

Das RSA-Kryptosystem

Finn Sohst

Fachbereich Informatik
Universität Hamburg

Gliederung

- **Problemstellung**
 - Am Beispiel Symmetrischer Verfahren
- **Das RSA Verfahren**
 - Die Entstehung
 - Der Algorithmus
 - Ein Beispiel mit niedrigen Werten
- **Ausblick**
 - Die Zukunft des RSA Verfahrens
- **Fazit**

Gliederung

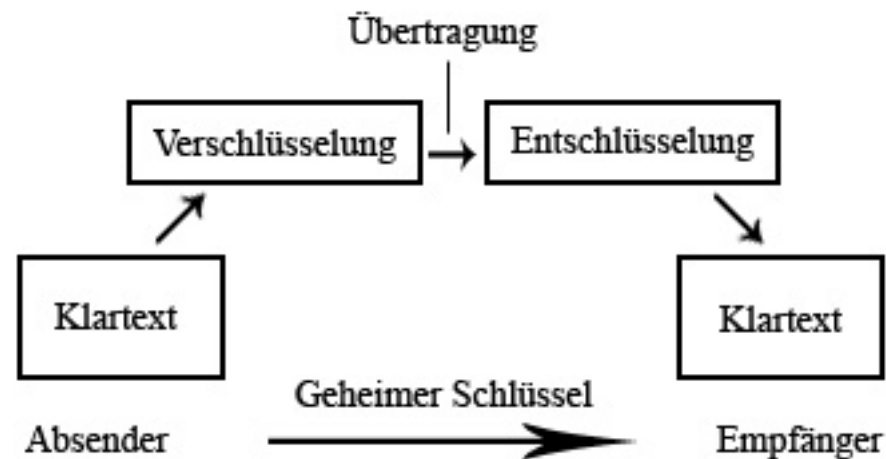
- **Problemstellung**
 - Am Beispiel Symmetrischer Verfahren
- **Das RSA Verfahren**
 - Die Entstehung
 - Der Algorithmus
 - Ein Beispiel mit niedrigen Werten
- **Ausblick**
 - Die Zukunft des RSA Verfahrens
- **Fazit**

Das Caesar Verfahren

- Buchstaben werden um einen bestimmten Wert im Alphabet verschoben
- Das nennt man Transposition
- Bei einer Verschiebung um 3 wird aus „A“ ein „D“
- So wird aus „hallo“ das Wort „kdoor“, wobei der Schlüssel 3 ist

Symmetrische Verfahren

- Die Verschlüsselung, Übertragung und Entschlüsselung bei einem Symmetrischen Verfahren



Sicherheit und Probleme

- Der geheime Schlüssel muss Absender und Empfänger bekannt sein
- Der Schlüssel muss also übertragen werden

Gliederung

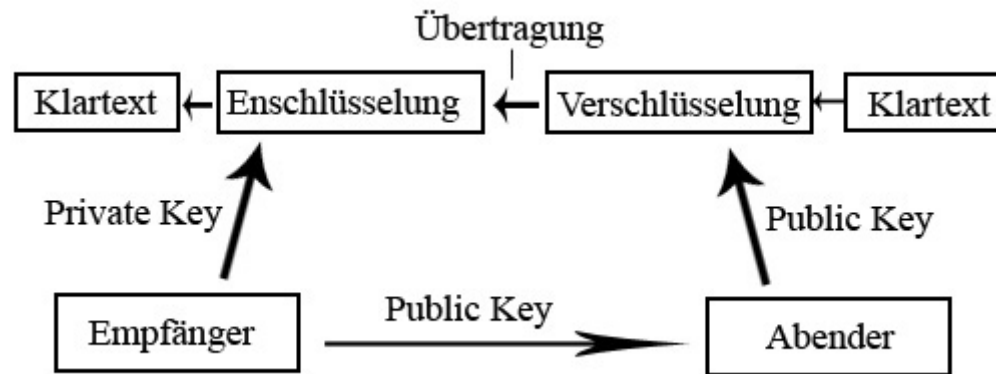
- **Problemstellung**
 - Am Beispiel Symmetrischer Verfahren
- **Das RSA Verfahren**
 - Die Entstehung
 - Der Algorithmus
 - Ein Beispiel mit niedrigen Werten
- **Ausblick**
 - Die Zukunft des RSA Verfahrens
- **Fazit**

Die Entstehung von RSA

- Erfunden von Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman
- An der Massachusetts Institute of Technology
- Im Jahre 1977
- RSA basiert auf der Schwierigkeit hohe Zahlen zu primfaktorisiieren

Warum RSA?

