

Kryptologie

Nicolas Bellm

24. November 2005

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

Einleitung

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.

Sie läßt sich unterteilen in

- Verschlüsselung von Informationen (Kryptographie)
- Verstecken von Informationen (Steganographie)
- Entschlüsselung von Informationen (Kryptoanalyse)

Einleitung

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.

Sie läßt sich unterteilen in

- Verschlüsselung von Informationen (Kryptographie)
- Verstecken von Informationen (Steganographie)
- Entschlüsselung von Informationen (Kryptoanalyse)

Einleitung

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.

Sie läßt sich unterteilen in

- Verschlüsselung von Informationen (Kryptographie)
- Verstecken von Informationen (Steganographie)
- Entschlüsselung von Informationen (Kryptoanalyse)

Einleitung

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.

Sie läßt sich unterteilen in

- Verschlüsselung von Informationen (Kryptographie)
- Verstecken von Informationen (Steganographie)
- Entschlüsselung von Informationen (Kryptoanalyse)

Einleitung

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.

Sie läßt sich unterteilen in

- Verschlüsselung von Informationen (Kryptographie)
- Verstecken von Informationen (Steganographie)
- Entschlüsselung von Informationen (Kryptoanalyse)

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

- 1 Einleitung
- 2 **Klassische Kryptologie**
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 **Moderne Kryptologie**
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

Inhalt

- 1 Einleitung
- 2 **Klassische Kryptologie**
 - **Skytale**
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 **Moderne Kryptologie**
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Skytale

- ca. 500 v.Chr. von den Spartanern verwendet.
- Holzstab mit bestimmtem Durchmesser

Verschlüsselung

- Absender wickelt Papyrusstreifen um den Stab
 - Nachricht wird längs auf den Stab geschrieben
 - Empfänger wickelt Nachricht auf einen gleichdicken Stab
-
- geheimer Schlüssel: Durchmesser des Stabs
 - **Transpositionsverfahren**

Inhalt

- 1 Einleitung
- 2 **Klassische Kryptologie**
 - Skytale
 - **Monoalphabetische Verfahren**
 - Polyalphabetische Verfahren
- 3 **Moderne Kryptologie**
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

Suetonius, De Vita Caesarum

»... si qua occultius preferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.«

Suetonius, De Vita Caesarum (Übersetzung)

„... wenn etwas Geheimes zu überbringen war, schrieb er in Chiffren, das heißt, er ordnete die Buchstaben so, daß kein Wort gelesen werden konnte: Um diese zu lesen, tausche man den vierten Buchstaben, also D, gegen A aus und ebenso mit den restlichen.“

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- benannt nach Gaius Julius Cäsar
- **monoalphabetische Substitution**
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch **Häufigkeitsanalyse** oder **Brute Force**
- Sonderfall: ROT13

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- bennant nach Gaius Julius Cäsar
- monoalphabetische Substitution
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch Häufigkeitsanalyse oder Brute Force
- Sonderfall: ROT13

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- benannt nach Gaius Julius Cäsar
- **monoalphabetische Substitution**
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch Häufigkeitsanalyse oder Brute Force
- Sonderfall: ROT13

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- bennant nach Gaius Julius Cäsar
- **monoalphabetische Substitution**
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch Häufigkeitsanalyse oder Brute Force
- Sonderfall: ROT13

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- bennant nach Gaius Julius Cäsar
- **monoalphabetische Substitution**
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch Häufigkeitsanalyse oder Brute Force
- Sonderfall: ROT13

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Beispiel: Cäsar-Chiffre

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

Aus GEHEIM
wird KILIMQ

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- bennant nach Gaius Julius Cäsar
- **monoalphabetische Substitution**
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch **Häufigkeitsanalyse** oder **Brute Force**
- Sonderfall: ROT13

Cäsar-Chiffre

- einfachstes Verfahren zum Verschlüsseln von Nachrichten
- bennant nach Gaius Julius Cäsar
- **monoalphabetische Substitution**
- zyklische Rotation um k Zeichen
- Schlüssel ist k
- knackbar durch **Häufigkeitsanalyse** oder **Brute Force**
- Sonderfall: ROT13

zufälliges Alphabet

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

langes Schlüsselwort: SCHMETTERLING

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

Schlüsselwort mit Z am Anfang: ZUGBEGLEITER

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

Atbash

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

Inhalt

- 1 Einleitung
- 2 **Klassische Kryptologie**
 - Skytale
 - Monoalphabetische Verfahren
 - **Polyalphabetische Verfahren**
- 3 **Moderne Kryptologie**
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Vigenère-Chiffre

