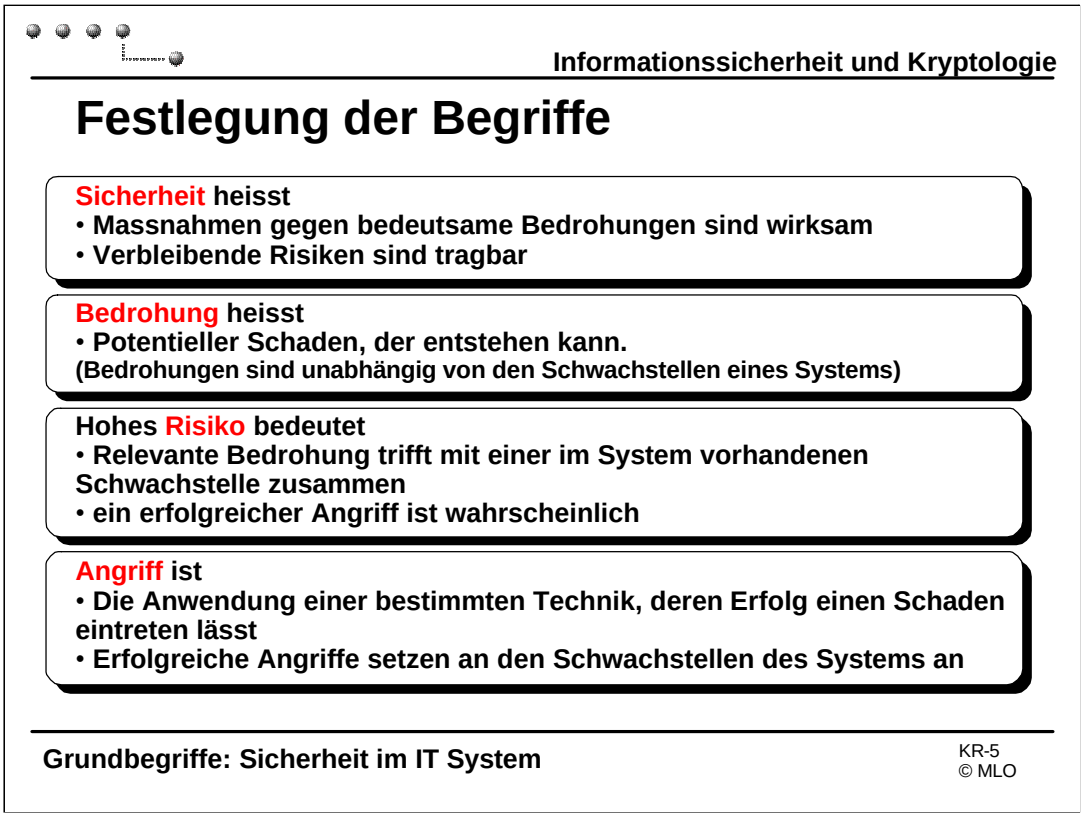
• Das Protokoll muss eindeutig sein: jeder Schritt klar definiert, keine Missverständnisse möglich

• Das Protokoll muss vollständig sein, für jede mögliche Situation muss die nächste Aktion klar sein

• In sicheren Protokollen darf es nicht möglich sein, etwas zu tun oder zu erfahren, das nicht im Protokoll vorgesehen ist

Zweck

Alle geschäftlichen Transaktionen unterstehen mehr oder weniger festgelegten Protokollen. Protokolle garantieren den korrekten Ablauf. Durch geeignete Wahl und Formalisierung von Protokollen kann dabei Betrug verhindert werden. Protokolle erlauben es die Transaktion unabhängig von der Implementation zu planen und analysieren.



Wichtige Merkmale dieser Definitionen sind die folgenden:

Sicherheit:

Sicherheit wird als eine Eigenschaft betrachtet, statt eine Tätigkeit oder eine Menge von Massnahmen.

Sie ist relativ, indem sie sich auf das Einsatzumfeld und die “als bedeutsam erachteten” Bedrohungen bezieht.

Sie ist realistisch, indem sie die Restrisiken miteinbezieht.

Bedrohung

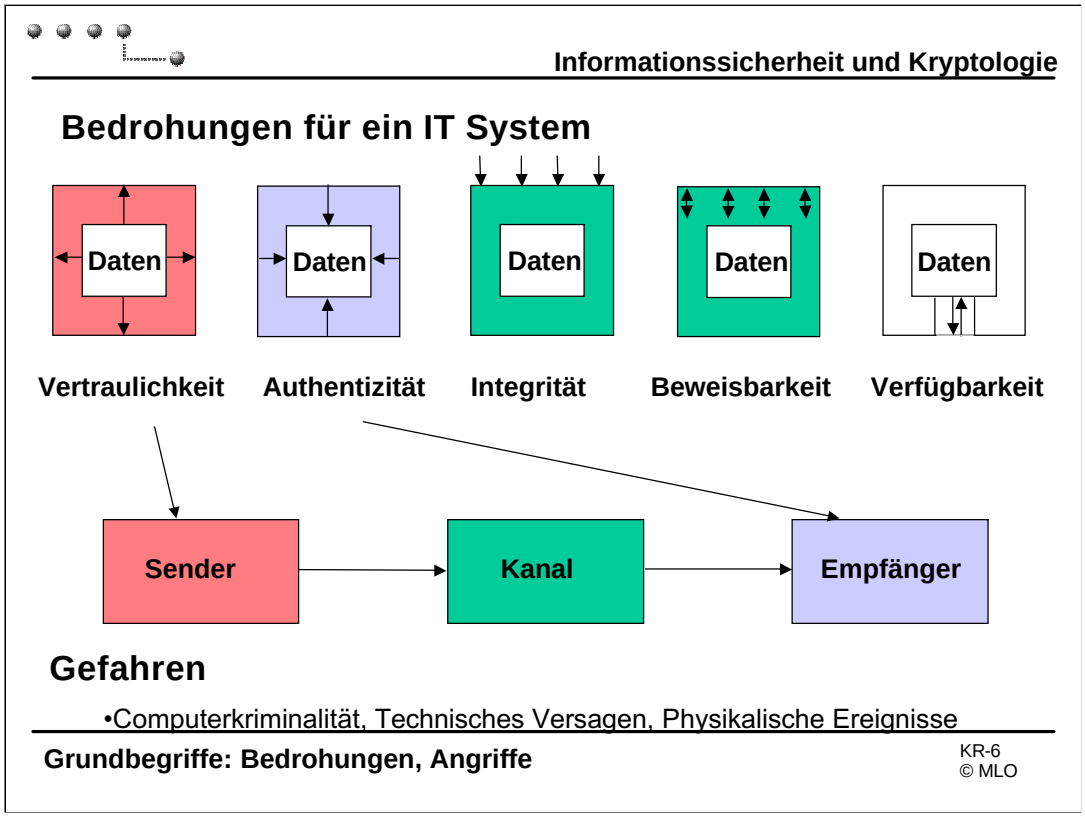
Bedrohung bezieht sich immer auf den potentiellen Schaden. Gibt es kein Schadenpotential ist auch keine Bedrohung da.

Risiko

Risiko ist das Aufeinandertreffen von Bedrohungen und Schwachstellen eines Systems. Schwachstellen ermöglichen die Realisierung einer Bedrohung zu einem Schaden durch einen Angriff. Das Risiko verbindet den potentielen Schaden mit der Wahrscheinlichkeit eines erfolgreichen Angriffs

Angriff

Angriffe nutzen Schwachstellen eines IT-Systems aus. Sie sind sowohl von den authorisierten Benutzern eines Protokolls wie von Dritten zu erwarten:
• Kunden, Partner
• Insider, Systemverantwortliche
• Externe Angreiffer
Sie umfassen passive und aktive Techniken (z.B. Mithören oder Stören einer Datenübertragung)



Als die klassischen **Bedrohungen** der Informationssicherheit gelten die folgenden Verluste:

- Verlust der Vertraulichkeit (Sender)
- Verlust der Authentizität (Empfänger)
- Verlust der Integrität
- Verlust der Nachweisbarkeit
- Verlust der Verfügbarkeit

Verlust der Vertraulichkeit tritt ein, wenn Informationen (der semantische Inhalt der Daten) von dazu Unbefugten zur Kenntnis genommen werden. Der Schutz gegen diese Bedrohung wurde früher und wird manchmal auch heute noch (fälschlicherweise) mit “Sicherheit” gleichgesetzt.

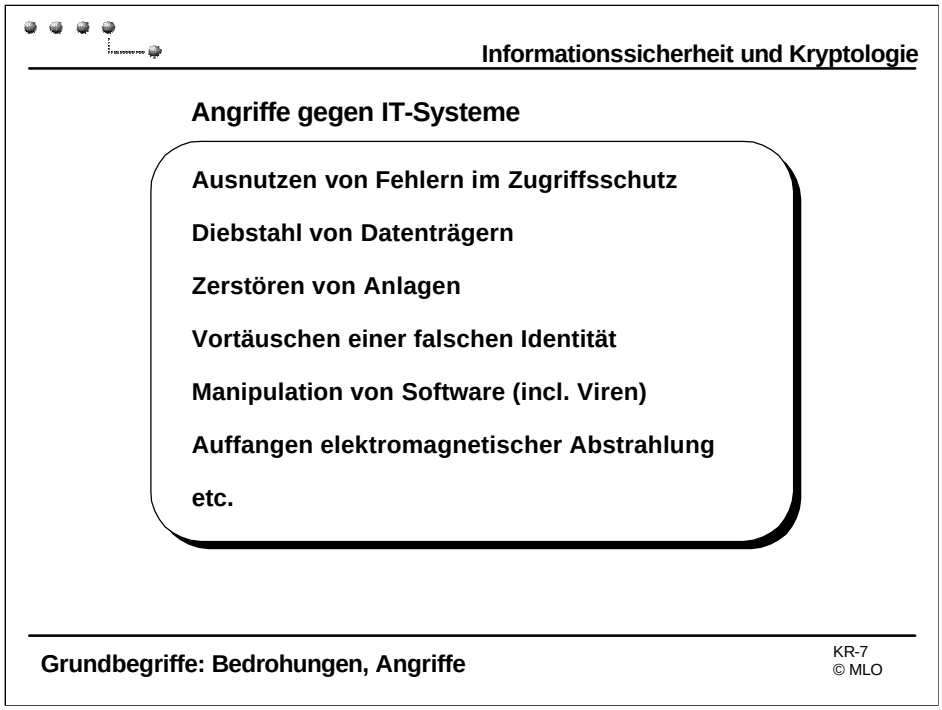
Ein heute häufiger gesondert genannter Aspekt dieser Bedrohung ist der **Verlust der Anonymität**. Er tritt ein, wenn die Identität eines Kommunikationspartners Unbefugten zur Kenntnis gelangt. Je nach Situation und Anwendung können auch die anderen Kommunikationspartner zum Kreis der unbefugten zählen.

Verlust der Authentizität tritt ein, wenn die Information nicht mehr eindeutig einem Autor zugewiesen werden kann. Diese Bedrohung betriff spezifisch den Empfänger einer Nachricht. Sie ist besonders in Geschäftstransaktionen relevant.

Verlust der Integrität tritt ein, wenn Daten unbefugt verändert werden. Dies schliesst ein, dass gefälschte Daten unter falscher Ursprungsangabe erzeugt werden oder Daten kopiert und in anderem Kontext wiedereingespielt werden.

Verlust der Beweisbarkeit tritt ein, wenn die Tatsache, dass eine Kommunikation mit dem Übertrag einer klar definierten Information überhaupt stattgefunden hat, nicht mehr nachweisbar ist. Es ist eigentlich ein Spezialfall der Integrität.

Verlust der Verfügbarkeit tritt ein, wenn die Funktionalität eines Systems unbefugt beeinträchtigt wird. Darunter fällt zum Beispiel auch die unautorisierte Benutzung von Ressourcen.



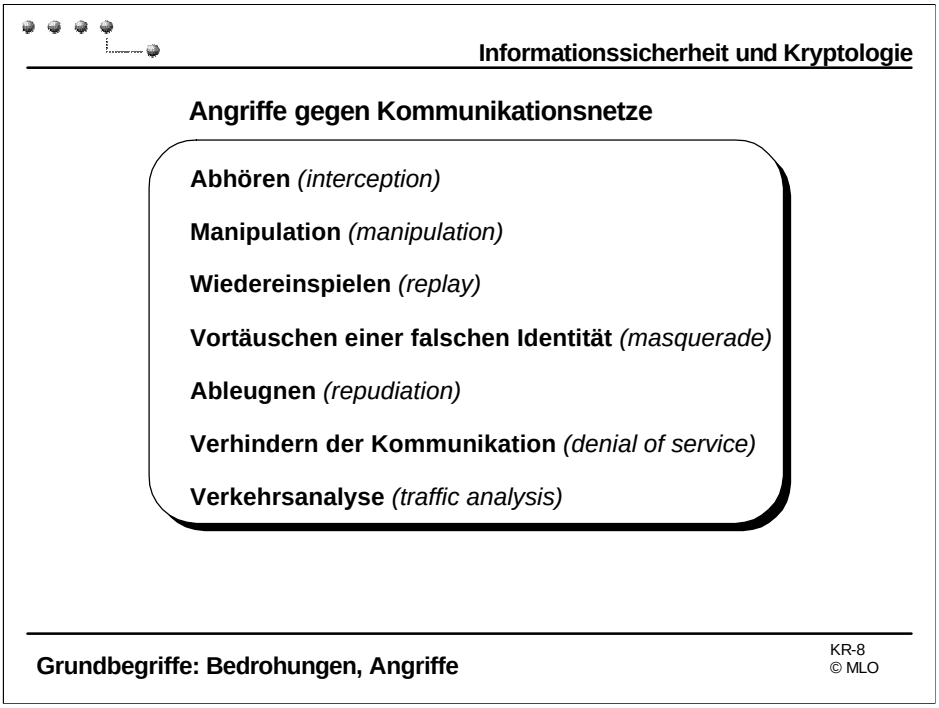
Die Abbildung enthält eine kleine Auswahl der wichtigsten Klassen von Angriffen gegen IT-Systeme. Es ist sehr schwierig, hierzu eine auch nur nahezu abschliessende Liste zu erstellen, da die Missbrauchsmöglichkeiten mit der rasch wachsenden Komplexität der Systeme zunehmen und der Lerneffekt im Bereich der Informationssicherheit durch die weit verbreitete Tendenz der Geheimhaltung von Problemen besonders erschwert ist.

Nach dem Militär sind die Banken diejenigen Anwender von Informationstechnik, bei denen Sicherheitsanforderungen am stärksten ausgeprägt sind. Während aus dem militärischen Bereich höchstens Informationen über historische Ereignisse zur Verfügung stehen, sind aus dem Bankwesen mehr Tatsachen über Sicherheitsprobleme an die Öffentlichkeit gedrungen.

Zur Illustration der grossen Bandbreite von Angriffsmöglichkeiten kann der besonders sensible Bereich der Geldausgabeautomaten betrachtet werden.

Geldausgabeautomaten geben deshalb gute Beispiele ab, weil ein erfolgreicher Angriff meist dazu führt, dass eine Abbuchung im Namen eines Bankkunden auftaucht und dieser behauptet, das Geld nicht erhalten zu haben. Diese Konstellation ist weniger als andere dazu geeignet, das Problem stillschweigend zu beseitigen.

Auf der einen Seite können die Banken natürlich nicht allen derartigen Reklamationen nachgeben, ohne eine Welle des Missbrauchs auszulösen. Auf der anderen Seite wollen sich unbescholtene Kunden nicht gern als Betrüger hingestellt sehen. Dies führt dazu, dass in zahlreichen Fällen von Geldautomatenbetrug eine gerichtliche Klärung angestrebt wird, die eine öffentliche Untersuchung der Sicherheitsprobleme durch Sachverständige einschliesst.



Kommunikationsnetze sind eine eingeschränkte Klasse von IT-Systemen, bei der kryptographische Verfahren die bedeutendste Anwendung finden. Die wichtigsten Klassen von Angriffen gegen Kommunikationsnetze können wie folgt klassifiziert werden:

Abhören:

Der unbefugte Zugriff auf alle oder Teile der Nutzdaten und Protokollfelder. Hierbei handelt es sich um einen sogenannten passiven Angriff.

