AES und Public-Key-Kryptographie

Jens Kubieziel
jens@kubieziel.de

Friedrich-Schiller-Universität Jena
Fakultät für Mathem atik und Informatik

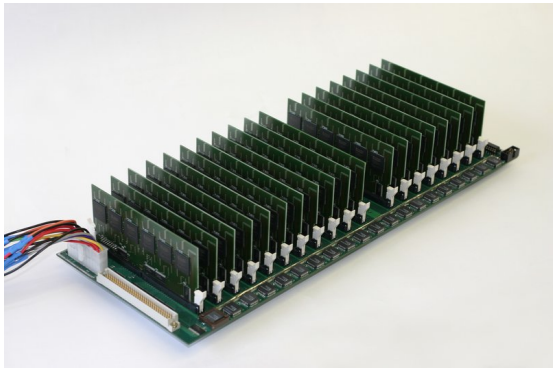
22. Juni 2009

Wichtige Algorithmen im 20. Jahrhundert

- ADFGVX
- Enigma
- DES
- und viele weitere

DES

- Data Encryption Standard, symmetrischer Algorithmus mit 56 Bit Schlüssellänge
- Standard seit 1976 (seit 2004 nicht mehr empfohlen)
- Durchprobieren aller Schlüssel dauert sechs Tage



Standardisierung von AES

Anforderungen

- symmetrische Blockchiffre
- Blocklänge 128 Bit, Schlüssellänge 128, 192 und 256 Bit
- leichte Umsetzung in Hard- und Software
- überdurchschnittliche Performance
- sicher gegen bekannte Angriffe
- frei von patentrechtlichen Ansprüchen

Standardisierung von AES

Rijndael

- Blockchiffre mit variabler Schlüssel- und Blocklänge
- von JOAN DAEMEN und VINCENT RIJMEN
- FIPS 197 vom Oktober 2000

Der AES-Algorithmus

Grundlagen

- Block in 16 Teile zu 8 Bit=1 Byte aufgeteilt
- Operation in $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/g\mathbb{F}_2[x]$ mit dem irreduziblen Polynom

$$g = x^8 + x^4 + x^3 + x + 1$$

- Byte $b_7b_6b_5b_4b_3b_2b_1b_0$ repräsentiert durch ein Polynom aus $\mathbb{F}_{2^8}$
- Schreibweise als 4×4-Matrix:

$$M = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix} \qquad a_{ij} \in \mathbb{F}_{2^8}$$

Der AES-Algorithmus

Rundentransformation

Insgesamt gibt es neun Runden mit den Operationen:

1. `AddRoundKey`
2. `SubBytes`
3. `ShiftRows`
4. `MixColumns`

und eine Abschlussrunde *ohne* die obige Operation `MixColumns`.
Weiterhin werden für jede Runde separate Schlüssel errechnet.

Der AES-Algorithmus

SubBytes

Sei $a_{ij} \in \mathbb{F}_{2^8}$ aus der Matrix M und $S = g \circ f$ mit

$$f(a) = \begin{cases} a^{-1} & x \neq 0 \\ 0 & x = 0 \end{cases} \text{ und}$$

$$g \begin{pmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a^7 \\ a^6 \\ a^5 \\ a^4 \\ a^3 \\ a^2 \\ a^1 \\ a^0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Der AES-Algorithmus

ShiftRows

$$\begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix} \rightarrow \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{pmatrix}$$

Der AES-Algorithmus

MixColumns

Jede Eingabespalte $a_{i.}$ wird mit einem Polynom $c(x) = 03 \cdot x^3 + 01 \cdot x^2 + 01 \cdot x + 02$ modulo $x^4 + 1$ multipliziert.
Schreibweise als Matrixmultiplikation:

$$\begin{pmatrix} b_{i0} \\ b_{i1} \\ b_{i2} \\ b_{i3} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_{i0} \\ a_{i1} \\ a_{i2} \\ a_{i3} \end{pmatrix}$$

Der AES-Algorithmus

AddRoundKey

Addition der Matrix M mit dem Rundenschlüssel modulo 2

Der effektivste Weg

Mögliche Angriffe

- Lineare und differenzielle Kryptoanalyse
- XSL-Angriff
- Darstellung als Kettenbruch

Mögliche Angriffe

Darstellung als Kettenbruch

$$a_{i,j}^{(6)} = K + \sum_{\substack{e_5 \in \mathcal{E} \\ d_5 \in \mathcal{D}}} \cfrac{C}{K^* + \sum_{\substack{e_4 \in \mathcal{E} \\ d_4 \in \mathcal{D}}} \cfrac{C}{K^* + \sum_{\substack{e_3 \in \mathcal{E} \\ d_3 \in \mathcal{D}}} \cfrac{C}{K^* + \sum_{\substack{e_2 \in \mathcal{E} \\ d_2 \in \mathcal{D}}} \cfrac{C}{K^* + \sum_{\substack{e_1 \in \mathcal{E} \\ d_1 \in \mathcal{D}}} \cfrac{C}{K^* + p_*^*}}}}}$$

