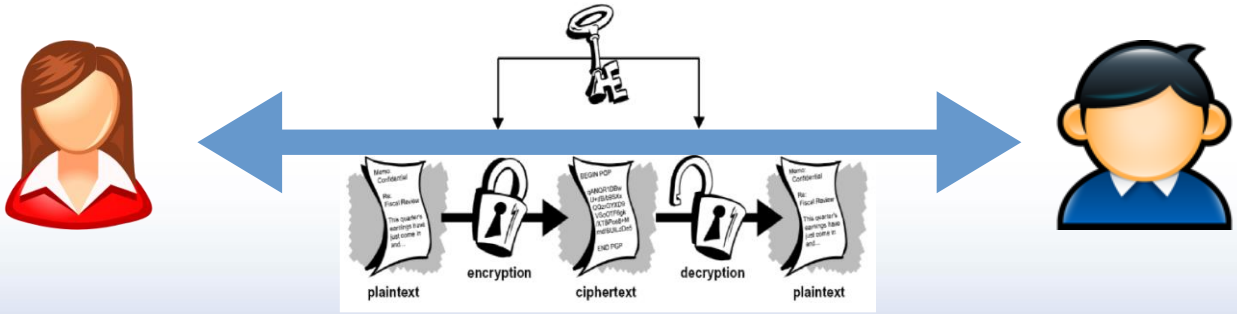
Was ist Kryptographie?

Hagen Knaf, März 2018

Überblick

1. Ursprünge der Kryptographie
2. Grundbegriffe
3. Attacken auf Kryptosysteme



Ursprünge der Kryptographie

ANGRIFF
VON
OSTEN

DQHKVMII
ZRQ
RXYHQ

Die Caesar-Chiffre

Ursprünge der Kryptographie

Die Caesar-Chiffre

- Der Überlieferung nach benutzte der römische Feldherr und Staatsmann Gaius Iulius Caesar folgendes Verfahren um vertrauliche, schriftliche Botschaften niederzuschreiben:
  1. Ersetze jeden Buchstaben durch den dritten im Alphabet folgenden Buchstaben.
  2. Wird dabei das Ende des Alphabets erreicht, setze die Zählung am Anfang fort.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	A	B	C

- Das Wort CAESAR zum Beispiel wird zu FDHXDV.
- Statt einer Verschiebung der Buchstaben um 3 kann man jede Zahl zwischen 1 und 23 wählen.
- Das römische Alphabet besitzt inklusive der Zahlzeichen nur 23 Buchstaben.

Ursprünge der Kryptographie

Klassische Kryptographie

- Seit ca. 3500 Jahren werden »Geheimschriften« für die *vertrauliche, schriftliche Kommunikation* zwischen zwei Parteien genutzt.
- Einsatzgebiete: Diplomatie, Militär, Verwaltung, Handel, kriminelle Organisationen.
- Im Mittelalter (6. – 15. Jahrhundert) entwickelt sich die Kryptographie zur Wissenschaft.
- K*lassische Kryptographie:* Die Buchstaben des Alphabets werden nach bestimmten Regeln durch andere Buchstaben ersetzt.
- Alle Verfahren der klassischen Kryptographie sind heute unbrauchbar, da viel zu unsicher.