Manipulation:

Das aktive, unbefugte Verändern von Daten, in der Regel mit dem Ziel, dass die Manipulation unbemerkt bleibt.

Wiedereinspielen:

Zu einem späteren Zeitpunkt werden zuvor aufgezeichnete Daten nochmals übertragen, um dadurch beim Empfänger bestimmte Reaktionen auszulösen.

Vortäuschen einer falschen Identität:

Diese kann sowohl dazu dienen, unbefugt auf Informationen zuzugreifen, als auch dazu,

Daten unter einer falschen Absenderadresse zu verbreiten.

Ableugnen:

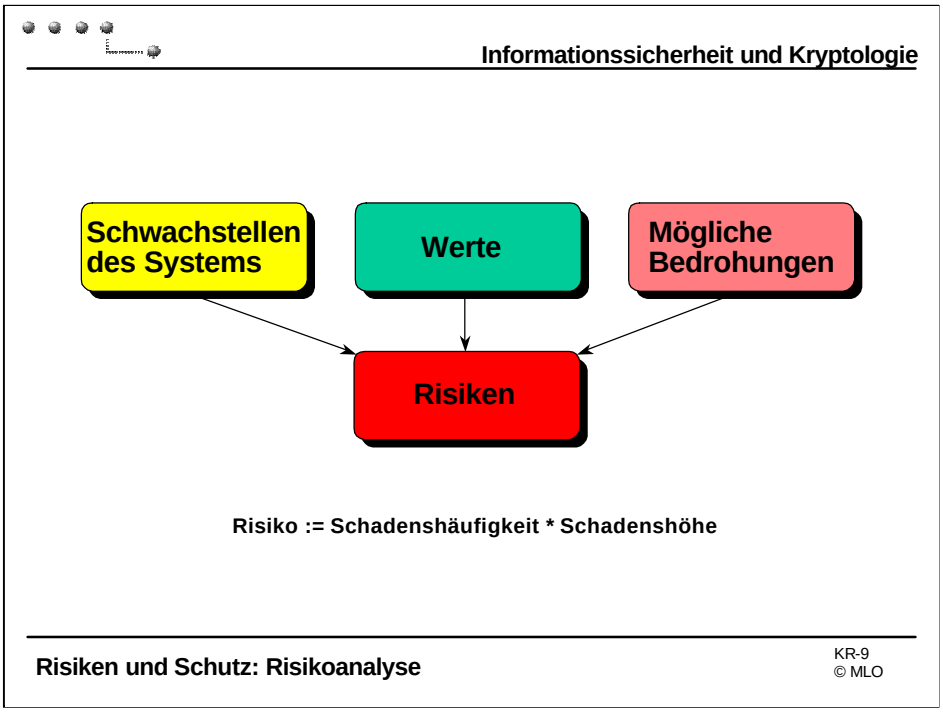
Gemeint ist das nachträgliche Ableugnen, bestimmte Daten erzeugt *(repudiation of origin)* oder empfangen zu haben *(repudiation of receipt)*, mit dem Ziel, den jeweiligen Kommunikaionspartner zu täuschen oder zu betrügen.

Verhindern der Kommunikation:

Dies ist eine komplexe Klasse von Angriffen, die u.a. auch das Unterbrechen von Verbindungen, das unautorisierte Verweigern der Benutzung von Ressourcen oder die Verzögerung von Reaktionen umfasst.

Verkehrsanalyse:

Darunter versteht man die Ableitung von inhaltlichen Informationen aus der Beobachtung der Existenz von Kommunikationsbeziehungen, sowie des Zeitpunkts, der Länge und der Häufigkeit von Nachrichten.



Unter Risikoanalyse versteht man den Prozess, in dem die relevanten Bedrohungen, die bedrohten Werte und die erkannten oder vermuteten Schwachstellen so miteinander in Beziehung gesetzt werden, dass daraus alle relevanten Risiken erkannt werden können und ihre relative Bedeutsamkeit beurteilt werden kann.

Eine bekannte, quantitative Risiko-Definiton ist:

Risiko := Schadenshäufigkeit * Schadenshöhe

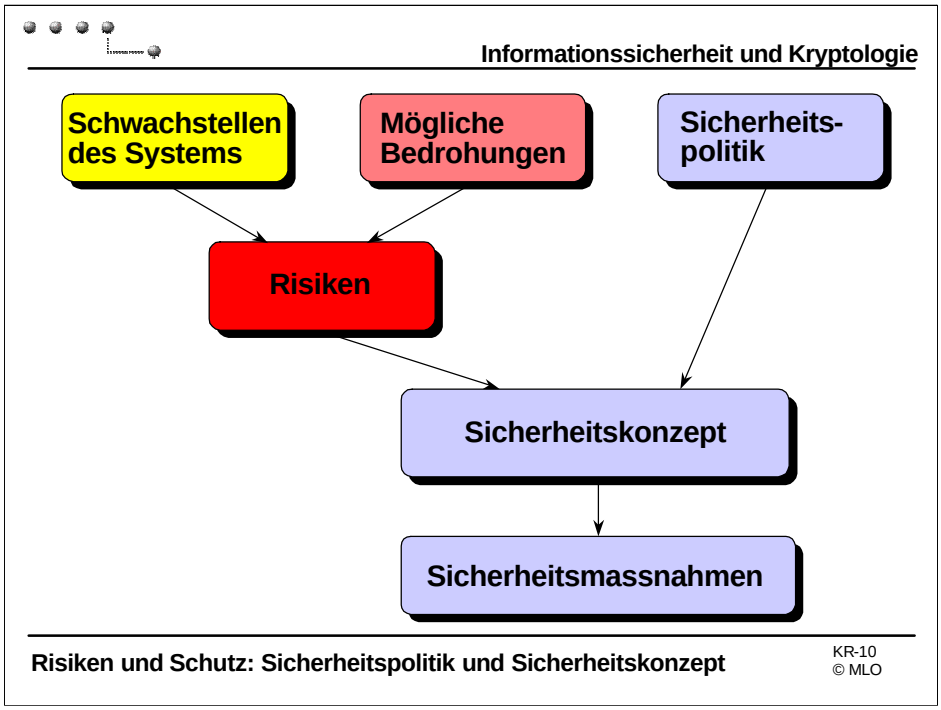
Das Problem in der Praxis ist, dass sowohl die Schadenshäufigkeit wie auch die Schadenshöhe für die meisten Ereignisse im voraus nur schwer zu bestimmten ist. Ein gewisses Mass an subjektiver Beurteilung ist dabei immer erforderlich.

Risikoanalyse-Methoden und -Werkzeuge können hier wertvolle Unterstützung liefern. Sie bestehen zu einem Teil meist aus einem mehr oder weniger komplexen Vorgehensschema, dessen einzelne Schritte durch Checklisten und Fragenkataloge unterstützt werden.

Die korrekten Informationen und Bewertungen zu finden, kann die Methode dabei natürlich nicht übernehmen. Sie kann jedoch in dieser Phase eine Hilfe sein, nichts zu vergessen.

Die Fragenkataloge und Checklisten sind oft sehr umfangreich, da sie alle Eventualitäten verschiedenster Einsatzumfelder abdecken müssen. Zudem ist es sinnvoll in einer Risikoanalyse nicht nur böswillige Angriffe sondern auch andere Ereignisse zu berücksichtigen, die zu den genannten Bedrohungen führen können. Dies sind z.B. Fehlbedienungen und Naturkatastrophen.

Ein weiteres Element einer Risikoanalyse-Methode sind Verfahren zur Auswertung der gewonnen Informationen. Oft werden dabei quantitative Bewertungen anhand der obigen Formel herangezogen, um eine Vergleichbar-keit verschiedener Risiken zu erreichen.



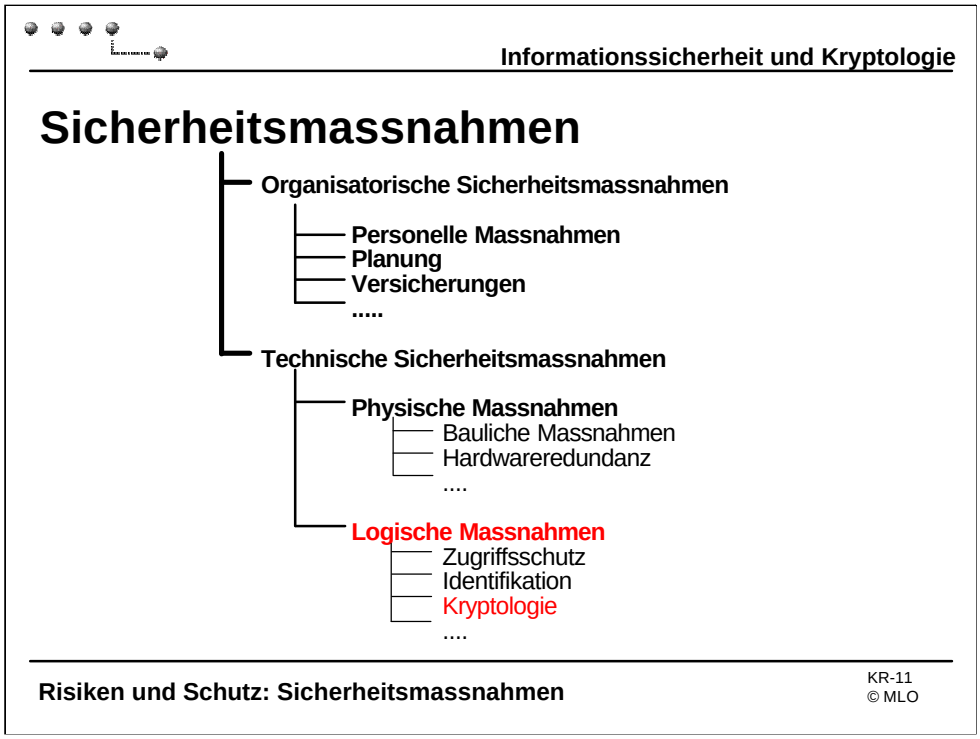
Nach der vergleichenden Bewertung der Risiken muss entschieden werden, welche Risiken noch tragbar sind und welche nicht, also einen Handlungsbedarf auslösen.

Die Festlegung einer solchen Grenze ist ein anschauliches Beispiel für eine Entscheidung, die nicht mehr im Kontext einer Methodik oder Technik getroffen werden kann, sondern als ein strategisches Element eingehen muss, bevor die Anforderungen für die zu implementierenden Sicherheitsmassnahmen bestimmt werden können.

Idealerweise werden solch generelle Beschlüsse zur Gestaltung der Sicherheit eines Systems nicht von Fall zu Fall komplett durchdiskutiert, sondern aus einer sogenannten Sicherheitspolitik (*security policy*) abgeleitet.

Eine **Sicherheitspolitik** (von engl. ‘security policy’, im deutschen auch häufig ‘Sicherheitsstrategie’ genannt) legt dabei in Form von mit der Unternehmenspolitik abgestimmten Grundsatzentscheidungen die im Sicherheitsbereich geltenden Zielsetzungen fest.

Risikoanalyse und Sicherheitspolitik münden in ein **Sicherheitskonzept**, in dem ein System untereinander abgestimmter Sicherheitsmassnahmen beschrieben wird, die in ihrem Zusammenwirken das Erreichen der gesetzten Ziele ermöglichen sollen.



Im oben erwähnten Beispiel von Angriffen gegen Geldausgabeautomaten gilt fast immer: Die Angriffe richten sich gegen ein unter anderem mit krypotgraphischen Verfahren gesichertes IT-System und sind erfogreich ohne das Chiffrierverfahren selbst zu brechen. Sie zeigen daher die hohe Bedeutung des umfassenden Sicherheitskonzepts auf, durch das allein ein wirklich hohes Sicherheitsniveau zu erreichen ist.

Bevor im weiteren Verlauf dieses Moduls vertieft auf kryptographische Verfahren für den Schutz von IT-Systemen eingegangen wird, soll daher die ganze Breite der zur Verfügung stehenden Sicherheitsmass-nahmen wenigstens in aller Kürze beleuchtet werden.

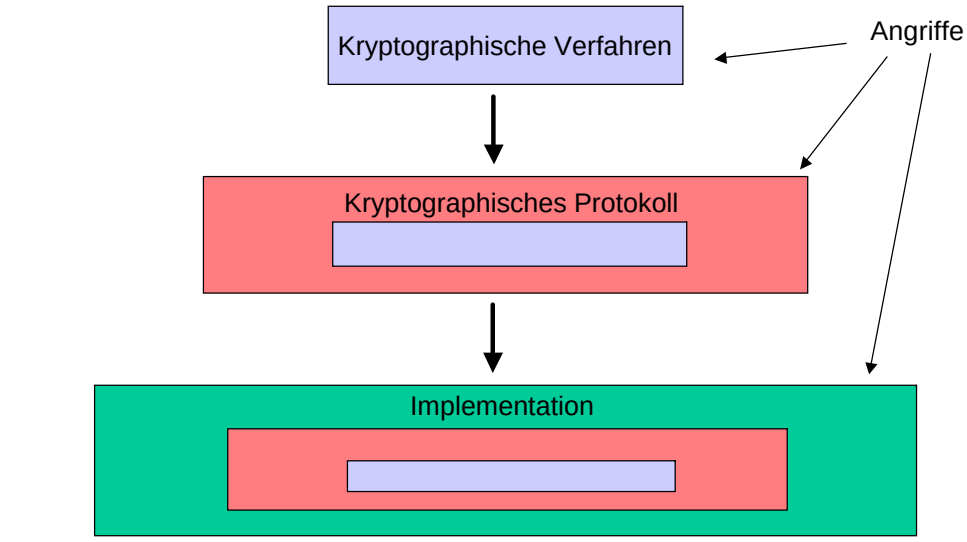
Ziel ist es aufzuzeigen, dass auch mit fortgeschrittenen kryptographischen Verfahren in der Praxis Sicherheit nur in Zusammenwirken mit geeigneten organisatorischen und anderen technischen Massnahmen zu erreichen ist.

Von der Beschaffung und Implementierung technischer Sicherheitsmassnahmen allein kann selten eine nennenswerte Steigerung der Sicherheit erwartet werden. Die technischen Massnahmen können nur in dem Masse wirksam sein, wie sie korrekt, in geeigneter Kombination und im Bewusstsein ihrer Grenzen eingesetzt werden.

Die wichtigste Voraussetzung dafür kann durch die klare Zuordnung von Verantwortlichkeiten geschaffen werden. Einführung und Betrieb technischer Massnahmen können dann in jedem Bereich den jeweils für die Sicherheit Verantwortlichen überlassen werden, was i.a. sowohl zur Optimierung als auch zur Akzeptanz beiträgt.

Sicherheitsmassnahmen werden von den unmittelbar Betroffenen zunächst fast immer als Last erlebt und daher häufig abgelehnt, wenn möglich umgangen oder zumindest nicht in optimaler Weise betrieben. Neben der technischen Aufgabe einer benutzerfreundlichen Gestaltung der Massnahmen, ist die Schulung in bezug auf die Verbesserung des Sicherheitsbewusstseins und auf den Umgang mit einzelnen Massnahmen unerlässlich.

Technische Sicherheitsmassnahmen finden immer da ihre Grenzen, wo Bedrohungen durch Aktionen von Individuen entstehen, die formal dazu durchaus autorisiert sind.



Logische Massnahmen: Elemente des Sicherheitssystems

Logische Schutzmassnahmen

Sie umfassen Sicherung der Datenübertragung (Kommunikation, Dateien), Personen-identifizierung, Nachrichtenauthentifizierung, Schlüsselerzeugung und -management, Digitale Unterschriften usw.

Realisiert werden sie durch die Anwendung von kryptographischen Algorithmen, sicheren Datenübertragungsprotokollen und sicheren Implementation der beiden Techniken.

