Über das Hüten von Geheimnissen

Gabor Wiese

Tag der Mathematik, 14. Juni 2008

Institut für Experimentelle Mathematik

Universität Duisburg-Essen

Rechnen mit Rest

Seien a, b, c, d und n ganze Zahlen mit $n \geq 1$.

Falls $a - b$ von n geteilt wird, schreiben wir

$$a \equiv b \mod n$$

(D.h. a und b lassen beim Teilen durch n denselben Rest).

Rechnen mit Rest

Seien a, b, c, d und n ganze Zahlen mit $n \geq 1$.

Falls $a - b$ von n geteilt wird, schreiben wir

$$a \equiv b \mod n$$

(D.h. a und b lassen beim Teilen durch n denselben Rest).

Falls

$$a \equiv b \mod n \quad \text{und} \quad c \equiv d \mod n$$

gelten, dann gelten auch

$$a + c \equiv b + d \mod n$$

und

$$a \cdot c \equiv b \cdot d \mod n.$$

Was ist eine Primzahl?

Eine Primzahl p ist eine natürliche Zahl größer als 1, die nur durch 1 und sich selbst teilbar ist.

Beispiele: 2, 3, 5, 7, 11, . . . , 37, . . . , 997, . . .

Der kleine Satz von Fermat

Sei p eine Primzahl. Sei a irgendeine natürliche Zahl zwischen 1 und $p-1$. Dann gilt:

$$a^{p-1} \equiv 1 \mod p.$$

(D.h. a^{p-1} lässt beim Teilen durch p den Rest 1.)

Der kleine Satz von Fermat

Sei p eine Primzahl. Sei a irgendeine natürliche Zahl zwischen 1 und $p-1$. Dann gilt:

$$a^{p-1} \equiv 1 \mod p.$$

(D.h. a^{p-1} lässt beim Teilen durch p den Rest 1.)

Folgerung: Sei b eine weitere natürliche Zahl, die

$$b \equiv 1 \mod (p-1)$$

erfüllt. Dann gilt:

$$a^b \equiv a \mod p.$$

Der Algorithmus von Euklid

Seien r und n natürliche Zahlen mit größtem gemeinsamen Teiler 1.

Dann kann man mit Euklids Algorithmus eine natürliche Zahl s bestimmen, die

$$r \cdot s \equiv 1 \mod n$$

erfüllt.

1. Lösung

Zeitung

(zu verteilen in ganz Deutschland):

Zur Kommunikation verwende man die große Primzahl p, zum Beispiel

269599466671506397946670150870196306736371444225405724811036102499 51.

(Jeder kennt sie und jeder darf sie auch kennen.)

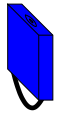

1. Lösung



1. Lösung


Wählt r, s mit

$r \cdot s \equiv 1 \bmod (p-1)$



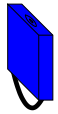
Wählt t, u mit

$t \cdot u \equiv 1 \bmod (p-1)$


1. Lösung

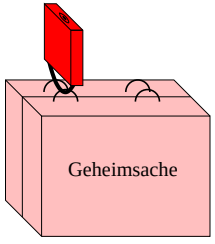

Wählt r, s mit

$r \cdot s \equiv 1 \bmod (p-1)$



Wählt t, u mit

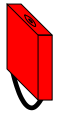
$t \cdot u \equiv 1 \bmod (p-1)$



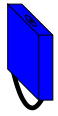
Abschließen:

$K_1 := m^r \bmod p$

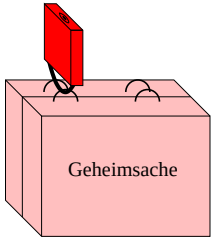

1. Lösung



Wählt r, s mit

$r \cdot s \equiv 1 \bmod (p-1)$

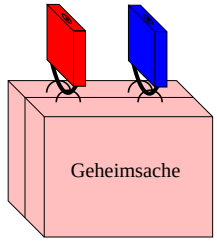

Wählt t, u mit

$t \cdot u \equiv 1 \bmod (p-1)$



Abschließen:

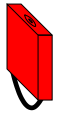
$K_1 := m^r \bmod p$



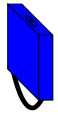
Abschließen:

