Kryptographie und Verschlüsselung

Jörg Thomas

Kryptographie und Verschlüsselung

- Begriffsbildung
- Geschichte
- Ziel moderner Kryptographie
- Sicherheit
- Public-Key-Kryptographie
- Ausblick

Begriffsbildung (1)

Kryptologie

Die Wissenschaft von der Verschlüsselung (Chiffrierung) und Entschlüsselung (Dechiffrierung) von Nachrichten.

Die Kryptologie war über Jahrhunderte hinweg von Diplomatie, Militär und Geheimdiensten gepflegte Geheimwissenschaft.

Begriffsbildung (2)

Kryptographie

Wissenschaft von den algorithmischen, insbesondere mathematischen, rechnergestützten Methoden zur Gewährleitung von

- gesicherter Ablage
- vertraulicher Kommunikation
- Authentität und Integrität der Nachrichten
- Authentität der Teilnehmer bzw. der Einheiten
- Anonymität und/oder Verbindlichkeit

Geschichte (1)

- Verschlüsselung ohne Schlüssel
- Caeser
- Monoalphabetische Verschlüsselung
- Polyalphabetische Verschlüsselung
- Enigma (griech. Rätsel)

Geschichte (2)

Verschlüsselung ohne Schlüssel

- Prinzip
  - Offene Übermittlung der vertraulichen Information
  - Gegner hat keine Chance, den Klartext zu ermitteln – so hoffen Sender und Empfänger
- Beispiel:
  - Freimaurer-Code

(siehe Excel-Blatt 1)

Geschichte (3)

Caeser

- Merkmal:
  - Keine Geheimzeichen
  - Dieselben Klar- und Geheimtextzeichen
  - Eingebaute Variabilität
- Prinzip
  - Mittels Geheimtextzeichen wird aus Klartextzeichen ein Code

(siehe Excel-Blatt 2)

Exkurs

- Verschlüsselungsverfahren bedeutet
  - Algorithmus
  - Schlüssel
- Wesentliche Merkmale
  - Schlüssel für Verschlüsselung und Entschlüsselung
  - Schlüssel ist klein
  - Sicheres Verfahren schützt Sender und Empfänger
  - Prinzip:
    Verfahren muss so gut sein, dass des Bekanntwerden des Systems das Verfahren nicht schwächt.

Geschichte (4)

Monoalphabetische Verschlüsselung

- Prinzip
  - Caesar-Code mit Geheimalphabet in nicht natürlicher Reihenfolge
- Problem
  - Statistische Eigenschaften der (deutschen) Sprache

(siehe Excel-Blatt 3)

Geschichte (5)

Polyalphabetische Verschlüsselung

- Prinzip
  - Verschlüsselung durch verschiedene Alphabete
  - Steuerung des Wechsels des Alphabets durch das Schlüsselwort
- Problem
  - Bei Wissen der Länge des Schlüsselwortes Reduktion auf Caesar-Entschlüsselung
  - Falls Länge unbekannt, Bestimmung der Schlüssellänge durch Mustervergleiche

(siehe Excel-Blatt 4+5)

Geschichte (6)

Enigma

- Prinzip
  - Mechanische Verschlüsselung

- Alan Turing mit Prototyp eines modernen Computers (Colossus)

Ziel moderner Krypthographie (1)

- Verschlüsselung von Daten
  (Verheimlichung von Nachrichten)
- Authentifikation der Daten
  (Echtheit der Nachrichten)

Ziel moderner Krypthographie (2)

Verschlüsselung von Daten
(Verheimlichung von Nachrichten)

- Nur derjenige, der den geheimen Schlüssel besitzt, kann die Nachricht entschlüsseln

Ziel moderner Krypthographie (3)

Authentifikation der Daten
(Echtheit der Nachrichten)

- Unter Zuhilfenahme eines geheimen Schlüssels lässt sich die Echtheit (insbesondere Unversehrtheit und Ursprung) nachweisen

Sicherheit (1)

- DES (Data Encryption Standard)
- PIN auf der EC-Card
- Nummernsystem der DB

Sicherheit (2)

DES (Data Encryption Standard)

Veröffentlicht 1976, basiert auf Algorithmus „Lucifer“ von IBM, die National Security Agency (NSA) hat den Algorithmus endgültig spezifiziert

Vorbildlicher Algorithmus

- DES-Algorithmus lebt seit 25 Jahren
- Anzahl Schlüssel sehr hoch (72.057.594.037.927.936, d.s. zweiundsiebzig Billiarden ...)