Hierarchische Struktur

Das logische Sicherheitsystem ist hierarchisch in drei Ebenen strukturiert:

- Kryptographische Verfahren für den Schutz der Information in den Daten

- Kryptographische Mechanismen (Protokolle) für den Schutz der Daten gegen Angriffe

- Sichere Implementation für den Schutz des Gesamtsystems (Elimination von Schwachstellen)

Methoden

Sichere kryptographische Algorithmen

Sicherheitsstufen:

- Einschränkungslos sicher (informationstheoretisch)
- Rechnerisch sicher (komlexitätstheoretisch)
- Technisch sicher (systemtheoretisch)

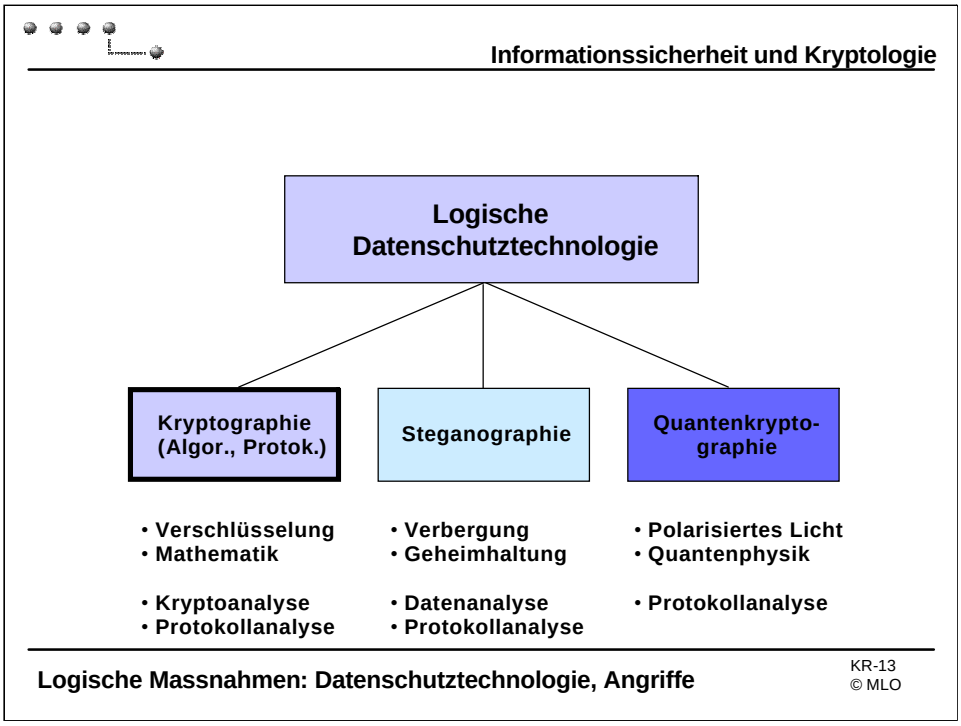
Sichere Protokolle

Sicherheitsvarianten:

- Protokolle mit Schiedsrichter
- Protokolle mit Richter
- Sicherheit erzwingende Protokolle

Sichere Implementation

Im Verbund mit technischen und organisatorischen Massnahmen



Datenschutztechnologien

Kryptographie (wichtigste und technisch weitaus am häufigsten angewandte Methode)

Schutz durch Verschlüsselung der Nachricht

Sicherheit basiert auf mathematisch unlösbaren oder schwierig zu lösenden Problemen

Gefahr droht durch mathematische und computertechnische Fortschritte der Analyse

Vorteil: Sicherheit und somit Risiko mathematisch quantifizierbar

Nachteil : Aufwendige Implementation und Management

Steganographie

Schutz durch Verstecken der geheimen in einer unverfänglichen Nachricht

Sicherheit basiert auf Geheimhaltung der Methode bzw. des Algorithmus

Gefahr droht durch Bekanntwerden des Protokolls, menschliches Versagen, Zufall

Vorteil: Implementation erfordert geringen Aufwand

Nachteil: Sicherheitsrisiko unbekannt und nicht steuerbar

Quantenkryptographie

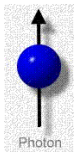
Schutz durch Kodierung der Nachricht in quantenphysikalischen Zustand

Sicherheit basiert auf dem Unbestimmtheitsprinzip der Quantenphysik

Der Kommunikationskanal ist prinzipiell abhörsicher

Vorteil: Absolute Sicherheit gewährleistet

Nachteil: Aufwendiges Protokoll, vorläufig nur für Glasfasertechnologie implementierbar



Photon mit ausgerichtetem elektrischen Feld

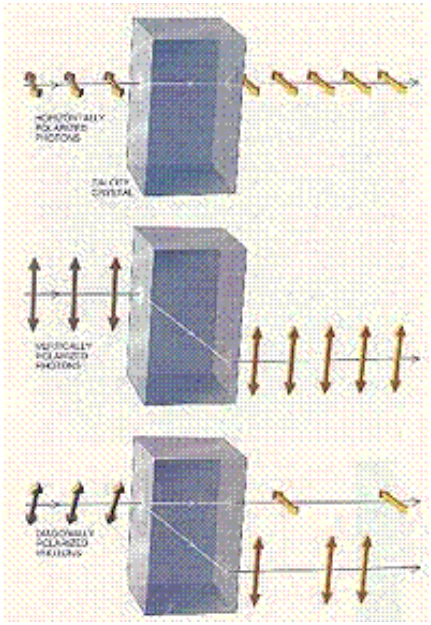
⇒Polarisiertes Photon

⇒Filter für polarisiertes Licht

Folgende Polarisationen entsprechen der 0 und 1 :

 und  entsprechen der 0

 und  entsprechen der 1



Logische Massnahmen: Quantenkryptographie

KR-14
© MLO

Quantenkryptographie

Ein Verschlüsselungsverfahren ist um so sicherer, je kürzer der verschickte Text bzw. je länger der Schlüssel ist. Absolute Sicherheit wird erreicht, wenn der Schlüssel gleich lang bzw. länger wird als die Nachricht. In diesem Falle sprechen Kryptologen von einem One-Time-Pad. Es ist absolut sicher, solange der Schlüssel nur einmal verwendet wird.

Doch das One-Time-Pad hat zwei Probleme: Zum ersten müssen erst einmal große Mengen an echten Zufallszahlen erzeugt werden, denn nur dann kann eine absolute Sicherheit garantiert werden. Dies ist praktisch über radioaktive Zerfälle realisierbar. Das zweite Problem betrifft die Übermittlung der Zufallszahlen. Die Zufallszahlen stellen den Schlüssel dar und dieser darf nicht in die falschen Hände gelangen. Daher muss die Übermittlung des Schlüssels, hier gleichbedeutend mit den Zufallszahlen, möglichst sicher sein. Genau das Problem dieser Übermittlung ist der Ansatzpunkt der Quantenkryptographie!

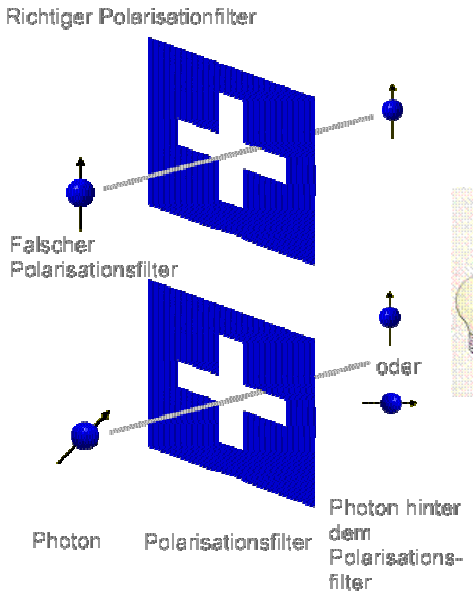
Licht besteht aus Photonen

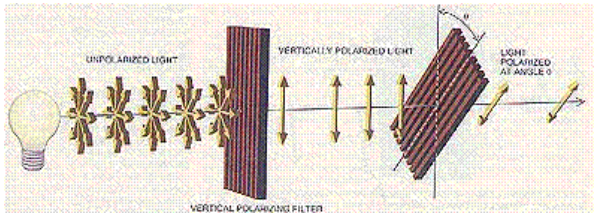
Aus quantenmechanischer Sichtweise besteht Licht aus Lichtteilchen, den sogenannten Photonen. Wenn wir Menschen etwas sehen, spielen hier pro Sekunde mehrere Milliarden Photonen mit. Quantenkryptographisch wird nur ein einziges Photon verwendet. Das hat seinen Grund: Ein einzelnes Photon kann man nicht mehr teilen. Im Photon steckt nun die Information, entweder 0 oder 1. Um diese herauszubekommen muss man Messungen am Photon durchführen.

Genau hier steckt eine der Grundideen: Wenn jede Messung eine Störung verursacht, dann muss nur dafür gesorgt werden, dass diese Störung erkannt wird! Ein Abhörversuch ist ja nichts anderes als eine Störung. Weist die Leitung eine Störung (= die Leitung wird abgehört) auf, dann wird dieser Schlüssel nicht mehr verwendet. In der Quantenkryptographie kann sehr genau erkannt werden, ob jemand gerade mithört. In solchen Fällen wird die Übertragung umgehend gestoppt.

Jedes Photon besitzt ein elektrisches Feld (transversal zur Ausbreitungsrichtung). Jedes Feld kann eine Richtung haben, und damit auch das Feld unseres Photons. Besitzen nun aus irgendwelchen Gründen alle ankommenden Photonen eines Lichtstrahls die gleiche Ausrichtung im elektrischen Feld, so wird dies polarisiertes Licht genannt. Für unsere Zwecke unterscheiden wir vier Richtungen des elektrischen Feldes: Senkrecht und Waagerecht sowie jeweils in 45 Grad dazu.

Mit diesem Hintergrund ist die Idee der Quantenkryptographie auch fast schon erklärbar: Sender, Alice genannt, und Empfänger (Bob) einigen sich, dass die Polarisation senkrecht (I) und diagonal (/) einer 0 entspricht. Damit bleibt für die 1 die waagerechte Richtung - und \.





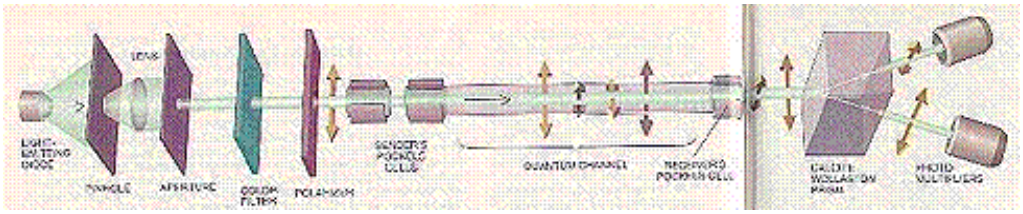
Logische Massnahmen: Quantenkryptographie

KR-15
© MLO

Photonen und Polfilter

Durchläuft ein polarisiertes Photon einen korrekt ausgerichteten Filter passiert nichts weiter. Ist der Filter falsch ausgerichtet, ändert sich die Polarisation entsprechend den Filterungen. Verwendet werden zwei verschiedene Filter: Filter die nur horizontal- und vertikal polarisierte Photonen passieren lassen und Filter die diagonal polarisierte Photonen passieren lassen.

Eine fundamentale Eigenschaft der Quantenmechanik ist das Ergebnis, wenn ein falscher Filter verwendet wird! Trifft ein senkrecht polarisiertes Photon auf einen diagonal ausgerichteten Filter, existieren statistisch zwei Möglichkeiten: Das Photon wird um 45Grad nach rechts oder um 45Grad nach links gedreht. Was passiert, kann man nicht vorhersagen, auch kann man mit einem falschen Filter nicht mehr feststellen, wie das Photon ursprünglich polarisiert war! Und das ist das Fundament der Quantenkryptographie.



1	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1
2	↕	↘	↙	↔	↗	↘	↕	↕	↗	↙	↔	↕	↘	↘	↔
3	✥	✥	✕	✥	✕	✥	✥	✕	✥	✥	✕	✥	✕	✥	✥
4	√	-	√	√	√	-	√	-	-	-	-	√	√	-	√
5	0	-	1	1	1	-	0	-	-	-	-	0	0	-	1

Logische Massnahmen: Quantenkryptographie

KR-16
© MLO

So funktioniert es

1. Alice, der Sender, erstellt die zu versendende Folge von 0 und 1, da es zu jeder Zahl zwei Varianten gibt (s.o.) wird zufällig zwischen beiden hin und her gesprungen.

2. Bob, der Empfänger, misst die Polarisation. Allerdings ist ihm nicht bekannt, wann Alice welche Variante der 0 (1 analog) genommen hat! Also wechselt er zufällig den Filter: Mal den Horizontal-Vertikalen und mal den Diagonalen. Statistisch gesehen wird er also in der Hälfte der Falle den falschen Filter nehmen.

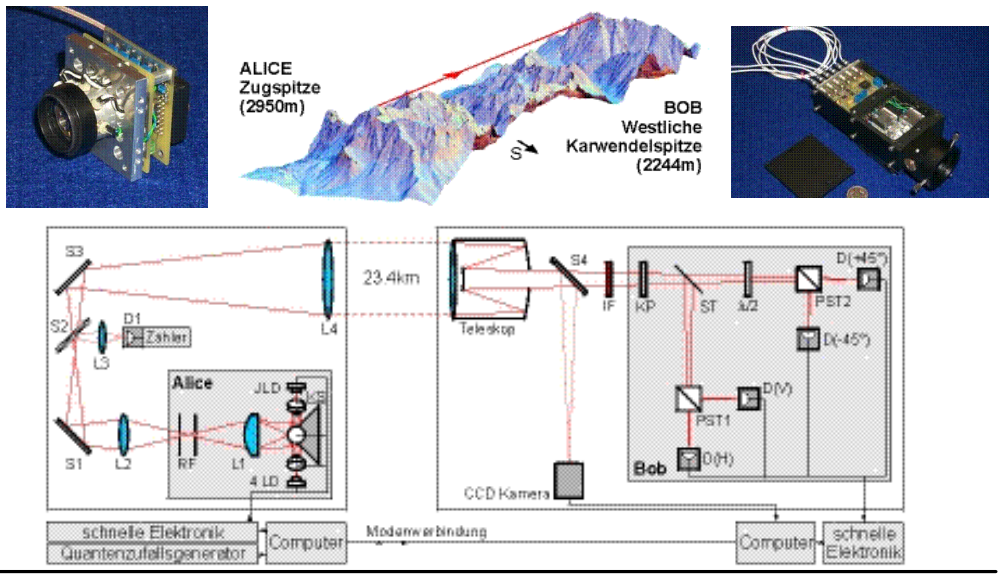
3. Alice ruft Bob an. Ganz normal per Telefon, dort teilt sie ihm mit, welche Variante sie wann genommen hat, nicht aber wie das Ergebnis war! Falls Bob das richtige Filter genommen hat, teilt er dies Alice mit. Damit wissen sowohl Bob und Alice, dass sie beide die das gleiche Bit vorliegen haben. Nutzte Bob den falschen Filter, so wird das Bit einfach gestrichen. Es bleibt von der gesendeten Zahlenfolge die Hälfte über, die nun zur Verschlüsselung der eigentlichen Nachricht verwendet werden kann.

Abhörversuche

Abhörversuche werden scheitern. Sollte Eve das Telefonat mithören, wird das nicht viel bringen. Es werden ja keine Ergebnisse übertragen. Wann was gemessen wurde bleibt unklar.

Hat Eve zusätzlich noch die Glasfaserleitung belauscht, greift die Quantenmechanik: Auch Sie kann nur raten, wann sie welchen Filter zu verwenden hat. Genau wie Bob auch, wird sie in der Hälfte der Fälle falsch liegen. Damit Bob Daten bekommt muss sie diese wieder in das Netz einspeisen - es wurde ja nur ein einzelnes Photon zur Datenübertragung benutzt, und das ist bei der Messung verschwunden. (Photonen kann man nicht mehr teilen) das bedeutet aber auch, dass Eve zwangsläufig falsche Daten übermitteln wird. Alice und Bob müssen einfach ein paar Bits des Schlüssels Opfern um solche Fehler bzw. Abhörversuche aufzudecken. Der Versuch ist damit erkannt.

