

Kryptografie

Die Mathematik hinter den Geheimcodes

Rick Schumann

www.math.tu-freiberg.de/~schumann

Institut für Diskrete Mathematik und Algebra,
TU Bergakademie Freiberg

Akademische Woche Sankt Afra / 08.02.2011



- 1 Einführung
- 2 Symmetrische Kryptosysteme
- 3 Asymmetrische Kryptosysteme



Bezeichnung

Kryptografie ist die Wissenschaft die sich mit der Informationssicherheit befasst. Wesentliche Aspekte dabei sind:

- Vertraulichkeit

Bezeichnung

Kryptografie ist die Wissenschaft die sich mit der Informationssicherheit befasst. Wesentliche Aspekte dabei sind:

- Vertraulichkeit
- Integrität

Bezeichnung

Kryptografie ist die Wissenschaft die sich mit der Informationssicherheit befasst. Wesentliche Aspekte dabei sind:

- Vertraulichkeit
- Integrität
- Authentizität

Aufgabe

Entschlüsseln Sie folgenden Text:

DHSKEATERLLRITENNICI



Lösung

Der Geheimtext ist durch eine Skytale verschlüsselt worden, wir probieren die ersten möglichen Zeilenanzahlen durch:

1 Zeile: DHSKEATERLLRITENNICT

Lösung

Der Geheimtext ist durch eine Skytale verschlüsselt worden, wir probieren die ersten möglichen Zeilenanzahlen durch:

1 Zeile: DHSKEATERLLRITENNICT
2 Zeilen: DSETRLIENC
 HKAELRTNIT

Lösung

Der Geheimtext ist durch eine Skytale verschlüsselt worden, wir probieren die ersten möglichen Zeilenanzahlen durch:

1 Zeile: DHSKEATERLLRITENNICT

2 Zeilen: DSETRLIENC

 HKAELRTNIT

3 Zeilen: DKTLINC

 HEELTNT

 SARREI

Lösung

Der Geheimtext ist durch eine Skytale verschlüsselt worden, wir probieren die ersten möglichen Zeilenanzahlen durch:

1 Zeile: DHSKEATERLLRITENNICT

2 Zeilen: DSETRLIENC
HKAELRTNIT

3 Zeilen: DKTLINE
HEELTNT
SARREI

4 Zeilen: DERIN
HALTI
STLEC
KERNT

Definition

Eine *Kryptosystem* $(\mathcal{P}(A), \mathcal{C}(B), \mathcal{K}, \mathcal{E}, \mathcal{D})$ besteht aus

- einer Menge \mathcal{P} von *Klartexten* über einem *Klartextalphabet* A ,

Definition

Eine *Kryptosystem* $(\mathcal{P}(A), \mathcal{C}(B), \mathcal{K}, \mathcal{E}, \mathcal{D})$ besteht aus

- einer Menge \mathcal{P} von *Klartexten* über einem *Klartextalphabet* A ,
- einer Menge \mathcal{C} von *Geheimtexten* über einem *Geheimtextalphabet* B ,

Definition

Eine *Kryptosystem* $(\mathcal{P}(A), \mathcal{C}(B), \mathcal{K}, \mathcal{E}, \mathcal{D})$ besteht aus

- einer Menge \mathcal{P} von *Klartexten* über einem *Klartextalphabet* A ,
- einer Menge \mathcal{C} von *Geheimtexten* über einem *Geheimtextalphabet* B ,
- einer Menge \mathcal{K} von *Schlüsseln*, dem *Schlüsselraum*,

Definition

Eine *Kryptosystem* $(\mathcal{P}(A), \mathcal{C}(B), \mathcal{K}, \mathcal{E}, \mathcal{D})$ besteht aus

- einer Menge \mathcal{P} von *Klartexten* über einem *Klartextalphabet* A ,
- einer Menge \mathcal{C} von *Geheimtexten* über einem *Geheimtextalphabet* B ,
- einer Menge \mathcal{K} von *Schlüsseln*, dem *Schlüsselraum*,
- der *Verschlüsselung* oder *Chiffrierung* \mathcal{E} , d. h. einer Familie von Abbildungen $E_K : \mathcal{P} \rightarrow \mathcal{C}$, $K \in \mathcal{K}$,

Definition

Eine *Kryptosystem* $(\mathcal{P}(A), \mathcal{C}(B), \mathcal{K}, \mathcal{E}, \mathcal{D})$ besteht aus