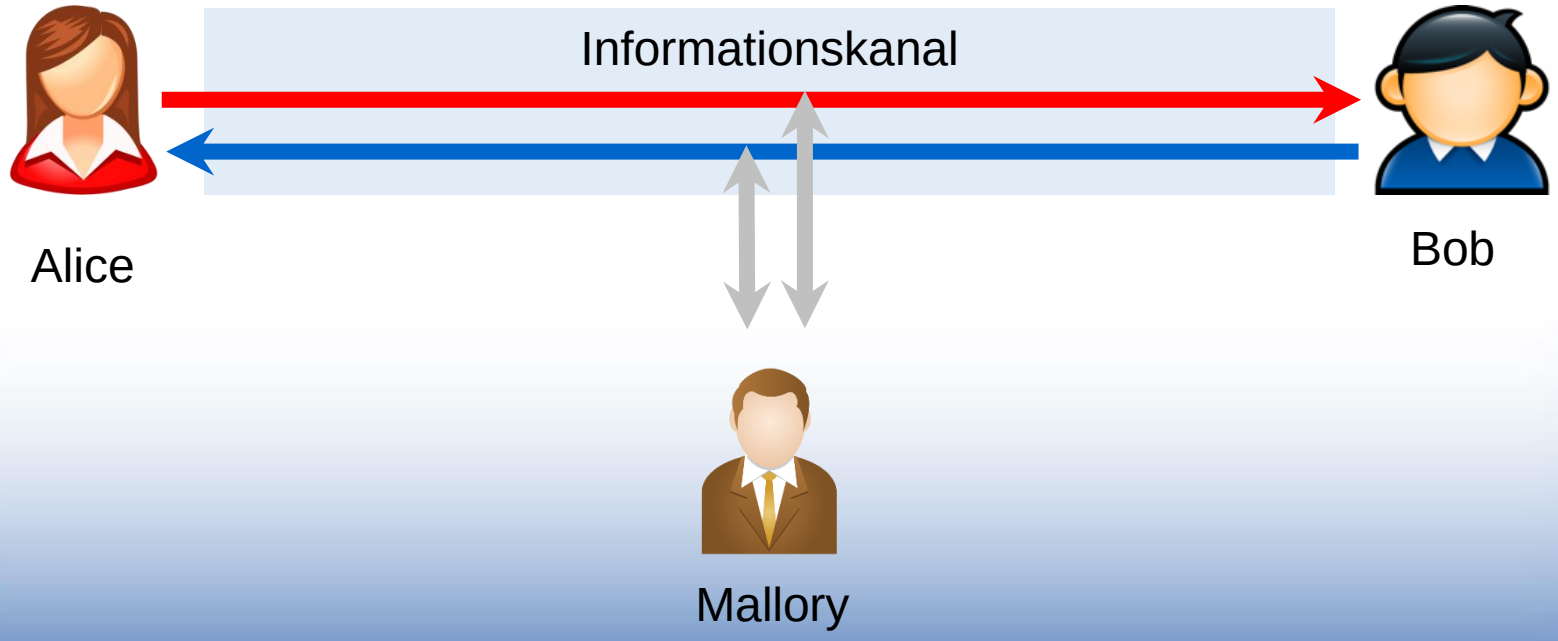
Leon Batista Alberti
1404 – 1472

Chiffrierscheibe

Ursprünge der Kryptographie

Moderne Kryptographie: Das Grundproblem

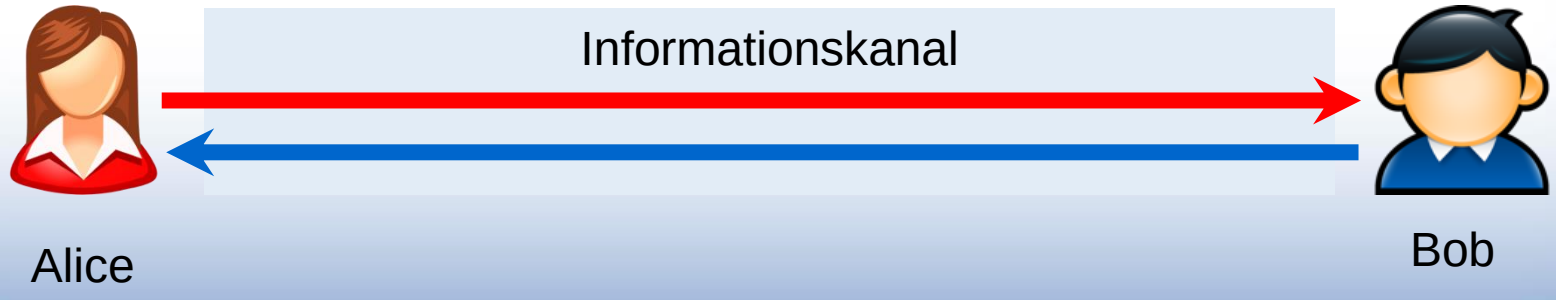
Zwei *Parteien* (Alice und Bob) wollen über einen *Informationskanal* vertraulich kommunizieren: Dritte (Mallory) sollen die ausgetauschten Informationen nicht »mitlesen« können.