Aus **Service**SiAs.de Bookmarken: http://www.sias.de/kryptologie-quantengraphie-details.html



Logische Massnahmen: Quantenkryptographie

KR-17
© MLO

Quantenkryptographie in der Praxis

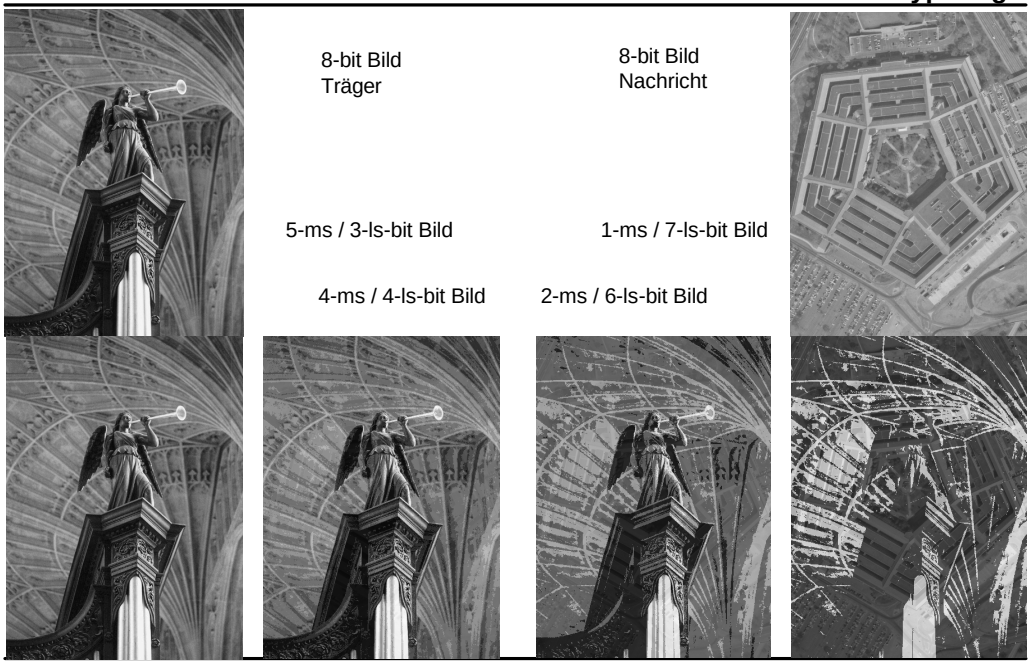
Tatsächlich ist die Quantenkryptographie Realität. Auf der CeBIT 2002 stellte die schweizerische Firma ID Quantique ein funktionierendes System vor.

Über eine Glasfaserleitung wird ein einzelnes Photon geleitet. Unter einer Glasfaserleitung, auch Lichtleiter genannt, kann man sich einen Schlauch vorstellen, dessen Wände von Innen verspiegelt sind. Ein an einem Ende eingespeister Lichtimpuls bewegt sich dann nach den optischen Gesetzen in diesem Schlauch bis zum anderen Ende. In der Praxis ist die Wand tatsächlich nicht verspiegelt, es wird beispielsweise der Effekt der Totalreflexion ausgenutzt.

Jeder Lichtleiter besitzt eine Dämpfung, d.h. je länger ein Glasfaserleiter ist, um so weniger Licht kommt am anderen Ende an. Es werden auf dem Weg Photonen verschluckt (= absorbiert). Bei einem einzelnen Photon gilt, entweder kommt es an, oder es kommt nicht an. Erreicht ein Photon nicht den Empfänger, fällt es einfach aus dem Schlüssel heraus. Da jedoch eine Mindestanzahl an Daten für den Schlüssel benötigt werden, gibt es Grenzen bezüglich der Länge des Lichtleiters.

Glasfaserleitungen werden etwa alle 80km verstärkt. Das ist hier nicht möglich, es käme einer Störung gleich. Da nur jeweils ein Photon verwendet wird, liegt die Grenze schon bei 70km. Der ID Quantique Prototyp wurde erfolgreich über eine Distanz von 67km betrieben. Dabei wurde ein herkömmliches Glasfaserkabel verwendet. Die Datenrate zur Übertragung des Schlüssels liegt bei 1000 bits/s

Interesse an dieser Technik dürfte bei den Banken, Versicherungen, dem Militär oder den Diplomaten und ähnlichen Kreisen zu finden sein. Für einen breiten Privateinsatz ist der Aufwand jeden Haushalt nachträglich mit einer Glaserfaserleitung zu versorgen zu aufwendig.



Logische Massnahmen: Steganographie

Steganographie (Stego)

Verschlüsselungsverbot und staatliche Kontrolle des (privaten) Mailverkehrs sind aktuelle Reizworte. Die *Steganographie* umgeht diese Verbote, in dem sie beliebige Dateien als Träger verwendet, um darin unsichbar verschlüsselte Informationen zu verstecken. Solche Dateien können Bilder, Tondateien aber auch - entsprechend grosse - Textfiles sein. Die *Steganographie* ist damit eine Ergänzung zur Verschlüsselung (Kryptographie).

Beschreibung der Steganographie

Während unter der Kryptographie im allgemeinen die erkennbare Benutzung eines Kryptosystems zur Chiffrierung einer Nachricht verstanden wird, bezeichnet die *Steganographie* den verdeckten Gebrauch eines Verfahrens, mit dessen Hilfe eine Botschaft in einem scheinbaren Klartext versteckt wird, d.h. auch die Tatsache des Verschlüsselns selbst bleibt geheim. *Steganographie* - wörtlich übersetzt: "verdecktes Schreiben" - ist die Wissenschaft vom Verstecken von Daten.

Einfache Regel zum Verstecken von Nachrichten in Texten basieren darauf, Buchstaben an einer verabredeten Position eines jeden Wortes (Absatzes etc.) zu verstecken bzw. interpretieren oder auf der Zahl der Leerstellen beim Blocksatz einer Nichtproportionalschrift.

Drei Eigenschaften von steganographischen Verfahren werden hier deutlich:

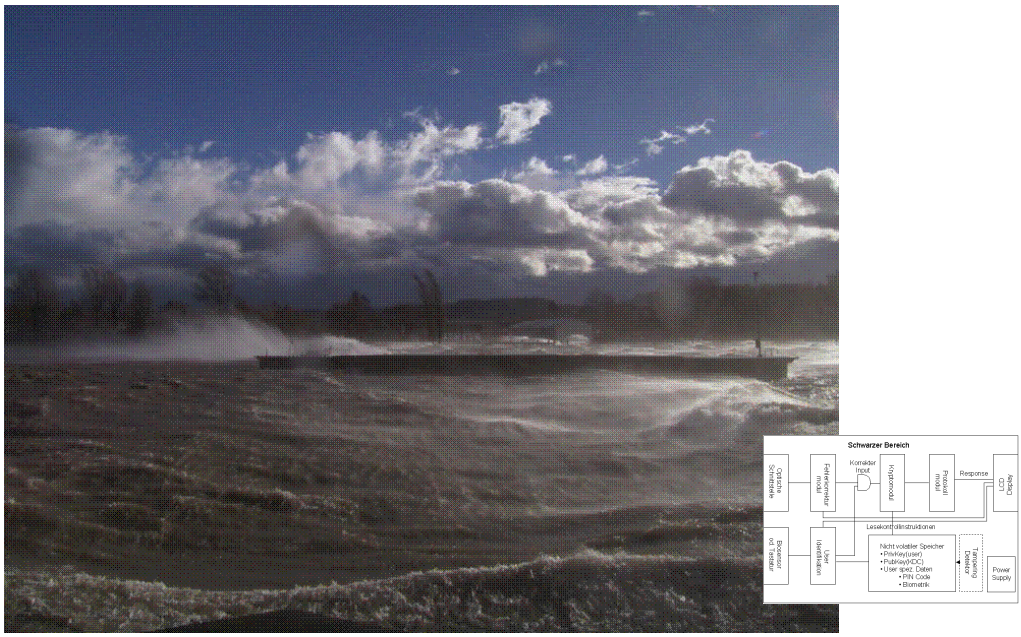
•Es ist eine riesige Vielfalt solcher Verfahren denkbar.

•Selbst bei Verdacht auf eine versteckte Nachricht lassen sich unterschiedliche Botschaften herauslesen.

•Die Menge der versteckten Daten ist sehr viel kleiner als die Nachricht, in die sie verpackt werden.

Beispiel: Verstecken von Bildern in Bildern

In der Trägerdatei werden die n less significant bits (lsb) durch die n most significant bit (msb) der Nachrichtendatei ersetzt. Das Resultat einer solchen Ersetzung mit verschiedenen Varianten von n in Dateien mit 8-bit Grauwertkodierung sieht man in den Bildern.



Logische Massnahmen: Steganographie

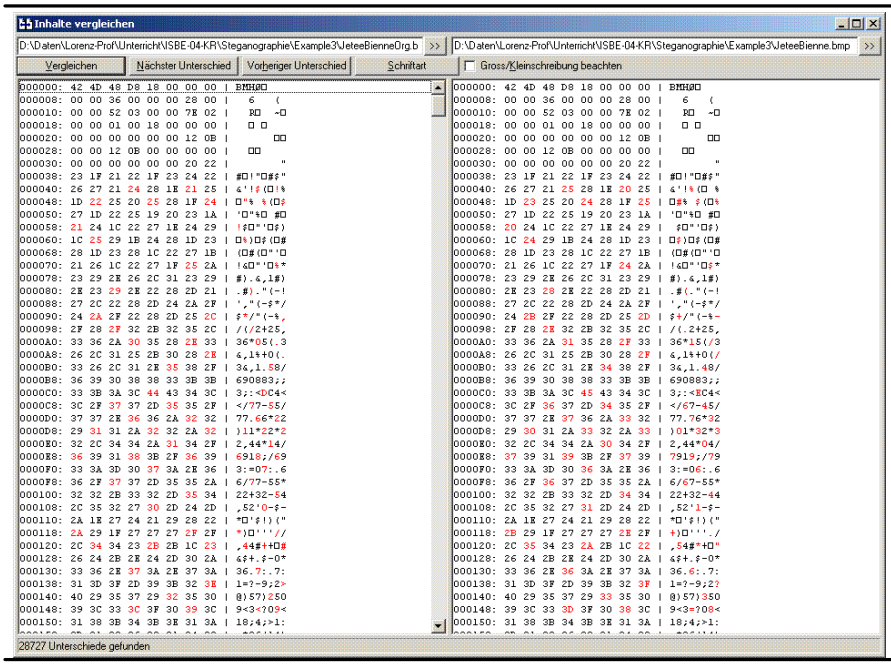
KR-19
© MLO

Beispiel: Steganos '95

Eines der besten - vielleicht sogar das beste - *Steganographie*-Programm ist ***Steganos 95*** für Windows '95 und Windows NT. Mit *Steganos* lässt sich ausprobieren, wie moderne *Steganographie* funktioniert. (Download z.B.: http://home.t-online.de/home/husky_college/steg95.exe)

Steganos '95 für Windows bietet verschiedene Funktionalitäten.
Neben dem Verschlüsseln und Verstecken von(Text-)Dateien in verschiedenen Formaten, gibt es auch die Option nur Verstecken, so daß eine Datei mit dem Programm Ihres Vetrauens (z.B. PGP) verschlüsseln und dann in einem File verstecken können.
Anhand der obigen Bilder (lothar Sturm auf Bielersee, Schema eines kryptographischen Tokens) lässt sich die Wirkungsweise verdeutlichen. Sie finden am Ende dieses Absatzes eine Gegenüberstellung dreier JPG-Dateien. Das Sturmbild enthält die Schemadatei und trotzdem lässt sich von blossem Auge nichts sehen.

Hinweis: Da *Steganos '95* Dateien nur in *.BMP-Files verstecken kann, muss ein Browser installiert sein, der dieses Format anzeigen kann.



Logische Massnahmen: Steganographie

Steganographie auf Bitebene

Nach dem Verstecken der Schemadatei mit Steganos 95 zeigt das Original- und das neue Bild kleine Abweichungen auf der Ebene der Bitmap.

Man sieht, dass wenige Bits an bestimmten Stellen geändert wurden, wenn man die Originaldatei zur Hand hat, sonst würde sich wohl nichts feststellen lassen.

Steganographie = ‚Versteckte Schrift'

Mikrotext

Logische Massnahmen: Steganographie

KR-21
© MLO

Geschichte der Steganographie

Die *Steganographie* ist wie die Kryptographie sehr viel älter als das Computerzeitalter. Seit tausenden von Jahren werden geheime Nachrichten versteckt übermittelt, insbesondere im militärischen Bereich. Schon der griechische Geschichtsschreiber Herodot (490-425 v. Chr.), berichtet von einem Adligen, der seine Geheimbotschaft auf den geschorenen Kopf eines Sklaven tätowieren ließ. Nachdem das Haar nachgewachsen war, machte sich der Sklave unbehelligt zu seinem Ziel auf, wo er zum Lesen der Nachricht wiederum kahlrasiert wurde.

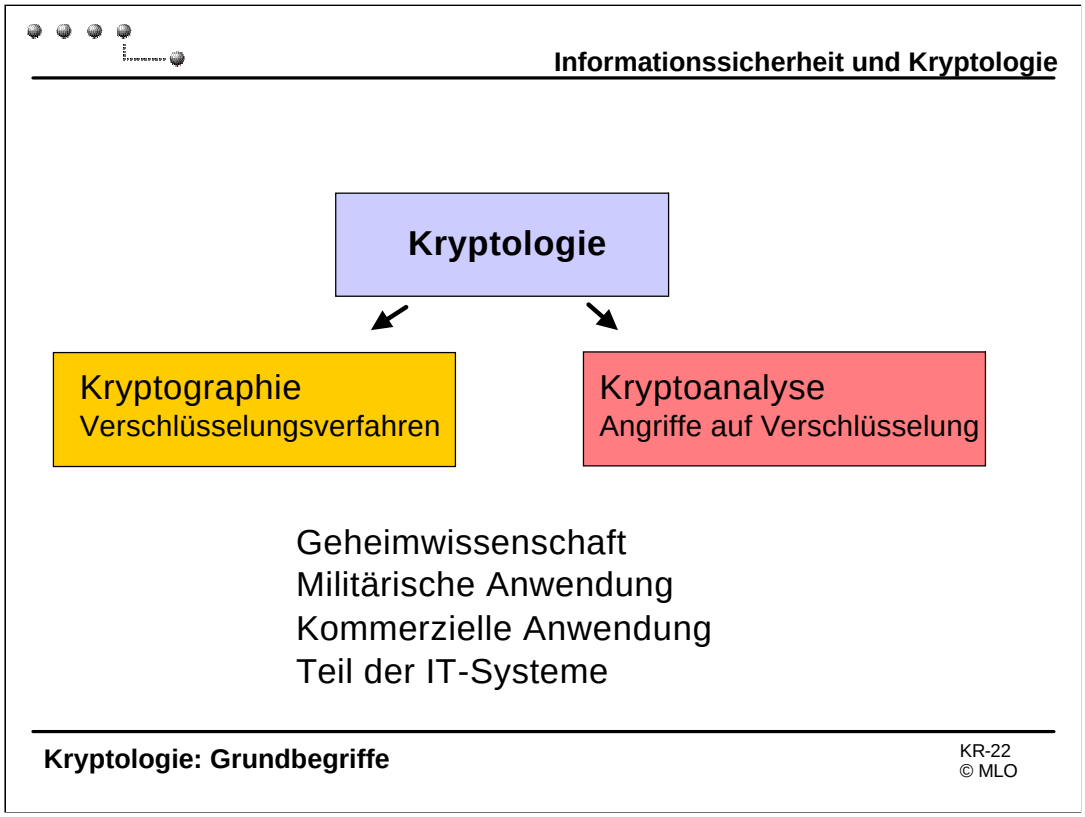
In einem anderen Bericht von Herodot geht es um Wachstafeln, auf die man damals schrieb. Als eine sensible Nachricht überbracht werden sollte, entfernte der Absender das Wachs, gravierte den Text in das Holz darunter und füllte das Wachs wieder auf. Den kontrollierenden Wachen erschienen die Tafeln leer.

