TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

DIPLOMARBEIT

Aufbau von Lehrinhalten anhand des Beispiels Kryptologie für den Informatikunterricht

Ausgeführt am Institut für
Softwaretechnik und Interaktive Systeme
der Technischen Universität Wien

unter der Leitung von
Univ.Doz. Dipl.-Ing. Dr.techn. Ernst Piller

durch

Stefan Greger

Wienerstraße 101, 2640 Gloggnitz

Inhaltsverzeichnis

1. Einleitung

„Informatische Bildung ist das Ergebnis von Lernprozessen, in denen Grundlagen, Methoden, Anwendungen und Arbeitsweisen erschlossen und die gesellschaftliche Dimension von Informations-und Kommunikationstechnologien verdeutlicht werden.
Es ist eine wesentliche Aufgabe des Informatikunterrichts, Schülerinnen und Schülern informatische und informationstechnische Grundkenntnisse zu vermitteln, um sie zu befähigen, diese zur Lösung einer Problemstellung sicher und kritisch einzusetzen."
Dieser Abschnitt stammt aus dem Lehrplan für Informatik für AHS. Ich möchte in meiner Arbeit das Thema Kryptologie unter der didaktischen Sicht behandeln.

2. Warum lernt man über das Gebiet Kryptologie?

2.1. Der Begriff Kryptologie

Der Begriff Kryptologie entstammt den griechischen Wörtern *kryptos*, das soviel bedeutet wie geheim, und *logos*, welches bedeutet Wort oder Sinn.
Kryptologie ist die Wissenschaft vom Verschlüsseln und Entschlüsseln von Informationen. Weiters umfasst das Gebiet der Kryptologie auch die Analyse kryptografischer Verfahren zum Zweck der Bedeutung ihrer Stärke.
Der Begriff Kryptologie umfasst zwei Gebiete:

- Kryptografie
- Kryptoanalyse

Kryptografie (griech. graphein bedeutet schreiben) ist die Lehre von der Verschlüsselung von Informationen.
Kryptoanalyse gibt die Analyse und Bewertung der Sicherheit von kryptografischen Verfahren an.

2.2. Warum Sicherheit und Kryptologie?

Durch die wachsende Mobilität der Gesellschaft, aber auch durch die technischen Entwicklungen im Bereich der Informationstechnologien in Richtung Miniaturisierung der Geräte ergibt sich eine zunehmende Vernetzung und damit Übertragung der Daten über die Unternehmensgrenzen hinaus. War es in den 90er-Jahren noch ausreichend, Firewall- oder Intrusion-Detection-Systeme zu installieren, so verteilen sich heutzutage die Sicherheitsrisiken auf alle MitarbeiterInnen und die Standorte, an denen sie die Arbeit verrichten. Laptops, PDAs oder ähnliche mobile Endgeräte dehnen das Unternehmensnetz in nicht mehr klar abgrenzbare Bereiche aus.
Home-Office ist heutzutage eine in vielen Unternehmen genutzte Arbeitsmöglichkeit. Damit steigen natürlich auch die Gefahren, die auf die IT-Infrastruktur wirken. Verschärft wird die Situation noch dadurch, dass immer mehr Prozesse des Unternehmens EDV-unterstützt abgebildet und abgewickelt werden. Bei fast allen Unternehmen entwickelt sich die EDV daher zu einer unternehmenskritischen Infrastruktur, die als besonders schützenswert gilt. Ein Ausfall des Rechenzentrums

bzw. der EDV-Services führt zum Stillstand in den meisten Unternehmen und damit zu schweren finanziellen und Image-Schäden.
Zum Beispiel weist das österreichische Datenschutzgesetz auf diese Situation hin und verpflichtet Datenverarbeiter, soweit sie dem Rahmen des Gesetzes entsprechende Tätigkeiten ausführen, auf die Einhaltung von entsprechenden Sicherheitsmaßnahmen. Der Bedarf nach umfassenden und detaillierten Regelungen hat in den letzten 15 Jahren eine Vielzahl von Arbeitskreisen und Normungsinstituten beschäftigt, die ihrerseits Richtlinien zu den verschiedensten Aspekten der IT-Security herausgegeben haben. Als Beispiele seien hier die ISO 17799 und die ISO 27001 als die international am weitesten verbreiteten Standards, aber auch das österreichische IT- Sicherheitshandbuch und das IT-Grundschutzhandbuch des BSI erwähnt.
Diesen sicherheitsrelevanten Entwicklungen wurde bisher in den meisten Unternehmen zu wenig Bedeutung beigemessen, war man ja mit dem Ausbau der Vernetzung und der Bereitstellung der Services für die Benutzer beschäftigt. Oft gab man sich auch mit der Installation von Firewall-Systemen und Viren-Scannern zufrieden. Bei der Analyse der Sicherheitsrisiken kann folgende Einteilung vorgenommen werden: organisatorische Mängel, technische Mängel, menschliche Fehler, Bösartigkeiten und höhere Gewalt. Bei den meisten Unternehmen wird der Fokus auf die Technik sowie auf Angriffe von außen gelegt. Werden diese Unternehmen angegriffen, so werden diese Unzulänglichkeiten erkannt und haben meist verheerende Auswirkungen. Viele Unternehmen, die bei einer Katastrophe wichtige Unternehmensdaten verloren haben, haben sich von dieser nicht mehr erholt.
Ich möchte in meiner Arbeit näher auf das Thema Kryptologie eingehen. Wenn ich persönliche Informationen versende oder empfange, will ich, dass diese Information nur einem von mir genau bestimmten Kreis von Personen zugänglich ist. Sogar der Umstand, dass ich mit jemandem kommuniziere, gehört meiner Privatsphäre an. Nun soll meine Privatsphäre geschützt werden. Durch welche Methoden, Arten, Vorgehensweisen, Verfahren, Rechte ich das durchführen kann, sollte meiner Meinung nach schon in der Schule gelehrt werden. Neben dem Schutz der Privatsphäre hat die Digitale Signatur immer mehr an Bedeutung erlangt. Daher habe ich mir Gedanken darüber gemacht, wie man am besten ein so komplexes Gebiet, zu mindestens wichtige Teile daraus, Lernenden didaktisch gut übermittelt.

3. Didaktisches Konzept

Die erste Frage, die sich bei so einem Thema wie Kryptologie stellt, ist, wie man dieses Thema didaktisch gut aufbereiten kann. Welche Hilfsmitteln nehme ich bzw. habe ich zur Verfügung?
Meine Wahl fiel auf die Präsentationssoftware Power Point:

- Die Präsentation soll den Vortrag unterstützen.
- Sie soll wichtige Punkte visualisieren und so mithelfen, dass das Gesagte lange erinnert wird.
- Erinnerungsleistung abhängig von der Art der Aufnahme:
  Größter Effekt durch Sehen und Hören.
- Gezeigte Folien können als Handout vor oder nach dem Vortrag ausgeteilt werden.
- Visualisierungsmöglichkeiten
- Gestaffelter Seitenaufbau
- Bei Effekten muss jedoch aufgepasst werden, dass diese sparsam eingesetzt werden. Soll keine Show werden!
- Grafiken und Piktogramme unterstützend verwenden, nicht als Selbstzweck
- manchmal beideutet weniger ist mehr: Nicht zuviel auf eine Folie!

Da Kryptografie ein recht trockenes Fachgebiet überdeckt, kam ich auf die Idee ein wenig Schwung in meine Präsentation hinein zu bringen. Besonders bei den mathematischen Teilen hat sich eine eher einfache Darstellungsart bewährt. Damit hoffe ich, dass auch nicht so Mathematik-Interessierte ihre Freude daran haben werden.
Bei vielen Verfahren in der Kryptologie ist es wichtig, dass man sie selbst einmal ausprobiert bzw. durchrechnet („Learning by doing!“). Das gilt besonders für das RSA Verfahren und den Diffie-Hellman-Schlüsselaustausch.

4. Präsentationsteil

Der Präsentationsteil umfasst folgende Themen der Kryptologie:

- Was bedeutet der Begriff Kryptologie?
- Geheimschrift
- Geheimsprache
- Historische Entwicklung
- Cäsars Verschlüsselung
- Warum eigentlich Kryptographie?
- Grundsituation bei Cäsar
- Kryptographie der Neuzeit
- One – Time – Pad
- Situation in der Neuzeit
- Was bedeutet Symmetrisch?
- Vorteil und Nachteil (Symmetrie)
- Symmetrische Verfahren
- XOR-Funktion
- Verlängerung von Schlüsseln
- Mathematik 1
- Kryptographie bis 1950
- Kryptographie heute
- Ist Symmetrie notwendig?
- Mathematik 2
- RSA am Beispiel
- RSA funktioniert
- RSA angreifen
- RSA Falltürfunktion
- Situation bei RSA
- Was bedeutet Asymmetrisch?
- Vorteil und Nachteil (Asymmetrie)
- Moderne Kryptographie
- Hybride Verfahren
- Beispiel eines Hybriden Verfahrens
- Kryptoanalyse
- Angriffsmöglichkeiten
- Differentielle Kryptoanalyse
- Lineare Kryptoanalyse
- Side-Channel Analysen
- Kryptoregulierungen
- Mathematik 3
- Hash-Funkionen
- Hash-Verfahren
    - Hash-Algorithmus SHA
    - Hash-Algorithmus MD5
    - RIPMED-16
    - TIGER
    - HAVAL
    - Whirlpool
- MAC (Message Authentication Code)
- Digitale Signatur
- Public Key Infrastrukturen
- SSL
- Schlüsselmanagement
    - u.a. Diffie-Hellman

Die folgenden Folien wurden ausschließlich von mir erstellt. Einige davon basieren auf anderen Präsentationen, insbesondere von Michael Nüsken und dem Seminar Security von Ernst Piller, sowie Textausschnitten aus Wikipedia.

TECHNISCHE UNIVERSITÄT WIEN
VIENNA UNIVERSITY OF TECHNOLOGY

Kryptologie

Mathematik für James Bond & Co.

oder

Wie bewahrt man das Geheimnis Ihrer Majestät?

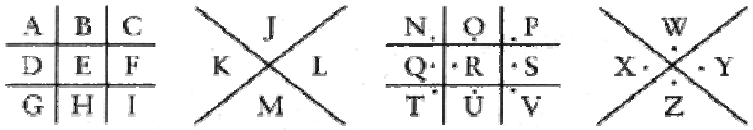
von Stefan Greger

Was bedeutet der Begriff Kryptologie?

- Kryptologie
  - die Wissenschaft der Verschlüsselung und Entschlüsselung von Informationen sowie Analyse kryptografischer Verfahren
  - umfasst folgende Gebiete:
    - Kryptografie:
      - Lehre von den Methoden zur Ver- und Entschlüsselung von Nachrichten zum Zweck der Geheimhaltung von Informationen gegenüber Dritten
      - bedeutet übersetzt Geheimschrift
    - Kryptoanalyse:
      - Analyse und Bewertung der Sicherheit von kryptografischen Verfahren gegen unbefugte Angriffe

Geheimschrift

- z.B.:



Zum Beispiel ist

nichts anderes als das Wort KRYPTOGRAPHIE.

Geheimsprache

KOKALOLLOLE

Geheimsprache

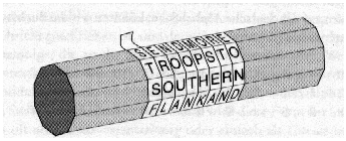
JOJAMOMESOS
BOBONONDOD

Geheimsprache

- Verschlüsseln: schwer zu lernen
- Entschlüsseln: leicht
- Knacken: leicht, selbst ohne Kenntnisse

Historische Entwicklung

- Griechen
  - einfache Formen der Verschlüsselung
  - mit Steganografie kombiniert
    - Methoden, die darauf abzielen, bereits die Existenz einer Nachricht zu verbergen und nicht nur den Informationsgehalt zu verschleiern
  - Botschaft um einen Stab gewickelt (Skytala)

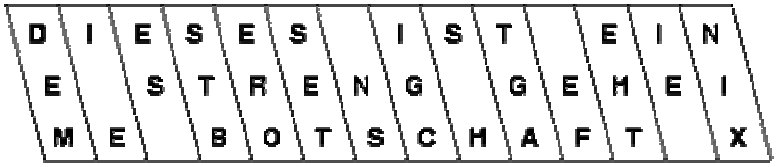


Historische Entwicklung (Skytala)

- ein Papyrusstreifen spiralförmig um einen Stab festen Durchmessers gewickelt
- in Stab-Längsrichtung zeilenweise ein Text darauf geschrieben
- nach dem Abrollen des Streifens ist der Text dann nicht mehr ohne weiteres lesbar
- Originaltext wieder erkennbar zu machen:
  - Streifen muss erneut um einen Stab des gleichen Durchmessers gewickelt werden
  - Stabdurchmesser: der zur Entschlüsselung notwendig geheime Schlüssel

Beispiel Skytala

- ein aufgewickelter Streifen, der mit drei Zeilen beschriftet ist:



Beispiel Skytala

- nach dem Abwickeln:

DEMI EES STBEROSET NSIGCS HTGA EFEHTIE NIX

- jedoch nur geringe Sicherheit

Historische Entwicklung

- Römer
  - haben die ersten, mathematisch mit heutigen vergleichbaren Verschlüsselungsalgorithmen entwickelt
  - Cäsar Verschlüsselung

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

D  3

Cäsar Verschlüsselung

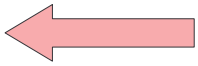
ABCDEFGHIJKLMNOPQRSTUVWXYZ

DE  3

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZ

 3

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Verschlüsseln:

JAMES 

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Verschlüsseln:

JAMES  M

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Verschlüsseln:

JAMES  MD

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Verschlüsseln:

JAMES → MDP

Cäsar Verschlüsselung

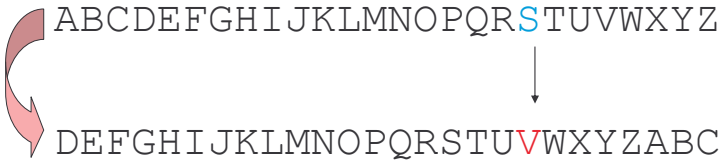
ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Verschlüsseln:

JAMES → MDPH

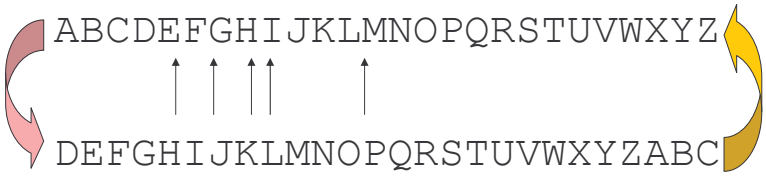
Cäsar Verschlüsselung



Verschlüsseln:

JAMES → MDPHV

Cäsar Verschlüsselung



Verschlüsseln:

JAMES → MDPHV

Entschlüsseln:

GEHEIM → JHKHLP

Cäsar Verschlüsselung

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Warum eigentlich Kryptografie?

- Vertraulichkeit
  - Geheimhaltung ist die offensichtlichste und bekannteste Anwendung kryptografischer Verfahren
- Integrität
  - für den Empfänger nachprüfbar sein, dass er die Nachricht unversehrt erhalten hat
- Authentizität
  - Identität des Absenders einer Nachricht soll für den Empfänger nachprüfbar sein

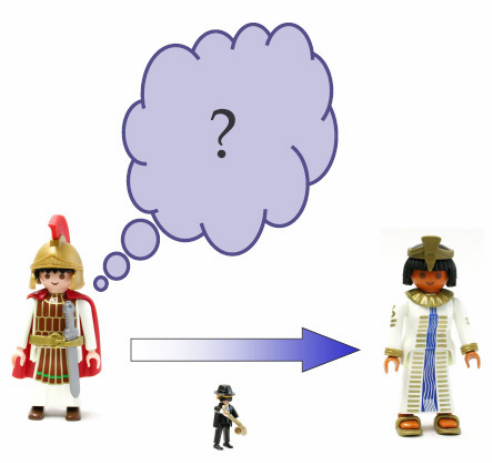
Warum eigentlich Kryptografie?