- einer Menge \mathcal{P} von *Klartexten* über einem *Klartextalphabet* A ,
- einer Menge \mathcal{C} von *Geheimtexten* über einem *Geheimtextalphabet* B ,
- einer Menge \mathcal{K} von *Schlüsseln*, dem *Schlüsselraum*,
- der *Verschlüsselung* oder *Chiffrierung* \mathcal{E} , d. h. einer Familie von Abbildungen $E_K : \mathcal{P} \rightarrow \mathcal{C}$, $K \in \mathcal{K}$,
- der *Entschlüsselung* oder *Dechiffrierung* \mathcal{D} , d. h. einer Familie von Abbildungen $D_K : \mathcal{C} \rightarrow \mathcal{P}$, $K \in \mathcal{K}$,

Definition

Eine *Kryptosystem* $(\mathcal{P}(A), \mathcal{C}(B), \mathcal{K}, \mathcal{E}, \mathcal{D})$ besteht aus

- einer Menge \mathcal{P} von *Klartexten* über einem *Klartextalphabet* A ,
- einer Menge \mathcal{C} von *Geheimtexten* über einem *Geheimtextalphabet* B ,
- einer Menge \mathcal{K} von *Schlüsseln*, dem *Schlüsselraum*,
- der *Verschlüsselung* oder *Chiffrierung* \mathcal{E} , d. h. einer Familie von Abbildungen $E_K : \mathcal{P} \rightarrow \mathcal{C}$, $K \in \mathcal{K}$,
- der *Entschlüsselung* oder *Dechiffrierung* \mathcal{D} , d. h. einer Familie von Abbildungen $D_K : \mathcal{C} \rightarrow \mathcal{P}$, $K \in \mathcal{K}$,

so daß für alle $K \in \mathcal{K}$ und alle Klartexte P gilt $D_K(E_K(P)) = P$. Die Zuordnungen von E_K und D_K zu $K \in \mathcal{K}$ stellen den *Chiffrier-* und den *Dechiffrieralgorithmus* dar.



Definition

Ein Kryptosystem, in dem Sender und Empfänger über den selben Schlüssel verfügen bezeichnet man als *symmetrisch*.

Falls der Empfänger zusätzliche Informationen zum Entschlüsseln besitzt, spricht man von einem *asymmetrischen* bzw. *Public-Key-Verfahren*.



- 1 Einführung
- 2 Symmetrische Kryptosysteme**
- 3 Asymmetrische Kryptosysteme



Definition

Als *Transpositionskryptosystem* bezeichnet man ein System, in dem die Buchstaben des Klartextes bei der Chiffrierung erhalten bleiben, aber sich die Positionen der Buchstaben ändern.



Definition

Als *Transpositionskryptosystem* bezeichnet man ein System, in dem die Buchstaben des Klartextes bei der Chiffrierung erhalten bleiben, aber sich die Positionen der Buchstaben ändern.

Definition

Als *Substitutionskryptosystem* bezeichnet man dagegen ein System, in dem die Buchstaben des Klartextes gegen bestimmte Zeichen eines Geheimentalphabets ausgetauscht werden, die Position der Buchstaben aber mit den der Chiffrierungen übereinstimmt.



Spezialfälle

Translationskryptosysteme, bei denen das Alphabet um eine gewisse Anzahl an Buchstaben verschoben wird (z.B. bei der sogenannten *Caesarchiffre* um 3 Stellen: $A \rightarrow D, B \rightarrow E, \dots, Z \rightarrow C$).

Spezialfälle

Translationskryptosysteme, bei denen das Alphabet um eine gewisse Anzahl an Buchstaben verschoben wird (z.B. bei der sogenannten *Caesarchiffre* um 3 Stellen: $A \rightarrow D, B \rightarrow E, \dots, Z \rightarrow C$).

Aufgabe

Von dem folgenden Geheimtext ist bekannt, daß er mit einer Translationschiffre verschlüsselt wurde.

