Einführung in die verschlüsselte Kommunikation

Loofmann

AFRA Berlin

25.10.2013

Ziele des Vortrages

- Wie funktioniert Verschlüsselung?
- Wie sicher sind heutige Verschlüsselungsmethoden?
- Welche Schritte werden benötigt, um verschlüsselt zu kommunizieren?

Inhalt

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

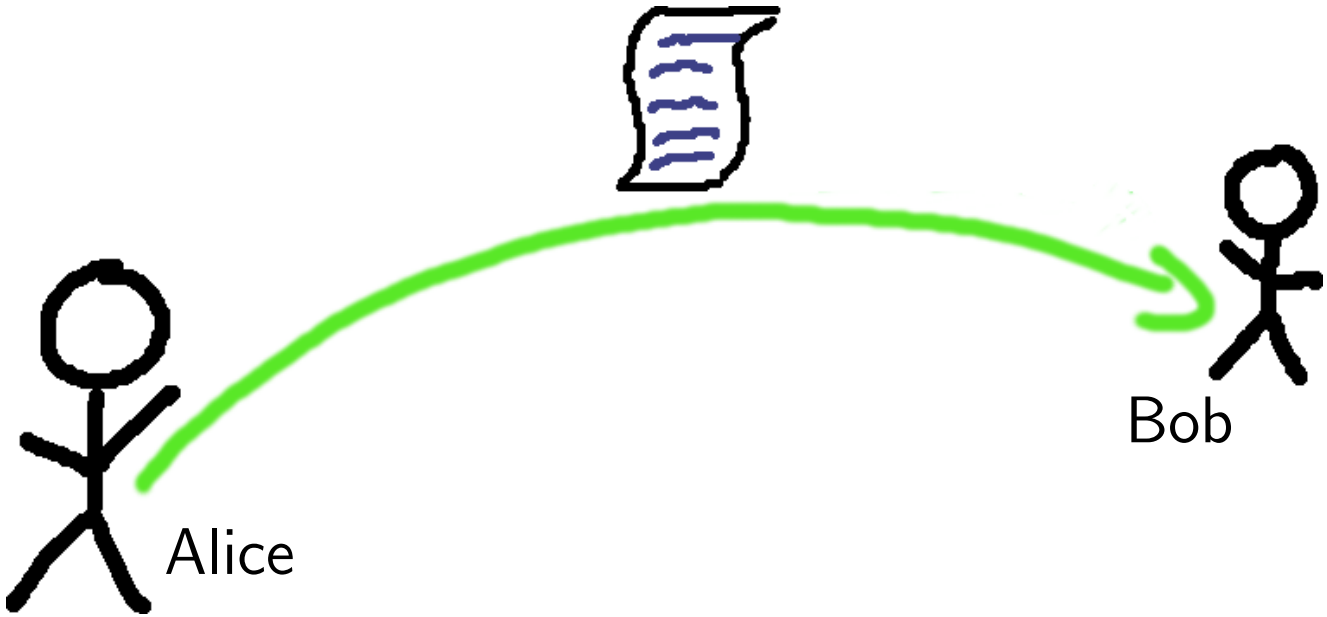
Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

Einführung

Was ist Kommunikation?