- Gültigkeit
  - Nachricht kann durch zwischenzeitliche Ereignisse ihre Bedeutung verlieren
- Nichtabstreitbarkeit
  - dass ein Absender einer Nachricht seine Urheberschaft später nicht verleugnen kann

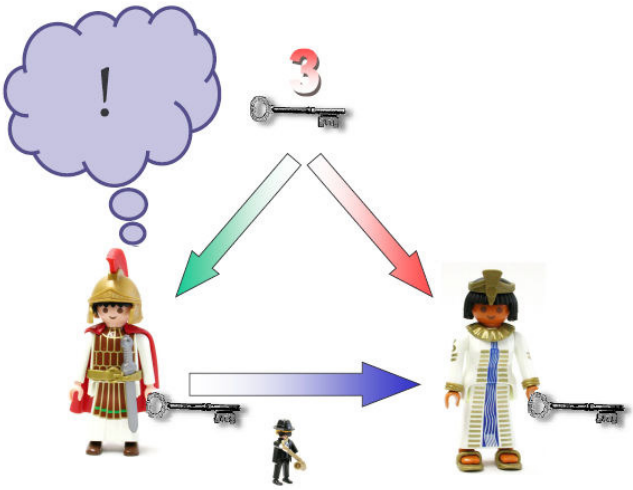
Grundsituation bei Cäsar

Grundsituation bei Cäsar

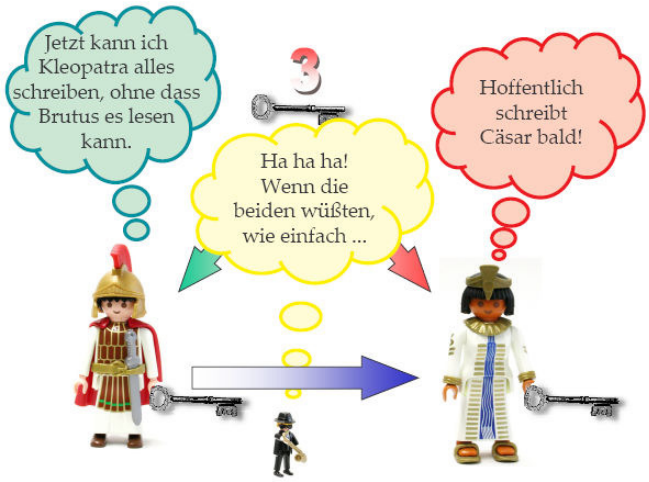
Grundsituation bei Cäsar



Grundsituation bei Cäsar



Grundsituation bei Cäsar



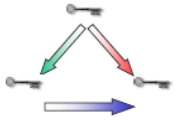
Kryptografie der Neuzeit

Giovan Battista della Porta (1563)

De furtivis literarum notis

Verschlüsselungsverfahren werden:

- verfeinert,
- mechanisiert und
- bleiben symmetrisch



Enigma (erfunden 1918)

Schlüsselgerät der deutschen Wehrmacht

Kryptografie der Neuzeit

Beispiel: Worte als Schlüssel

Ursprüngliche Nachricht

Das geheime Schlüsselwort

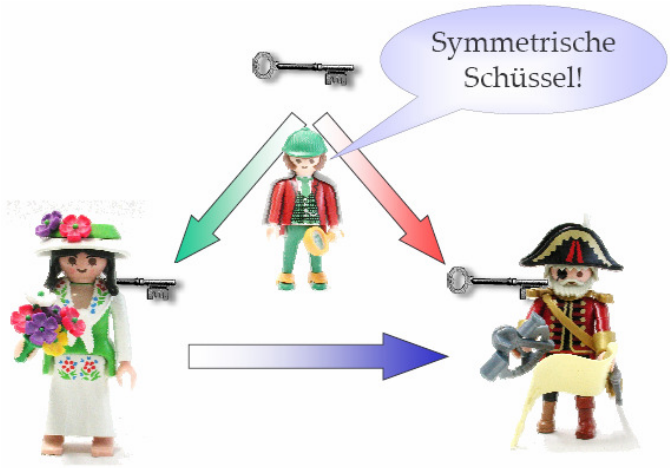
```
IHREMAJESTAETDIEKOENIGIN
+
GAUNERGAUNERGAUNERGAUNER
=
OHLRQRPEMGEVZDCROFKNCTME
```

One – Time – Pad (Einmalverschlüsselung)

Kleiderbügel einer Stasi-Spionin mit versteckten One-Time-Pad

- Zufallsfolge statt Worte als Schlüssel
- Absolut sicher!
- beweisbar
- damit einzigartig
- Problem: Schlüssellänge

Situation in der Neuzeit



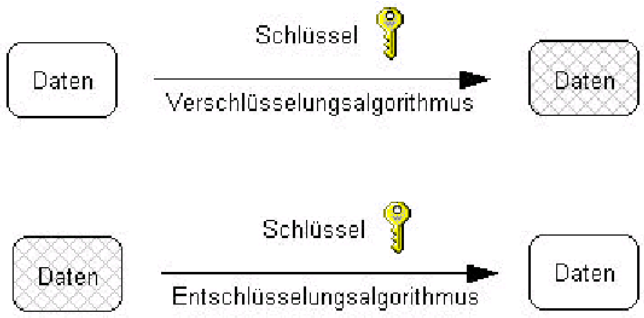
Was bedeutet symmetrisch?

- Allgemeines:
  - Verschlüsselungsalgorithmus E
    - Vorgehensweise, wie man eine Nachricht verschlüsselt
  - Entschlüsselungsalgorithmus D
    - Vorgehensweise, wie man eine Nachricht entschlüsselt
  - Schlüssel S_E und S_D
  - E (Klartext, S_E) => Ciphertext
  - D (Ciphertext, S_D) => Klartext
  - D (E (Klartext, S_E), S_D) => Klartext

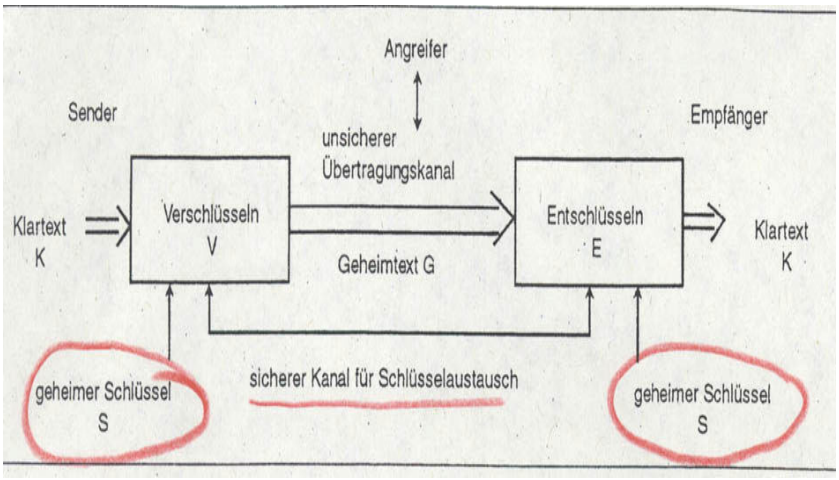
Was bedeutet symmetrisch?

- symmetrisch: $S_E = S_D$
- gleicher Schlüssel zum Verschlüsseln und Entschlüsseln
- meist gleicher Schlüssel zum Signieren und Verifizieren (etwas bestätigen/beglaubigen)
- je zwei Teilnehmer benötigen einen Schlüssel
- beide müssen Schlüssel streng geheim halten
- Anzahl der Schlüssel wächst quadratisch mit der Teilnehmerzahl

Was bedeutet symmetrisch?



Was bedeutet symmetrisch?



Vorteil und Nachteil (Symmetrie)

- Vorteil: große Datenmengen können schnell verschlüsselt werden
- Nachteil: sichere Verteilung des Schlüssels
  - Telefon, schriftlich, ...
- → Nicht für Verteilung über Internet geeignet

Symmetrische Verfahren

Es gibt:

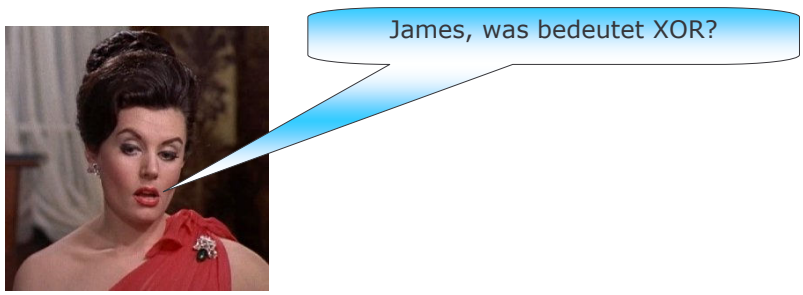
- Blockchiffre:
  - Algorithmus, der einen Datenblock von typisch 64 oder 128 Bit mittels eines Schlüsselwerts verschlüsselt
  - Eingabeblöcke fester Länge (z.B. 64 Bit)
  - Padding des letzten Blocks
  - Klartext liegt vollständig vor
  - Schlüssellänge: 112, 128 und 168 Bit
  - z.B.: DES, AES

Symmetrische Verfahren

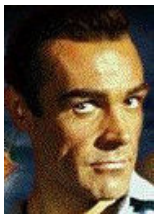
und

- Stromchiffre:
  - symmetrische, kontinuierliche und verzögerungsfreie Ver- oder Entschlüsselung eines Datenstroms
  - Pseudozufallszahlengenerator
  - Initialwert
  - kleinere Klartexteinheiten
  - RC4: XOR

Blockweise XOR-Funktion

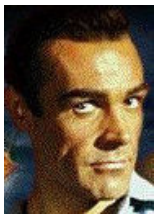


Blockweise XOR-Funktion



- bei diesem Verfahren werden die zu schützenden Daten in Blöcke der Länge n unterteilt (z.B. n = 8 Byte)
- z.B. bedeutet XOR-16, dass die gewählte Blocklänge 16 Byte ist
- beim Verfahren erfolgt zuerst eine blockweise XOR-Verknüpfung über die gesamten zu schützenden Daten

Blockweise XOR-Funktion



- das Ergebnis daraus wird den Daten als Prüfblock angehängt
- vor jeder Datenbenutzung kann dieses Verfahren von Neuem über alle Daten berechnet und das Ergebnis mit dem angehängten Prüfblock verglichen werden
- es können mit diesem Verfahren nur 1 Bit-Fehler pro Blockposition erkannt werden

Symmetrische Verfahren

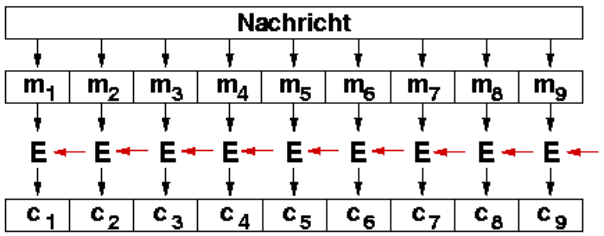
- Arbeitsweise bei Stromchiffre:
  - Schlüsselstrom wird erzeugt
  - Schlüsselstromgenerator (Pseudozufallsfolge: eine Folge von Zeichen, die nur mit Kenntnis des geheimen Schlüssels erzeugt werden kann)
  - jedes Zeichen des Schlüsselstroms mit dem Zeichen des Klartextes XOR verknüpft
  - auf Gegenseite Strom wieder entschlüsselt:
    - indem der chiffrierte Bitstrom wieder mit dem Output des genau selben Schlüsselstromgenerators XOR verknüpft wird (Generatoren muss auf beiden Seiten synchron arbeiten)

Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - ECB: Electronic Code Book
    - einzelne Verschlüsselung jedes Klartextblocks
    - stets gleicher Schlüssel
    - keine Fortpflanzung von Störungen

Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - ECB: Electronic Code Book
    - Verschlüsselung

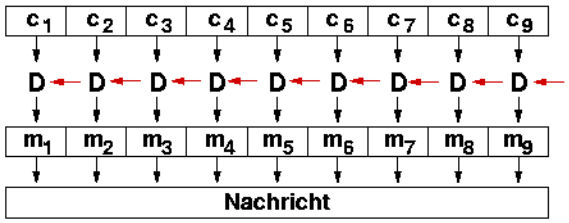


in Blöcke aufspalten

Verschlüsselung mit Secret Key

Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - ECB: Electronic Code Book
    - Entschlüsselung



Entschlüsselung mit Secret Key

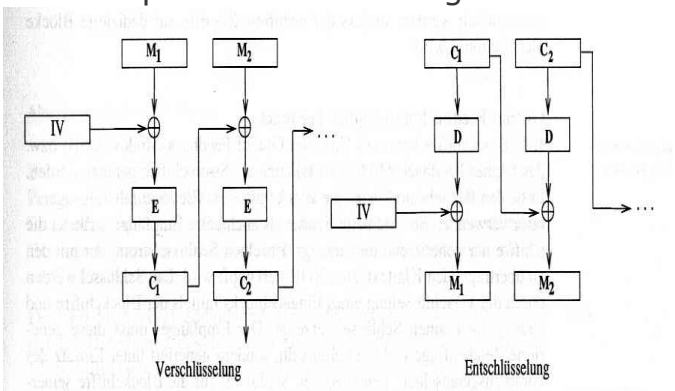
Blöcke wieder zusammenfügen

Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - CBC: Cipher Block Chaining
    - Verkettung der Blöcke
    - E (M_1 XOR IV, S_E) => C_1
    - E (M_2 XOR C_1, S_E) => C_2

Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - CBC: Cipher Block Chaining



Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - CBC: Cipher Block Chaining:
    - vor dem Verschlüsseln eines Klartextblocks wird dieser erst mit dem im letzten Schritt erzeugten Geheimtextblock per XOR verknüpft
    - die Verschlüsselung ist im CBC-Modus rekursiv definiert
    - zugehörige Entschlüsselung ist im CBC-Modus hingegen nicht rekursiv

Symmetrische Verfahren

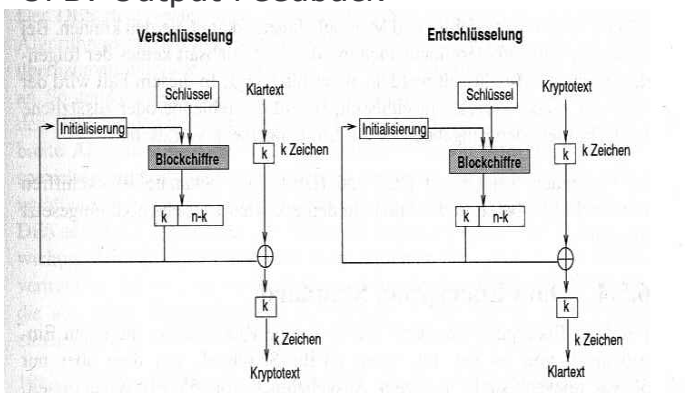
- Betriebsmodi von Blockchiffren:
  - CBC: Cipher Block Chaining Vorteile:
    - Klartextmuster werden zerstört
    - jeder Geheimtextblock hängt von allen vorherigen Klartextblöcken ab
    - identische Klartextblöcke ergeben unterschiedliche Geheimtexte
    - Angriffe werden erschwert

Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - Verwendung als Stromchiffre
    - Blockchiffre als Pseudozufallszahlengenerator

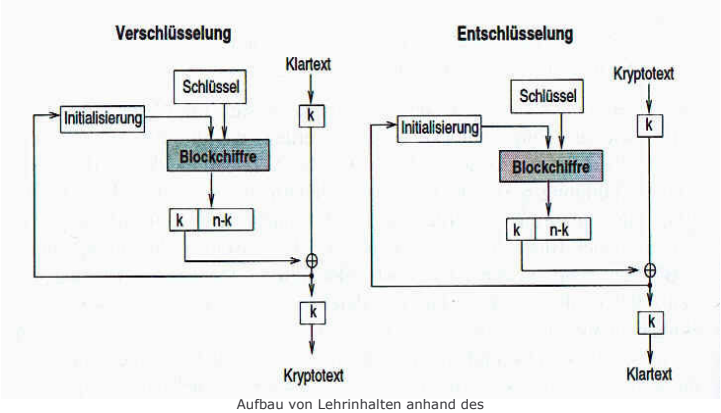
Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - OFB: Output Feedback



Symmetrische Verfahren

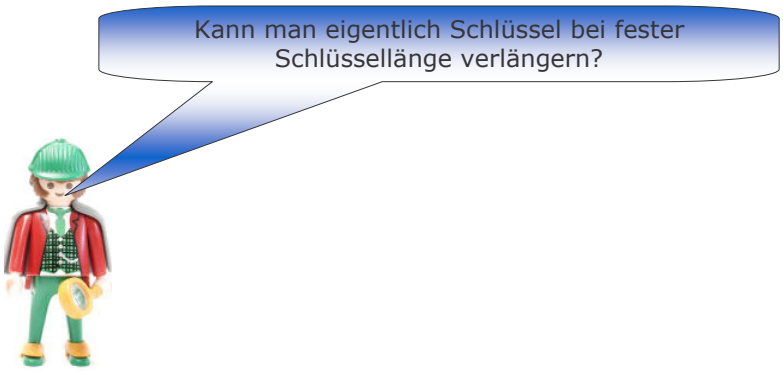
- Betriebsmodi von Blockchiffren:
  - CFB: Cipher Feedback



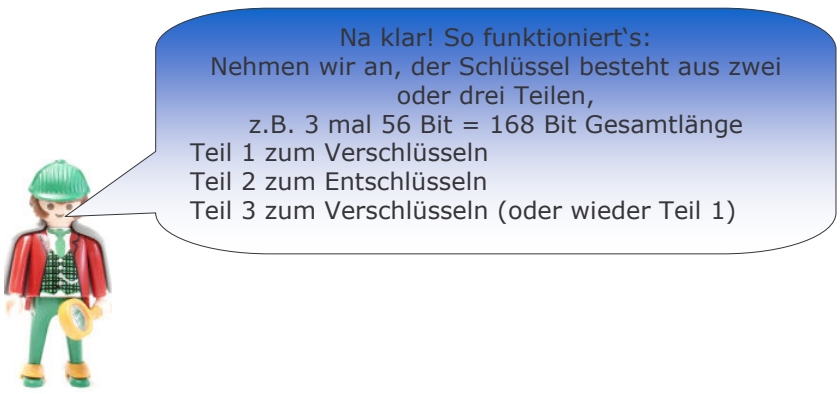
Symmetrische Verfahren

- Betriebsmodi von Blockchiffren:
  - bei CFB und OFB nutzt man eine Blockchiffre zur Konstruktion eines Pseudozufallszahlen-generators und verknüpft dessen Ausgabe über XOR mit dem Klar- bzw. Geheimtext
  - Auf diese Weise entsteht eine Stromchiffre
  - der Schlüsselstrom kann beim OFB im Gegensatz zum CFB beliebig weit vorausberechnet werden

Verlängerung von Schlüsseln



Verlängerung von Schlüsseln



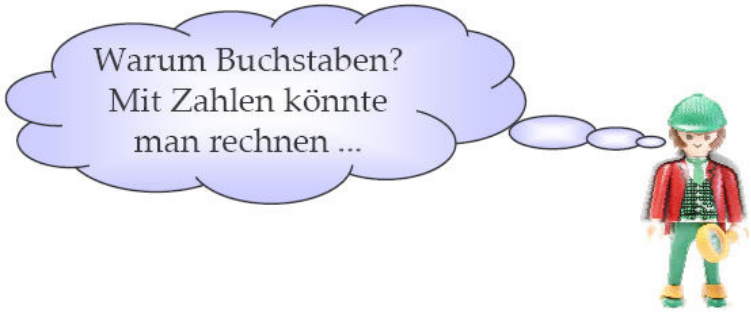
Verlängerung von Schlüsseln

Einwenig anschaulicher:

Mathematik 1

Buchstaben

ABCDEFGHIJKLMNOPQRSTUVWXYZ



Mathematik 1

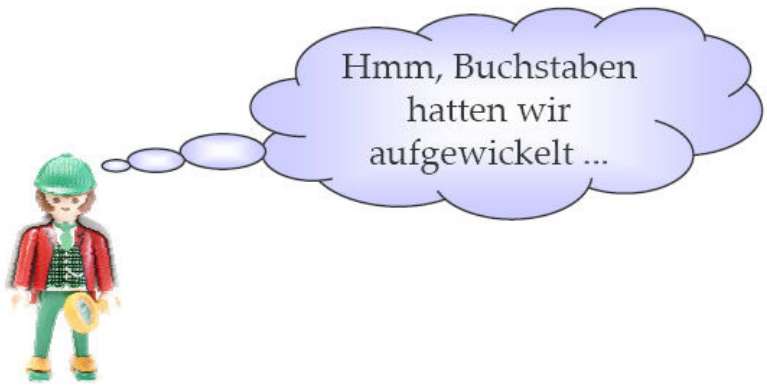
Zahlen statt Buchstaben

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

Vorteil: Zahlen können wir

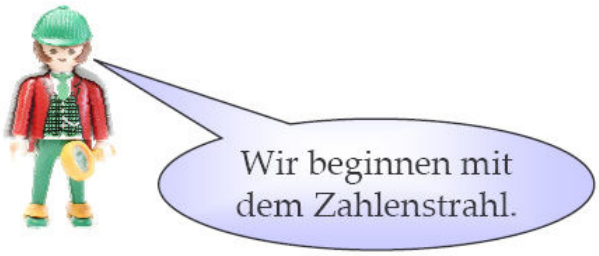
- addieren 17+10=27
- multiplizieren 10 . 5 =50

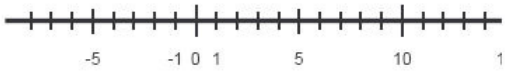
Mathematik 1



Mathematik 1

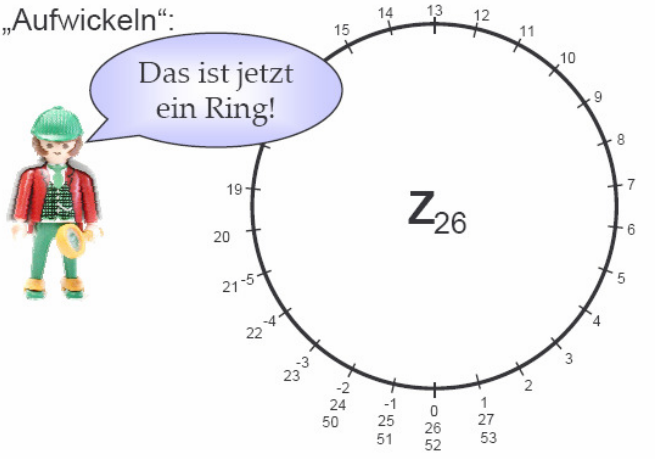
„Aufwickeln“





Mathematik 1

„Aufwickeln“:



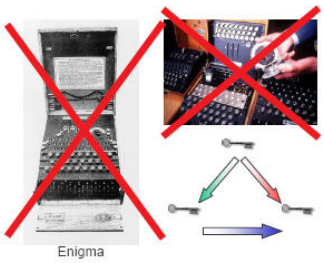
Mathematik 1

Im Ring $\mathbf{Z}_{26}$ können wir:

- Addieren: 17+10=1
- Multiplizieren: 10 . 5 =24

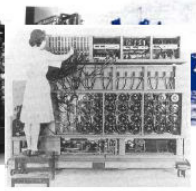
Übrigens, Mathematiker nennen das:
Rechnen Modulo 26

Kryptografie bis 1950


Enigma

Alan M. Turing (1912-1954)


Turing Bombe


NCR Bombe (Dayton,USA)


Bletchley Park Manson

Kryptografie heute

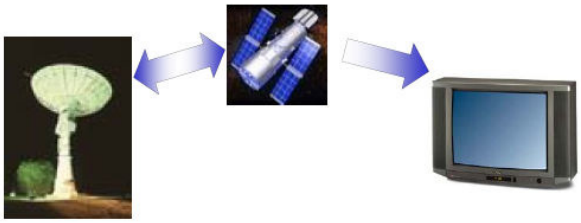
- Euroscheckkarten, Geldautomaten

Kryptografie heute

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken

Kryptografie heute

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, Pay TV



Kryptografie heute

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, Pay TV
- Telefon, Handy

Kryptografie heute

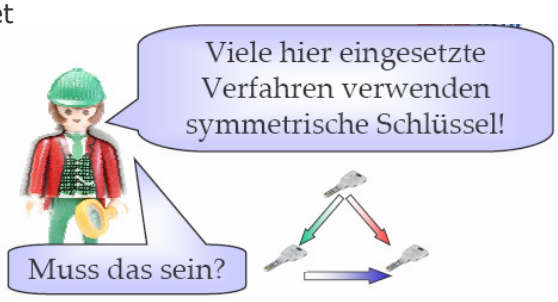
- Euroscheckkarten, Geldautomaten 
- Geldverkehr zwischen Banken 
- Satellitenfernsehen, Pay TV 
- Telefon, Handy 
- Einkauf im Internet

Kryptografie heute

- Euroscheckkarten, Geldautomaten 
- Geldverkehr zwischen Banken 
- Satellitenfernsehen, Pay TV 
- Telefon, Handy 
- Einkauf im Internet
- und vieles mehr …

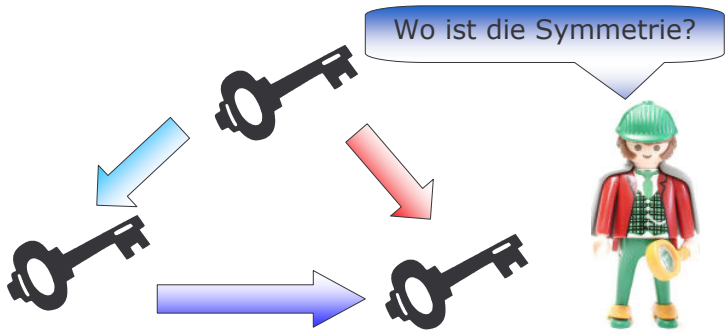
Kryptografie heute

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, Pay TV
- Telefon, Handy
- Einkauf im Internet
- und vieles mehr …



Ist Symmetrie notwendig?

Betrachten wir die Situation noch einmal:

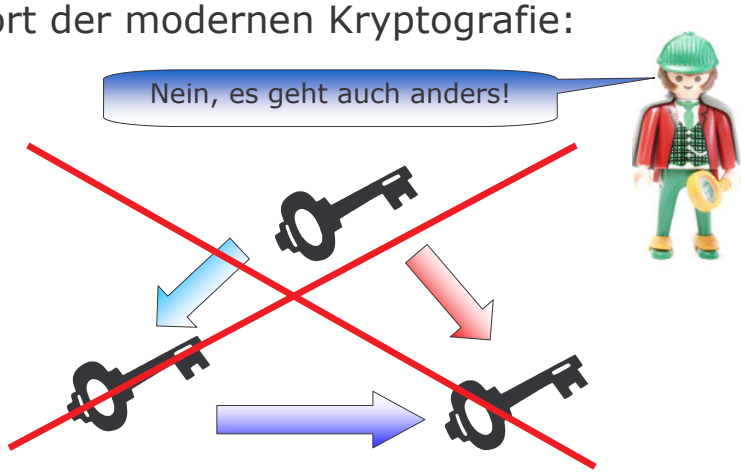


Ist Symmetrie notwendig?

Betrachten wir die Situation noch einmal:

Ist Symmetrie notwendig?

Antwort der modernen Kryptografie:



Ist Symmetrie notwendig?

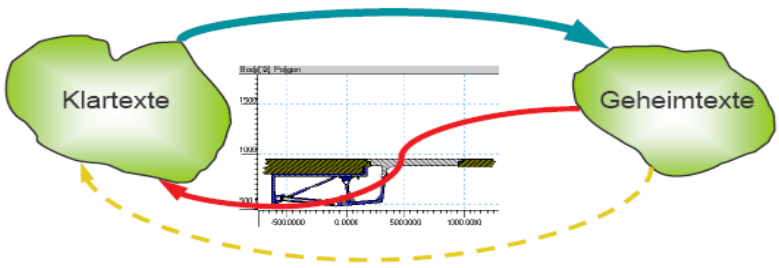
Diese Antwort geben schon

- 1970-74:Der Britische Geheimdienst CESG
- 1976: Diffie & Hellman
- 1978: Rivest, Shamir & Adleman:

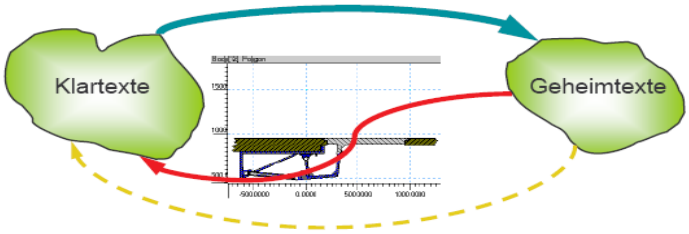
RSA

Ist Symmetrie notwendig?

Es geht ohne Symmetrie?! Ja, wie denn?
Mit einer Einwegfunktion mit Falltür:



Ist Symmetrie notwendig?



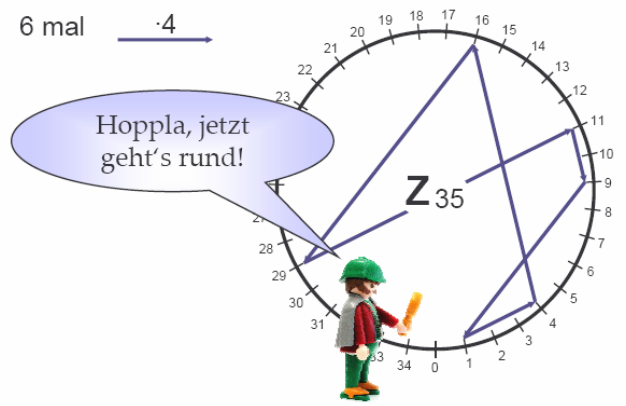
Verschlüsseln ist einfach.

Knacken ist schwer.

Entschlüsseln ist leicht mit der Falltür!