Der Gebrauch unsichtbarer Tinte war bereits zur Zeit des römischen Schriftstellers *Plinius der Ältere* (23-79 n. Chr.) bekannt.
Viele haben in ihrer Kindheit mit Zitronensaft auf Papier geschrieben und diese leeren Blätter an ihre Freunde und Klassenkameraden weitergegeben.
Der Empfänger mußte nur das Dokument über einer Kerzenflamme erhitzen - schon tauchte die Schrift wieder auf.
Im Zweiten Weltkrieg arbeiteten deutsche Spione nach demselben Prinzip: Mit einer Kupfersulfatlösung auf einen Handschuh gebrachte Nachrichten blieben unsichtbar, bis er mit Ammoniakdämpfen in Berührung kam.

Ebenfalls von den Nationalsozialisten entwickelt wurde der sogenannte *Microdot*, ein Stück Mikrofilm in der Größe eines I-Punktes, der in unverdächtigen Schreibmaschinenseiten als Satzzeichen oder oberhalb des Buchstabens "i" eingeklebt wurde. Solche *Microdots* konnten riesige Datenmengen einschließlich technischer Zeichnungen und Fotos enthalten.

Beispiel mit Verstecken einer Schrift

Mikrotext auf CH-Banknoten. Dies ist eine von mehreren Sicherheitsmassnahmen gegen Fälschungen von Banknoten.



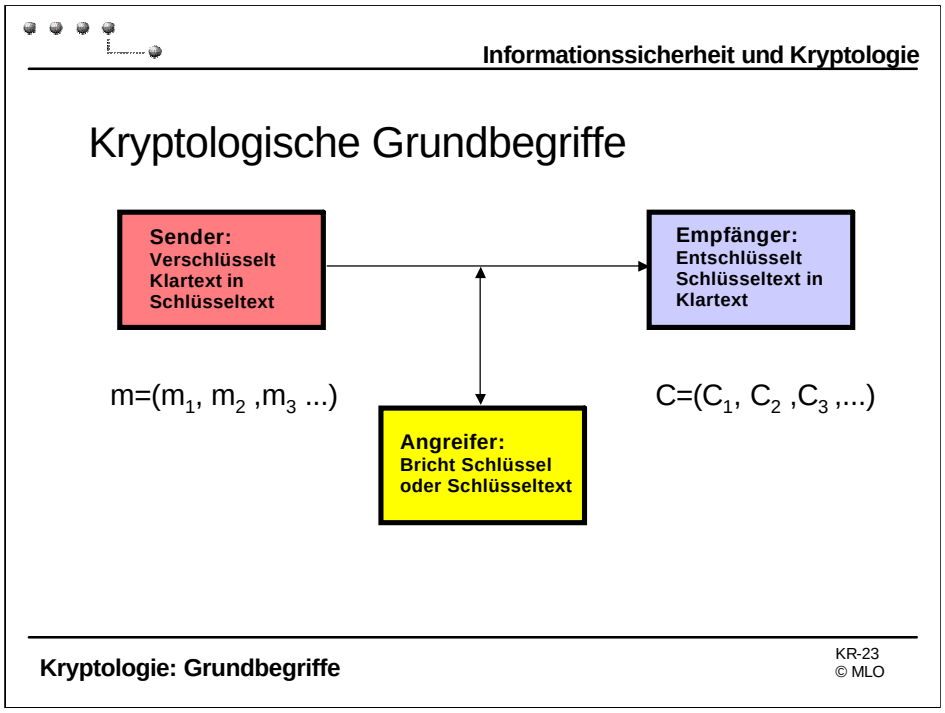
Der Begriff ***Kryptologie*** stammt aus dem Griechischen und bedeutet sinngemäss 'verborgenes Wort'. Die Verschlüsselung von Nachrichten ist eine sehr alte Kunst, die bereits in der Antike von den Griechen und Römern angewendet wurde. Bis Ende der 60er Jahre war die Kryptologie ein Teilgebiet der Mathematik und Codierungstheorie und interessierte ausschliesslich Militärs und staatliche Stellen. Als eigenständige wissenschaftliche Disziplin konnte sich die Kryptologie erst mit dem Aufkommen
der digitalen Informations- und Kommunikationssysteme etablieren.

Die eigentliche Geburtsstunde der Kryptologie als Wissenschaft ist der zweite Weltkrieg, wo kryptologische Kenntnisse kriegsentscheidende Bedeutung hatten. Die aus den Arbeiten während des Krieges resultierenden Erkenntnisse wurden 1948 und 1949 von C. E. Shannon in grundlegenden, theoretisch ausgerichteten Werken zusammengefasst (*A Mathematical Theory of Communication, Communication Theory of Secrecy Systems*) und sind noch heute Basis der Informationstheorie und ihrer Anwendung auf sichere Kommunikation.

Die Kryptologie umfasst die beiden komplementären Richtungen

Kryptographie: Entwicklung von sicheren Verschlüsselungsverfahren

Kryptoanalyse: Entwicklung von Angriffen auf Verschlüsselungsverfahren



Grundbegriffe der Kryptologie im Kanalmodell

Nachricht, Klartext, Schlüsseltext, Schlüssel

Nachrichten sind die sinnvollen Zeichenfolgen in einer Sprache

Klartext ist die Codierung der Nachricht in einem n-Gramm aus dem Alphabet

Schlüsseltext ist die kryptographisch transformierte Zeichenfolge C zur Nachricht m. Die Zeichen C_i brauchen nicht aus dem selben Alphabet *A* zu kommen

Kryptographie

Sender: ***Alice***

Verschlüsselt (encryptiert) Nachricht in **Klartext *m*** in **Schlüsseltext *C***
evt. mit Hilfe eines **Schlüssels *k***

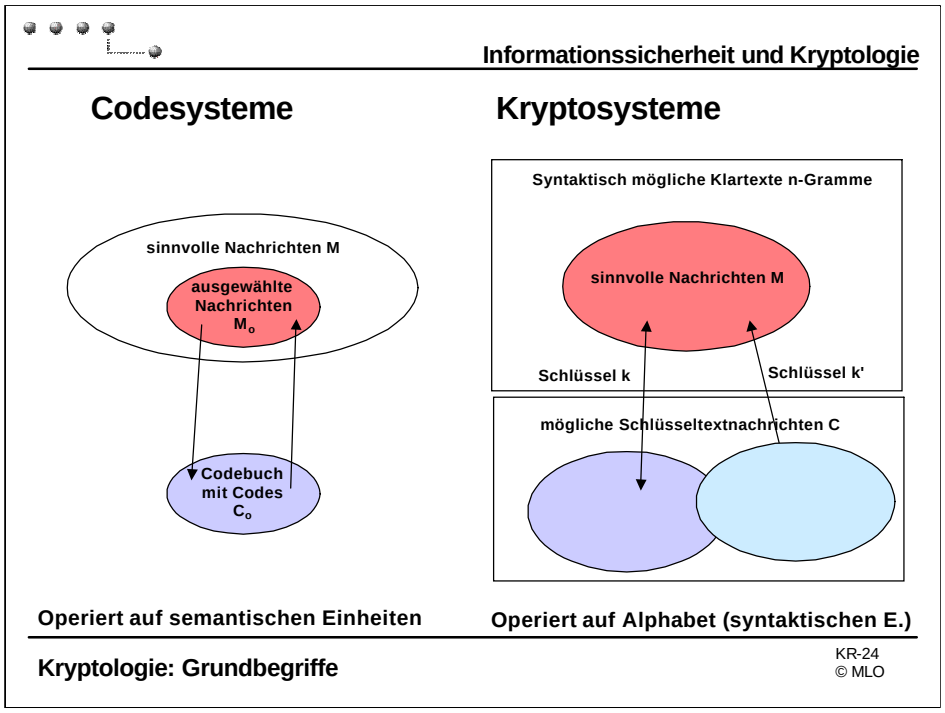
Empfänger: ***Bob***

Entschlüsselt (decryptiert) Nachricht in **Schlüsseltext *C*** in **Klartext *m***
evt. mit Hilfe eines **Schlüssels *k***

Kryptoanalyse

Angreifer: ***Eve***

Bricht in Kommunikationskanal ein und analysiert **Schlüsseltext *C*** um
Klartext *m* bzw. einen evt. **Schlüssel *k*** zu finden



Kryptographische Verschlüsselungsverfahren

Codesysteme:

Operieren auf **semantischen Einheiten $\mathbf{m}_0$** in einem vordefinierten beschränkten Nachrichtenraum M_0 (Wörtern, Phrasen, Sätzen, ganze Nachrichten usw.)

Verschlüsselung erfolgt durch Zuordnung der Nachricht $\mathbf{m}_0$ zu **vordefiniertem Code $\mathbf{c}_0$** aus einem **Codebuch**

Entschlüsselung erfolgt durch die Umkehroperation mit Hilfe eines nach den Codewörtern geordneten Codebuches

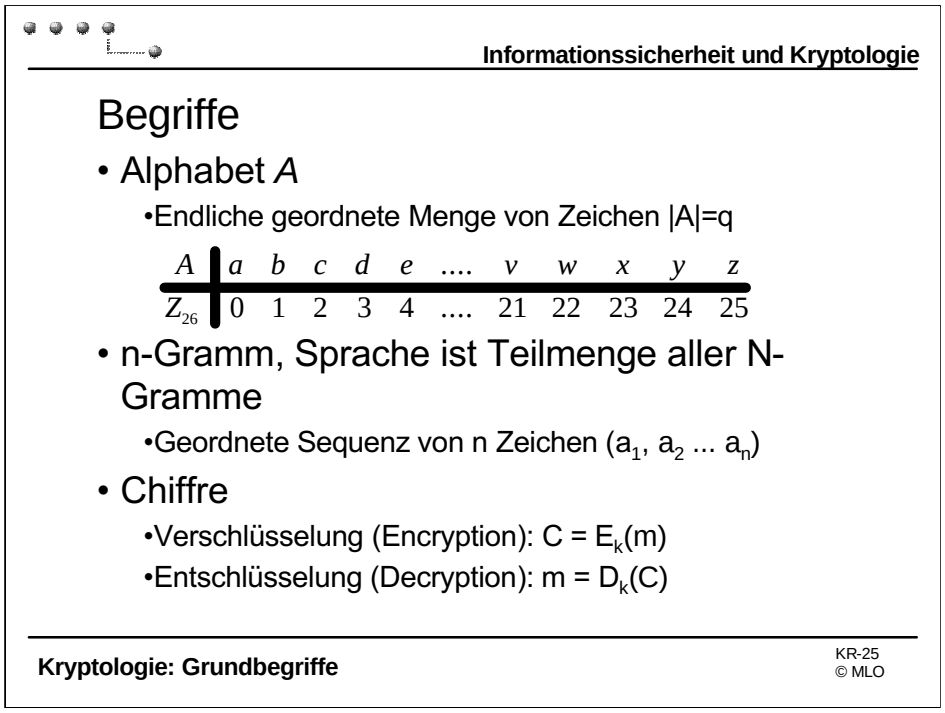
Beispiel: Int. Radiofunk 'Q'-Code

Klartext	**Code**
Are you busy?	QRL
Does my frequency vary?	QRH
Is my keying correct?	QSD
Shall I increase power?	QRO

Kryptosysteme: (technisch wichtige Systeme)

Operieren auf **syntaktischen Einheiten $\mathbf{m}_i$** des Klartextes mit beliebigem Nachrichtenraum*M* (Buchstaben, Zeichen, Buchstabenblöcke) ohne Rücksicht auf ihre semantische Bedeutung

Ver- und Entschlüsselung erfolgt durch **Chiffrierung** (cipher) der Zeichen des **Alphabets**



Erläuterungen zu den Begriffen

Alphabet A

Mächtigkeit des Alphabets (Anzahl der Zeichen) |A|=q

Identifikation des Alphabets *A* mit Restklassenring Z_q erlaubt die Definition von Additions- und Multiplikationsoperationen auf *A (siehe Vigeneretableau: Klass. Kryptosysteme)*

Beispiele:

b+c = d	<==>	1+2 = 3
c*d = g	<==>	2*3 = 6

Andere Alphabete sind:

ASCII-Code	|A| = 128	Z_{128}
Binärcode	|A| = 2	Z_2
DES-Block	|A| = 2^{64}	$Z_{2^{64}}$

n-Gramm

n-Gramme umfassen alle möglichen Sequenzen von n Zeichen aus dem Alphabet. Nur ein kleiner Bruchteil aller n-Gramme kommt in einer natürlichen (formalen) Sprache vor.

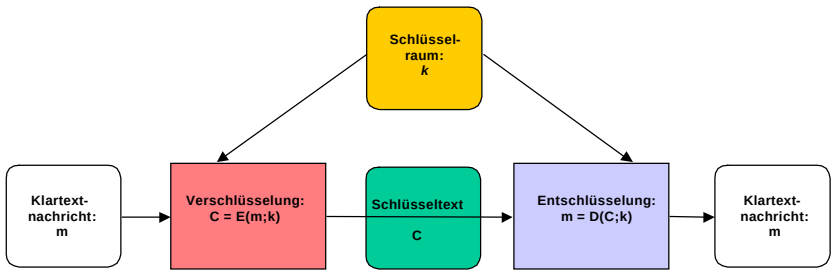
Auftretenswahrscheinlichkeit spezieller n-Gramme ist charakteristisch für eine Sprache

Chiffre

C=E(m;k) Verschlüsselung (Encryption), m=D(C;k) Entschlüsselung (Decryption)

Das Paar komplementärer Transformationen (E,D) heisst Chiffre, k heisst Schlüssel

Formale Definition eines Kryptosystems



Ein Kryptosystem ist ein System mit 5 Komponenten

- **Raum von Klartextnachrichten *M***
- **Raum von Schlüsseltextnachrichten *C***
- **Raum von Schlüsseln *K***
- **Eine parametrisierte Schar von Verschlüsselungstransformationen**

$$E_k : M \rightarrow C$$

mit $k \in K$ **und E_k injektiv**

- **Eine parametrisierte Schar von Entschlüsselungstransformationen**

$$D_k : C \rightarrow M$$

mit $k \in K$ **und D_k surjektiv**

so dass, für jeden Schlüssel k ein Paar von zueinander inversen Ver- und Entschlüsselungstransformationen (E_k,D_k) bestimmt ist:

$$m \xrightarrow{E_k} C \xrightarrow{D_k} m$$

$D_k(C) = D_k[E_k(m)] = m$

Symmetrische und asymmetrische Kryptosysteme

Sind die Schlüssel k für **D_k** und **E_k** gleich oder in einfachem Zusammenhang heisst das Kryptosystem **symmetrisch**, sonst **asymmetrisch**

Allgemeine Eigenschaften

- Effiziente Chiffretransformationen
- Kryptosystem ist einfach im Gebrauch
- Sicherheit hängt nicht von Geheimhaltung von (E_k,D_k) ab, sondern nur von Geheimhaltung von k
- Verschlüsselung maximiert ***Konfusion*** und ***Diffusion***

Anforderungen

• Für alle Schlüssel k ist **(E_k, D_k)** effizient berechenbar, dh. das System muss ohne wesentliche Kommunikationsverzögerung verschlüsseln und entschlüsseln (2-100 Mb/s)

• Das Kryptosystem darf den Systemgebrauch für den User nicht beeinträchtigen

• Sicherheit des Kryptosystems sollte nie von der Geheimhaltung des Algorithmus abhängen, da in einem verteilten System das Risiko sonst unkalkulierbar wird

• **E_k** soll

- **Konfusion**, dh. eine möglichst komplexe Beziehung zwischen Klartext, Schlüsseltext und Schlüssel erzeugen
- **Diffusion**, dh. eine möglichst breite Streuung der Klartext- und Schlüsselinformation auf dem Schlüsseltext erzeugen

Gemessen wird Konfusion und Diffusion durch die **starke zwischensymbolische Abhängigkeit (strong intersymbol dependence)**:

Jedes Schlüsseltextzeichen muss von jedem Klartextzeichen und jedem Schlüsselzeichen abhängen

Beispiel: DES Alphabet mit 64-bit Blöcken und 56-bit Schlüssel

$|M| = |C| = 2^{64}$; $|K| = 2^{56}$; Anzahl der potentiell möglichen Verschlüsselungen $2^{64}!$
Realisierbar mit DES ist aber nur ein Bruchteil.