(siehe Excel-Blatt 6)

Sicherheit (3)

PIN auf der EC-Card

- Breiteste und populärste Anwendung des DES-Algorithmus
- Verfahren:
- in der Regel: Berechnung der PIN aus BLZ, KtoNr, und Verfalldatum

(siehe Excel-Blatt 7)

Sicherheit (4)

Nummernsystem der DB

Ein integrierte Kontrollzahl:

(siehe Excel-Blatt 8)

Public-Key-Kryptographie (1)

- Theorie und Praxis
- RSA-Algorithmus
- Digitale Signatur
- HACH-Funktionen
- PGP

Public-Key-Kryptographie (2)

Theorie und Praxis (1)

Frage: Kann ich jemandem, mit dem ich noch nie Kontakt hatte, insbesondere noch nie ein Geheimnis hatte, eine verschlüsselte Nachricht schicken, die nur er entschlüsseln kann?

Mathematisch gesprochen: Existiert eine trapdoor Einwegfunktion, dann ist die Frage der Verschlüsselung ohne vorhergehenden Geheimaustausch gelöst.

Public-Key-Kryptographie (3)

Theorie und Praxis (2)

Rivest, Shamir und Adleman entwickelten 1977 den berühmten Public-Key-Algorithmus, den sogenannten RSA-Algorithmus

- Kriterien:

Ein Dokument so gestalten, dass

- niemand anderer dies tun kann
- jeder verifizieren kann, dass dies von mir stammt

Public-Key-Kryptographie (4)

RSA-Algorithmus (Theorie)

Man nehme zwei Primzahlen p und q und bilde das Produkt $n = p \cdot q$.

Es gilt der Eulersche Satz:

Für jede natürliche Zahl m mit $m = n$ und jeder natürlichen Zahl s gilt:

$m^{s \cdot (p-1) \cdot (q-1) + 1} \bmod n = m$.

Was heißt das (ein Beispiel):

$n = 10$ ($p = 2$, $q = 5$), $s = 1$

dann gilt: $s \cdot (p-1) \cdot (q-1) = 5$

für $m = 2$ gilt z.B.: $2^5 \bmod 10 = 32 \bmod 10 = 2$

Public-Key-Kryptographie (5)

RSA-Algorithmus (im Einsatz)

- Für jeden Teilnehmer werden zwei Primzahlen p und q genommen, bilde das Produkt $n = p \cdot q$, bestimme zwei natürliche Zahlen e und d mit $e \cdot d = s \cdot (p-1) \cdot (q-1) + 1$.
- Dem Teilnehmer wird d als sein geheimer Schlüssel zugeordnet, e und n bilden den dazugehörigen öffentlichen Schlüssel.
- Nachricht wird in eine natürliche Zahl m kleiner n übersetzt
- Man erhält den Geheimtext c, in dem man m mit dem öffentlichen Schlüssel e des Empfängers potenziert und modulo n reduziert.