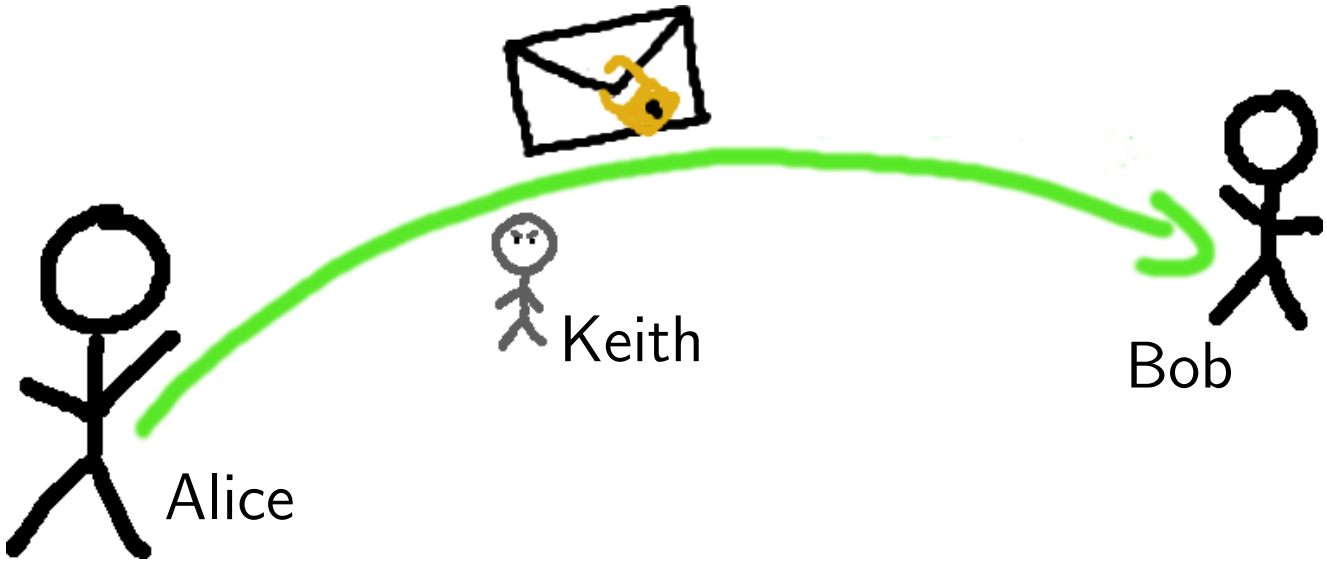
Eine Nachricht wird von Senderin zur Empfängerin übermittelt.



Einführung

Was ist Verschlüsselung?

Nachricht soll nur für Senderin und Empfängerin verständlich sein



Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

Exkurs: Kryptoanalyse

Geheimnachrichten entschlüsseln

Exkurs: Kryptoanalyse

Geheimnachrichten entschlüsseln

- Wunsch so alt, wie die Verschlüsselung

Exkurs: Kryptoanalyse

Geheimnachrichten entschlüsseln

- Wunsch so alt, wie die Verschlüsselung
- basiert auf verschiedenen mathematischen Methoden

Exkurs: Kryptoanalyse

Geheimnachrichten entschlüsseln

- Wunsch so alt, wie die Verschlüsselung
- basiert auf verschiedenen mathematischen Methoden
- nicht wichtig für den Alltag

Exkurs: Kryptoanalyse

Geheimnachrichten entschlüsseln

- Wunsch so alt, wie die Verschlüsselung
- basiert auf verschiedenen mathematischen Methoden
- nicht wichtig für den Alltag

aber:

Wichtig zur Bewertung von Verschlüsselungsmethoden

Exkurs: Kryptoanalyse

Häufigkeit von Buchstaben

Exkurs: Kryptoanalyse

Häufigkeit von Buchstaben

- bekannte Texte wurden analysiert

Exkurs: Kryptoanalyse

Häufigkeit von Buchstaben

- bekannte Texte wurden analysiert
- charakteristische Häufigkeiten wurden gefunden

Exkurs: Kryptoanalyse

Häufigkeit von Buchstaben

- bekannte Texte wurden analysiert
- charakteristische Häufigkeiten wurden gefunden
- bilden einfachste Grundlage zur Entschlüsselung

Exkurs: Kryptoanalyse

Häufigkeit von Buchstaben

- bekannte Texte wurden analysiert
- charakteristische Häufigkeiten wurden gefunden
- bilden einfachste Grundlage zur Entschlüsselung

einige Häufigkeiten (Top 5)