Ursprünge der Kryptographie

Moderne Kryptographie: Das Grundproblem

- Die Kommunikation findet statt über: Sprache, Schrift, Bilder.
- Die ausgetauschten Informationen können von unterschiedlicher Art sein: Ton, Text, Bilder, Zahlen.
- Als Kanal kann benutzt werden: Telefonie, Fax, Funk, direkte Übergabe von Daten usw.



Ursprünge der Kryptographie

Moderne Kryptographie

- … basiert auf mathematischen Methoden.
- Relevante Gebiete: Zahlentheorie, abstrakte Algebra, Stochastik, Informationstheorie.
- … entwickelt sich ab ca. 1900 motiviert durch die leicht abhörbare Telegraphie-Technik.
- Getrieben durch die Anwendungen in zwei Weltkriegen, den »kalten Krieg« (1947 – 1989), die Computerisierung (ab etwa 1935) und den Aufbau des Internet (ab 1969) erlebt die Kryptographie ein andauerndes starkes Wachstum an Bedeutung und als Wissenschaft.

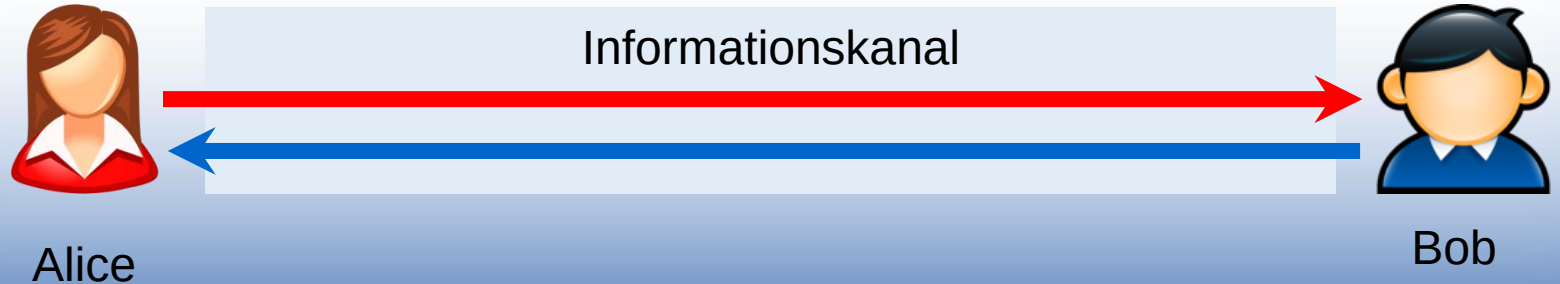
Claude Shannon
1916 – 2001

Enigma

Ursprünge der Kryptographie

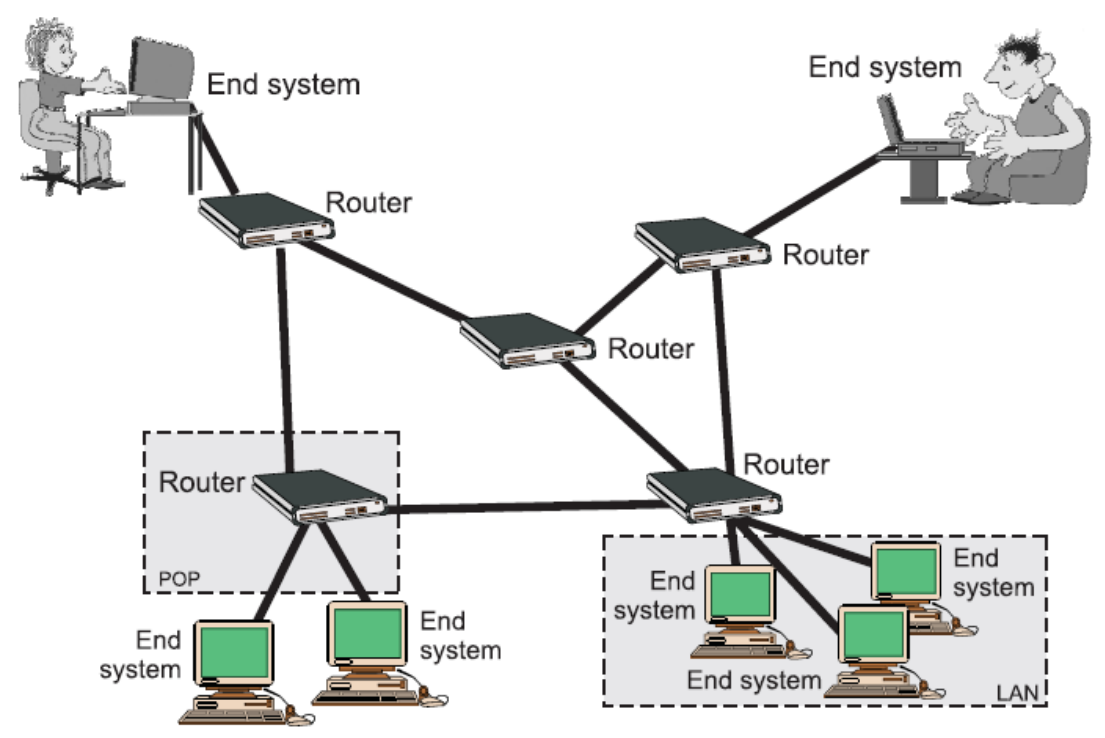
Kryptographische Maßnahmen

- In der klassischen Kryptographie wurde nur geschriebener Text behandelt.
- Die Digitalisierung ermöglicht heute auch die kryptographische Bearbeitung von Ton- und Bildinformation.
- Kryptographische Maßnahmen hängen auch vom verwendeten Informationskanal ab: Analogtelefonie, Funk, Fax, Internet.
- Während dieser MINT-Veranstaltung wird meistens der sichere Austausch elektronisch vorliegender Texte zwischen Alice und Bob über das Internet betrachtet.



Ursprünge der Kryptographie

Abhören im Internet



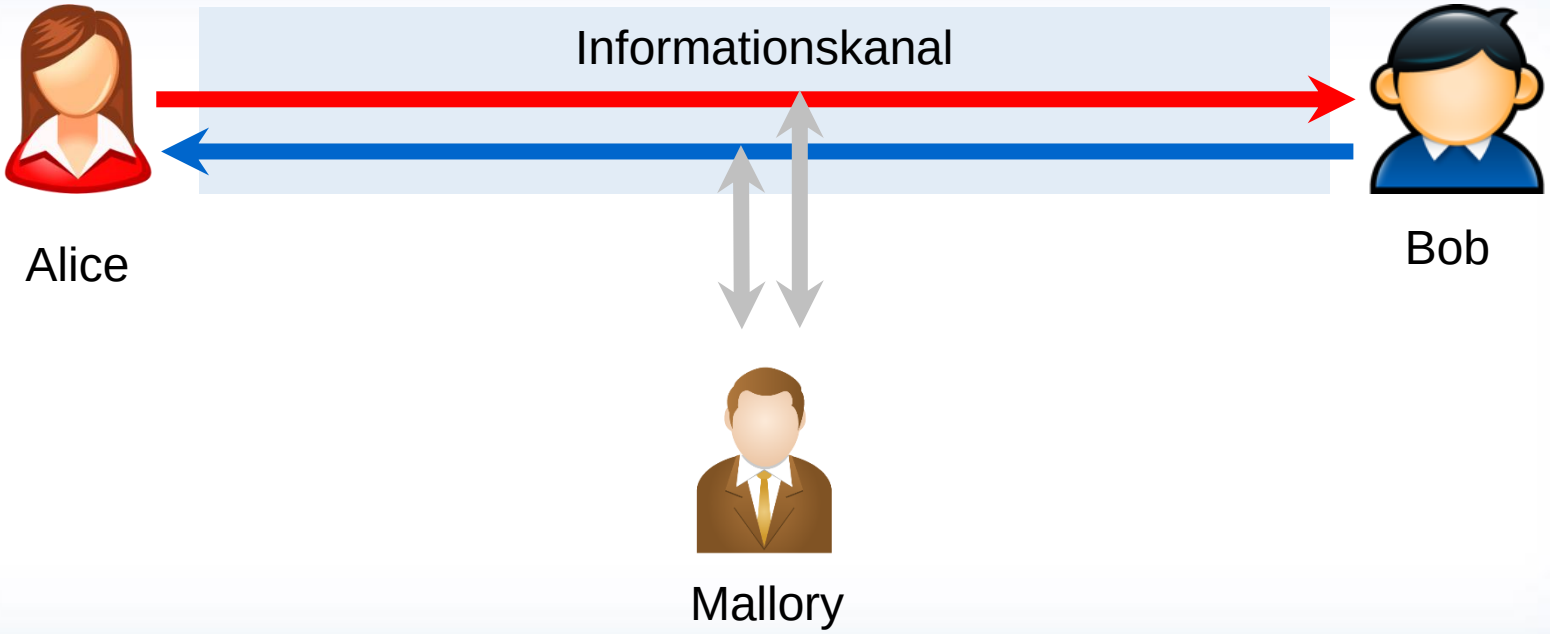
Emails, WhatsApp etc. werden mitgelesen …