- benannt nach Blaise de Vigenere
- verschiedene Geheimtextalphabete
- **polyalphabetische Substitution**

Verschlüsselung

- man benutzt ein Schlüsselwort, z.B. MATHE
- Klartextbuchstaben werden zu den Geheimtextbuchstaben addiert
- Hilfsmittel: Vigenère-Quadrat

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Beispiel: Vigenère-Chiffre

Klartext:	P	O	L	Y	N	O	M
Schlüssel:	M	A	T	H	E	M	A
Geheimtext:	B	O	E	F	R	A	M

Aufgabe: Vigenère-Chiffre

Ihr habt den Geheimtext WRRWXALHNMQ abefangen. Ihr wißt, daß die Nachricht mit der Vigenère-Chiffre verschlüsselt wurde und der Schlüssel MATHE heißt. Wie lautet der Klartext?

One-Time-Pad

- funktioniert genauso wie die Vigenère-Chiffre
- Schlüssel ist genauso lang wie der Text
- Sender und Empfänger besitzen den gleichen Block mit völlig zufälligen Zeichen
- für jede Nachricht wird eine neue Seite des Blocks verwendet
- Vorteil: perfekte Sicherheit
- Nachteil: unhandlicher Schlüssel

One-Time-Pad

- funktioniert genauso wie die Vigenère-Chiffre
- Schlüssel ist genauso lang wie der Text
- Sender und Empfänger besitzen den gleichen Block mit völlig zufälligen Zeichen
- für jede Nachricht wird eine neue Seite des Blocks verwendet
- Vorteil: perfekte Sicherheit
- Nachteil: unhandlicher Schlüssel

One-Time-Pad

- funktioniert genauso wie die Vigenère-Chiffre
- Schlüssel ist genauso lang wie der Text
- Sender und Empfänger besitzen den gleichen Block mit völlig zufälligen Zeichen
- für jede Nachricht wird eine neue Seite des Blocks verwendet
- Vorteil: perfekte Sicherheit
- Nachteil: unhandlicher Schlüssel

One-Time-Pad

- funktioniert genauso wie die Vigenère-Chiffre
- Schlüssel ist genauso lang wie der Text
- Sender und Empfänger besitzen den gleichen Block mit völlig zufälligen Zeichen
- für jede Nachricht wird eine neue Seite des Blocks verwendet
- Vorteil: perfekte Sicherheit
- Nachteil: unhandlicher Schlüssel

One-Time-Pad

- funktioniert genauso wie die Vigenère-Chiffre
- Schlüssel ist genauso lang wie der Text
- Sender und Empfänger besitzen den gleichen Block mit völlig zufälligen Zeichen
- für jede Nachricht wird eine neue Seite des Blocks verwendet
- Vorteil: perfekte Sicherheit
- Nachteil: unhandlicher Schlüssel

One-Time-Pad

- funktioniert genauso wie die Vigenère-Chiffre
- Schlüssel ist genauso lang wie der Text
- Sender und Empfänger besitzen den gleichen Block mit völlig zufälligen Zeichen
- für jede Nachricht wird eine neue Seite des Blocks verwendet
- Vorteil: perfekte Sicherheit
- Nachteil: unhandlicher Schlüssel

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 **Moderne Kryptologie**
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 Ausblick

Moderne Kryptologie

- entscheidende Fortschritte in der Kryptologie im 20. Jahrhundert

Wendepunkte

- mechanische und elektromechanische Verschlüsselungsmaschinen im 2. Weltkrieg
- aufkommende Computerisierung
- Diffie und Hellmann veröffentlichen das Konzept des „Public-Key- Cryptosystems“

Moderne Kryptologie

- entscheidende Fortschritte in der Kryptologie im 20. Jahrhundert

Wendepunkte

- mechanische und elektromechanische Verschlüsselungsmaschinen im 2. Weltkrieg
- aufkommende Computerisierung
- Diffie und Hellmann veröffentlichen das Konzept des „Public-Key- Cryptosystems“

Moderne Kryptologie

- entscheidende Fortschritte in der Kryptologie im 20. Jahrhundert

Wendepunkte

- mechanische und elektromechanische Verschlüsselungsmaschinen im 2. Weltkrieg
- aufkommende Computerisierung
- Diffie und Hellmann veröffentlichen das Konzept des „Public-Key- Cryptosystems“

Moderne Kryptologie

- entscheidende Fortschritte in der Kryptologie im 20. Jahrhundert

Wendepunkte

- mechanische und elektromechanische Verschlüsselungsmaschinen im 2. Weltkrieg
- aufkommende Computerisierung
- Diffie und Hellmann veröffentlichen das Konzept des „Public-Key- Cryptosystems“