Buchstabe	E	N	I	S	R
Häufigkeit	17,4%	9,8%	7,8%	7,3%	7,0%

Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

Cäsar-Chiffre

Grundprinzip

Cäsar-Chiffre

Grundprinzip

- Verschiebung der Buchstaben des Klartextes

Cäsar-Chiffre

Grundprinzip

- Verschiebung der Buchstaben des Klartextes
- festgelegtes Geheimtextalphabet (monoalphabetische Substitution)

Cäsar-Chiffre

Grundprinzip

- Verschiebung der Buchstaben des Klartextes
- festgelegtes Geheimtextalphabet (monoalphabetische Substitution)
- klassisches Cäsar-Chiffre ist Verschiebung um 3 Buchstaben

Cäsar-Chiffre

Grundprinzip

- Verschiebung der Buchstaben des Klartextes
- festgelegtes Geheimtextalphabet (monoalphabetische Substitution)
- klassisches Cäsar-Chiffre ist Verschiebung um 3 Buchstaben

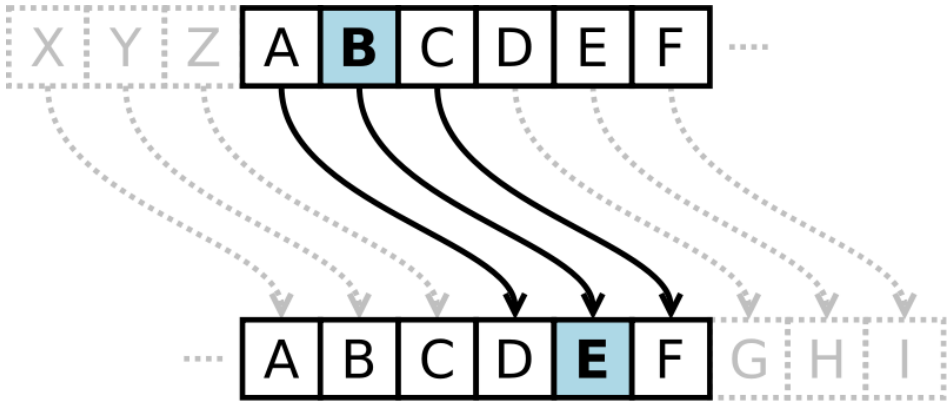


Abb. 1 : Quelle: https://de.wikipedia.org/wiki/Datei:Caesar3.svg

Cäsar-Chiffre

Beispiel

Cäsar-Chiffre

moderne Variante

Cäsar-Chiffre

moderne Variante

- Verschiebung um 13 Buchstaben

Cäsar-Chiffre

moderne Variante

- Verschiebung um 13 Buchstaben
- Ver- und Entschlüsselung durch denselben Vorgang

Cäsar-Chiffre

moderne Variante

- Verschiebung um 13 Buchstaben
- Ver- und Entschlüsselung durch denselben Vorgang
- Verwendung im Internet als Spoilerschutz (sog. ROT13)

Cäsar-Chiffre

Wie sicher ist es?

Cäsar-Chiffre

Wie sicher ist es?

- einziges Geheimnis ist die Verschiebung

Cäsar-Chiffre

Wie sicher ist es?

- einziges Geheimnis ist die Verschiebung
- jedes Zeichen wird gleich verschoben, Charakteristik des Geheimtextes bleibt erhalten

Cäsar-Chiffre

Wie sicher ist es?

- einziges Geheimnis ist die Verschiebung
- jedes Zeichen wird gleich verschoben, Charakteristik des Geheimtextes bleibt erhalten
- Häufigkeitsanalyse der Zeichen zeigt die Verschiebung an

Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

Vigenère-Verschlüsselung

Grundprinzip

Vigenère-Verschlüsselung

Grundprinzip

- im 16. Jh. von Blais de Vigenère beschrieben

Schlüssel	Text: 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	Geheimtext
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	

Abb. 2 : Quelle: https://de.wikipedia.org

Vigenère-Verschlüsselung

Grundprinzip

- im 16. Jh. von Blais de Vigenère beschrieben
- versch. Verschiebung für versch. Klartextzeichen durch Schlüsselwort