- zum Schutz vor Viren,
- zu Werbezwecken,
- zu Spionagezwecken,
- zu polizeilichen / geheimdienstlichen Zwecken.

Besitzt jeder Bürger das Recht auf vertrauliche Kommunikationsmöglichkeiten?

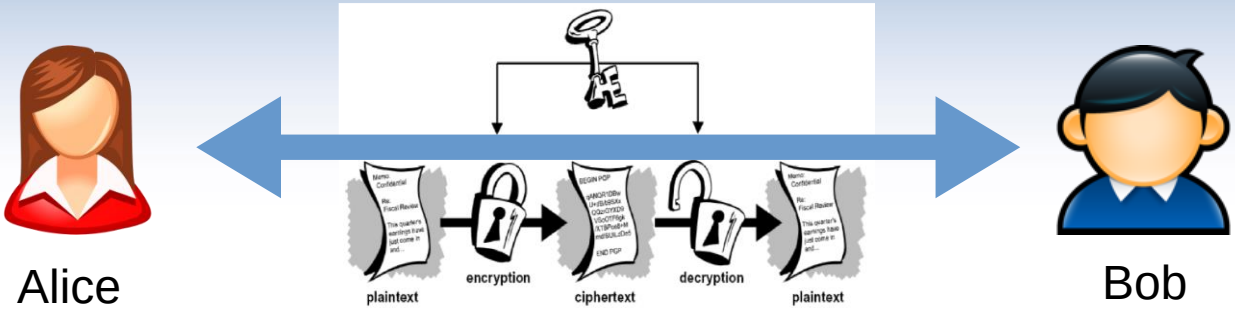
Grundbegriffe

Das kryptographische »Worst Case« Modellszenario



- kann alle ausgetauschten Daten mitlesen, beeinflussen und verändern,
- kann Bob im Namen von Alice Daten schicken, und umgekehrt,
- wird bei diesen Operationen nicht erkannt.

Grundbegriffe



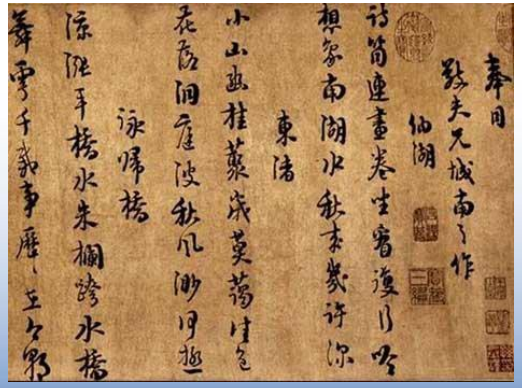
- *Verschlüsseln*: Das systematische Umwandeln von lesbarer Information, dem *Klartext*, in den direkt nicht lesbaren *Chiffretext*.
- *Schlüssel*: Eine Information, die den Verschlüsselungsprozess festlegt.