Public-Key-Kryptographie (6)

RSA-Algorithmus (im Einsatz Fortsetzung)

- Es gilt:
  $c = m^e \bmod n$ mit $m = n$
- Entschlüsselung des Geheimtexts c durch den Empfänger mit geheimen Schlüssel:
  $m' = c^d \bmod n$
- Nun gilt:
  $m' = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$
- Nach dem Eulerschen Satz gilt:
  $m^{ed} \bmod n = m$
- Also folgt: $m' = m$

Public-Key-Kryptographie (7)

Digitale Signatur

- Prinzip

  Elektronisches Dokument so gestalten, dass
  - für jeden nachvollziehbar ist, dass der Teilnehmer dies erstellt hat
  - niemand das Dokument fälschen kann
- Methode
  - Ausbau der RSA-Idee zu einem Signaturverfahren

Public-Key-Kryptographie (8)

HACH-Funktionen

- Prinzip
  - Digitale Signatur genauso lang wie die eigentliche Nachricht
  - Alle bekannten Signaturverfahren sind sehr langsam
- Methode
  - Kompressionseigenschaft
  - Kollisionsfreiheit

Public-Key-Kryptographie (9)

PGP (Pretty Good Privacy)

- Phil Zimmermann
- Anarchie ist machbar mit
  - bestem zur Verfügung stehenden Verfahren
  - Entscheidungsfähigkeit beim Benutzer belassen
- Zertifizierung des öffentlichen Schlüssels

Ausblick (1)

- Kryptographie ist für alle da
- Kryptographie ist gut für uns
- Die Segnungen der Kryptographie sind nicht für alle da

Ausblick (2)

Kryptographie ist für alle da

- kein Privileg der Geheimdienste, sondern für alle
- Die Sicherheit kryptographischer Verfahren kann mathematisch analysiert (und bewiesen) werden
- Somit kann sich jeder schützen

Ausblick (3)

Kryptographie ist gut für uns

- Geldautomaten
- Mobilfunk
- Pay-TV
- Wegfahrsperre bei Autos
- Fernbedienungen

Ausblick (4)

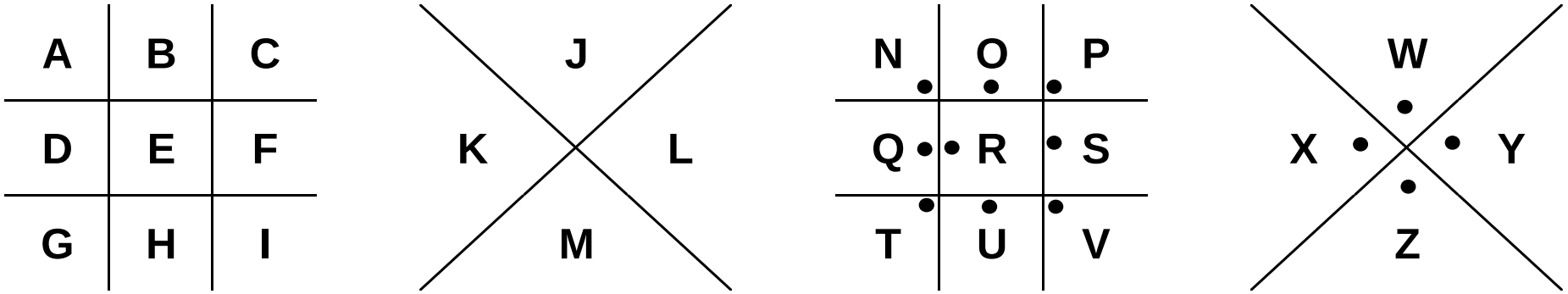
Die Segnungen der Kryptographie sind nicht für alle da

- Probleme bei der Verhinderung und Aufdeckung von Verbrechen
- Auseinandersetzung von Staaten, Geheimdiensten

Hinweise

- http://www.bsi.de
  Bundesamt für Sicherheit in der Informationstechnik
- Literatur:
  - Albert Beutelspacher: Geheimsprachen. C.H.Beck 2000

Freimauerer-Code



K R Y P T O G R A P H I E

Caesar-Code

Klartextalphabet (KTA):	**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**
Geheimtextalphabet (GTA):	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

Text:	**K**	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**I**	**E**
ergibt Code:	**N**	**U**	**B**	**S**	**W**	**R**	**J**	**U**	**D**	**S**	**K**	**L**	**H**