Mathematik 2

Potenzieren heißt mehrfach multiplizieren:

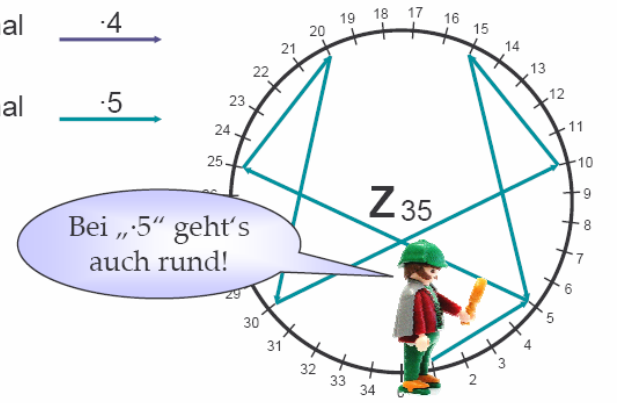


Mathematik 2

Potenzieren heißt mehrfach multiplizieren:

6 mal ·4

6 mal ·5



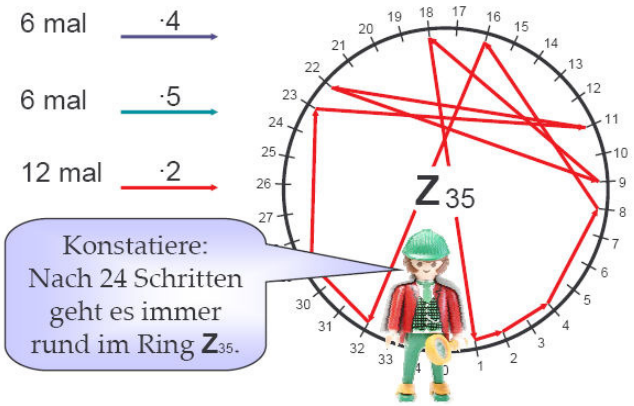
Mathematik 2

Potenzieren heißt mehrfach multiplizieren:

6 mal ·4

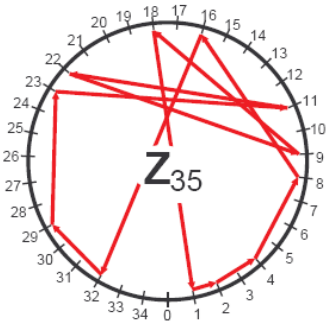
6 mal ·5

12 mal ·2



Mathematik 2

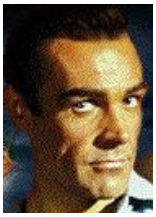
Wie bitte?
Q erklären Sie das!?



Ja, Bond. Die Mathematik sagt:

Weil 35=5.7 ist, hat Potenzieren im Ring $\mathbf{Z_{35}}$ *Wiederholfrequenz* L = 4.6 = 24.

RSA am Beispiel



Ja. Hallo?

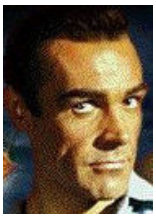
RSA am Beispiel



Moneypenny, hören Sie!
Ich brauche unbedingt die geheimen Informationen über Fort Knox. Aber Goldfinger darf sie nicht bekommen.

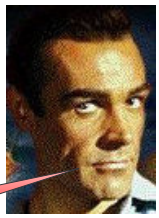
RSA am Beispiel





Ja, aber Q hat gestern alle Geheimschlüssel für ungültig erklärt …

RSA am Beispiel



Ja, ich weiß! Hören Sie zu,
Q hat mir für diesen Fall RSA
erklärt: Sagen Sie mir zuerst
wie lange der Text ist.

RSA am Beispiel

Na gut, auf Ihre
Verantwortung.
Es ist nur ein Buchstabe.

RSA am Beispiel

Hmm, jetzt brauche ich zwei Primzahlen, sagen wir: p=5 und q=7. Dann ist die Ringgröße N=p.q=35 groß genug und die Wiederholungsfrequenz L=(p-1).(q-1)=4.6=24.

RSA am Beispiel

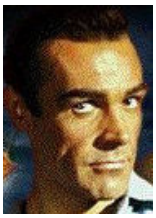
Weiters brauche ich noch zwei Zahlen e und d, so dass e.d=1+Vielfaches von L ist. Mein L=24 und e=5. Und jetzt müsste d=5 klappen, ja: 5.5=1+24.

RSA am Beispiel

OK, ich hab's. Mein öffentlicher Schlüssel ist N=35 und e=5. Nehmen Sie also bitte die Nummer x des Buchstaben im Ring $\mathbf{Z}_{35}$ fünfmal mit sich mal und sagen sie mir $y=x^e$, also in unserem Fall ist $y=x^5=x.x.x.x.x$

p=5, q=7.
N=35, L=24.
e=5, d=5.

RSA am Beispiel

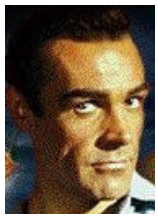


N=35, e=5.

p=5, q=7.
N=35, L=24.
e=5, d=5.

Was sie mir da wieder zumuten, Bond! Also ich rechne …

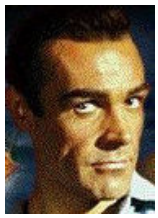
RSA am Beispiel



p=5, q=7.
N=35, L=24.
e=5, d=5.

Na, Bond glaubt wahrscheinlich, ich kann das nicht! Ha! Gut: N=35, e=5. Der Buchstabe ist ein D und x=4 ist die Zahl auf dem Ring. Also ist $y=x^e=4.4.4.4.4=9$.

RSA am Beispiel



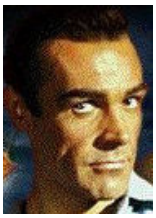
N=35, e=5.

p=5, q=7.
N=35, L=24.
e=5, d=5.

N=35, e=5,
x=4:
$y=x^e$
$=4.4.4.4.4=9$.

OK, y=9.

RSA am Beispiel

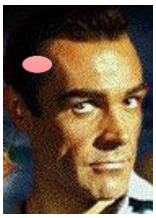


Danke, Moneypenny. Sie waren mir eine große Hilfe.

p=5, q=7.
N=35, L=24.
e=5, d=5.

N=35, e=5,
x=4:
$y=x^e$
=4.4.4.4.4=9.

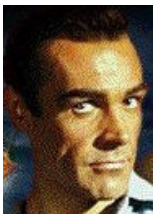
RSA am Beispiel



So, jetzt mal sehen:
N=35, d=5 und y=9.
Also ist das Ergebnis
$z=y^d=9.9.9.9.9=4$.
Also ist der
Buchstabe D!

p=5, q=7.
N=35, L=24.
e=5, d=5.

RSA am Beispiel



N=35, e=5.

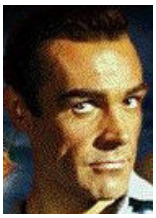
p=5, q=7.
N=35, L=24.
e=5, d=5.

N=35, e=5,
x=4:
$y=x^e$
=4.4.4.4.4=9.

y=9.

y=9:
$z=y^d$
=9.9.9.9.9=4.

RSA allgemein



N, e

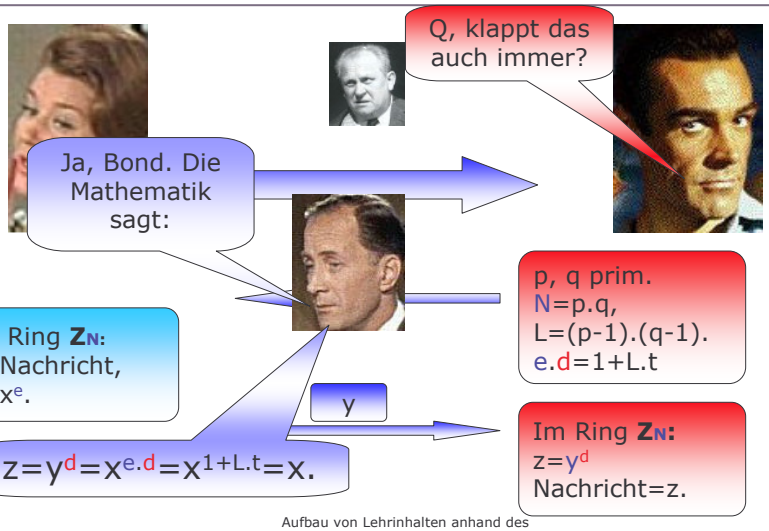
p, q prim.
N=p.q,
L=(p-1).(q-1).
e.d=1+L.t

Im Ring $\mathbf{Z_N}$:
x=Nachricht,
$y=x^e$.

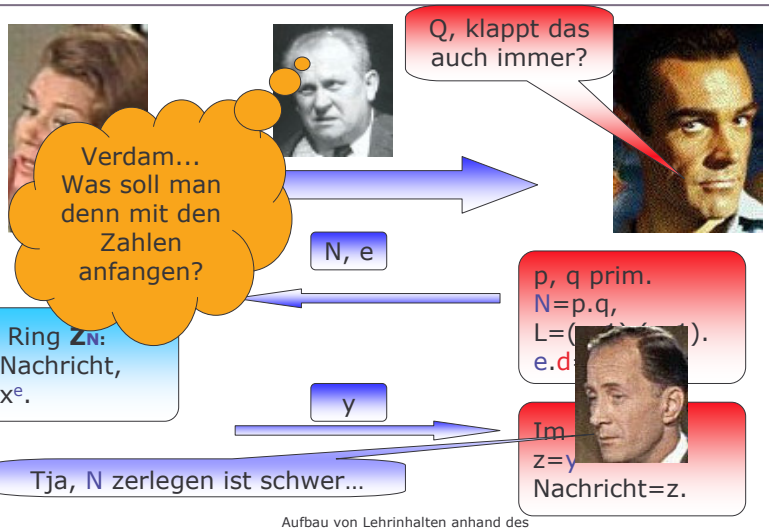
y

Im Ring $\mathbf{Z_N}$:
$z=y^d$
Nachricht=z.

RSA funktioniert



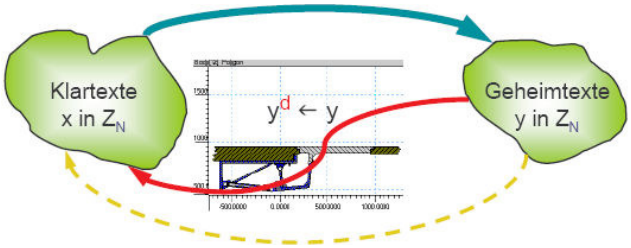
RSA angreifen



RSA Falltürfunktion

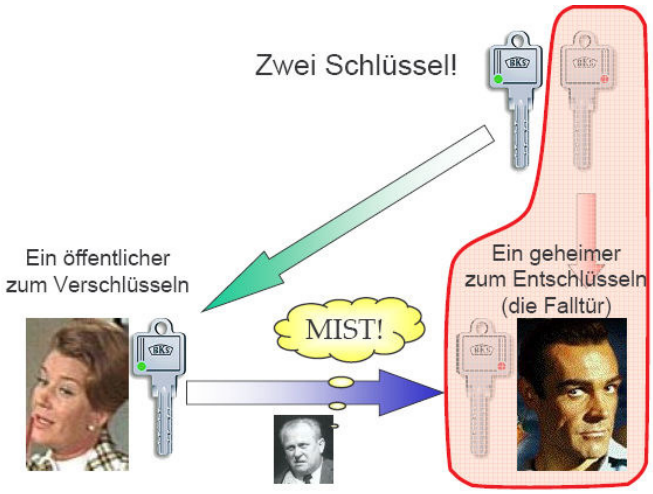
Und wo ist da die Falltürfunktion ?
Hier legen N und e die RSA-Falltürfunktion fest:

$x \rightarrow x^e$ im Ring $\mathbf{Z_N}$



Verschlüsseln ist einfach: N und e sind genug.
Knacken ist schwer.
Entschlüsseln ist leicht mit der Falltür d!

Situation bei RSA



Was bedeutet Asymmetrisch?

- das RSA Verfahren ist ein so genanntes asymmetrisches Verfahren
- haben nun gesehen, dass es nicht nur symmetrische Verfahren gibt
- zwischen dem Chiffrierschlüssel *K* und dem Dechiffrierschlüssel *K'* besteht kein "einfacher" Zusammenhang
- aus *K* nicht direkt auf *K'* zu schließen
  - Aufwand zu hoch

Was bedeutet Asymmetrisch?

- Erzeuger eines Schlüsselpaares behält den Dechiffrierschlüssel als geheimen Schlüssel (*Private Key*) für sich
- Chiffrierschlüssel als öffentlichen Schlüssel (*Public Key*) bekannt
- als Public-Key-Systeme bezeichnet
- jeder in der Lage unter Verwendung des öffentlichen Schlüssels eine Nachricht zu chiffrieren
- nur vom Besitzer des geheimen Schlüssel kann die Nachricht dechiffriert werden

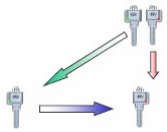
Vorteil und Nachteil (Asymmetrie)

- Vorteil: höhere Sicherheit
  (z.B. internetfähig)
- Nachteil: sehr langsam, deshalb nicht geeignet für größere Dateien

Moderne Kryptografie

- Moderne symmetrische Verfahren
  - gemeinsame Schlüssel
  - hohe Sicherheit
  - sehr schnell

- Verfahren wie RSA (Public Key)
  - asymmetrisch
  - keine gemeinsame Schlüssel
  - sehr hohe Sicherheit
  - nicht ganz so schnell



- Praxis: Beide Arten kombiniert
  - Hybride Verfahren

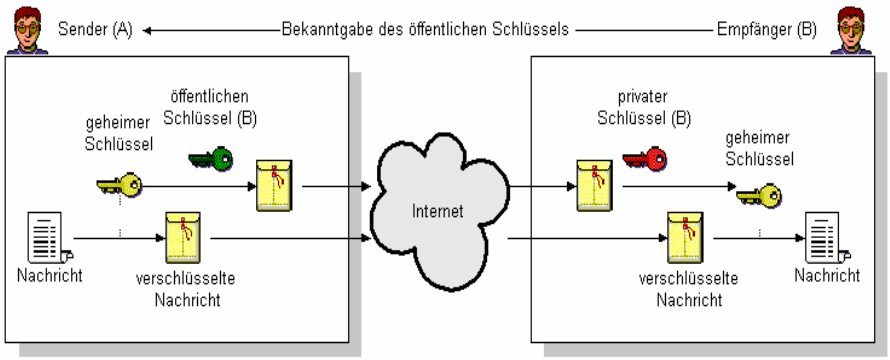
Hybride Verfahren

- symmetrische Verschlüsselung
- asymmetrischer Schlüsselaustausch
- Nachricht durch den Empfänger zunächst mit einem speziellen geheimen Schlüssel symmetrisch verschlüsselt
- anschließend wird dieser Schlüssel mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und übertragen

Hybride Verfahren

- Empfänger kann nun asymmetrisch mit seinem privaten Schlüssel den speziellen geheimen Schlüssel und somit die eigentliche Nachricht symmetrisch entschlüsseln

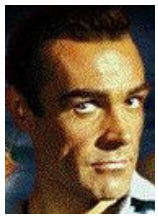
Beispiel eines Hybriden Verfahrens



Kryptoanalyse

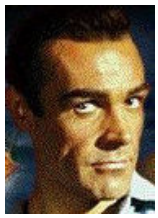
- Verschlüsselungsverfahren brechen, um damit eine geheime Nachricht lesen zu können
- sich als fremde Person oder Institution ausgeben können
- eine Nachricht unbemerkt verändern oder abfangen

Angriffsmöglichkeiten



Ich muss Bond Neuigkeiten von Fort Knox mitteilen: Neue Lieferung!