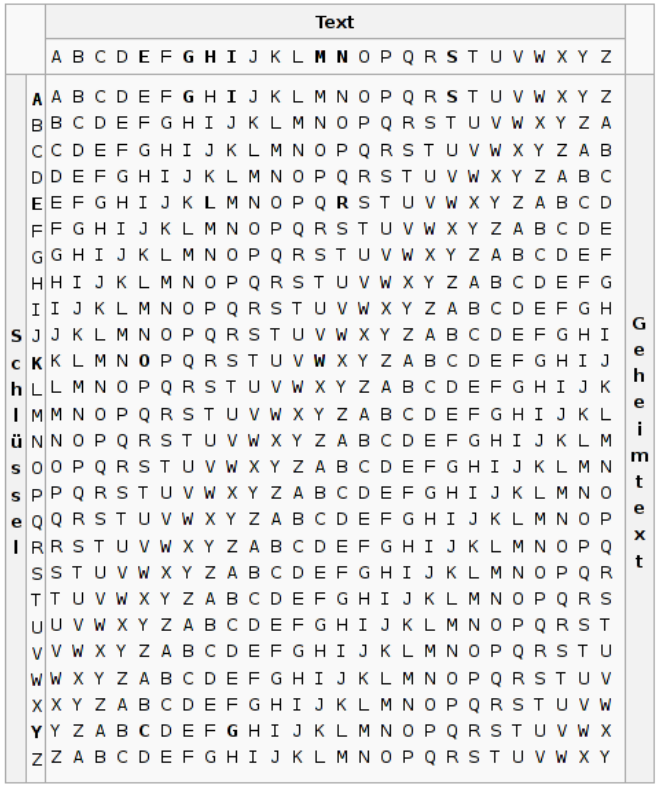
Schlüssel	Text: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	Geheimtext
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A	
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B	
D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C	
E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

Abb. 2 : Quelle: https://de.wikipedia.org

Vigenère-Verschlüsselung

Grundprinzip

- im 16. Jh. von Blais de Vigenère beschrieben
- versch. Verschiebung für versch. Klartextzeichen durch Schlüsselwort
- somit mehrere Geheimtextalphabete (polyalphabetische Substitution)



Schlüssel \ Text	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Geheimtext

Abb. 2 : Quelle: https://de.wikipedia.org

Vigenère-Verschlüsselung

Beispiel

Vigenère-Verschlüsselung

Beispiel

Vigenère-Verschlüsselung

Varianten

Vigenère-Verschlüsselung

Varianten

- Vernam-Chiffre: Schlüssellänge = Klartextlänge

Vigenère-Verschlüsselung

Varianten

- Vernam-Chiffre: Schlüssellänge = Klartextlänge
- One-Time-Pad: zufällig erzeugter Schlüssel mit Gleichverteilung

Vigenère-Verschlüsselung

Varianten

- Vernam-Chiffre: Schlüssellänge = Klartextlänge
- One-Time-Pad: zufällig erzeugter Schlüssel mit Gleichverteilung
- Rotormaschinen: Schlüssel durch Walzeneinstellung (z.B. Enigma)

Abb. 3 : Quelle:
https://commons.wikimedia.org/wiki/File:Enigma_beschriftet_cropped.jpg

Vigenère-Verschlüsselung

Wie sicher ist es?

Vigenère-Verschlüsselung

Wie sicher ist es?

- besser als Cäsar-Chiffre

Vigenère-Verschlüsselung

Wie sicher ist es?

- besser als Cäsar-Chiffre
- abhängig vom Schlüssel, also Anzahl der Geheimtextalphabete

Vigenère-Verschlüsselung

Wie sicher ist es?

- besser als Cäsar-Chiffre
- abhängig vom Schlüssel, also Anzahl der Geheimtextalphabete
- auch komplizierte Permutationsverfahren mit Walzen (z.B. Enigma) konnten geknackt werden

Vigenère-Verschlüsselung

Wie sicher ist es?