	64-bit als HEX-Zahlen
m	**1000000000000001**
k	**30000000000000**
C = $E_{k(m)}$	**958E6E627A05557B**
C'	**858E6E627A05557B**
k	**30000000000000**
m' = $D_{k(C')}$	**8D4893C2966CC211**

	64-bit als HEX-Zahlen
m	1000000000000001
k	30000000000000
$C = E_{k(m)}$	958E6E627A05557B
C'	858E6E627A05557B
k	30000000000000
$m' = D_{k(C')}$	8D4893C2966CC211

DES Alphabet mit 64-bit Blöcken und 56-bit Schlüssel

$|M| = |C| = 2^{64}$; $|K| = 2^{56}$;

Anzahl der potentiell möglichen Verschlüsselungen 2^{64}!

Realisierbar mit DES ist aber nur ein Bruchteil 2^{56}.

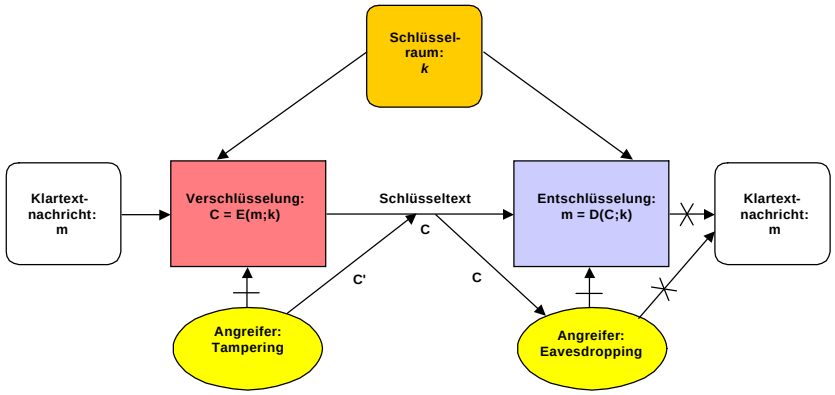
DES als Illustration für

•**Konfusion**: Schlüsseltextzeichen haben komplexe Abhängigkeit von Klartext- und Schlüsselzeichen

•**Diffusion**: Jedes Bit im Schlüsseltext steht mit jedem Bit im Klartext in Beziehung.

•**Avalancheffekt:** Der Wechsel eines Bits im Input verändert im Mittel 50 % der Bits im Output

Spezifische Eigenschaften



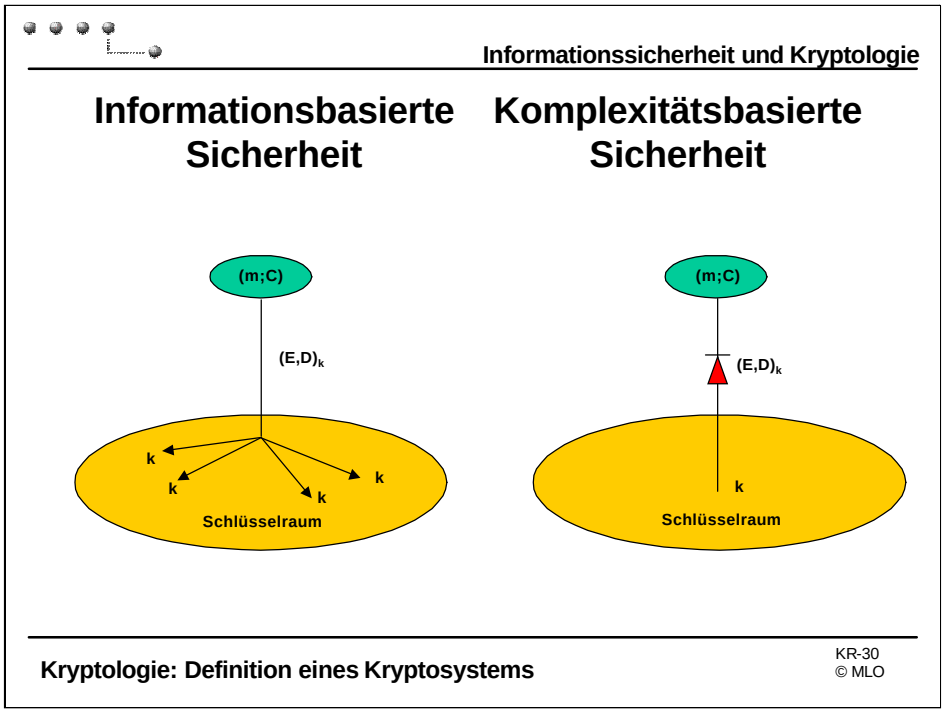
Kryptologie: Definition eines Kryptosystems

KR-29
© MLO

Spezifische Anforderungen

- Schutz der **Vertraulichkeit**, Entschlüsselungstransformation ist gefährdet
  - Rekonstruktion des Schlüssels **k** von $\mathbf{D_k}$ aus abgehörtem Schlüssel- und Klartext ist unmachbar (unmöglich oder zu aufwendig)
  - Rekonstruktion des Klartextes $\mathbf{m = D_k (C)}$ aus abgehörtem Schlüsseltext ist unmachbar (unmöglich oder zu aufwendig)
- Schutz der **Authentizität**, Verschlüsselungstransformation ist gefährdet
  - Rekonstruktion des Schlüssels **k** von $\mathbf{E_k}$ aus abgehörtem Schlüssel- und Klartext ist unmachbar (unmöglich oder zu aufwendig)
  - Konstruktion von korrektem Schlüsseltext $\mathbf{C = E_k (m)}$ zu selbstgewähltem Klartext ist unmachbar (unmöglich oder zu aufwendig)
  - Zueinander gehörender Schlüssel- und Klartext **(C,m)** sind eindeutig einem Schlüsselbesitzer bzw. Schlüssel **k** zuweisbar.

Je nach Anwendung steht die eine oder andere Anforderung im Vordergrund.



Sicherheitsgrad

Die Sicherheit eines Kryptosystems beruht auf:

- **Informationstheoretischer (kombinatorischer)** Sicherheit

  wenn der Angreifer über zuwenig Information verfügt, um das System zu knacken (zu jedem Paar (m,C) existieren noch viele mögliche Schlüssel)

  Diese Sicherheit ist absolut und unabhängig von irgendwelchen neuen Angriffstechniken

  Realisiert wird diese Sicherheit durch einen Schlüsselraum K mit

  $|K| >> |M|$

  und/oder durch eine redundanzfreie Sprache (alle Klar- und Schlüsseltextpaare) gleich wahrscheinlich

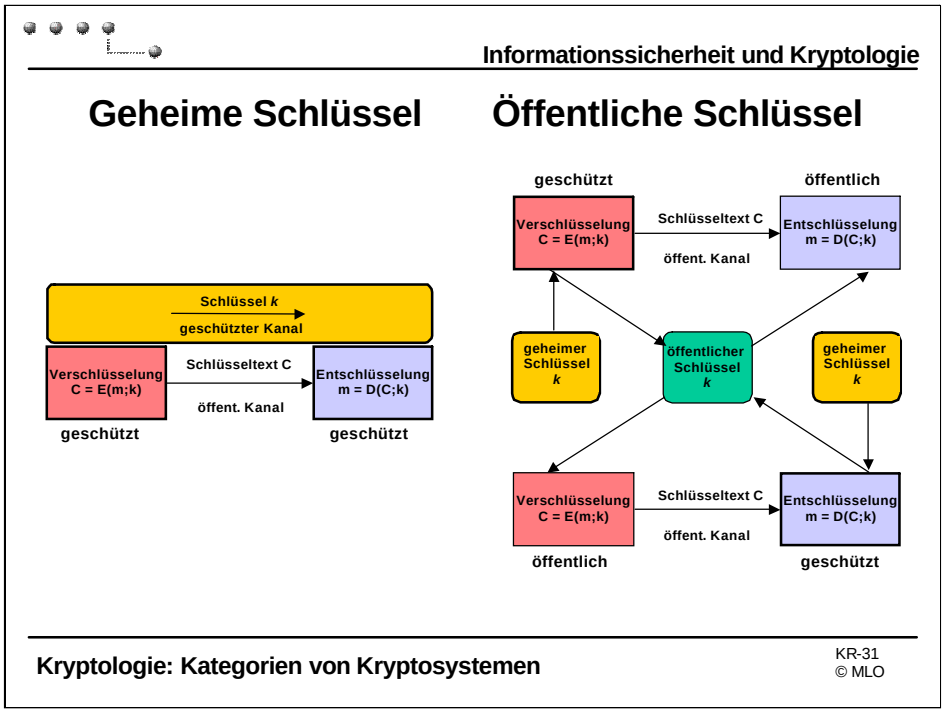
- **Kompexitätstheoretischer (mathematischer)** Sicherheit

  wenn der Angreifer über zuwenig Speicher oder Zeit verfügt, um das System zu knacken (Berechnung von k aus (m,C) ist zu aufwendig)

  Diese Sicherheit ist relativ und abhängig von möglichen neuen Angriffstechniken oder besseren Rechenhilfsmitteln

  Realisiert wird diese Sicherheit durch die Konstruktion eines mathematisch schwierig zu beschreibenden Algorithmus (DES, IDEA) oder durch den Einbezug eines bekannten schwierig zu lösenden Problems (NP vollständig)

- Eine Mischform ist die systemtheoretische Sicherheit. Der Angreifer verfügt entweder über zuwenig Information und/oder Rechenkapazität (Kombination DES-Public key)



Kategorien

Symmetrische Kryptosysteme

Symmetrische Kryptosysteme haben **geheime Schlüssel**

Nur Berechtigte können ver- und entschlüsseln

Simultane Gewährleistung der **Geheimhaltung** und der **Authentizität** von m

Schlüssel müssen über **sicheren Kanal** vom Sender zum Empfänger gelangen

Schlüsselkommunikation erfolgt oft via ein asymmetrisches Kryptosystem

Asymmetrische Kryptosysteme

Asymmetrische Kryptosysteme haben einen **öffentlichen** und einen **geheimen Schlüssel**

Geheimhaltung wird durch Schutz der Entschlüsselung $\mathbf{D_k}$ gewährleistet

Authentizität wird durch Schutz der Verschlüsselung $\mathbf{E_k}$ gewährleistet

Öffentliche Schlüssel können publiziert werden

Geheime Schlüssel müssen nicht kommuniziert werden

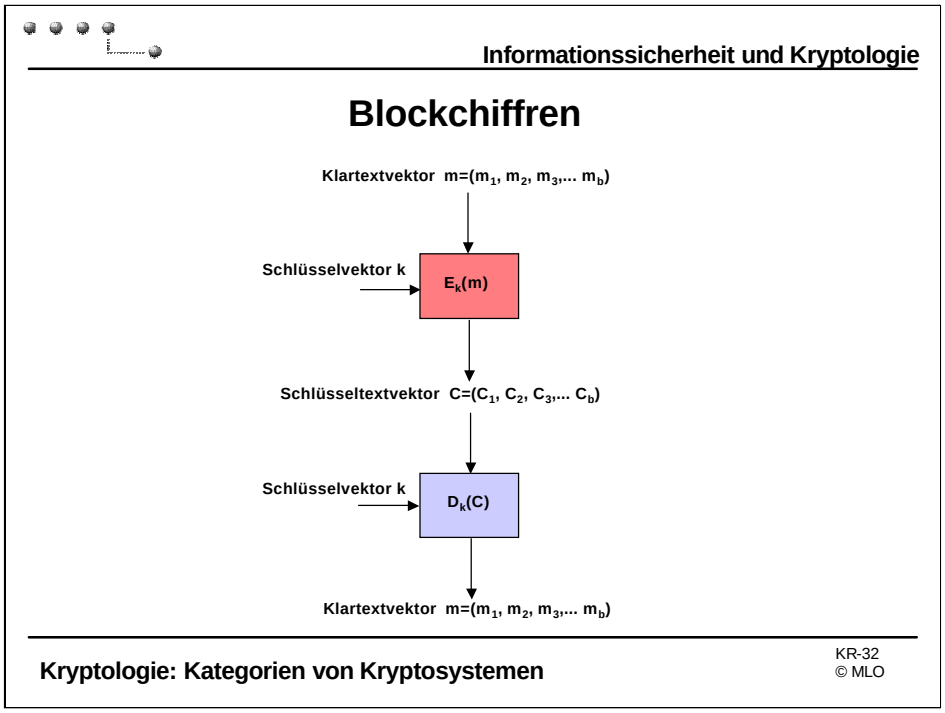
Simultane Gewährleistung der Geheimhaltung und Authentizität erfolgt durch Iteration

$$C = E_{k_2}^{\text{öffentlich}}\left[\underbrace{E_{k_1}^{\text{geschützt}}(m)}_{\text{Authentizität}}\right] \xrightarrow{\text{Kanal}} E_{k_1}^{\text{öffentlich}}\left[\underbrace{E_{k_2}^{\text{geschützt}}(C)}_{\text{Geheimhaltung}}\right]$$

Schlüssellose Systeme

Für Passwörter, Identifikation (zB. Pincode) usw. ist nur eine Verschlüsselungs-transformation notwendig

Realisierung durch schlüsselunabhängige Transformation **E(m)** (z.B. Hashfunktion)



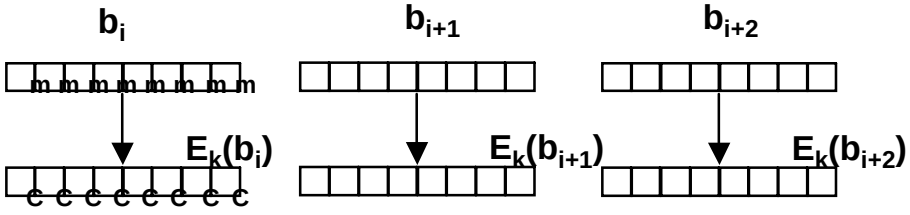
Kryptographische Verarbeitung

Blockchiffren

Zeichen des Klartextes werden in Blöcke der Länge b zusammengefasst

$$m = (b_1, b_2, b_3, \Lambda)$$
$$b_i = (m_{ib+1}, m_{ib+2}, m_{ib+3}, \Lambda\, m_{ib+b}) \quad (i = 0,1,\Lambda)$$

Jeder Block **b** wird als Argument in den Verschlüsselungalgorithmus eingegeben und es entsteht (in der Regel) ein Schlüsseltextblock **B** der gleichen Länge



Die Blöcke können als Zeichen eines neuen Alphabets mit $|A|^b$ Zeichen aufgefasst werden, auf dem eine Substitution ausgeführt wird. Je grösser die Blocklänge ist desto grösser ist das Alphabet und umso grösser ist der Raum der möglichen Sustitutionen

Anzahl Substitutionen = Anzahl Permutationen = $|A|^b$ **!**

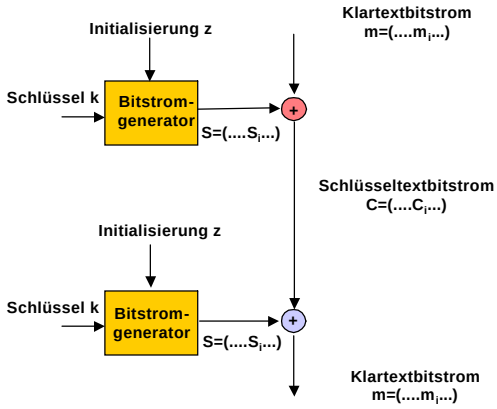
Beispiel DES

Blocklänge: b=64, Grundalphabet binär: |A|=2, Anzahl mögliche 'Blockzeichen': 2^{64}

Anzahl mögliche Substitutionen: 2^{64}!

Viel grösser als Schlüsselraum: 2^{56}

Stromchiffren



Stromchiffren

Zeichen des Klartextes werden bit-weise mit XOR ver- und entschlüsselt

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

$A \oplus A = 0$

$A \oplus 0 = A$

$A \oplus 1 = \overline{A}$

$A \oplus B = C$

$B \oplus C = A$

Ein Angriff mit Klar- und Schlüsseltext erlaubt sofort die Rekonstruktion des kryptographischen Bit-Stromes S.