$K_2 := (K_1)^t \bmod p$

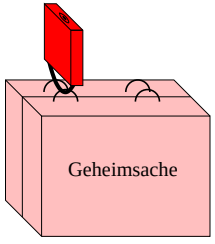

1. Lösung



Wählt r, s mit

$r \cdot s \equiv 1 \bmod (p-1)$

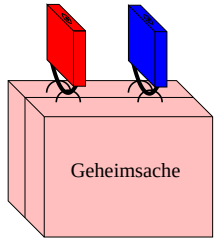

Wählt t, u mit

$t \cdot u \equiv 1 \bmod (p-1)$



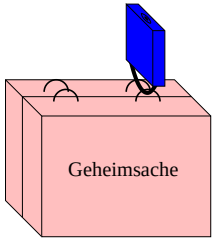
Abschließen:

$K_1 := m^r \bmod p$



Abschließen:

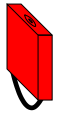
$K_2 := (K_1)^t \bmod p$



Aufschließen:

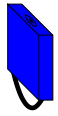
$K_3 := (K_2)^s \bmod p$


1. Lösung

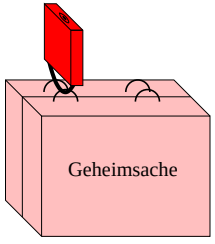
Wählt r, s mit

$r \cdot s \equiv 1 \bmod (p-1)$



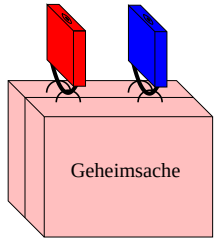
Wählt t, u mit

$t \cdot u \equiv 1 \bmod (p-1)$



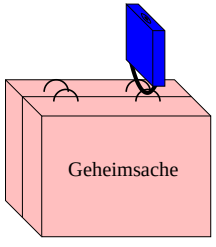
Abschließen:

$K_1 := m^r \bmod p$



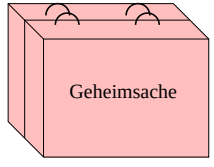
Abschließen:

$K_2 := (K_1)^t \bmod p$



Aufschließen:

$K_3 := (K_2)^s \bmod p$



Aufschließen:

$(K_3)^u \equiv m \bmod p$

2. Lösung

Eine große Zahl kann zum Verschlüsseln dienen.

2. Lösung

Eine große Zahl kann zum Verschlüsseln dienen.

Ziel: Tausche Schlüssel (große Zahl) aus.

2. Lösung

Eine große Zahl kann zum Verschlüsseln dienen.

Ziel: Tausche Schlüssel (große Zahl) aus.

Zeitung

(zu verteilen in ganz Deutschland):

Zur Kommunikation verwende man die große Primzahl p, zum Beispiel

26959946667150639794667015087019630673637144422540572481103610249951

und eine Zahl $0 < g < p$.

(Jeder kennt sie und jeder darf sie auch kennen.)

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.




Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.


1. Wählt $a \in \mathbb{N}$.


1. Wählt $b \in \mathbb{N}$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $r = g^a$.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $s = g^b$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $r = g^a$.
3. Verschickt r.

4. Empfängt s.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $s = g^b$.
3. Verschickt s.

4. Empfängt r.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $r = g^a$.
3. Verschickt r.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $s = g^b$.
3. Verschickt s.


4. Empfängt s.
5. Berechnet $s^a = (g^b)^a$.

4. Empfängt r.
5. Berechnet $r^b = (g^a)^b$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: Primzahl p und $0 < m < p$.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $r = g^a$.
3. Verschickt r.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $s = g^b$.
3. Verschickt s.


4. Empfängt s.
5. Berechnet $s^a = (g^b)^a$.

4. Empfängt r.
5. Berechnet $r^b = (g^a)^b$.

Gemeinsames Geheimnis:  $= g^{(a \cdot b)}$.

Einfach und praktisch unmöglich

Sei p eine Primzahl und g und a natürliche Zahlen.

Es ist einfach, $g^a \mod p$ auszurechnen.

Einfach und praktisch unmöglich

Sei p eine Primzahl und g und a natürliche Zahlen.

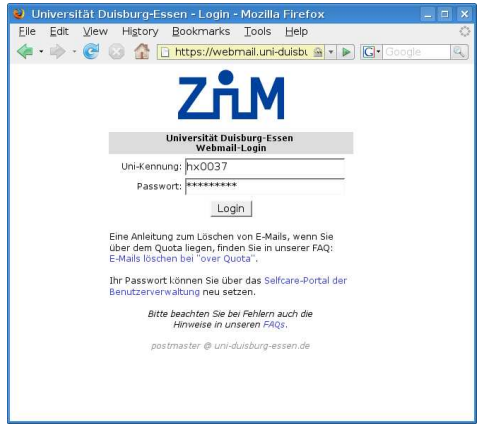
Es ist einfach, $g^a \mod p$ auszurechnen.