- besser als Cäsar-Chiffre
- abhängig vom Schlüssel, also Anzahl der Geheimtextalphabete
- auch komplizierte Permutationsverfahren mit Walzen (z.B. Enigma) konnten geknackt werden
- One-Time-Pad ist nachweislich unknackbar

Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

Problem des Schlüsselaustausches

Ursprung

Problem des Schlüsselaustausches

Ursprung

- Feststellung, dass gute Verschlüsselung nur mit langen und komplizierten Schlüsseln funktioniert

Problem des Schlüsselaustausches

Ursprung

- Feststellung, dass gute Verschlüsselung nur mit langen und komplizierten Schlüsseln funktioniert
- Austausch des Schlüssels genauso schwierig, wie die verschlüsselte Kommunikation selbst

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

- Schlüssel direkt austauschen

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

- Schlüssel direkt austauschen
  - vorherige Absprache

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

- Schlüssel direkt austauschen
  - vorherige Absprache
  - vorgefertigte Codebücher

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

- Schlüssel direkt austauschen
  - vorherige Absprache
  - vorgefertigte Codebücher
- Informationen zur Schlüsselerzeugung austauschen

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

- Schlüssel direkt austauschen
  - vorherige Absprache
  - vorgefertigte Codebücher
- Informationen zur Schlüsselerzeugung austauschen
  - Konstruktion aus dem Datum

Problem des Schlüsselaustausches

verschiedene Möglichkeiten

- Schlüssel direkt austauschen
  - vorherige Absprache
  - vorgefertigte Codebücher
- Informationen zur Schlüsselerzeugung austauschen
  - Konstruktion aus dem Datum
  - Buch als Schlüsseltext verwenden, Seite je nach Datum

Problem des Schlüsselaustausches

heutige Probleme

Problem des Schlüsselaustausches

heutige Probleme

- durch weltweite Vernetzung meist nur elektronische Kommunikation

Problem des Schlüsselaustausches

heutige Probleme

- durch weltweite Vernetzung meist nur elektronische Kommunikation
- Schlüsselinformationen sicher ohne persönlichen Kontakt austauschen

Problem des Schlüsselaustausches

heutige Probleme

- durch weltweite Vernetzung meist nur elektronische Kommunikation
- Schlüsselinformationen sicher ohne persönlichen Kontakt austauschen
- Kommunikation soll komplett verschlüsselt werden

Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

Symmetrische Verschlüsselung

Symmetrische und Asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- es gibt einen geheimen Schlüssel

Symmetrische und Asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- es gibt einen geheimen Schlüssel
- wird zur Ver- und Entschlüsselung verwendet