Klartext m	0	1	0	1
Kryptographischer Bit - Strom S	0	0	1	1
Schlüsseltext C	0	1	1	0
Schlüsseltext C	0	1	1	0
Kryptographischer Bit - Strom S	0	0	1	1
Klartext m	0	1	0	1

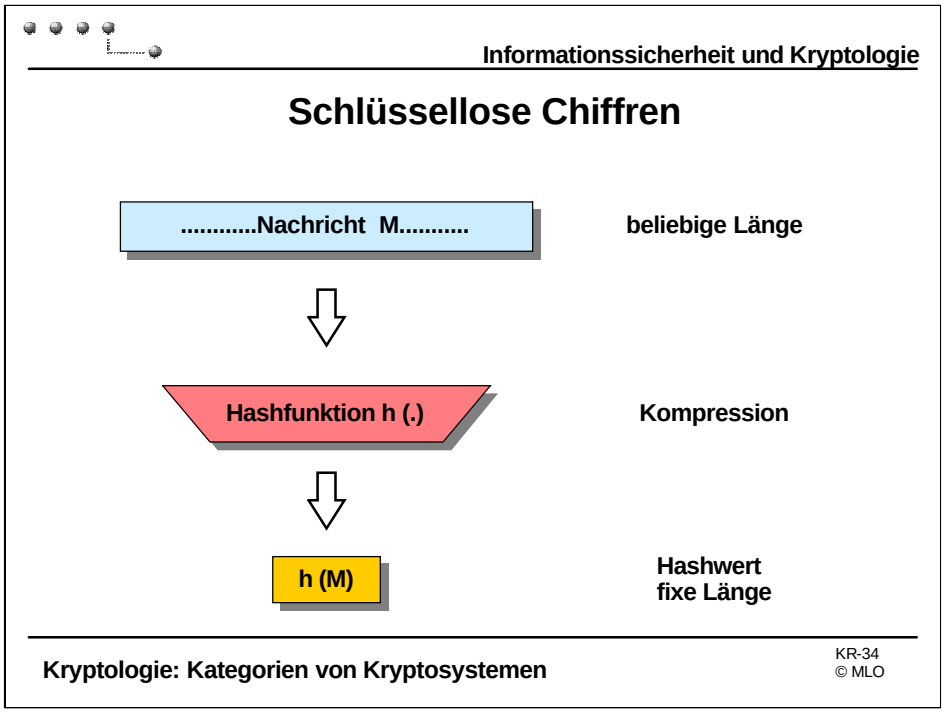
Die kryptographische Sicherheit muss somit in der komplexen Beziehung zwischen S, z und k liegen (gleiche Konfusions und Diffusionskriterien wie für Blockchiffre).

Damit ein Angreifer nicht einfach den Bit-Strom S rekonstruiert, muss S eine sehr lange Periode haben. Dies wird durch die zufällige Initialisierung mit z erreicht.

z ist eine (pseudo) zufällige (nicht unbedingt geheime) Bitfolge

Verkettung

Eine zusätzliche Schwierigkeit ergibt sich durch die Verkettung des Zufallsgenerators z mit der Schlüsseltextausgabe. Damit wird der Schlüsseltext an der Stelle i von allen früheren Stellen abhängig. Die gleiche Operation ist auch für Blockchiffren möglich.



Schlüssellose Chiffren - Einwegfunktionen

Das Funktionsschema für eine beliebige Hashfunktion ist sehr einfach. Die Hashfunktion h(.) nimmt als Input eine Nachricht M beliebiger Länge und bildet diese auf einen sogenannten **Hashwert h(M)** ab, der eine vorgegebene, **fixe Länge** hat. Oft wird der Wert h(M) auch als **Hashcode** oder als **elektronischer Fingerabdruck** bezeichnet um auf seinen häufigen Verwendungszweck als nicht manipulier-bares Merkmal von Nachrichten hinzuweisen. Gebräuchliche Bezeichnungen im Englischen sind: *Modification-* oder *Manipulation Detection Code, Fingerprint, Cryptographic Checksum*.

Typische Längen für Hashcodes sind 64 bits, oder 128 bits. Für den Standard für digitale Unterschriften wird die Verwendung einer 160 bit Hashfunktion vorgeschrieben, zur Garantie der Langzeitsicherheit von Unterschriften.

Hashfunktionen funktionieren ohne Schlüssel und sind sogenannte Einwegfunktionen.

$$H : M \xrightarrow{\text{einfach}} C$$

$$H^{-1} : C \xrightarrow[\text{nicht eindeutig}]{\text{schwierig}} \mathrm{M}$$

Der Hashcode darf nicht mit dem Message Authentication Code (MAC) verwechselt werden, welcher viele Eigenschaften mit den Hashcodes teilt, zu dessen Berechnung aber immer ein geheimer Schlüssel benützt wird.

Moderne symmetrische Kryptosysteme

- DES
  Data Encryption Standard
- AES
  Der neue Advanced Encryption Standard
- IDEA
  International Data Encryption Algorithm
- FEAL
  FEAL-Algorithmus
- RC4
  RC4-Stromchiffre von RSA
- RC5/RC6/RC2
  RC5, RC6 und RC2 sind Blockalgorithmen von RSA
- SAFER
  Secure And Fast Encryption Routine von James Massey
- Blowfish
  Blockchiffre von Bruce Schneier von Counterpane Systems
- Twofish
  AES-Kandidat von Counterpane Systems
- CAST
  CAST-128/ CAST-256
- Skipjack
  Skipjack-Algorithmus der NSA
  Clipper chip

Kryptologie: Kategorien von Kryptosystemen

KR-35
© MLO

Siehe: http://www.infoserversecurity.org/crypto.php

Moderne asymmetrische und schlüssellose Kryptosysteme

Public Key Chiffren

- RSA
  der bekannte Public Key Algorithmus von Rivest, Shamir und Adleman

  Diffie-Hellmann
  das asymmetrische Kryptosystem nach Diffie und Hellmann für Schlüsseltausch

  Digital Signature Standard
  der amerikanische Signaturstandard

  ElGamal
  ein asymmetrisches Schema basierend auf dem discrete-logarithm-problem

  ECC
  Elliptic Curve Cryptography

Hash Funktionen

- MD4/MD5
  zwei Hash-Algorithmen von Ron Rivest

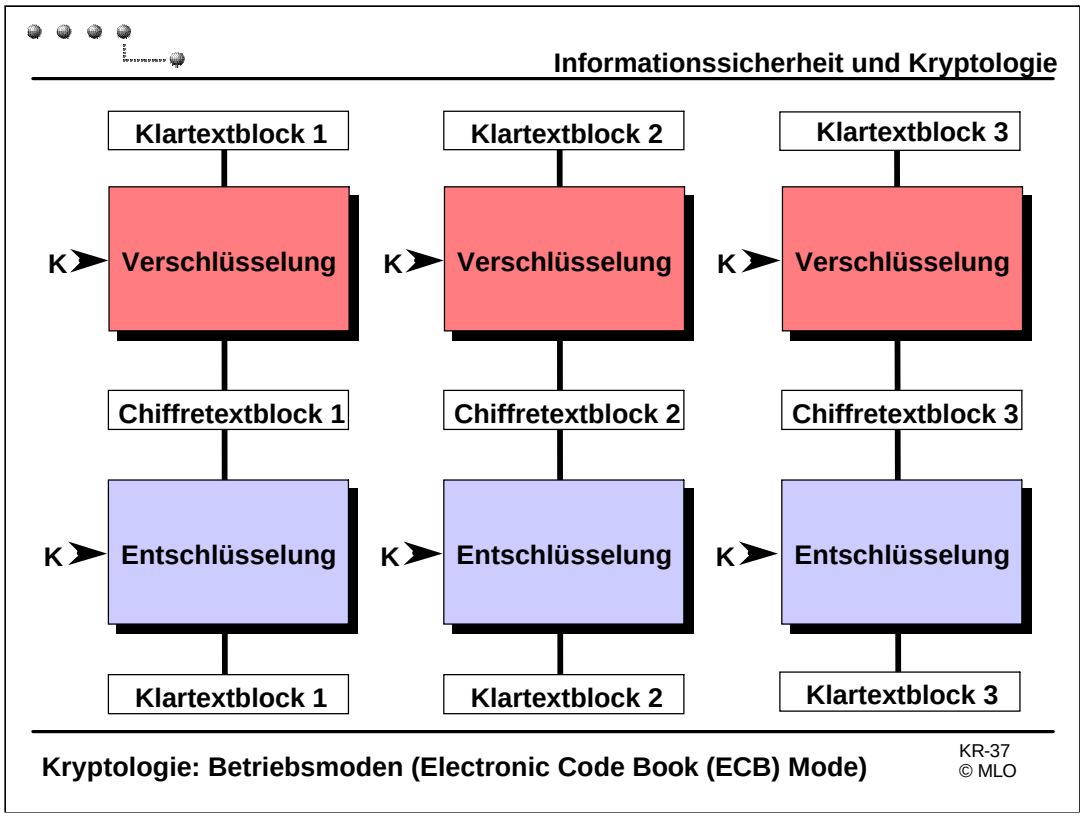
  Secure Hash Standard
  Entwicklung des NIST und der NSA

  RIPEMD-160
  eine europäische Hashfunktion

Kryptologie: Kategorien von Kryptosystemen

KR-36
© MLO

Siehe: http://www.infoserversecurity.org/crypto.php



Die in der Abbildung dargestellte Betriebsart einer Blockchiffre wird als ECB-Modus bezeichnet. In dieser Betriebsart bildet die Chiffrierung mit einem Schlüssel K eine Folge von Klartextblöcken jeweils unab-hängig voneinander in eine Folge von Chiffretextblöcken ab.

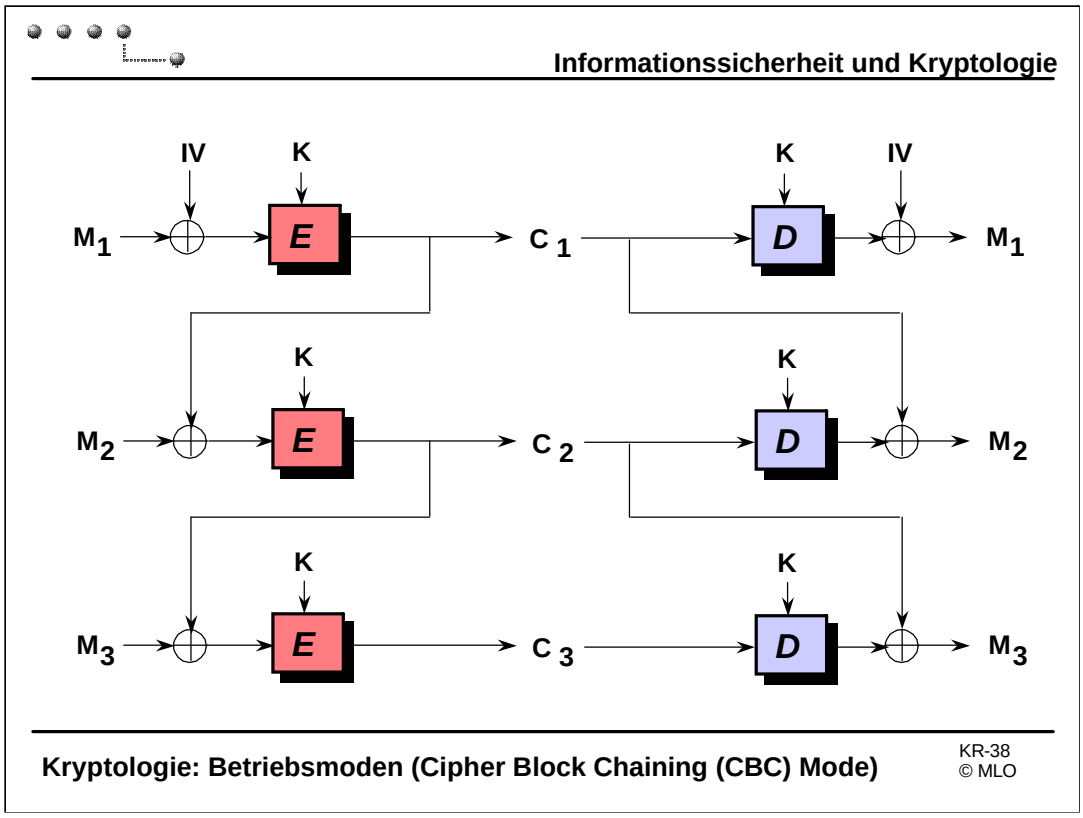
Das Problem mit dem ECB-Modus liegt in erster Linie darin, dass identische Klartext-blöcke auf identische Chiffretextblöcke abgebildet werden, was in vielen Fällen eine Codebuchanalyse ermöglicht.

Die Klartext-Nachrichten sind häufig stark strukturiert, so dass bestimmte Teile sich nicht selten sogar innerhalb einer einzelnen Nachricht mehrfach wiederholen. Auch weisen verschiedene Nachrichten häufig gemeinsame Teile auf (z.B. Floskeln am Anfang und Ende). Nachrichten, die von Computerprogrammen erzeugt werden (z.B. Zahlungsanweisungen) sind oft besonders stark strukturiert.

Neben der Gefahr der Codebuchanalyse weist der ECB Modus eine weitere Schwachstelle auf, nämlich die Möglichkeit, einzelne Chiffretextblöcke sehr einfach und unbemerkt zu löschen, einzufügen und zu vertauschen.

Daher sollte ECB eigentlich niemals zur Verschlüsselung von Nachrichten gebraucht werden, die länger als ein einzelner Block sind.

Aber auch mit kurzen Nachrichten gibt es ein Problem. Wegen der Gefahr der Codebuchanalyse darf ein unvollständiger Klartextblock nicht immer mit demselben Bitmuster (etwa lauter Nullen) aufgefüllt werden, sondern sollte mit einem zufälligen Bitmuster ergänzt werden.



Eine bessere Methode, mehrere zusammen-gehörige Blöcke zu verschlüsseln, ist der sogenannte Cipher Block Chaining Mode. Der wesentliche Vorteil dieser Betriebsart ist, dass gleiche Klartext-Blöcke nicht automatisch auf gleiche Chiffretext-Blöcke abgebildet werden.

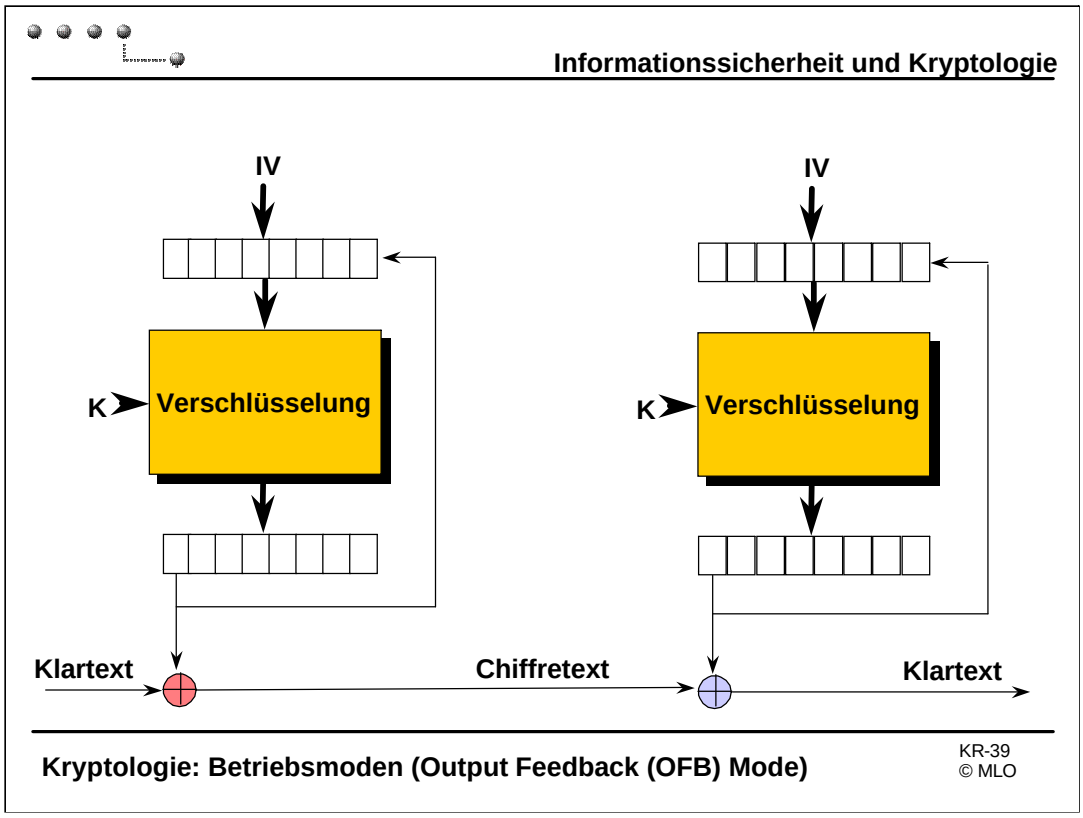
Wenn zudem für jede Nachricht ein zufällig gewählter IV zum Einsatz kommt, können selbst Nachrichten mit identischen Anfangs-stücken nach der Chiffrierung nicht als solche erkannt werden. Der IV braucht zu diesem Zweck nicht geheim gehalten zu werden.