MRNBACNGCRBCWRLQCPNQNRV



Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: $E \rightarrow N$

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: E → N

Entschlüsselungstabelle:

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
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

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: $E \rightarrow N$

Entschlüsselungstabelle:

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
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

Daraus ergibt sich dann die Entschlüsselung:

MRNBACNGCRBCWRLQCPNQRV

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: $E \rightarrow N$

Entschlüsselungstabelle:

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
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

Daraus ergibt sich dann die Entschlüsselung:

MRNBNA CNGCRBCWRLQCPNQNRV

D

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: E \rightarrow N

Entschlüsselungstabelle:

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
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

Daraus ergibt sich dann die Entschlüsselung:

MRNBNACNGCRBCWRLQCPNQRV

DI

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: $E \rightarrow N$

Entschlüsselungstabelle:

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
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

Daraus ergibt sich dann die Entschlüsselung:

MRNBACNGCRBCWRLQCPNQRV

DIE

Lösung

Häufigkeitsanalyse:

M	R	N	B	A	C	G	W	L	Q	P	V
1	4	5	2	1	4	1	1	1	2	1	1

Annahme: E \rightarrow N

Entschlüsselungstabelle:

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
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

Daraus ergibt sich dann die Entschlüsselung:

MRNBNA CNGCRBCWRLQCPNQRV
DIESERTEXTISTNICHTGEHEIM

Definition

Wird bei einem Substitutionskryptosystem jedem Buchstaben unabhängig von seiner Position im Klartext eine festes Zeichen zugeordnet, spricht man von einem *monoalphabetischen Kryptosystem*. Falls bei der Verschlüsselung die Position des Zeichens von Bedeutung ist, handelt es sich um ein *polyalphabetisches Kryptosystem*.



Beispiel

- Vigenère Verschlüsselung

Klartext: KLARTEXT

Beispiel

- Vigenère Verschlüsselung

Klartext: KLARTEXT

Schlüssel: ⊕ ZEBRAZEB



Beispiel

- Vigenère Verschlüsselung

Klartext: KLARTEXT

Schlüssel: ⊕ ZEBRAZEB

Geheimtext: = JPBITDBU

Beispiel

- Vigenère Verschlüsselung

Klartext: KLARTEXT

Schlüssel: ⊕ ZEBRAZEB

Geheimtext: = JPBITDBU

- Einmalschlüssel-Verfahren

Hierbei wird eine zufällige Buchstabenfolge verwendet, welche mindestens genauso lang ist wie der Klartext. Der Schlüssel darf nur einmalig genutzt werden.



Spezialfall

Visuelle Kryptografie

- Entschlüsselung mittels Übereinanderlegen 2er Folien



Spezialfall

Visuelle Kryptografie

- Entschlüsselung mittels Übereinanderlegen 2er Folien
- 4 Teilpunkte pro Bildpunkt:  , 



Spezialfall

Visuelle Kryptografie

- Entschlüsselung mittels Übereinanderlegen 2er Folien
- 4 Teilpunkte pro Bildpunkt:  , 
- Schlüssel folie (zufällige Kombination) und Nachrichten folie (abhängig von Schlüssel folie und Bild)

Spezialfall



Visuelle Kryptografie

- Entschlüsselung mittels Übereinanderlegen 2er Folien
- 4 Teilpunkte pro Bildpunkt:  , 
- Schüsselfolie (zufällige Kombination) und Nachrichtenfolie (abhängig von Schüsselfolie und Bild)
 - heller Bildpunkt:

$$\begin{array}{ccccc} \begin{array}{c} \text{Schüsselfolie} \\ \img alt="2x2 grid of squares" data-bbox="260 560 285 585" \end{array} & + & \begin{array}{c} \text{Nachrichtenfolie} \\ \img alt="2x2 grid of squares" data-bbox="505 560 530 585" \end{array} & = & \begin{array}{c} \text{geheimes Bild} \\ \img alt="2x2 grid of squares" data-bbox="755 560 780 585" \end{array} \end{array}$$

Spezialfall

Visuelle Kryptografie

- Entschlüsselung mittels Übereinanderlegen 2er Folien
- 4 Teilpunkte pro Bildpunkt:  , 
- Schüsselfolie (zufällige Kombination) und Nachrichtenfolie (abhängig von Schüsselfolie und Bild)

- heller Bildpunkt:

$$\begin{array}{ccccc} \begin{array}{c} \text{Schüsselfolie} \\ \text{Nachrichtenfolie} \end{array} & + & \begin{array}{c} \text{Schüsselfolie} \\ \text{Nachrichtenfolie} \end{array} & = & \begin{array}{c} \text{Schüsselfolie} \\ \text{geheimes Bild} \end{array} \end{array}$$

- dunkler Bildpunkt:

$$\begin{array}{ccccc} \begin{array}{c} \text{Schüsselfolie} \\ \text{Nachrichtenfolie} \end{array} & + & \begin{array}{c} \text{Schüsselfolie} \\ \text{Nachrichtenfolie} \end{array} & = & \begin{array}{c} \text{Schüsselfolie} \\ \text{geheimes Bild} \end{array} \end{array}$$

- 1 Einführung
- 2 Symmetrische Kryptosysteme
- 3 Asymmetrische Kryptosysteme**



Grundprinzip

- 1 Empfänger B konstruiert eine Verschlüsselungsfunktion E_B als *Einwegfunktion mit Falltür*. Dies sind Funktionen, deren Umkehrung D_B nur mittels einer geheimen Zusatzinformation einfach bestimmt werden kann.