Symmetrische und Asymmetrische Verschlüsselung

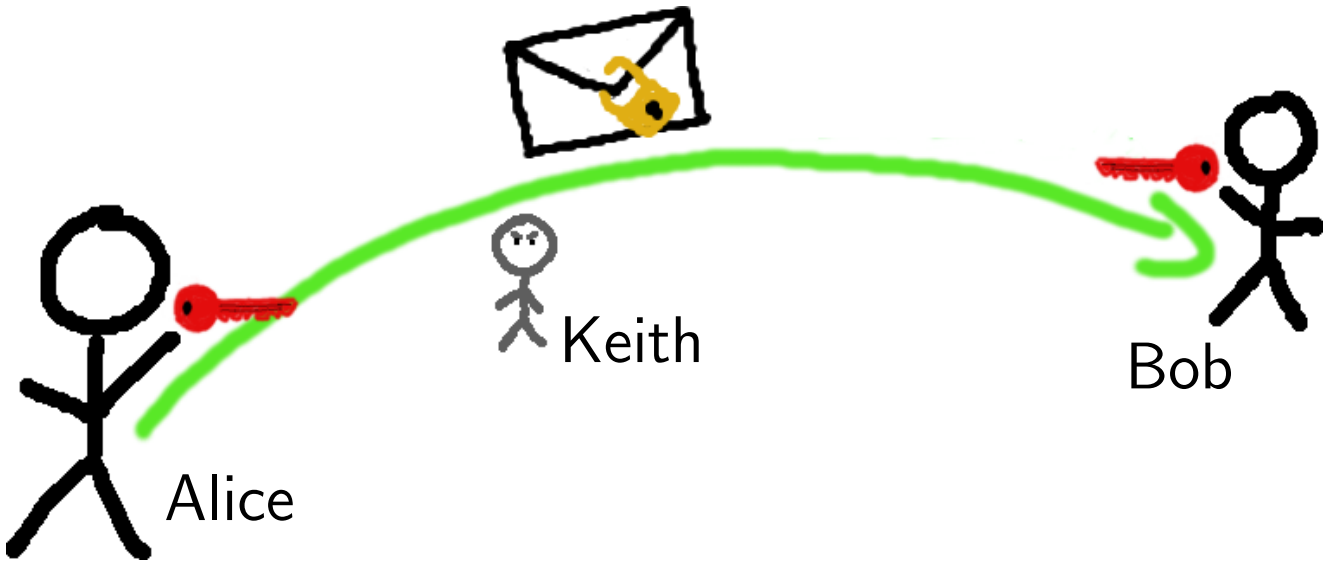
Symmetrische Verschlüsselung

- es gibt einen geheimen Schlüssel
- wird zur Ver- und Entschlüsselung verwendet
- geheimer Schlüssel muss vorher zwischen Senderin und Empfängerin ausgetauscht werden

Symmetrische und Asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- es gibt einen geheimen Schlüssel
- wird zur Ver- und Entschlüsselung verwendet
- geheimer Schlüssel muss vorher zwischen Senderin und Empfängerin ausgetauscht werden



Asymmetrische Verschlüsselung

Symmetrische und Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

- Senderin und Empfängerin besitzen jeweils ein Schlüsselpaar

Symmetrische und Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

- Senderin und Empfängerin besitzen jeweils ein Schlüsselpaar
- öffentlicher Schlüssel dient zum Verschlüsseln

Symmetrische und Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

- Senderin und Empfängerin besitzen jeweils ein Schlüsselpaar
- öffentlicher Schlüssel dient zum Verschlüsseln
- privater Schlüssel dient zum Entschlüsseln