Angriffsmöglichkeiten



Tja, Pech gehabt! Hab die Nachricht abgefangen. Moneypenny hätte vorsichtiger sein müssen. Das Schlüsselwort „Bond" …

Angriffsmöglichkeiten

- man sucht nach den Schwachstellen eines Verschlüsselungsverfahrens
- Ansatzpunkte:
  - Eigenheiten der Sprache:
    - Buchstaben treten in einer Sprache in bestimmten Häufigkeiten auf
  - Eigenschaften der Chiffrierverfahren
    - es existieren direkte Abhängigkeiten zwischen Klartext, Schlüssel und Chiffre
  - Fehler der am Verschlüsselungsprozess beteiligten Personen
    - sorgloser Umgang mit Schlüsseln und Zugangsdaten
    - einfache Schlüssel

Angriffsmöglichkeiten

- Komplexität des Verschlüsselungsalgorithmus
  - z.B. Cäsar Verschlüsselung:
    es genügt eine einfache Häufigkeitsanalyse

Differentielle Kryptoanalyse

- aus Unterschieden im Klartext auf Unterschiede im verschlüsselten Text zu stoßen
- damit auf den Verschlüsselungsalgorithmus Rückschlüsse ziehen können

Lineare Kryptoanalyse

- basiert auf statistischen linearen Zusammenhängen zwischen Klartext, Geheimtext und Schlüssel
- man untersucht:
  - beliebig viele (gestohlene) Klartexte
  - und die zugehörigen, mit dem unbekannten Schlüssel chiffrierten (abgefangenen) Geheimtexte

Side-Channel Analysen

- eine Form der Schwachstellenanalyse
- Systeme werden über die Auswertung der Informationen aus Seitenkanälen angegriffen
- Seitenkanäle: z.B.:
  - Stromaufnahme von Komponenten,
  - elektromagnetische Abstrahlung
  - Ausführzeit von Operationen
- Attacken zielen nicht auf die theoretische Sicherheit der zugrunde liegenden Algorithmen ab
- sondern auf deren praktische Implementierung

Kryptoregulierungen

- Wunsch nach Reglementierung von Verschlüsselungsverfahren

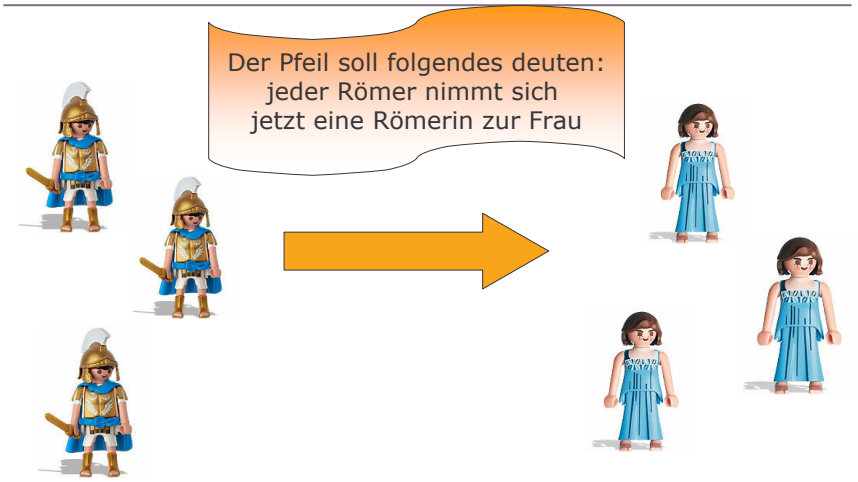
Mathematik 3

- Betrachten wir nun folgende Situation

Mathematik 3

- es gibt drei Römer und drei Römerinnen
- jeder Römer nimmt sich jetzt eine Römerin zur Frau:

Mathematik 3

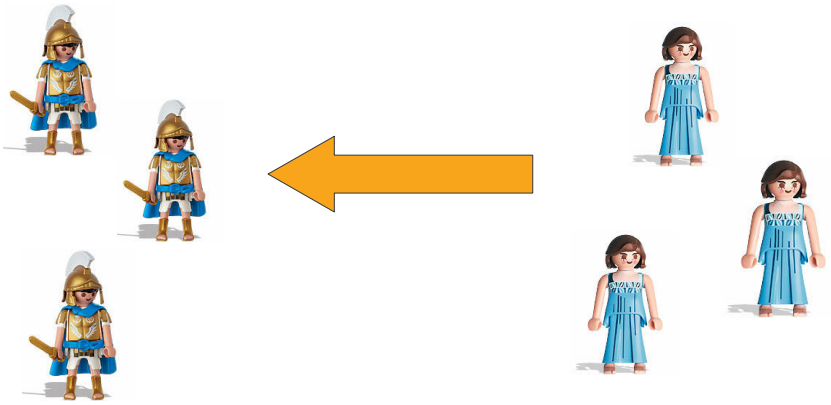


Mathematik 3

- folglich hat jetzt auch jede Römerin einen Mann

Mathematik 3

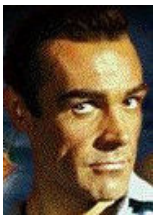
- das heißt, wir können den Pfeil auch umdrehen:



Mathematik 3

- In der Mathematik nennt man so einen Sachverhalt eine Funktion (f):
  - **Jedem** *x*-Wert aus dem Definitionsbereich wird **genau ein** y-Wert zugeordnet.
  - bei uns sind die x-Werte die Männer und die y-Werte die Frauen
  - der Definitionsbereich sind Männer bzw. Frauen

Mathematik 3



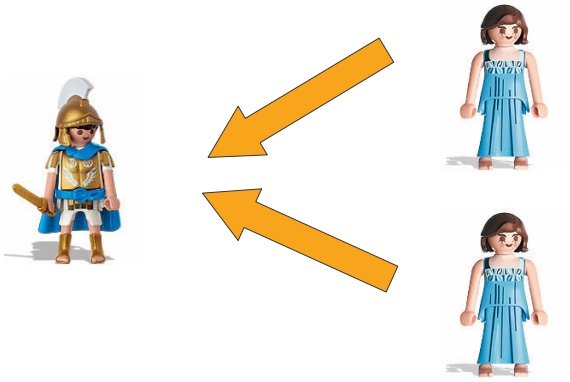
Sag mal James, hatten die Männer im alten Rom nicht mehrere Frauen gleichzeitig?

Mathematik 3

Du hast recht mein Engel! Ein Mann konnte durchaus mehrere Frauen haben. So wie …

Mathematik 3

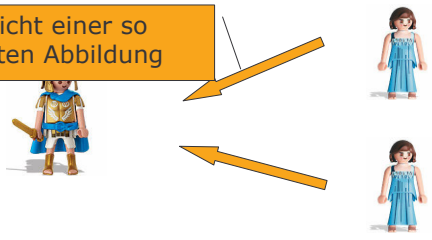
- Betrachten wir diese Situation:



Mathematik 3

- Aus der Sicht der Mathematik:
  - bezeichnen wir die Anzahl der Frauen als F und die Anzahl der Männer als M
  - so wird die Anzahl der Frauen (F) auf die Anzahl der Männer (M) „abgebildet“

entspricht einer so genannten Abbildung

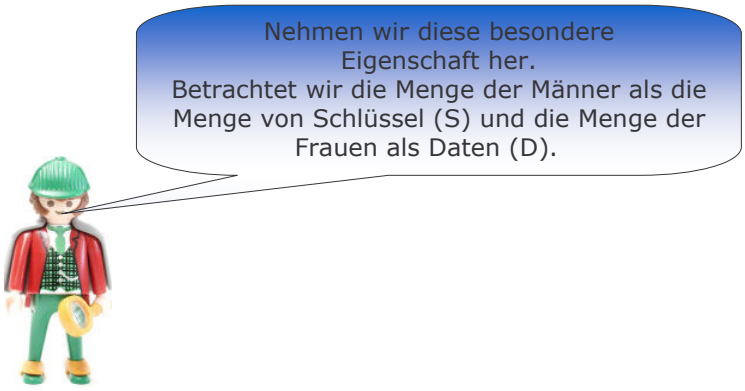


Mathematik 3

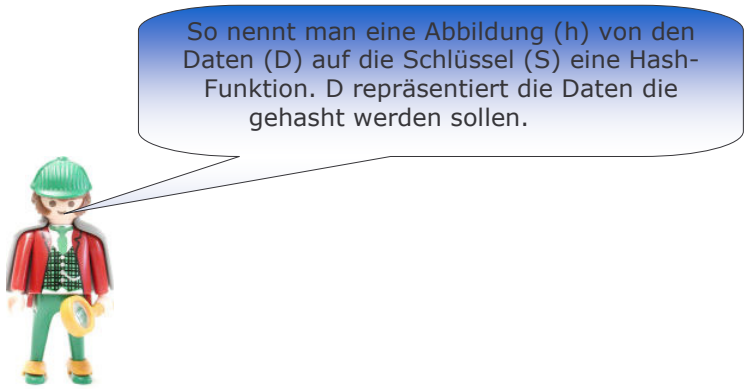
Nun ist die Anzahl der Männer kleiner als die Anzahl der Frauen!

- jede Frau gehört eindeutig zu einem Mann
- aber nicht jeder Mann gehört eindeutig zu einer Frau (sondern zu 2 oder mehreren)

Mathematik 3



Mathematik 3



Kriterien für gute Hash-Funkionen

- Eindeutigkeit
  - wiederholtes Berechnen des Hash-Wertes desselben Quellelements muss dasselbe Ergebnis liefern
- Effizenz
  - Funktion schnell berechenbar
  - kein großer Speicherbedarf
- Kollisionsfreiheit
  - ss sollen keine zwei Quellelemente mit demselben Hash-Wert auffindbar sein

Kriterien für gute Hash-Funkionen

- nicht umkehrbar
  - für ein gegebenes Zielelement soll kein passendes Quellelement zu finden sein
- mit einer Hash-Funktion können große Datenmengen in eine kleine Datenmenge (meist fixer Länge) übergeführt werden
- ein erneutes Aufrufen der Funktion unter Verwendung der Quelldaten liefert dasselbe Ergebnis

Übersicht über Hash-Verfahren

- SHA
- MD2, MD4, MD5
- RIPEMD-160
- Tiger
- HAVAL
- Whirlpool

Hash-Algorithmus SHA (SHA-1)

- secure hash algorithm (sicherer Hash-Algorithmus)
- aufgrund des großen Hashwertes und ausreichender Analysen wurde SHA als ausreichend für eine starke Hashfunktion eingestuft

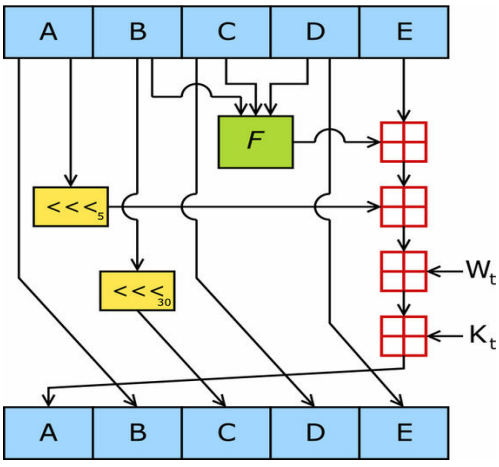
Hash-Algorithmus SHA (SHA-1)

- Algorithmus erzeugt einen 160 Bit Hashwert
- Objekt wir in *n* Blöcke zu je 512 Bit zerlegt
- jeder Block wird in 16 Worte zu je 32 Bit zerlegt
- die 16 Wörter werden mittels XOR-Operationen auf insgesamt 80 Wörter zu je 32 Bit vergrößert

Hash-Algorithmus SHA (SHA-1)

- für die 80 Verarbeitungsschritte stehen insgesamt 4 Nicht-Lineare Funktionen die für jeweils 16 Runden verwendet werden zur Verfügung
- zusätzlich: zwei Linksverschiebungen eingebaut

Hash-Algorithmus SHA (SHA-1)



Hash-Algorithmus MD5

- MD5 (*Message Digest Algorithm 5*) wurde 1991 von Rivest (MIT) entwickelt
- der MD5 entstand durch Verbesserungen aus dem MD4
- 1994 wurden die ersten Mängel gemeldet
- 1996 meldete Dobbertin eine Kollision in der Kompressionsfunktion von MD5. Dies war zwar kein Angriff auf die vollständige MD5-Funktion, dennoch empfahlen Kryptografen bereits damals, wenn möglich auf sicherere Algorithmen wie SHA-1 oder RIPEMD-160 umzusteigen.
- Im August 2004 fanden chinesische Kryptologen Kollisionen für die vollständige MD5-Funktion. Wie sich diese Entdeckung auf die Verwendung von MD5 auswirkt, bleibt abzuwarten.

Hash-Algorithmus MD5

- MD5-Hash erzeugt aus einer Nachricht ein 128 Bit langes Wort das normalerweise im Hexadezimalsystem notiert wird
- Grundfunktionen des Algorithmus teilweise die des SHA
- Konstanten nicht Bestandteil der Grundfunktion
- in jedem Verarbeitungsschritt wird eine andere Konstante verwendet

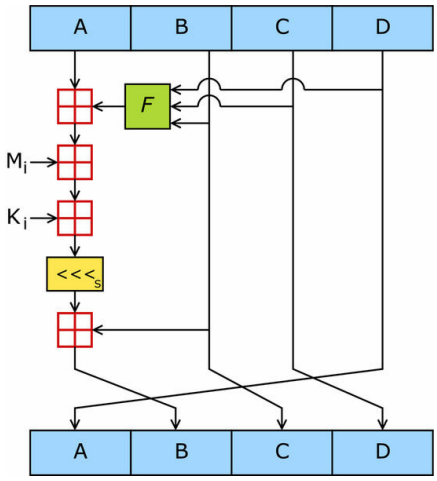
Hash-Algorithmus MD5

- die Eingabe wird so aufgefüllt, dass sie ohne Rest durch 512 teilbar ist
- dazu wird zunächst ein ‚1' und anschließend so lange ‚0' angehängt, bis 64 Bits zum auffüllen übrig bleiben
- Die letzten 64 Bits beinhalten die Datei-Länge
- Die Nachricht wird in 512 Bit Blöcke geteilt
- Der Algorithmus arbeitet mit einem 128 Bit Puffer

Hash-Algorithmus MD5

- der Puffer wird in vier 32 Bit Wörter, A, B, C und D, die für den ersten Block mit Konstanten initialisiert werden, eingeteilt
- Somit wird jeder Block in 16 32 Bit Einheiten eingeteilt
- so stehen uns 64 Operationen zur Verfügung
- Jeder 512 Bit Block wird also in vier Runden erledigt
- Jeder Runde steht eine andere Funktion zur Verfügung

Hash-Algorithmus MD5



RIPMED-16

- bis jetzt keine Angriffe gefunden
- baut auf MD4 auf
- frei zugänglich, kaum eingesetzt

TIGER

- ähnlich zum MD5
- arbeitet auf 64 Bit Systemen
- großer Performancegewinn gegenüber MD5

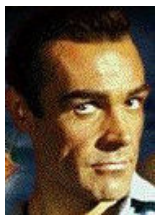
HAVAL

- Hashes variabler Länge zu erzeugen
- vor allem von 128 Bit, 160 Bit, 192 Bit, 224 Bit und 256 Bit
- variable Anzahl von Runden (3, 4, oder 5)

Whirlpool

- Whirlpool funktioniert mit Daten von weniger als 2^{256} Bit Größe und gibt einen Hash-Wert von 512 Bit aus

MAC (Message Authentication Code)

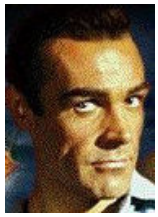


Hallo, James! Ich schicke Ihnen jetzt ein wichtiges Dokument!

MAC (Message Authentication Code)

- Kommunikation mit Hilfe von MACs

Wie weiß nun Bond, ob die Nachricht wirklich von Moneypenny ist?