A	B	C	D	…	V	X	Y	Z
D	E	F	G	…	Z	A	B	C

- *Entschlüsseln*: Gewinnen des Klartexts aus dem Chiffretext unter Verwendung des zugehörigen Schlüssels.
- Der Schlüssel muss im Besitz beider Kommunikationspartner sein und sonst geheim bleiben. (*Private-Key-Cryptography*)

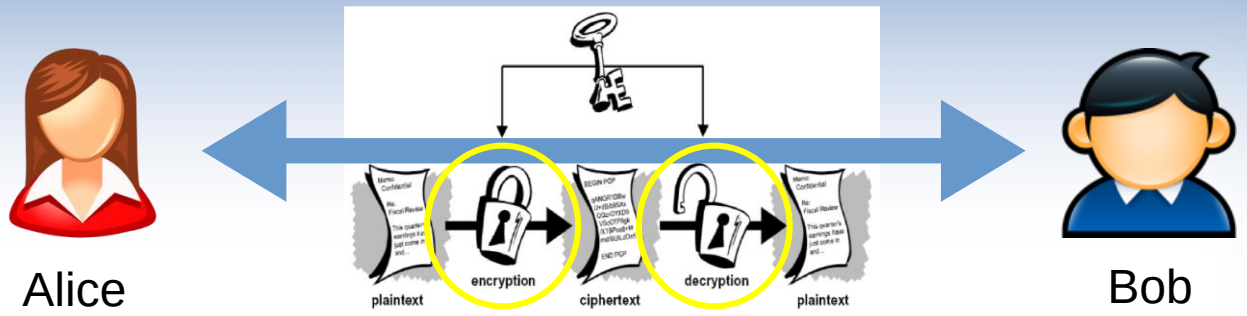
Grundbegriffe

- *Alphabet*: Eine endliche Menge von Zeichen, die benutzt werden um Texte zu erzeugen.
  - Das römische Alphabet {A,B,C,…,Z}.
  - Die Menge der 128 Zeichen einer europäischen Computertastatur.
  - Die Menge der mehr als 50000 Zeichen der japanischen Kanji-Schrift.
  - Die vier Basen {A,G,T,C} der DNS des Menschen.
- *Text in/über einem Alphabet*: Jede endlich lange Folge von Zeichen aus einem bestimmten Alphabet. Ob der Text sinnvoll ist oder nicht, spielt keine Rolle.



```
CTGGTGGTGCTCAGCTGCAAGTCAAGCTGCTCTCTGGGCTGTGATCTCCCTGAGACC
CACAGCCTGGATAACAGGAGGACCTTGATGCTCCTGGCACAAATGAGCAGAATCTCT
CCTTCCTCCTGTCTGATGGACAGACATGACTTTGGATTTCCCCAGGAGGAGTTTGAT
GGCAACCAGTTCCAGAAGGCTCCAGCCATCTCTGTCCTCCATGAGCTGATCCAGCAG
ATCTTCAACCTCTTTACCACAAAAGATTCATCTGCTGCTTGGGATGAGGACCTCCTA
GACAAATTCTGCACCGAACTCTACCAGCAGCTGAATGACTTGGAAGCCTGTGTGATG
CAGGAGGAGAGGGTGGGAGAAACTCCCCTGATGAATGCGGACTCCATCTTGGCTGTG
AAGAAATACTTCCGAAGAATCACTCTCTATCTGACAGAGAAGAAATACAGCCCTTGT
GCCTGGGAGGTTGTCAGAGCAGAAATCATGAGATCCTCTCTTTATCAACAAACTTGC
AAGAAAGATTAAGGAGGAAGGAATAA, TGTGATCTCCCTGAGACCCACAGCCTGGA
TAACAGGAGGACCTTGATGCTCCTGGCACAAATGAGCAGAATCTCTCCTTCCTCCTG
TCTGATGGACAGACATGACTTTGGATTTCCCCAGGAGGAGTTTGATGGCAACCAGTT
CCAGAAGGCTCCAGCCATCTCTGTCCTCCATGAGCTGATCCAGCAGATCTTCAACCT
```