Ein weiterer Vorteil des CBC.Modus besteht darin, dass sich jede Veränderung am Chiffretext beim Entschlüsseln auf die nachfolgenden Blöcke fortpflanzt. Wenn die Nachricht Redundanz enthält, wird dadurch die Wahrscheinlichkeit für das Erkennen von Manipulationen (inklusive Vertauschen, Weglassen und Duplizieren von Blöcken) beträchtlich erhöht.

Falls die übertragenen Nachrichten jedoch keine Redundanz enthalten oder Verfälschungen vom Empfänger aus anderen Gründen nicht leicht erkannt werden können, bietet auch die Verschlüsselung im *Cipher Block Chaining Mode* keinen ausreichenden Schutz gegen Manipulationen.

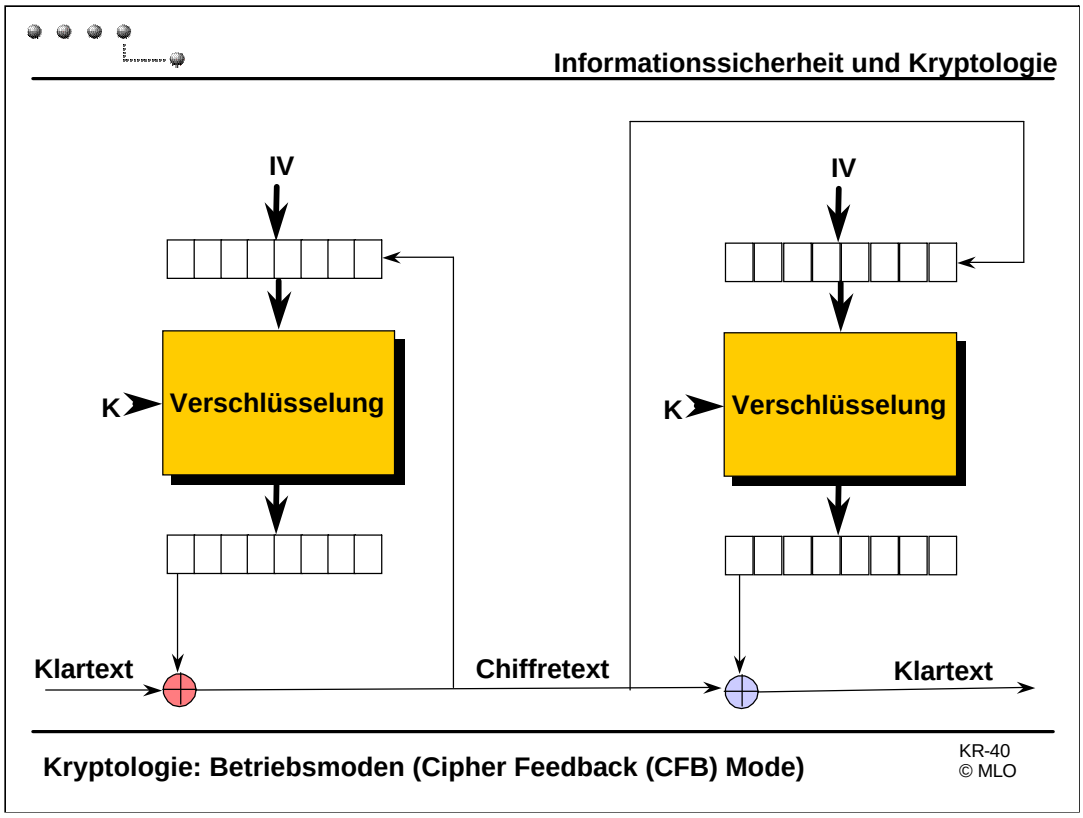
K = Key

IV = Initialisation Value



Der OFB-Modus ist eine Betriebsart, in der eine Blockchiffre als Pseudozufallsgenerator für eine Stromchiffre dient. Dazu wird jeweils ein m-Bit Block des Outputs der Verschlüsselungsoperation in das mit einem Initialisierungsvektor vorbesetzte Input-register zurückgekoppelt. Dieser Teilblock stellt auch das jeweils nächste Glied der Schlüsselfolge dar und wird mit m Bit der Klartextfolge XOR-verknüpft.

Der Wert m kann dabei zwischen 1 und der gesamten Blocklänge frei gewählt werden. Der Modus wird dann auch oft mit OFB-m bezeichnet. Zur Verschlüsselung von m Bit des Klartextes ist in dieser Betriebsart eine Verschlüsselungsoperation nötig, so dass der Durchsatz im allgemeinen (und ganz besonders im Fall m=1) nur einen Bruchteil des Wertes für den ECB- oder CBC-Modus erreicht.



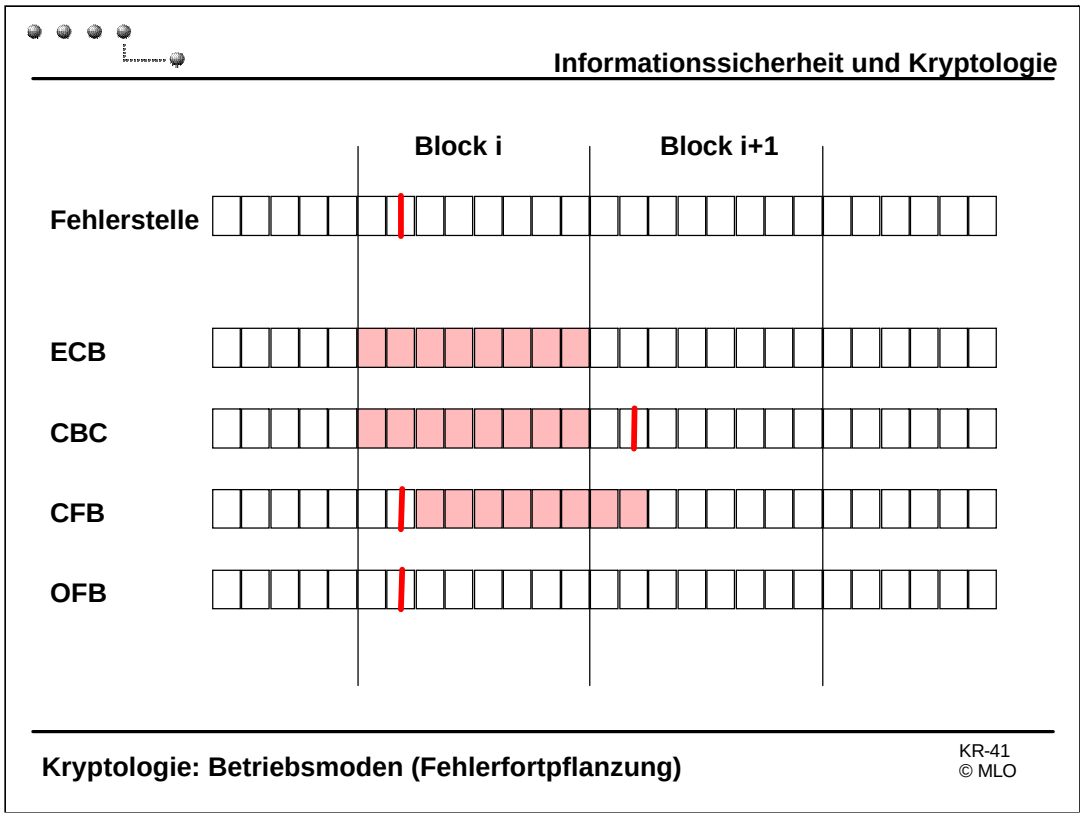
Der CFB Modus ist eine andere Art und Weise, eine Blockchiffre als Stromchiffre einzusetzen. Wie im OFB-m Modus werden auch im CFB-m Modus jeweils m Bit aus dem Ergebnis der Verschlüsselungs-operation mit dem Klartext verknüpft. Zurückgekoppelt wird nun allerdings nicht der Output der Verschlüsselungsoperaton, sondern der resultierende Chiffretext.

Durch die Vorwärtskopplung des Chiffre-textes beim Empfänger ist der CFB-Modus selbstsynchronisierend, d.h. das System erholt sich von selbst von Synchroni-sierungsfehlern, sobald die Fehlerstelle aus dem Inputregister des Empfängers heraus-geschoben wurde.

Auf der anderen Seite ergibt sich im CFB-Modus im Gegensatz zum OFB-Modus eine Fehlerfortpflanzung. Ein Fehler wirkt sich ausser auf das betroffene Zeichen auch auf die folgenden so lange aus, bis er das Input-register verlassen hat.

Die hier vorgestellten Betriebsarten sind wurden als Betriebsarten für DES zusammen mit diesem normiert und können im Detail im entsprechenden NIST-Standard nachgelesen werden, der unter weiterführender Literatur im WebCT vorhanden ist.

Natürlich kommen die beschriebenen Betriebsarten nicht nur mit DES sondern in derselben Weise auch mit anderen Blockchiffren¨zum Einsatz.



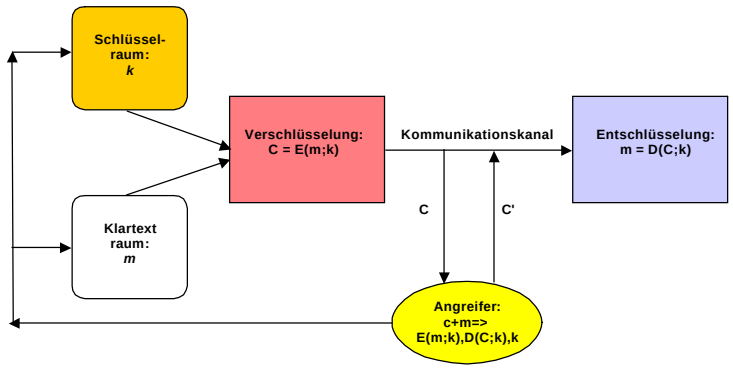
Die Abbildung fasst das Verhalten bei einem Bitfehler in jeder der Standardbetriebsarten von Blockchiffren zusammen, wobei für m ein Achtel der Blockgrösse gewählt wurde.

Unter Fehlerfortpflanzung versteht man den Effekt, dass ein einzelner Übertragungs-fehler beim Chiffretext durch den Dechiffriervorgang verstärkt wird und sich im Klartext auf einen grösseren Bereich “fortpflanzt”.

Ein wichtiger Vorteil des OFB-Modus ist, dass er im Gegensatz zu allen anderen Betriebsarten keine Fehlerfortpflanzung aufweist. Dies ist zum Beispiel dann von Bedeutung , wenn die Verschlüsselung nachträglich in ein bezüglich seines Fehlerverhaltens optimiertes Kommuni-kationssystem integriert wird.

Blockchiffren sind sehr vielseitig einsetzbar, nicht nur zur Geheimhaltung von Infor-mationen sondern, wie noch gezeigt wird, auch zum Schutz der Integrität von Daten. Für diesen Zweck ist ein gewisses Mass an Fehlerfortpflanzung aber geradezu die Voraussetzung.

Formen von kryptoanalytischen Angriffen



Klassifizierung der Angriffe

- ***Entschlüsselungsangriff (ciphertext only)***

  Bekannt: C
  Gesucht: m, (k)

  Extensive Suche, Sprachredundanz, Statistik, Kontext, Algorithmus (schwierig)

- ***Klartextangriff (known plaintext)***

  Bekannt: C, m
  Gesucht: k

  Analyse, extensive Suche, Sprachredundanz, Statistik, Kontext, Algorithmus

- ***Wählbarer Klartextangriff (choosen plaintext)***

  Gewählt: m Bekannt: C
  Gesucht: k, E(m,k)

  Gezielte Analyse, Algorithmus

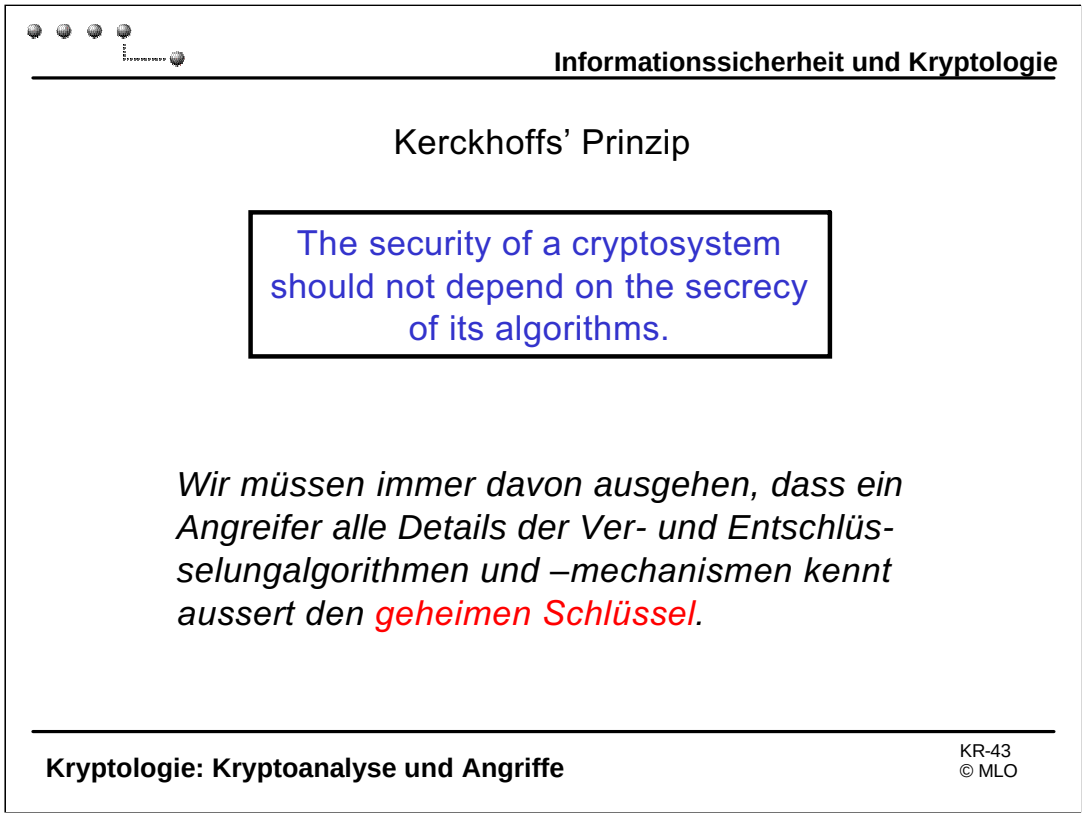
- ***Wählbarer Schlüsseltext (choosen ciphertext)***

  Gewählt: C Bekannt: m
  Gesucht: k, D(m,k)

  Gezielte Analyse, Algorithmus

Methoden

- ***Apriori Wissen*** Kontext, semantischer Hintergrund
- ***Extensive Suche*** Schlüsselraum, Klartextraum
- ***Mathematische Analyse*** Gleichungssystem, Differentialanalyse
- ***Statistische Analyse*** Sprachredundanz, n-Gramm Häufigkeiten



Prinzip des öffentlichen Reviews

Alle Algorithmen müssen durch einen öffentlichen Reviewprozess als sicher verifiziert werden. Die Geheimhaltung von Algorithmen führt zu einer undefinierten (nicht mathematisch quantifizierbaren) Risikosituation.