MAC (Message Authentication Code)

- Kommunikation mit Hilfe von MACs

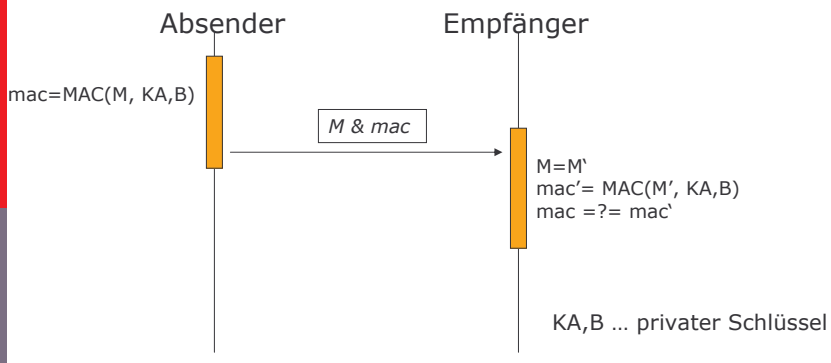
Das ist kein Problem! Eine Abhilfe für dieses Problem gibt der MAC!

MAC (Message Authentication Code)

- *Message Authetication Codes* werden dazu verwendet um den Datenursprung eines Dokuments sicherzustellen
- Grundlage dazu ist ein gemeinsamer, privater Schlüssel der in die Hashfunktion hineinfließt
- Schlüssel ist nur den Kommunikationspartner bekannt
- Schlüssel wird in diesem Fall MAC-Code genannt

MAC (Message Authentication Code)

- Kommunikation mit Hilfe von MACs



MAC (Message Authentication Code)

- Kommunikation mit Hilfe von MACs
  - Absender errechnet den MAC
    mac=MAC(M, KA,B)
    eines Dokuments *M* und schickt beide an den Empfänger
  - Empfänger erhält den MAC *mac* und die Nachricht *M'*
  - mit seinem privaten Schlüssel *KA,B* errechnet er sich den MAC *mac'= MAC(M', KA,B)*
  - stimmen mac und mac', also
    MAC(M, KA,B)=mac=mac'= MAC(M', KA,B),
    überein so wurde das Dokument vom Absender selber verschickt

Digitale Signatur

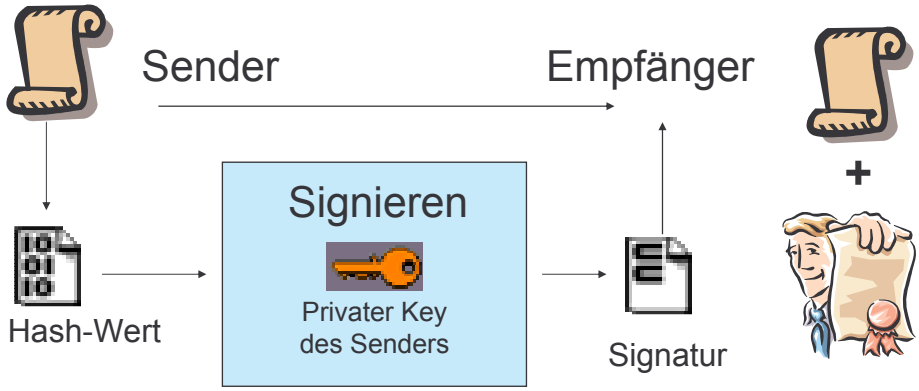
- das elektronische Äquivalent zur eigenhändigen Unterschrift
- elektronische Unterschrift mit folgenden Anforderungen:
  - Verifizierbarkeit: jeder kann die Echtheit der Unterschrift überprüfen
  - Fälschungssicherheit: nur der Besitzer kann die Unterschrift erzeugen
  - Verbindlichkeit: der Signator kann die Unterschrift nicht nachträglich leugnen

Digitale Signatur

- Funktionsweise:
  - Sender:
    - zuerst wird der Hashwert der zu sendenden Nachricht ermittelt, welcher dann vom Sender mit dessen privaten Schlüssel verschlüsselt wird
    - verschlüsselte Teil wird schließlich an die Nachricht angehängt
  - Empfänger:
    - bei Empfang der Nachricht ermittelt der Empfänger den Hashwert der Nachricht ohne Signatur, und vergleicht ihn mit der mit dem öffentlichen Schlüssel des Empfängers entschlüsselten Signatur
    - ist der Wert gleich, weiß man auch ob man den Absender wirklich kennt und ob die Nachricht verändert wurde

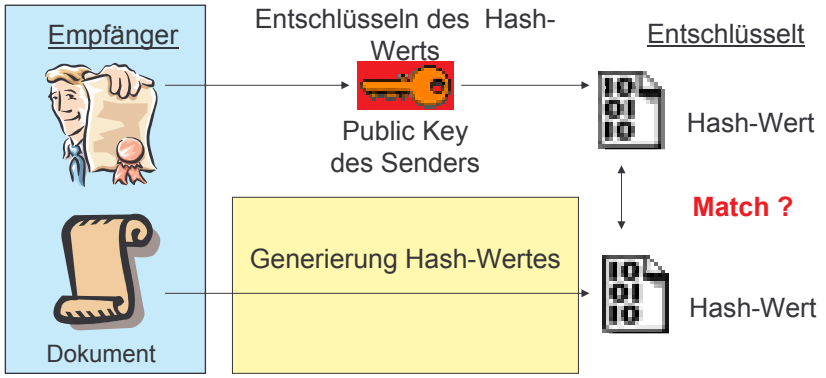
Digitale Signatur

Beispiel 1: Signier-Prozess



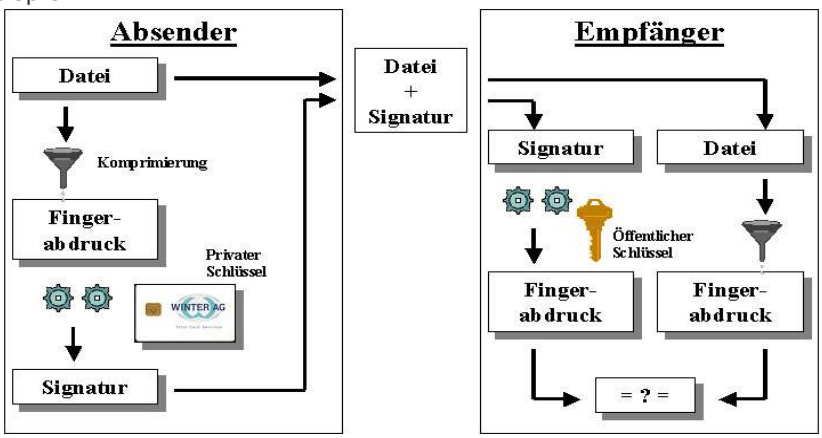
Digitale Signatur

Beispiel 1: Überprüfungs-Prozess



Digitale Signatur

Beispiel 2:



Digitale Signatur

- rechtliche Relevanz:
  Nun stellt sich die Frage der Rechtswirkung solcher Digitalen Signatur:
  - Inwiefern kommt eine Digitale Signatur einer normalen Unterschrift gleich?

  In Österreich finden sich die Antworten auf diese Frage im Signaturgesetz (SigG) nähers findet man unter

  www.ris.bka.gv.at
  http://www.signatur.rtr.at/repository/legal-directive-20000119-de.pdf (EU-Signaturrichtline)

  Man unterscheidet 2 Arten der Elektronischen Signatur:

Digitale Signatur

- „einfache" Elektronische Signatur:
  - kein oder nur ein einfaches Zertifikat
  - keine strengen Richtlinien
  - kann als Beweis verwendet werden (freie richterliche Beweiswürdigung)
  - Anwendung bei private Kommunikation (z.B: zum Signieren von E-Mails)

Digitale Signatur

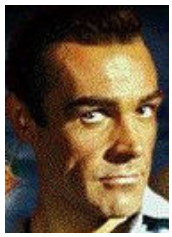
- sichere elektronische Signatur
  - erfüllt das rechtliche Erfordernis der Schriftlichkeit (mit Ausnahmen gleiche Wirkung wie eigenhändige Unterschrift)
  - beruht auf qualifiziertes Zertifikat
  - kann ausschließlich dem Signator zugeordnet werden
  - Sicherheitsanforderung des Bundesgesetzes

Digitale Signatur

- In folgenden Fälle gilt keine sichere elektronische Signatur:
  - Rechtsgeschäfte des Familien und Erbrechts wie z.B. Testamente
  - anderen Rechtsgeschäfte, die z.B. eine richterliche oder notarielle Beglaubigung oder auch eine Notariatsakt für ihre Gültigkeit benötigen
  - Rechtsgeschäfte, die eine Eintragung ins Grundbuch, Firmenbuch oder andere öffentliche Register zu Folge haben und dafür eine notarielle Beglaubigung benötigen
  - Bürgschaftserklärungen, die von Privatpersonen fernab von ihrer geschäftlichen, beruflichen oder gewerblichen Tätigkeit abgegeben werden

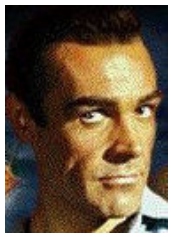
Digitale Signatur

Wie wird so eine Digitale Signatur erzeugt?



Digitale Signatur

Der so genannte Digital Signature Standard (DSS) dient der Erzeugung von digitalen Signaturen. Der DSS besteht aus dem Digital Signature Algorithm. Die Benutzung des Digital Signature Standard ist übrigens frei.



Digitale Signatur

- Zertifikate:

  Es gibt 2 Arten:
  - einfaches Zertifikat
  - qualifiziertes Zertifikat
- ss handelt sich hier prinzipiell um eine Bescheinigung mit der man einen öffentlichen Schlüssel einer Person zu ordnen kann

Digitale Signatur

- einfaches Zertifikat:
  - nicht direkt im Gesetz erwähnt
  - grundsätzlich einfach: elektronische Bescheinigung mit Prüfdaten mit denen man eine öffentlichen Schlüssel einer Person zuordnen kann
  - einfacher zu erhalten, z.B. Zertifikate bei E-Mailversand

Digitale Signatur

- qualifiziertes Zertifikat:
  - Voraussetzung für sichere elektronische Signatur muss nach den Anforderung des §5 Signaturgesetz mindestes folgendes enthalten:
    - Es muss einen Hinweis enthalten, dass es sich um ein qualifiziertes Zertifikat handelt.
    - Es muss ein unverwechselbarer Name des Zertifizierungsdienstanbieters und dessen Anschrift enthalten sein.
    - Es müssen der Name des Signators oder dessen Pseudonym enthalten sein.
    - Es könnten auf Verlangen des Signator die Vertretungsmacht oder andere rechtlich erhebliche Angaben zu diesem enthalten sein.
    - Es müssen die elektronischen Prüfdaten des Signators enthalten sein.

Digitale Signatur

- qualifiziertes Zertifikat:
  - Voraussetzung für sicher elektronische Signatur muss nach den Anforderung des §5 Signaturgesetz mindestes folgendes enthalten:
    - Es muss die Gültigkeitsdauer angegeben werden.
    - Das Zertifikat muss eine eindeutige Kennung haben.
    - Auf Verlangen des Signators kann ein Transaktionsrahmen angeben werden.
    - Auf Verlange des Signators können weitere rechtserhebliche Angaben gemacht werden.
    - Das Zertifikat muss mit der sicheren elektronischen Signatur des Zertifizierungsdienstanbieters signiert sein.

Digitale Signatur

- Zertifizierungsdienstanbieter:
  - autorisierte Stelle zur Erstellung von Zertifikaten
  - Aufgaben: Erstellung, Verlängerung, Widerruf, Verzeichnisdienst usw. von Zertifikaten
  - unterschiedliche Anforderung abhängig von auszustellenden Zertifikaten

Digitale Signatur

- Zertifizierungsdienstanbieter:
  - es gibt Aufsichtsbehörden, die diese vor allem im Zusammenhang mit der sicheren elektronischen Signatur kontrollieren
  - In Österreich ist das die **T**elekom**k**ontrol**k**omission (TKK) www.rtr.at
  - weiteren Informationen zu Zertifizierungsdienstanbietern finden man im Signaturgesetz in den §§6-26

Digitale Signatur

- Digitale Signatur in Österreich:
  - Weg meistens über A-Trust

    www.asign.at , www.trust.at
  - Partner meist Bank und Postfilialen
  - verschieden Produkte
    - a.sign premium (sichere elekt. Signatur)
    - a.sign token („einfache" elekt. Signatur)
    - a.sign light („einfache" elekt. Signatur)
    - a.sign client (Standard-Software)
    - a.sign developer (zum Signieren von Programmen)

Digitale Signatur

- Was braucht man zusätzlich zur Registrierung?
  - signaturfähige Bankomatkarte

    siehe www.maestro.at

    oder Bürgerkarte (im falle von a.sign Premium) sonst andere Signaturkarte
  - Kartenleser
  - Software

Digitale Signatur

- Bürgerkarte:
  - grundsätzlich eine Karte mit sichere elektronischer Signatur
  - Möglichkeit in Österreich Amtsgeschäfte übers Web zu erledigen

    Beispiele: Studienbeihilfe, Einkommenssteuererklärung etc.

    Nähere Information darüber unter:

    www.buergerkarte.at

Digitale Signatur

- Variante:
  - Maestrokarte oder A-Trust Bürgerkarte
  - e-card www.chipkarte.at
  - A1-Signatur über das Handy http://www.a1.net/privat/a1signatur
  - etc.

Digitale Signatur

- Vorteile:
  - Elektronische Unterschrift ist sicherer als händische Unterschrift
    - sichert das ganze Dokument
    - enthält geheime Komponente
  - rasch weltweit übertragbar
  - rechtsgültig (Signaturgesetz)
  - einfach und elektronisch archivierbar
  - sichert innerbetriebliche „Kultur"

Digitale Signatur

- Wirtschaftliche Bedeutung:
  - hohes Rationalisierungspotenzial in Wirtschaft und öffentlicher Verwaltung
    - raschere Übermittlung von rechtssicheren Anboten, Bestellungen, Verträgen
    - effizientere Kommunikation von Bürgern und Unternehmen mit der öff. Verwaltung
    - fälschungssichere Kommunikation
    - elektronische Archivierung

Public Key Infrastrukturen

- System, das digitale Zertifikate ausstellt
- digitale Zertifikate:
  - bestätigen die Zugehörigkeit eines kryptografischen Schlüssels zu
    - einer Person/Firma/Institution
    - einer Maschine (z.B. Website-Verkehr)

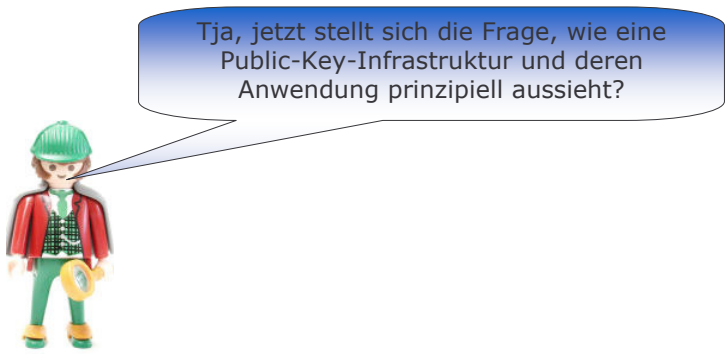
Public Key Infrastrukturen

- Die Komponenten einer Public-Key-Infrastruktur:
  - **Policy (Politik)**
    - Sicherheitskonzept
    - Benutzerrichtlinien
    - Organisations- und Arbeitsanweisungen
  - **RA - Registration Authority (Registrierungsstelle)**
    - Schnittstelle zum Teilnehmer
    - Identitätsfeststellung (inkl. Registrierung) der Teilnehmer entsprechend der Policy
  - **CA - Certification Authority (Zertifizierungsstelle**)
    - Schlüsselgenerierung für die Zertifizierungsstelle
    - Zertifizierung öffentlicher Teilnehmerschlüssel, Attribute
    - Personalisierung des PSEs für Zertifikat, Schlüsselpaar etc.