Grundbegriffe

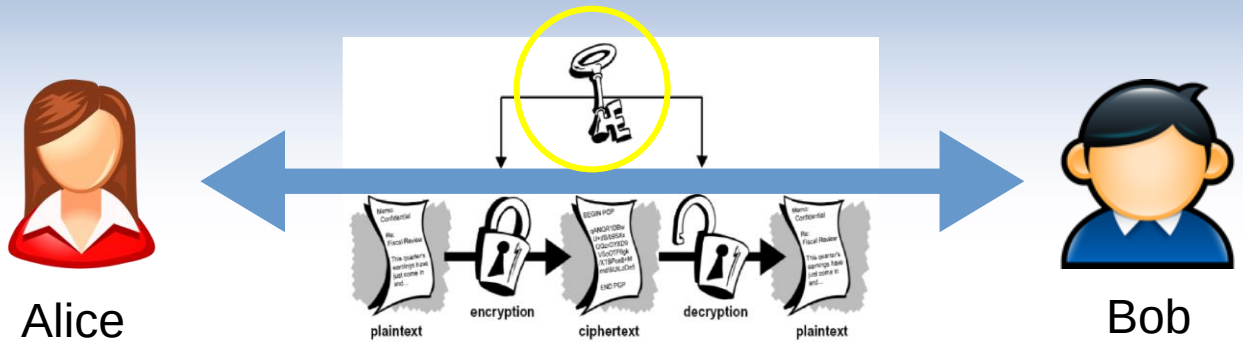


- *Kryptographie*: Die Wissenschaft der Verschlüsselungsverfahren mit der zentralen Frage:

Wie kann man Information so verschlüsseln, dass das Entschlüsseln ohne Besitz des Schlüssels sehr schwierig ist?

- Den Versuch verschlüsselte Nachrichten ohne den zugehörigen Schlüssel zu entschlüsseln nennt man eine *Attacke* auf das Verschlüsselungs-verfahren.
- *Schwierig* heißt *langwierig:*
  - es wird nicht versucht erfolgreiche Attacken unmöglich zu machen, …
  - weil das mit hoher Wahrscheinlichkeit unmöglich ist.

Grundbegriffe



Das Schlüsseltauschproblem

- Im Worst-Case-Szenario wird angenommen, dass Mallory das von Alice und Bob verwendete Verschlüsselungsverfahren kennt …
- nicht aber den von ihnen verwendeten Schlüssel !

Wie können sich Alice und Bob über den von Mallory abgehörten Informationskanal auf einen Schlüssel einigen ?

Grundbegriffe

- *Kryptosystem:* Software zum Verschlüsseln von (Text)-Dateien.
- Mathematisch betrachtet besitzt ein Kryptosystem fünf Teile:

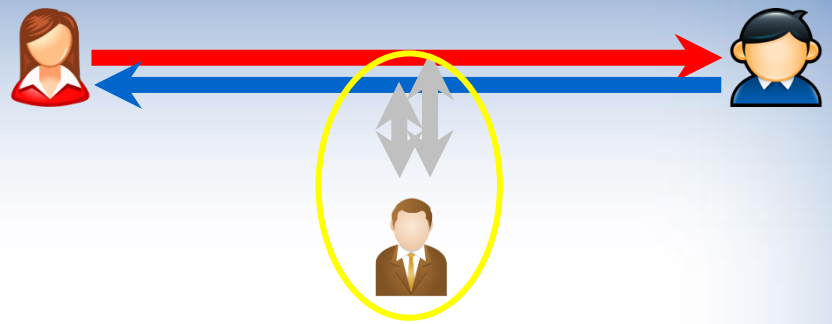
1. der Menge P zulässiger Klartexte,
2. der Menge C vorkommender Chiffretexte,
3. der Menge K möglicher Schlüssel,
4. zu jedem Schlüssel $k \in K$ ein Verschlüsselungsverfahren
$$e_k: P \to C,$$
auch als *Chiffre* bezeichnet,
5. zu jedem Schlüssel $k \in K$ ein Entschlüsselungsverfahren
$$d_k: C \to P$$
mit der Eigenschaft
$$d_k\big(e_k(T)\big) = T \text{ für jedes } T \in P.$$

Grundbegriffe

Die Caesar-Chiffre als Kryptosystem

1. *Zulässige Klartexte*: P = Alle im römischen Alphabet schreibbaren Texte.
2. *Vorkommende Chiffretexte*: C = Alle endlich langen Folgen von Buchstaben des römischen Alphabets.
3. *Mögliche Schlüssel*: K={1,2,3,…,23}
4. *Verschlüsselungsverfahren* $e_k: P \to C$: Ersetzen jedes Buchstabens durch den k-ten Folgebuchstaben.
5. *Entschlüsselungsverfahren* $d_k: C \to P$: Ersetzen jedes Buchstabens durch den k-ten Vorgängerbuchstaben.