Symmetrische und Asymmetrische Verschlüsselung

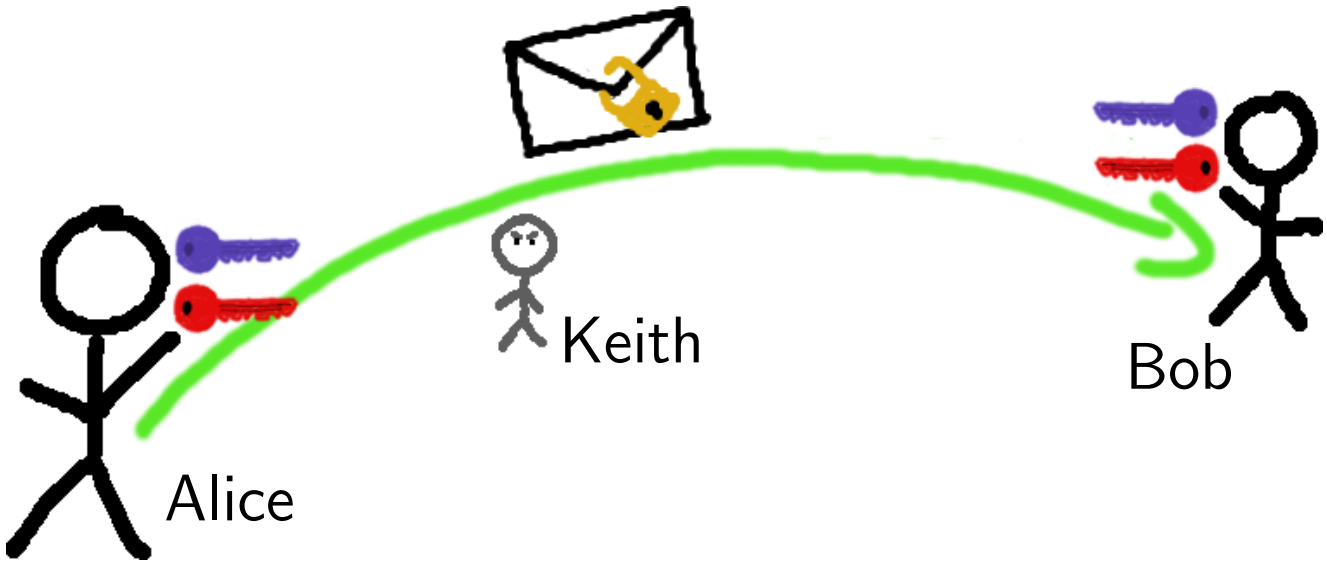
Asymmetrische Verschlüsselung

- Senderin und Empfängerin besitzen jeweils ein Schlüsselpaar
- öffentlicher Schlüssel dient zum Verschlüsseln
- privater Schlüssel dient zum Entschlüsseln
- privater Schlüssel darf niemals weitergegeben werden

Symmetrische und Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

- Senderin und Empfängerin besitzen jeweils ein Schlüsselpaar
- öffentlicher Schlüssel dient zum Verschlüsseln
- privater Schlüssel dient zum Entschlüsseln
- privater Schlüssel darf niemals weitergegeben werden



Navigation

1. Einführung
2. Exkurs: Kryptoanalyse
3. Cäsar-Chiffre
4. Vigenère-Verschlüsselung
5. Problem des Schlüsselaustausches
6. Symmetrische und Asymmetrische Verschlüsselung
7. RSA-Kryptosystem
8. Abschluss

RSA-Kryptosytem

Historie

[1] Massachusetts Institute of Technology

RSA-Kryptosytem

Historie

- 1977 am MIT[1] entwickelt

[1] Massachusetts Institute of Technology

RSA-Kryptosytem

Historie

- 1977 am MIT[1] entwickelt
- drei Mathematiker: **R**ivest, **S**hamir, **A**dleman

[1] Massachusetts Institute of Technology

RSA-Kryptosystem

Kryptosystem?

RSA-Kryptosystem

Kryptosystem?

1. Erzeugen von Schlüsselpaaren

RSA-Kryptosystem

Kryptosystem?

1. Erzeugen von Schlüsselpaaren
2. Unterschreiben von Nachrichten, Prüfen von Unterschriften

RSA-Kryptosystem

Kryptosystem?

1. Erzeugen von Schlüsselpaaren
2. Unterschreiben von Nachrichten, Prüfen von Unterschriften
3. Ver- und Entschlüsseln von Nachrichten

RSA-Kryptosystem

Erzeugen von Schlüsselpaaren

[2]Funktion, welche in eine Richtung leicht und in der Rückrichtung schwer zu berechnen ist

RSA-Kryptosystem

Erzeugen von Schlüsselpaaren

- durch Multiplikation großer Primzahlen (sog. Einwegfunktion[2])

[2] Funktion, welche in eine Richtung leicht und in der Rückrichtung schwer zu berechnen ist

RSA-Kryptosystem

Erzeugen von Schlüsselpaaren

- durch Multiplikation großer Primzahlen (sog. Einwegfunktion[2])
- ein geheimer Schlüssel (Unterschreiben, Entschlüsseln)

[2] Funktion, welche in eine Richtung leicht und in der Rückrichtung schwer zu berechnen ist

RSA-Kryptosystem

Erzeugen von Schlüsselpaaren

- durch Multiplikation großer Primzahlen (sog. Einwegfunktion[2])
- ein geheimer Schlüssel (Unterschreiben, Entschlüsseln)
- ein öffentlicher Schlüssel (Prüfen, Verschlüsseln)