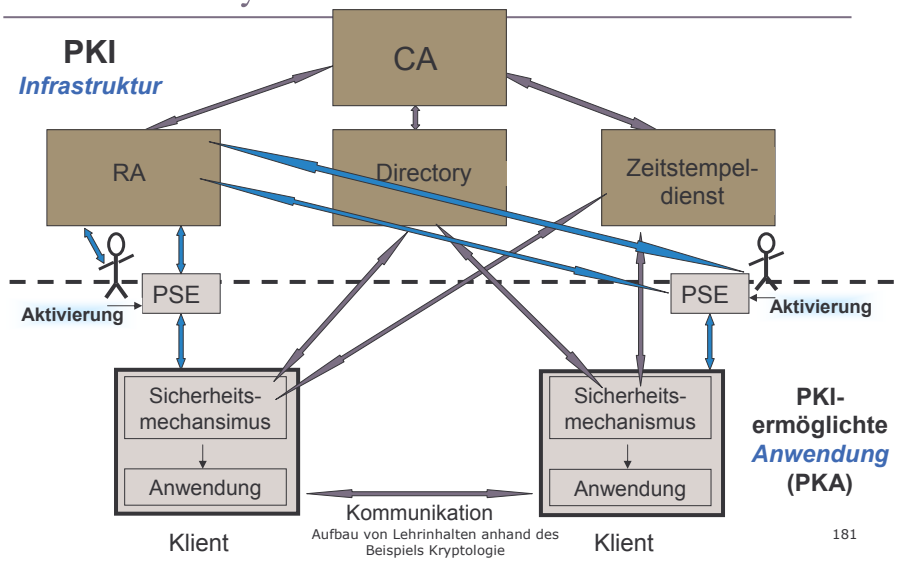
Public Key Infrastrukturen

- Die Komponenten einer Public-Key-Infrastruktur:
  - **Zeitstempeldienst**
    - Service für die Erstellung gesicherter Zeitsignaturen gemäß Policy
  - **DIR - Directory Services**
    - Verzeichnisdienst für Zertifikate und Sperrlisten
  - **PSE (Personal Security Environment)**
    - Sammlung aller sicherheitsrelevanter Daten (Zertifikate und die geheimen Schlüssel des Teilnehmers sowie der öffentliche Schlüssel der Zertifizierungsinstanz)

Public Key Infrastrukturen



Public Key Infrastrukturen



Public Key Infrastrukturen

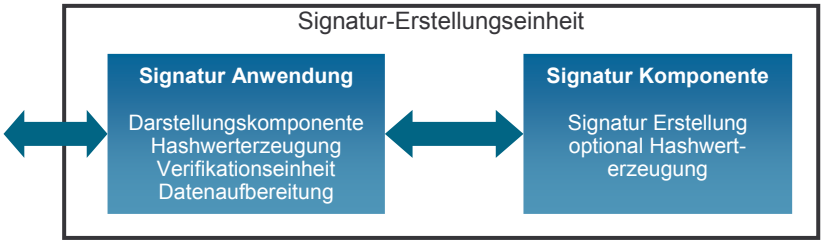
- Aufgaben einer PKI:
  - **Betrieb von Registrierungsstellen (RA)**
    - Benutzeranfragen zur Zertifizierung erfassen
    - Identifizierung der Benutzer
    - Weiterleitung des Antrages an die CA
  - **Vergabe von eindeutigen Identitäten (CA)**
    - gemäß der Identitätsfeststellung der RA
  - **Herausgabe und Verwaltung von Zertifikaten (CA)**
    für die Verifizierung von:
    - öffentlichen Schlüsseln
    - Attributen (Position/Rechte im Unternehmen, ...)
  - **Bereitstellung von Verzeichnissen für**
    - Zertifikate
    - Sperrliste für Zertifikate (CRL)
  - **Bereitstellung von Zusatzdiensten (Zeitstempel u.a.)**

Public Key Infrastrukturen

- Was ist eine PKI-enabled Application (PKA) (PKI-ermöglichte Anwendung)?
  - ein Anwendung, die von der Public-Key-Infrastruktur zur Verfügung gestellten Sicherheitsdienste nutzt, um eine vertrauenswürdige Anwendung zu realisieren

Public Key Infrastrukturen

- Was ist eine PKI-enabled Application (PKA) (PKI-ermöglichte Anwendung)?
  - Beispiel digitale Signatur: eine Signatur-Erstellungseinheit besteht immer aus einer Signaturkomponente, die die Signatur erzeugt und der Signatur Anwendung



Public Key Infrastrukturen

- Ziele von PKIs und PKAs.

Mehr Vertrauenswürdigkeit in den Geschäftsprozessen

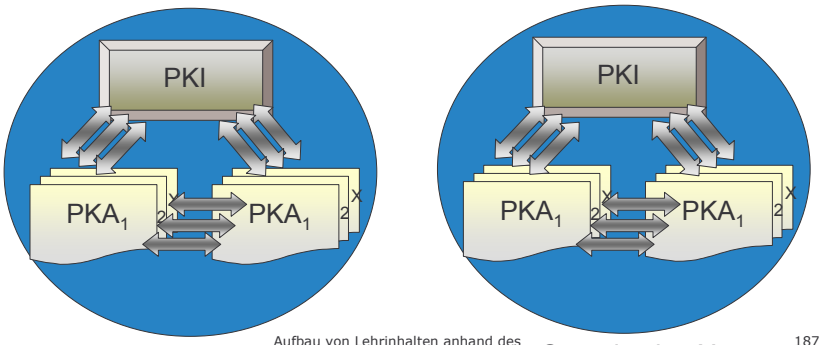
Anforderungen:		Lösungen:
Authentizität	→	Signatur
Integrität	→	Signatur
Verbindlichkeit	→	Signatur
Einmaligkeit	→	TimeStamp
Vertraulichkeit	→	Verschlüsselung

Public Key Infrastrukturen

- Nutzung von Public-Key-Infrastrukturen
  - PKIs sind kein Selbstzweck!
  - Sicherheitsinfrastrukturen bilden eine Basis für vertrauenswürdige Anwendungen (PKI-enabled Applications) wie:
    - E-Mail
    - Dokumente (Word, Excel, PowerPoint, ...)
    - Transaktionen (EDIFACT, XML, ...)
    - SSL-Kommunikation
    - VPN-Kommunikation
    - Identifikations- und Authentifikationsprozesse (Anthentifikation: Vorgang der Überprüfung der Identität eines Gegenübers)
    - Bezahlsysteme
    - ...

Public Key Infrastrukturen

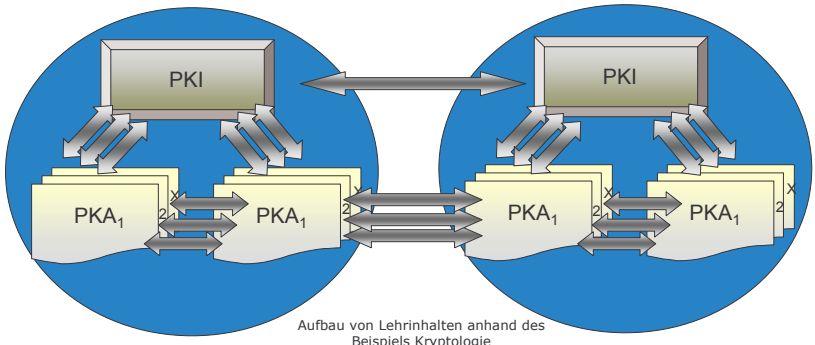
- Modelle von Public-Key-Infrastrukturen
  - Geschlossene Systeme:
    - eine Organisation betreibt die PKI für eine oder mehrere Anwendungen, die in ihrem eigenen Verantwortungsbereich liegen



Organisation 1 Organisation X

Public Key Infrastrukturen

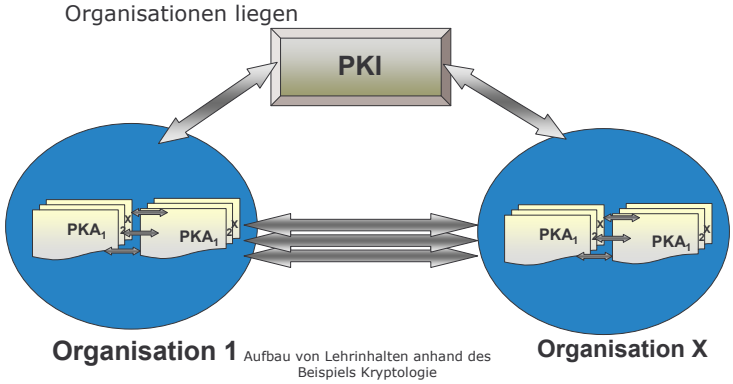
- Modelle von Public-Key-Infrastrukturen
  - Offene Systeme :
    - Organisationen betreiben PKIs für eine oder mehrere Anwendungen. Die Verantwortung liegt bei der jeweiligen Organisation



Organisation 1 Organisation X

Public Key Infrastrukturen

- Modelle von Public-Key-Infrastrukturen
  - Offene Systeme :
    - ein PKI-Anbieter betreibt die PKI für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der nutzenden Organisationen liegen



Public Key Infrastrukturen

- Probleme in der Praxis:
  - **Bei geschlossenen Systemen**
    - Nicht nutzbar für organisationsübergreifende Prozesse
      -> sehr starke Einschränkung
  - **Bei offenen Systemen**
    - unterschiedliche Policies
      - Sicherheitslevel/Modell
        - Personenbezogen (Kostengesichtspunkt):
          - nach dem Signaturgesetz
          - nicht nach dem Signaturgesetz
        - dienstbezogen
        - unterschiedliche PSEs

Public Key Infrastrukturen

- Probleme in der Praxis:
  - **Bei offenen Systemen**
    - Vertrauen in die Sicherheit der Lösung
    - Standards
      (sehr viele, sehr komplex, ständige Weiterentwicklung, ...)
    - verschiedene Anwendungen haben unterschiedliche Anforderungen (SSL, E-Mail, ...)

Public Key Infrastrukturen

- Probleme in der Praxis:
  - **Unterschiedliche Verantwortung von PKIs und PKAs in den Unternehmen**
    - die Abhängigkeit voneinander
    - erst mehrere PKAs führen zu hohem Nutzen
  - **Henne-Ei-Problem**
    - nur wenn viele mitmachen, dann macht es ökonomisch Sinn
  - **hoher personeller und organisatorischer Aufwand**
    - Sensibilisierung der Anwender für die IT-Sicherheit
    - Schulung der Anwender auf die Produkte
  - **Key-Recovery bei der Verschlüsselung**
  - **...**

Public Key Infrastrukturen

- Umsetzungskonzepte:
  - Verschiedene Anwendungen haben unterschiedliche Sicherheitsbedürfnisse!
  - Unterschiedliche Sicherheitsbedürfnisse können isoliert einfacher realisiert werden!
  - Isolierte Lösungen haben einen klareren Fokus!
  - Ein klarerer Fokus hat wenige Probleme und ist daher schnell, einfacher und kostengünstiger zu realisieren.
  - **Wir brauchen pragmatische Ansätze!**

Public Key Infrastrukturen

- Umsetzungskonzepte z.B.: SSL
  - Vertrauliche Kommunikation zwischen Client und Web-Server
    - die ausgetauschten Daten sollen nicht mitgelesen werden
    - eine explizite Datenschutzanforderung!
    - Infrastruktur ist bereits heute schon vorhanden, PKI etabliert, Clients unterstützen den Standard (Browser)
    - Web Server sind für die SSL Verschlüsselung vorbereitet
    - SSL als Open Source etabliert im Markt
    - Industrie hat den Markt erkannt
    - Aspekt der leichten Anwendbarkeit (integrierte Zertifikate)

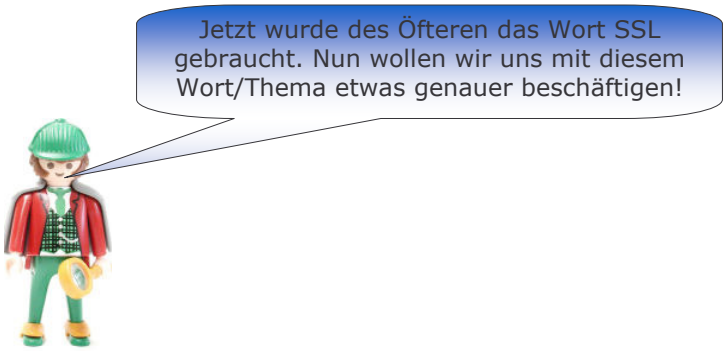
Public Key Infrastrukturen

- Umsetzungskonzepte z.B.: E-Mail-Sicherheit
  - zu schützende Unternehmensdaten sollen ausgetauscht werden (personenorientiert)
  - Vertraulichkeit der Kommunikation zwischen sich kennenden Personen ist von zentraler Bedeutung!
  - Verbindlichkeit, wenn eine kostenintensive Aktion aus der E-Mail abgeleitet wird
  - E-Mail als Medium ist dem Nutzer bekannt und vertraut, sicherheitsrelevante Funktionen sollen sich verständlich in das Benutzerinterface einfügen, um den Nutzer nicht zu verwirren
  - bei der E-Mail-Sicherheit hat der Benutzer eine aktive Rolle gegenüber der passiver Rolle bei SSL

Public Key Infrastrukturen

- Umsetzungskonzepte z.B.: Verbindlicher Austausch von Transaktionsdaten
  - Der Empfänger muss die Verbindlichkeit abschätzen können, weil er kostenintensive Aktionen daraus ableitet!
  - Diese Anwendungen sind meist firmen- bzw. geräteorientiert
  - basieren meistens auf geschlossenen Systemen
  - Ziel ist immer die Integration in bestehende Workflows (Arbeitsabläufe)
  - von kleinen Datenmengen pro Monat bis hin zu einer hohen Anzahl von Transaktionen pro Minute

SSL



SSL

- SSL (Secure Sockets Layer) ist ein Protokoll um verschlüsselte Kommunikation zwischen Clients im Internet zu ermöglichen
- ursprünglich von Netscape entwickelt
- hat sich im World Wide Web für verschlüsselte Kommunikation durchgesetzt
- SSL läuft über dem TCP/IP Layer aber noch unter High-Level Layern wie HTTP, LDAP oder IMAP

SSL

- erlaubt einem SSL fähigen Server sich gegenüber einem SSL fähigen Client zu authentifizieren und umgekehrt
- haben sich beide authentifiziert können sie eine sichere Verbindung aufbauen

SSL

- SSL wird für folgende Funktionen verwendet:
  - zur Authentifizierung
  - zur Datenverschlüsselung
  - Überprüfung auf Integrität der Daten

SSL

- SSL Protokoll beinhaltet:
  - SSL Record Protokoll:
    - beschreibt das Format mit dem die Daten übertragen werden
  - SSL Handshake Protokoll
    - nutzt das SSL Record Protokoll um Messages zwischen Client und Server auszutauschen (bei bestehender Verbindung)

SSL

- Aktionen (mit Hilfe dieser Messages):
  - den Server gegenüber dem Client zu authentifizieren
  - Zwischen dem Server und dem Client kryptografische Algorithmen oder Chiffren auszumachen
  - optional den Client gegenüber dem Server zu authentifizieren
  - gemeinsame Geheimnisse mittels Public Key Verschlüsselungstechniken zu generieren
  - eine verschlüsselte SSL Verbindung aufzubauen