Grundprinzip

- 1 Empfänger B konstruiert eine Verschlüsselungsfunktion E_B als *Einwegfunktion mit Falltür*. Dies sind Funktionen, deren Umkehrung D_B nur mittels einer geheimen Zusatzinformation einfach bestimmt werden kann.
- 2 B gibt E_B als seinen öffentlichen Schlüssel bekannt, hält aber D_B geheim.

Grundprinzip

- 1 Empfänger B konstruiert eine Verschlüsselungsfunktion E_B als *Einwegfunktion mit Falltür*. Dies sind Funktionen, deren Umkehrung D_B nur mittels einer geheimen Zusatzinformation einfach bestimmt werden kann.
- 2 B gibt E_B als seinen öffentlichen Schlüssel bekannt, hält aber D_B geheim.
- 3 Ein Sender A einer Nachricht P an B verschlüsselt sie gemäß $C = E_B(P)$ und sendet sie an B .



Grundprinzip

- 1 Empfänger B konstruiert eine Verschlüsselungsfunktion E_B als *Einwegfunktion mit Falltür*. Dies sind Funktionen, deren Umkehrung D_B nur mittels einer geheimen Zusatzinformation einfach bestimmt werden kann.
- 2 B gibt E_B als seinen öffentlichen Schlüssel bekannt, hält aber D_B geheim.
- 3 Ein Sender A einer Nachricht P an B verschlüsselt sie gemäß $C = E_B(P)$ und sendet sie an B .
- 4 B entschlüsselt den Geheimtext C mittels D_B und erhält $D_B(C) = D_B(E_B(P)) = P$.



Satz

Seien $n > 0$ eine natürliche Zahl und $e \in \mathbb{Z}$. Genau dann existiert ein $d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{n}$, wenn $\text{ggT}(e, n) = 1$ gilt.

Satz

Seien $n > 0$ eine natürliche Zahl und $e \in \mathbb{Z}$. Genau dann existiert ein $d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{n}$, wenn $\text{ggT}(e, n) = 1$ gilt.

Definition

Für jede natürliche Zahl $n > 0$ ist $\varphi(n)$ die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n . Für jede Primzahl p gilt daher $\varphi(p) = p - 1$.



Satz

Seien $n > 0$ eine natürliche Zahl und $e \in \mathbb{Z}$. Genau dann existiert ein $d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{n}$, wenn $\text{ggT}(e, n) = 1$ gilt.

Definition

Für jede natürliche Zahl $n > 0$ ist $\varphi(n)$ die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n . Für jede Primzahl p gilt daher $\varphi(p) = p - 1$.

Satz

Genau dann ist die natürliche Zahl $n > 1$ Produkt paarweise verschiedener Primzahlen, wenn für alle ganzen Zahlen a gilt

$$a^{\varphi(n)+1} \equiv a \pmod{n}.$$



RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .

RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .

RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .
- 3 B wählt eine zu $\varphi(n_B)$ teilerfremde Zahl e_B , den *Verschlüsselungsexponenten* von B zwischen 1 und $\varphi(n_B) - 1$.

Satz

Seien $n > 0$ eine natürliche Zahl und $e \in \mathbb{Z}$. Genau dann existiert ein $d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{n}$, wenn $\text{ggT}(e, n) = 1$ gilt.

Definition

Für jede natürliche Zahl $n > 0$ ist $\varphi(n)$ die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n . Für jede Primzahl p gilt daher $\varphi(p) = p - 1$.

Satz

Genau dann ist die natürliche Zahl $n > 1$ Produkt paarweise verschiedener Primzahlen, wenn für alle ganzen Zahlen a gilt

$$a^{\varphi(n)+1} \equiv a \pmod{n}.$$



RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .
- 3 B wählt eine zu $\varphi(n_B)$ teilerfremde Zahl e_B , den *Verschlüsselungsexponenten* von B zwischen 1 und $\varphi(n_B) - 1$.
- 4 B bestimmt den *Entschlüsselungsexponenten* d_B mit $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ und $1 \leq d_B < \varphi(n_B)$.

RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .
- 3 B wählt eine zu $\varphi(n_B)$ teilerfremde Zahl e_B , den *Verschlüsselungsexponenten* von B zwischen 1 und $\varphi(n_B) - 1$.
- 4 B bestimmt den *Entschlüsselungsexponenten* d_B mit $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ und $1 \leq d_B < \varphi(n_B)$.
- 5 B gibt n_B und e_B öffentlich bekannt, hält die anderen Zahlen aber geheim.

RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .
- 3 B wählt eine zu $\varphi(n_B)$ teilerfremde Zahl e_B , den *Verschlüsselungsexponenten* von B zwischen 1 und $\varphi(n_B) - 1$.
- 4 B bestimmt den *Entschlüsselungsexponenten* d_B mit $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ und $1 \leq d_B < \varphi(n_B)$.
- 5 B gibt n_B und e_B öffentlich bekannt, hält die anderen Zahlen aber geheim.
- 6 Sender A stellt den Klartext P als Folge natürlicher Zahlen n_1, \dots, n_r zwischen 0 und $n_B - 1$ dar. Dann bestimmt er zu jeder dieser Zahlen n_i den Geheimtext $c_i \equiv n_i^{e_B} \pmod{n_B}$ und sendet die Folge c_1, \dots, c_r an B .

RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .
- 3 B wählt eine zu $\varphi(n_B)$ teilerfremde Zahl e_B , den *Verschlüsselungsexponenten* von B zwischen 1 und $\varphi(n_B) - 1$.
- 4 B bestimmt den *Entschlüsselungsexponenten* d_B mit $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ und $1 \leq d_B < \varphi(n_B)$.
- 5 B gibt n_B und e_B öffentlich bekannt, hält die anderen Zahlen aber geheim.
- 6 Sender A stellt den Klartext P als Folge natürlicher Zahlen n_1, \dots, n_r zwischen 0 und $n_B - 1$ dar. Dann bestimmt er zu jeder dieser Zahlen n_i den Geheimtext $c_i \equiv n_i^{e_B} \pmod{n_B}$ und sendet die Folge c_1, \dots, c_r an B .
- 7 B bildet zu den empfangenen Geheimtexten c_i die Potenzen $c_i^{d_B} = n_i^{e_B d_B} \equiv n_i \pmod{n_B}$, die dann noch in die Klartexte zurückverwandelt werden müssen.

Satz

Seien $n > 0$ eine natürliche Zahl und $e \in \mathbb{Z}$. Genau dann existiert ein $d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{n}$, wenn $\text{ggT}(e, n) = 1$ gilt.

Definition

Für jede natürliche Zahl $n > 0$ ist $\varphi(n)$ die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n . Für jede Primzahl p gilt daher $\varphi(p) = p - 1$.

Satz

Genau dann ist die natürliche Zahl $n > 1$ Produkt paarweise verschiedener Primzahlen, wenn für alle ganzen Zahlen a gilt

$$a^{\varphi(n)+1} \equiv a \pmod{n}.$$



RSA-Algorithmus

- 1 B wählt zufällig zwei große Primzahlen p und q .
- 2 B berechnet $n_B = pq$ und $\varphi(n_B) = (p - 1)(q - 1)$. Man nennt n_B den *RSA-Modul* von B .
- 3 B wählt eine zu $\varphi(n_B)$ teilerfremde Zahl e_B , den *Verschlüsselungsexponenten* von B zwischen 1 und $\varphi(n_B) - 1$.
- 4 B bestimmt den *Entschlüsselungsexponenten* d_B mit $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ und $1 \leq d_B < \varphi(n_B)$.
- 5 B gibt n_B und e_B öffentlich bekannt, hält die anderen Zahlen aber geheim.
- 6 Sender A stellt den Klartext P als Folge natürlicher Zahlen n_1, \dots, n_r zwischen 0 und $n_B - 1$ dar. Dann bestimmt er zu jeder dieser Zahlen n_i den Geheimtext $c_i \equiv n_i^{e_B} \pmod{n_B}$ und sendet die Folge c_1, \dots, c_r an B .
- 7 B bildet zu den empfangenen Geheimtexten c_i die Potenzen $c_i^{d_B} = n_i^{e_B d_B} \equiv n_i \pmod{n_B}$, die dann noch in die Klartexte zurückverwandelt werden müssen.

Links

- [Unsere Kryptographieseite](#)
- www.kryptographiespielplatz.de
- [Visuelle Kryptographie](#)



Vielen Dank für die
Aufmerksamkeit.