Moderne Kryptologie

- entscheidende Fortschritte in der Kryptologie im 20. Jahrhundert

Wendepunkte

- mechanische und elektromechanische Verschlüsselungsmaschinen im 2. Weltkrieg
- aufkommende Computerisierung
- Diffie und Hellmann veröffentlichen das Konzept des „Public-Key- Cryptosystems“

Inhalt

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 **Moderne Kryptologie**
 - **Symmetrische Kryptologie**
 - Assymetrische Kryptologie
- 4 Ausblick

Symmetrische Kryptologie

- gleicher Schlüssel zum Ver- und Entschlüsseln
- Nachteil: für jede Sender-Empfänger-Beziehung wird ein eigener Schlüssel benötigt
- bekannte Vertreter: DES, IDEA, AES, RC4

Symmetrische Kryptologie

- gleicher Schlüssel zum Ver- und Entschlüsseln
- Nachteil: für jede Sender-Empfänger-Beziehung wird ein eigener Schlüssel benötigt
- bekannte Vertreter: DES, IDEA, AES, RC4

Symmetrische Kryptologie

- gleicher Schlüssel zum Ver- und Entschlüsseln
- Nachteil: für jede Sender-Empfänger-Beziehung wird ein eigener Schlüssel benötigt
- bekannte Vertreter: DES, IDEA, AES, RC4

Inhalt

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 **Moderne Kryptologie**
 - Symmetrische Kryptologie
 - **Assymetrische Kryptologie**
- 4 Ausblick

Assymetrische Kryptologie

- verschiedene Schlüssel zum Ver- und Entschlüsseln
- Vorteil: kein sicherer Kanal zum Schlüsselaustausch nötig
- Nachteil: Schlüssel bei gleicher Sicherheit länger als bei symmetrischer Kryptologie
- bekannte Vertreter: Diffie/Hellmann, ElGamal, RSA

Assymetrische Kryptologie

- verschiedene Schlüssel zum Ver- und Entschlüsseln
- Vorteil: kein sicherer Kanal zum Schlüsselaustausch nötig
- Nachteil: Schlüssel bei gleicher Sicherheit länger als bei symmetrischer Kryptologie
- bekannte Vertreter: Diffie/Hellmann, ElGamal, RSA

Assymetrische Kryptologie

- verschiedene Schlüssel zum Ver- und Entschlüsseln
- Vorteil: kein sicherer Kanal zum Schlüsselaustausch nötig
- Nachteil: Schlüssel bei gleicher Sicherheit länger als bei symmetrischer Kryptologie
- bekannte Vertreter: Diffie/Hellmann, ElGamal, RSA

Assymetrische Kryptologie

- verschiedene Schlüssel zum Ver- und Entschlüsseln
- Vorteil: kein sicherer Kanal zum Schlüsselaustausch nötig
- Nachteil: Schlüssel bei gleicher Sicherheit länger als bei symmetrischer Kryptologie
- bekannte Vertreter: Diffie/Hellmann, ElGamal, RSA

- 1 Einleitung
- 2 Klassische Kryptologie
 - Skytale
 - Monoalphabetische Verfahren
 - Polyalphabetische Verfahren
- 3 Moderne Kryptologie
 - Symmetrische Kryptologie
 - Assymetrische Kryptologie
- 4 **Ausblick**

- Entwicklung der Kryptologie geht weiter
- immer mehr Einfluß durch Computerisierung
- Bedrohung der Kryptologie durch Angst vor Terrorismus
- jeder sollte seine E-Mails verschlüsseln, z.B. mit PGP oder GnuPG

- Entwicklung der Kryptologie geht weiter
- immer mehr Einfluß durch Computerisierung
- Bedrohung der Kryptologie durch Angst vor Terrorismus
- jeder sollte seine E-Mails verschlüsseln, z.B. mit PGP oder GnuPG

- Entwicklung der Kryptologie geht weiter
- immer mehr Einfluß durch Computerisierung
- Bedrohung der Kryptologie durch Angst vor Terrorismus
- jeder sollte seine E-Mails verschlüsseln, z.B. mit PGP oder GnuPG

- Entwicklung der Kryptologie geht weiter
- immer mehr Einfluß durch Computerisierung
- Bedrohung der Kryptologie durch Angst vor Terrorismus
- jeder sollte seine E-Mails verschlüsseln, z.B. mit PGP oder GnuPG

Literatur



<http://home.nordwest.net/hgm/krypto/index.html>



Wikipedia