SSL

- Wie läuft nun eine SSL Verbindung ab?
  - ein Client fordert eine über HTTP**S** erreichbare Webseite an
    - so beginnen sein Rechner und der Server der Webseite miteinander zu kommunizieren
  - nun wird festgestellt, welche Version von SSL sie verwenden wollen
  - danach Festlegen, welches asymmetrische Verfahren sie verwenden, um den Schlüssel für die schnellere symmetrische Verschlüsselung auszutauschen

SSL

- Wie läuft nun eine SSL Verbindung ab?
  - Wenn das erledigt:
    - Austausch von Zertifikaten
    - zumindest jedoch sendet der Server seines an den Client, der überprüft
      - ob das Zertifikat zum URL passt,
      - ob er die digitale Signatur bereits kennt. Falls nicht, gibt er eine Warnung aus, verschlüsselt aber bei entsprechender Entscheidung des Benutzers trotzdem.
  - Austausch der Schlüssel über das vorher gewählte, asymmetrische Verschlüsselungsverfahren

SSL

- Wie läuft nun eine SSL Verbindung ab?
  - legen so fest, welchen sie für die symmetrische, schnellere Verschlüsselung verwenden
  - Client erhält eine "Session ID", eine eindeutige Nummer, welche die Transaktion identifiziert

Schlüsselmanagement

- Schlüsselerzeugung:
  - Erzeugung (Festlegung) der Schlüsselinformation (Schlüssel) für eine Verschlüsselung
  - Mögliche Formen:
    - Berechnung von Primzahlen beim RSA-Verfahren
    - Generierung von Zufallszahlen
    - Festlegung eines Codewortes

Schlüsselmanagement

- Schlüsselerzeugung:
  - Kriterien:
    - der erzeugte Schlüssel bleibt während der Erzeugung geheim
    - Qualität der Schlüssel muss hinreichend sein
    - verwendeten Schlüssel dürfen nicht angreifbar sein
    - Schlüssel nicht vorhersehbar sein
  - schwache Schlüssel oder auch zu kurze Schlüssel sollten vom Generierungsverfahren vermieden werden

Schlüsselmanagement

- Schlüsselvernichtung
  - Gegenstück zur Schlüsselerzeugung
  - nur wenn ein Schlüssel mit absoluter Sicherheit nicht mehr existent ist, hat man Gewissheit, dass der Schlüssel nicht mehr verwendet werden kann

Schlüsselmanagement

- Schlüsselverteilung:
  - Synonym für Schlüsselübergabe
    - größeren Systemen: Schlüsselverteilung
    - kleinere Systeme: Schlüsselübergabe
  - Vorgang, der vor der Aufnahme einer verschlüsselten Kommunikation vollzogen werden muss
  - Weg, auf dem die Übergabe erfolgt, muss sicher sein

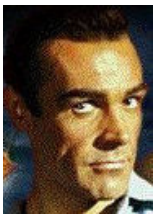
Schlüsselmanagement

- Schlüsselverteilung:
  - Zwei Möglichkeiten:
    - Schlüsselübergabe bei Kommunikation mit asymmetrischer Verschlüsselung (public key encryption)
    - Schlüsselübergabe bei Kommunikation mit symmetrischer Verschlüsselung (symmetric encryption)

Schlüsselmanagement

- Schlüsselverteilung



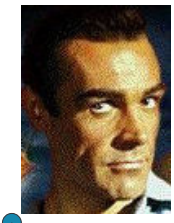



Moneypenny und Bond tauschen Daten über das Internet aus, die Goldfinger mitlesen und manipulieren kann.

Schlüsselmanagement

- Schlüsselverteilung:
  - Asymmetrische Schlüsselverteilung



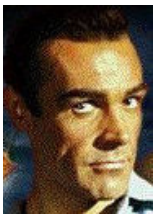



Wie kommt Bond eigentlich auf zuverlässige Weise in den Besitz von Moneypennys öffentlichen RSA-Schlüssel?

Schlüsselmanagement

- Schlüsselverteilung:
  - Asymmetrische Schlüsselverteilung






Moneypenny könnte den Schlüssel beispielsweise über das Netz an Bond schicken. Jedoch könnte dieser in die Hände Goldfingers gelangen, durch seinen eigenen austauschen und dadurch eine man-in-the-middle-Attacke starten.

Schlüsselmanagement

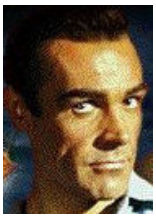
Was ist eine man-in-the-middle-Attacke?

Schlüsselmanagement

Eine so genannte dritte Person greift bei einer man-in-the-middle-Attacke aktiv in die Kommunikation zwischen zwei anderen Kommunikationspartnern ein und stellt großen Schaden an.
Beispielsweise könnte diese ein Passwort abfangen und dieses selbst benutzen (z.B. bei einer Bankverbindung!!).

Schlüsselmanagement

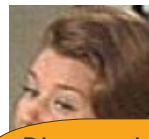
- Schlüsselverteilung:
  - Asymmetrische Schlüsselverteilung

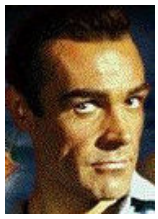


Nach Übersenden des Schlüssels vergleichen Moneypenny und Bond einen Hashwert davon per Telefon. Stimmen diese Werte überein, kann mit dem Nachrichtenaustausch begonnen werden.

Schlüsselmanagement

- Schlüsselverteilung:
  - Asymmetrische Schlüsselverteilung

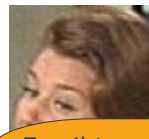


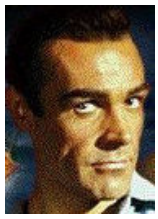



Die man-in-the-middle-Attacke könnte aber auch durch eine Zertifizierung öffentlicher Schlüssel verhindert werden.
Moneypenny kann ihren öffentlichen Schlüssel von jemandem (Signierungsstelle) signieren lassen, den sie und Bond kennen.

Schlüsselmanagement

- Schlüsselverteilung:
  - Symmetrische Schlüsselverteilung



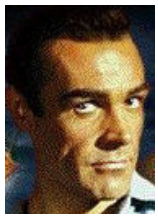



Es gibt auch die Möglichkeit, dass man keine Public Key Kryptografie einsetzt.
Moneypenny und Bond wollen weiterhin über ein unsicheres Medium verschlüsselt kommunizieren und wollen ein symmetrisches Kryptosystem verwenden.

Schlüsselmanagement

- Schlüsselverteilung:
  - Symmetrische Schlüsselverteilung



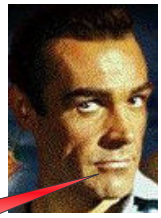



Dazu benötigen beide jedoch zunächst einen Schlüssel, den sie über den Diffie-Hellman-Schlüsselaustausch vereinbaren.

Schlüsselmanagement

- Schlüsselverteilung:
  - Symmetrische Schlüsselverteilung





Wie sieht den so eine Schlüsselaustausch aus?

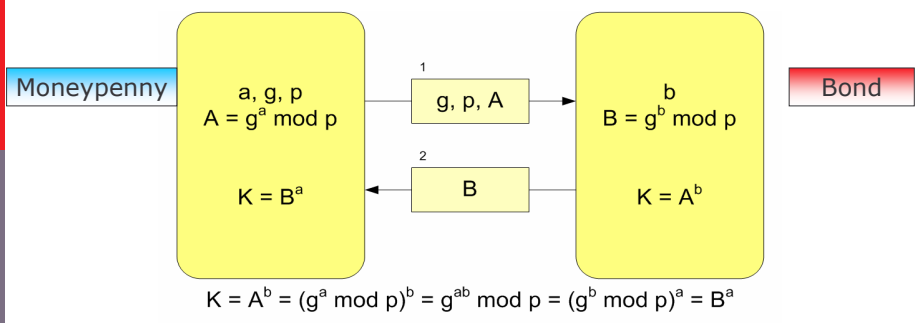
Schlüsselmanagement

- Schlüsselverteilung:
  - Symmetrische Schlüsselverteilung

In unserem Fall wollen Sie Bond und Moneypenny über ein unsicheres Medium, etwa eine Kabel- oder Funkleitung, verschlüsselt kommunizieren. Das sieht wie folgt aus:

Schlüsselmanagement

- Schlüsselverteilung:
  - Symmetrische Schlüsselverteilung (Diffie-Hellman-Schlüsselaustausch)



$K = A^b = (g^a \bmod p)^b = g^{ab} \bmod p = (g^b \bmod p)^a = B^a$

Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch:
    - Zuerst einigt euch auf eine Primzahl p und eine Primitivwurzel g mod p mit $2 \leq g \leq p-2$. Diese Parameter müssen nicht geheim bleiben, können also insbesondere auch über ein unsicheres Medium übertragen werden.
    - Dann erzeugt jeder von euch eine geheim zu haltende Zufallszahl a bzw. b aus der Menge $\{1,\ldots,p-2\}$. a und b werden nicht übertragen, bleiben also dem jeweiligen Kommunikationspartner, aber auch potenziellen Lauschern unbekannt.

Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch:
    - Nun berechnet ihr euch $A = g^a \bmod p$ bzw. $B = g^b \bmod p$. Nun werden A und B über das unsichere Medium übertragen.
    - Jetzt berechnet beide $B^a \bmod p = (g^b \bmod p)^a \bmod p = (g^{ba}) \bmod p = (g^{ab}) \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p = K$. Das Ergebnis K ist für beide von euch gleich und kann als Schlüssel für die weitere Kommunikation verwendet werden.

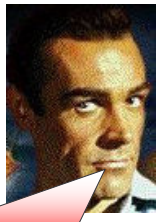
Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch

Einfacher zu verstehen ist das Ganze an einem Beispiel. Wie gesagt: „Learning by doing!"

Schlüsselmanagement

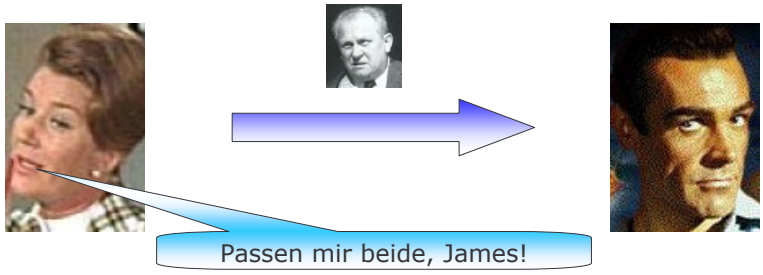
- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



Nun ja, wir werden es mal probieren. Moneypenny, sind dir die Zahlen $p = 13$ und $g = 2$ recht?

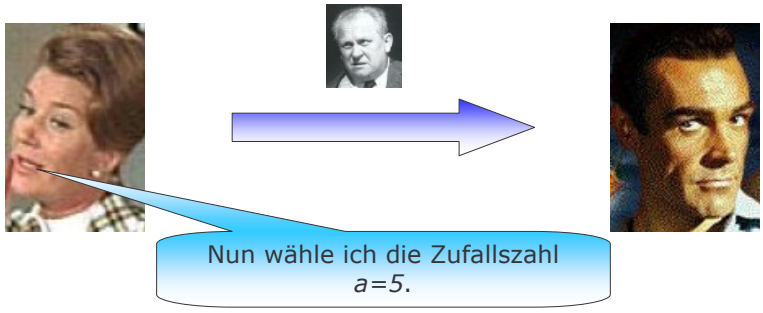
Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



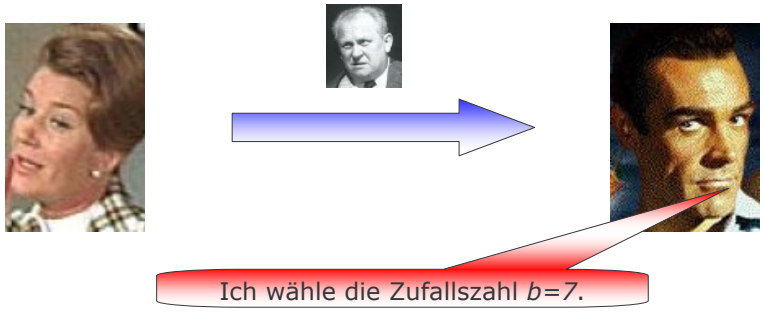
Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



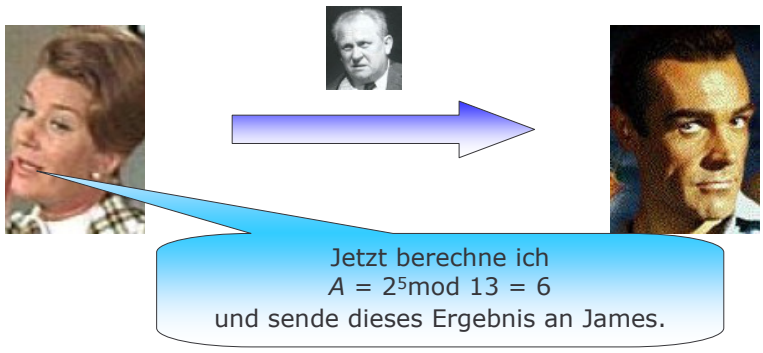
Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



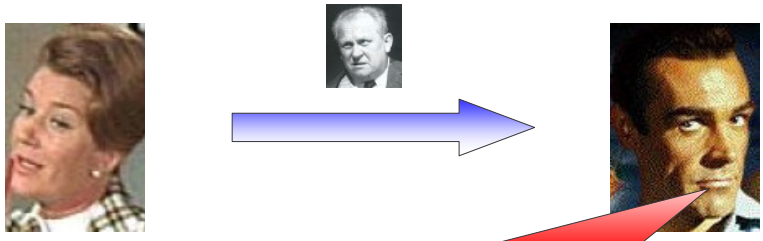
Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



Schlüsselmanagement

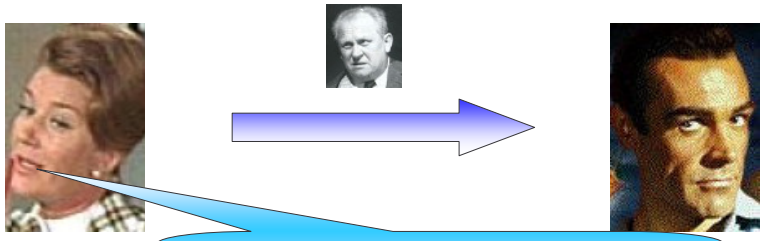
- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



Ich berechne
$B = 2^7 \bmod 13 = 11$
und sende dieses Ergebnis an Moneypenny.

Schlüsselmanagement

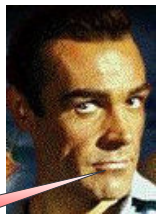
- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



Ich berechne jetzt noch
$K = 11^5 \bmod 13 = 7$.

Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch



Nun noch
$K = 6^7 \bmod 13 = 7.$

Schlüsselmanagement

- Schlüsselverteilung:
  - Diffie-Hellman-Schlüsselaustausch

Beide erhalten das gleiche Ergebnis $K = 7$.
Ein eventuell vorhandener Lauscher könnte zwar die Zahlen 13, 2, 6 und 11 mithören, das eigentliche gemeinsame Geheimnis von Moneypenny und Bond
$K = 7$ bleibt ihm aber verborgen.

Schlüsselmanagement

- Schlüsselspeicherung
  - bei symmetrischen Verfahren ist dies nicht notwendig, da die Schüssel ständig gewechselt werden
  - asymmetrische Schlüssel müssen dagegen gespeichert werden, z.B. auf einem Speichermedium wie Diskette bzw. Festplatte (geringe Sicherheit) oder auf einer Chipkarte (hohe Sicherheit)

Kryptologie