- Das RSA-Verfahren hat einen entscheidenden Vorteil



Der geheime Schlüssel ist nur noch einer Person bekannt

Der Algorithmus(1)

- Das Schlüsselset besteht aus 3 Zahlen
 - Öffentlicher Schlüssel E
 - Privater Schlüssel D
 - Systemmodul N
- N ist das Produkt von 2 Primzahlen (p,q)
- E wird zufällig gewählt
 - Muss aber teilerfremd zu $\varphi(N)$ sein $(p-1)*(q-1)$
- D ist das Inverse zu E mod $\varphi(N)$

Der Algorithmus(2)

- Zum verschlüsseln einer Nachricht m rechnet man

$$c = m^E \bmod N$$

- Zum entschlüsseln der Nachricht c rechnet man

$$m = c^D \bmod N$$

Ein Beispiel

$$p = 13$$

$$q = 17$$

$$N = p * q = 13 * 17 = 221$$

$$\varphi(N) = (p-1) * (q-1) = 192$$

Öffentlicher Schlüssel

für E gilt: $\text{ggT}(E, \varphi(N)) = 1$; $1 < E < \varphi(N)$

wähle $E = 71$

Privater Schlüssel(1)

Für D gilt: $(E \cdot D) - \varphi(N) \cdot k = 1$

Also muss das Multiplikative Inverse von E berechnet werden

Dazu wird der Euklidische Algorithmus zur Ermittlung des ggt von E und $\varphi(N)$ angewendet

Privater Schlüssel(2)

$$192 = 2 \cdot 71 + 50$$

$$71 = 1 \cdot 50 + 21$$

$$50 = 2 \cdot 21 + 8$$

$$21 = 2 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Privater Schlüssel(3)

Wie vermutet ist der $\text{ggT}(71, 192) = 1$

Jetzt wird anhand der Zahlen aus dem Euklidischem Algorithmus das Inverse von E Berechnet

Es gilt, wenn $\text{ggT}(a, b) = 1$ dann gibt es (c, d) mit denen $c \cdot a - d \cdot b = 1$ gilt. Also folgt aus $\text{ggT}(71, 192)$ dass es (D, k) gibt mit denen $D \cdot 71 - k \cdot 192 = 1$ gilt.

Also berechnen wir jetzt D

Privater Schlüssel(4)

$$1 = 3 - 1*2$$

$$= 3 - 1*(5 - 1*3) = -1 * 5 + 2*3$$

$$= -1 * 5 + 2*(8-1*5) = 2*8 - 3*5$$

$$= 2*8 - 3*(21-2*8) = -3*21 + 8*8$$

$$= -3*21 + 8*(50-2*21) = 8*50 - 19*21$$

$$= 8*50 - 19*(71-1*50) = -19*71+27*50$$

$$= -19*71 + 27*(192 - 2 * 71) = 27*192 - 73*71$$

$$\Rightarrow k = 27, D = -73$$

Privater Schlüssel(5)

da $-73 < 0$:

$$D = 192 - 73 = 119$$

$$D = 119 \text{ denn } 119 * 71 - 44 * 192 = 1$$

also ist $k = 44$

Verschlüsseln

$$C_n = K_n^E \bmod N$$

Wir nehmen an: $a = 1$, $b = 2$, $c = 3 \dots$

hallo = 8|1|12|12|15

$$C_1 = 8^{71} \bmod 221 = 83$$

$$C_2 = 1^{71} \bmod 221 = 1$$

$$C_3 = 12^{71} \bmod 221 = 194$$

$$C_4 = 12^{71} \bmod 221 = 194$$

$$C_5 = 15^{71} \bmod 221 = 59$$

hallo = 83|1|194|194|59

Entschlüsseln

$$K_n = C_n^D \bmod N$$

$$K_1 = 83^{119} \bmod 221 = 8$$

$$K_2 = 1^{119} \bmod 221 = 1$$

$$K_3 = 194^{119} \bmod 221 = 12$$

$$K_4 = 194^{119} \bmod 221 = 12$$

$$K_5 = 59^{119} \bmod 221 = 15$$

$\Rightarrow 8|1|12|12|15 = \text{hallo}$

Gliederung

- **Problemstellung**
 - Am Beispiel Symmetrischer Verfahren
- **Das RSA Verfahren**
 - Die Entstehung
 - Der Algorithmus
 - Ein Beispiel mit niedrigen Werten
- **Ausblick**
 - Die Zukunft des RSA Verfahrens
- **Fazit**

Sicherheit

- Die Firma RSA Security stellt für die Faktorisierung von RSA Zahlen ein Preisgeld von maximal \$200.000 aus
- Allerdings muss hierfür eine 2048-Bit Zahl faktorisiert werden
- Die Zahl hat 617 Stellen

Sicherheit(2)

25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357

Sicherheit(3)

- Am 4. November 2005 wurde eine 640-Bit RSA Zahl mit 193 Stellen faktorisiert
- Das \$20.000 Preisgeld erhielten die deutschen F. Bahr, M. Boehm, J. Franke und T. Kleinjung
- 30 2,2Ghz Rechner brauchten dafür über 5 Monate

Die Zukunft

- Momentan ist RSA noch sicher wenn das Produkt aus p und q mehr als 1024 Bit hat
- Peter W. Shor entwickelte allerdings 1994 einen Algorithmus zur Primzahlfaktorisation
- Dieser Algorithmus funktioniert jedoch nur auf einem Quantencomputer
- Quantencomputer existieren noch nicht

Gliederung

- **Problemstellung**
 - Am Beispiel Symmetrischer Verfahren
- **Das RSA Verfahren**
 - Die Entstehung
 - Der Algorithmus
 - Ein Beispiel mit niedrigen Werten
- **Ausblick**
 - Die Zukunft des RSA Verfahrens
- **Fazit**

Faszit

- Mit dem RSA-Verfahren ist in den nächsten Jahren noch ein sehr sicheres Verschlüsselungsverfahren gegeben
- Erst eine völlig neue Hardwaretechnik könnte das Verfahren effizient knacken