Es ist praktisch unmöglich,

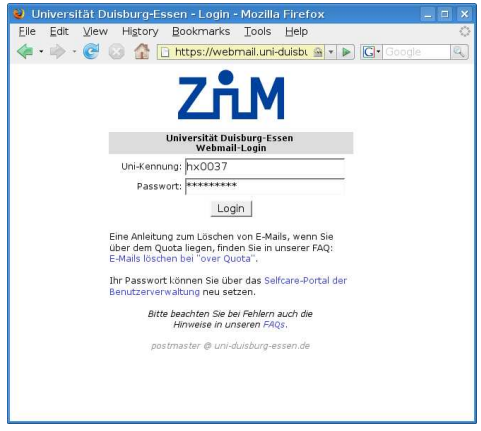
aus $g^a \mod p$ und g wieder a auszurechnen.

Probleme unseres Alltags

- E-Mails lesen
  Niemand soll meine Mails lesen!

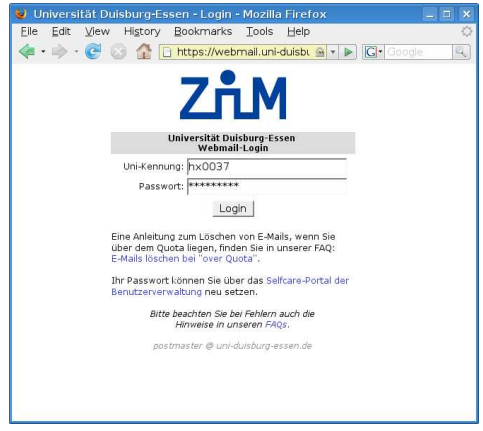


Probleme unseres Alltags



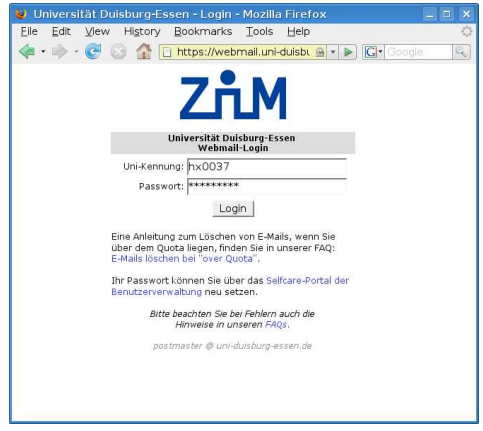
- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.

Probleme unseres Alltags



- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.
- Geld abheben mit der EC-Karte
  ...

Probleme unseres Alltags



- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.
- Geld abheben mit der EC-Karte
  ...

- Telefonieren mit dem Handy
  Niemand soll auf meine Kosten telefonieren!

- etc.

Kryptographie

Verschlüsselungsverfahren:

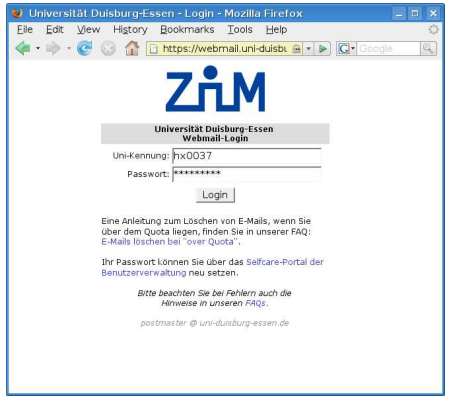
- Diskrete Logarithmen in endlichen Körpern (Diffie-Hellman)
- Elliptische Kurven
- RSA

Kryptographie

Verschlüsselungsverfahren:

- Diskrete Logarithmen in endlichen Körpern (Diffie-Hellman)
- Elliptische Kurven
- RSA

Anwendungen:



. . .

Kryptographie

Im neuen deutschen Reisepass wird Kryptographie benutzt.

Kryptographie

Im neuen deutschen Reisepass wird Kryptographie benutzt.

Verwendung:

- Signieren der Daten (Echtheitsgarantie).
- Sichere Kommunikation mit dem Lesegerät.

Da hilft nur noch eins...