Attacken auf Kryptosysteme



In der Analyse der Attackensicherheit von Kryptosystemen, die im öffentlichen Raum genutzt werden, geht man von folgendem Szenario aus:

1. Das betrachtete Kryptosystem ***K*** ist allen bekannt.
2. Die jeweils konkret verwendeten Schlüssel k sind geheim.
3. Die jeweils verschlüsselten Klartexte sind geheim.

Kann unter diesen Voraussetzungen eine erfolgreiche Attacke gegen das Kryptosystem durchgeführt werden?

Attacken auf Kryptosysteme

Ziele einer Attacke

- Kenntnis des verwendeten Schlüssels k.
  - Ermöglicht zum Beispiel das ständige Abhören eines Informationskanals ...
  - … aber auch das Versenden gefälschter Informationen.

- Vollständige Kenntnis eines bestimmten Klartexts.
  - Zum Beispiel Industriespionage:
    Bauplan eines neuen Motortyps.

- Kenntnis von Teilen eines bestimmten Klartexts.
  - Zum Beispiel Angebotsvergabe im öffentlichen Dienst:
    Preis des Angebots eines Konkurrenten.

Attacken auf Kryptosysteme

Cipher-Text-only-Attack

- Mallory stehen nur ein oder mehrere verschlüsselte Klartexte als Grundlage zur Verfügung.

Exhaustive-Key-Search

- Der Schlüsselraum K und die Entschlüsselungsfunktionen D sind bekannt.
- Mallory kann also den bekannten Chiffretext mit allen Entschlüsselungs-funktionen übersetzen.
- Unter den wenigen so erhaltenen sinnvollen Texten ist der Klartext.
- Mit schnellen Rechnern und Textanalysesystemen ist diese Methode manchmal erfolgreich.

Attacken auf Kryptosysteme

Known-Plain-Text-Attack

- Mallory kennt einige Klartext-Chiffretext-Paare und nutzt diese zusammen mit der Kenntnis des Kryptosystems ***K*** um Rückschlüsse auf den Klartext zu einem neuen Chiffretext zu ziehen.
- Beispiel: Gruß- und Einleitungsphrasen in Emails werden je nach Kryptosystem stets gleich chiffriert.
- Beispiel: Militärische Manöver
  - Militärs eines Landes A beobachten militärische Manöver eines Landes B und schicken chiffrierte Zusammenfassungen über diese Manöver an eine Stabsstelle.
  - Teil der Zusammenfassung ist die Anzahl und Größe beteiligter Schiffe oder ähnliche strukturierte Information.
  - Land B führt Fake-Manöver mit bestimmten Schiffsanzahlen und Größen durch, und fängt die chiffrierten Zusammenfassungen ab.
  - So geschehen während des zweiten Weltkriegs.

Attacken auf Kryptosysteme

Chosen-Plain-Text-Attack

- Mallory kann Chiffretexte zu vorgegebenen Klartexten und damit Klartext-Chiffretext-Paare erzeugen.
- Dies ist immer möglich, wenn der Verschlüsselungsschlüssel bekannt ist.
- Beispiel: Passwortverschlüsselung
  - Die verschlüsselten Passworte eines Multiuser-Computers stehen in einer für einen Nutzer mit Administratorrechten (=Mallory) lesbaren Datei (.passwd unter Unix).
  - Dieser Nutzer kann sein Passwort ändern, und ermitteln wie das chiffrierte Passwort aussieht.
  - Mit dieser Information kann er versuchen die Passworte anderer Nutzer zu ermitteln.

Danke für die Aufmerksamkeit.