[2] Funktion, welche in eine Richtung leicht und in der Rückrichtung schwer zu berechnen ist

RSA-Kryptosystem

Unterschreiben von Nachrichten, Prüfen von Unterschriften

RSA-Kryptosystem

Unterschreiben von Nachrichten, Prüfen von Unterschriften

1. charakteristische Zahl des Klartextes (sog. Hash) verschlüsseln (geheimer Schlüssel des Senders)

RSA-Kryptosystem

Unterschreiben von Nachrichten, Prüfen von Unterschriften

1. charakteristische Zahl des Klartextes (sog. Hash) verschlüsseln (geheimer Schlüssel des Senders)
2. Empfänger entschlüsselt Zahl mit öffentlichem Schlüssel des Senders

RSA-Kryptosystem

Unterschreiben von Nachrichten, Prüfen von Unterschriften

1. charakteristische Zahl des Klartextes (sog. Hash) verschlüsseln (geheimer Schlüssel des Senders)
2. Empfänger entschlüsselt Zahl mit öffentlichem Schlüssel des Senders
3. Übereinstimmung mit Hash des Klartextes

RSA-Kryptosystem

Unterschreiben von Nachrichten, Prüfen von Unterschriften

1. charakteristische Zahl des Klartextes (sog. Hash) verschlüsseln (geheimer Schlüssel des Senders)
2. Empfänger entschlüsselt Zahl mit öffentlichem Schlüssel des Senders
3. Übereinstimmung mit Hash des Klartextes
4. Sender ist authentifiziert

RSA-Kryptosystem

Ver- und Entschlüsseln von Nachrichten

RSA-Kryptosystem

Ver- und Entschlüsseln von Nachrichten

1. Sender verschlüsselt Nachricht mit öffentlichem Schlüssel des Empfängers

RSA-Kryptosystem

Ver- und Entschlüsseln von Nachrichten

1. Sender verschlüsselt Nachricht mit öffentlichem Schlüssel des Empfängers
2. Empfänger entschlüsselt Nachricht mit seinem geheimen Schlüssel

RSA-Kryptosystem

Wie sicher ist es?

RSA-Kryptosystem

Wie sicher ist es?

- Sicherheit basiert auf Primfaktorzerlegung

RSA-Kryptosystem

Wie sicher ist es?

- Sicherheit basiert auf Primfaktorzerlegung
- zu großer Aufwand bei großen Primzahlprodukten (größer 500 Stellen)

RSA-Kryptosystem

Wie sicher ist es?

- Sicherheit basiert auf Primfaktorzerlegung
- zu großer Aufwand bei großen Primzahlprodukten (größer 500 Stellen)
- angeblich könnten Quantencomputer gefährlich werden

Verbesserungen in der Praxis

RSA-Kryptosystem

Verbesserungen in der Praxis

- Mischung aus symmetrischer und asymmetrischer Verschlüsselung aufgrund des Rechenaufwandes (z.B. PGP)

RSA-Kryptosystem

Verbesserungen in der Praxis

- Mischung aus symmetrischer und asymmetrischer Verschlüsselung aufgrund des Rechenaufwandes (z.B. PGP)
- Bearbeitung des Klartextes vor der Verschlüsselung (sog. Padding)

Zum Abschluss

weiterführende Informationen

- Kippenhahn, Rudolf: Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte, Rowohlt 2001.
- Wikipedia: *Caesar-Verschlüsselung, Polyalphabetische Substitution, One-Time-Pad, Symmetrisches Kryptosystem, Public-Key-Verschlüsselungsverfahren, Verschlüsselungsverfahren, RSA-Kryptosystem, Optimal Asymmetric Encryption Padding, Padding (Informatik), Pretty Good Privacy, Buchstabenhäufigkeit, Enigma (Maschine)*
- http://www.cryptool-online.org/

Zum Abschluss

Gibt es noch Fragen?

Vielen Dank für die Aufmerksamkeit!