Monoalph. Verschlüsselung

Klartextalphabet (KTA):	**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**
Geheimtextalphabet (GTA):	**M**	**U**	**C**	**D**	**L**	**K**	**X**	**W**	**J**	**Q**	**A**	**N**	**E**	**Z**	**O**	**V**	**F**	**B**	**G**	**H**	**I**	**P**	**T**	**Y**	**R**	**S**

Text:	**K**	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**I**	**E**
ergibt Code:	**A**	**B**	**R**	**V**	**H**	**O**	**X**	**B**	**M**	**V**	**W**	**J**	**L**

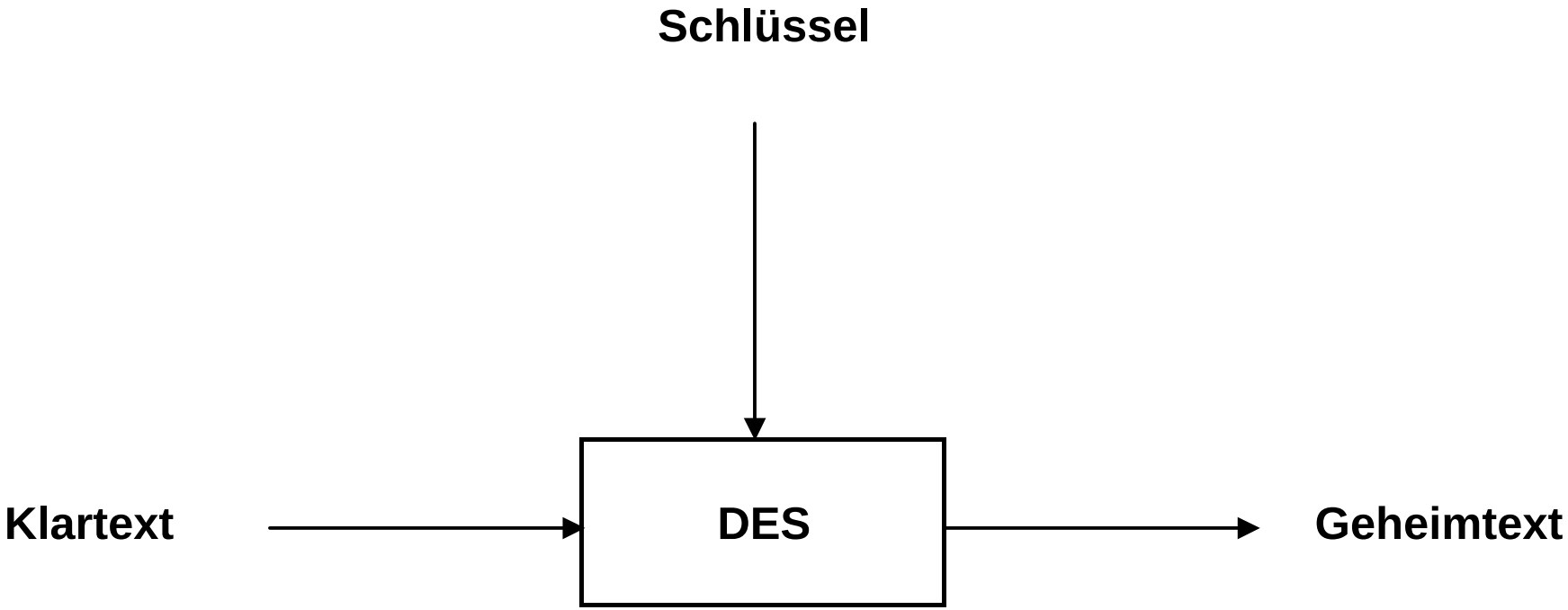
Caesar-Alphabet:

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

Polyalph. Verschlüsselung

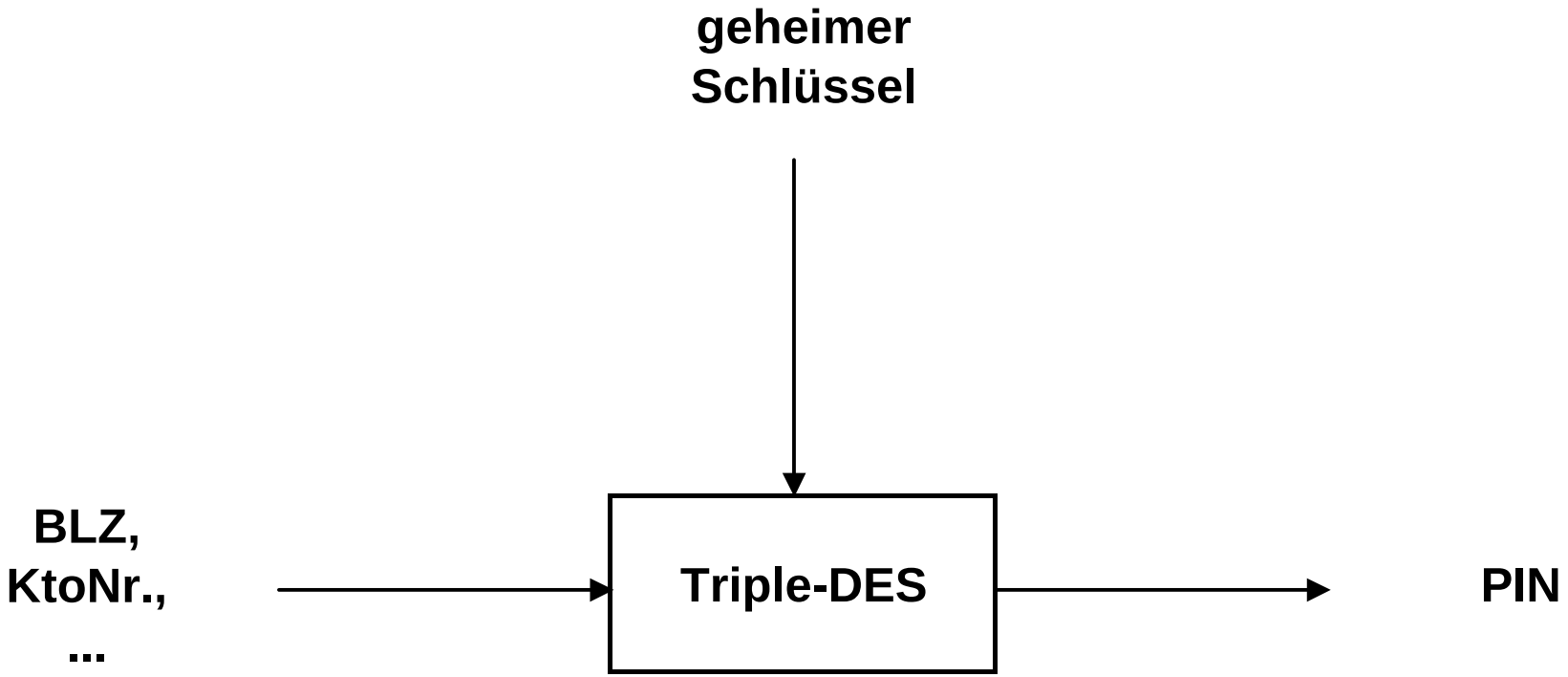
Schlüsselwort:	**B**	**E**	**R**	**L**	**I**	**N**	**B**	**E**	**R**	**L**	**I**	**N**	**B**
Klartext:	**K**	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**I**	**E**
Geheimcode:	**L**	**V**	**P**	**A**	**B**	**B**	**H**	**V**	**R**	**A**	**P**	**V**	**F**

Data Encryption Standard



Grobstruktur des DES

PIN auf EC-Card



Funktionsweise PIN

Nummernsystem DB

	Baureihennummer			Ordnungsnummer				Kontrollziffer
	2	1	8	3	1	1	-	9
X	1	2	1	2	1	2		
	2	2	8	6	1	2		21