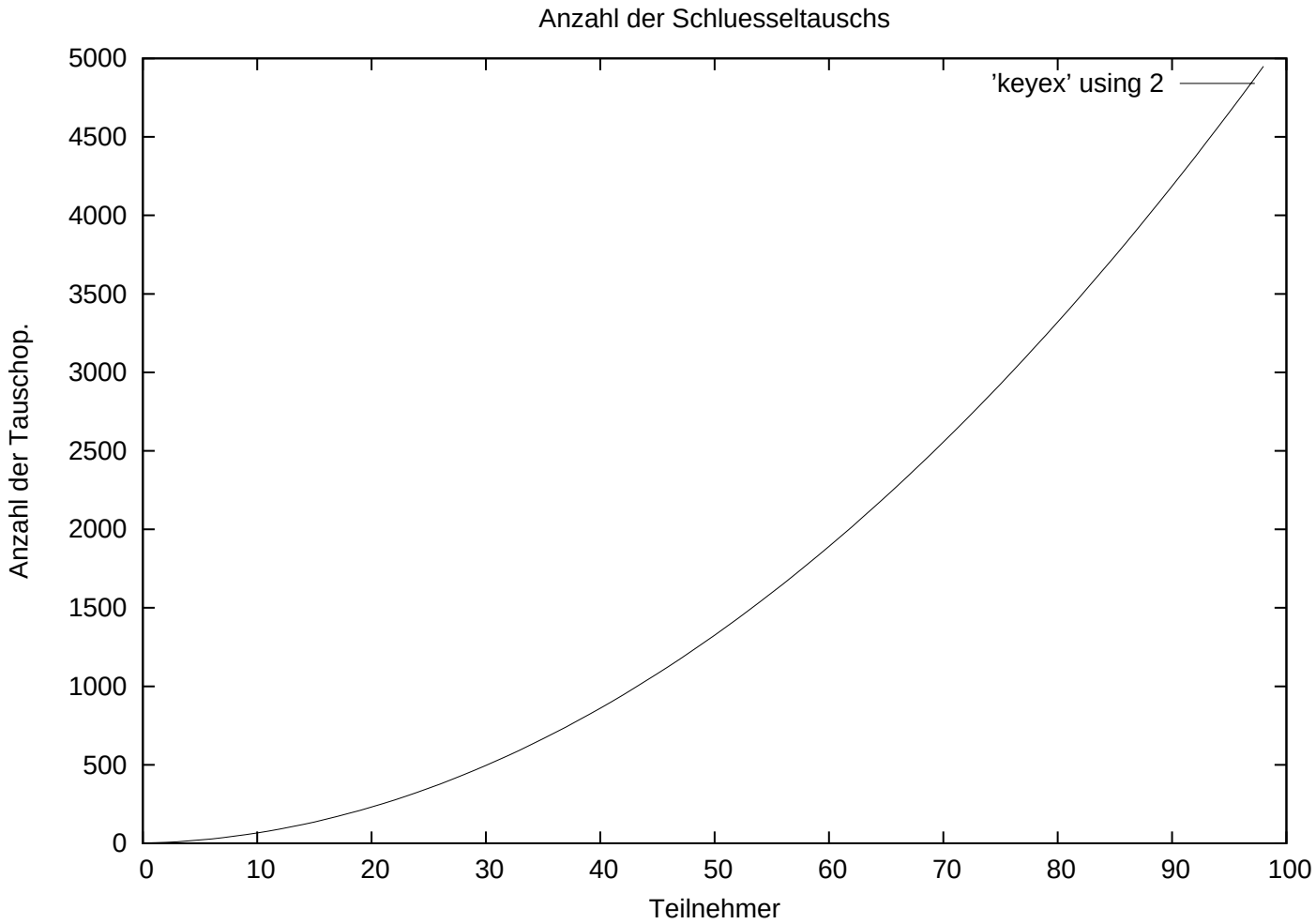
Problem der Schlüsselverteilung

Für n Teilnehmer müssen k-mal Schlüssel verteilt werden:

$n = 2$	$k = 1$
$n = 3$	$k = 3$
$n = 4$	$k = 6$
$n = 5$	$k = 10$
$n = 10$	$k = 45$
$n = 50$	$k = 1225$
$n = 100$	$k = 4950$

Insgesamt quadratisches Wachstum

Problem der Schlüsselverteilung



Schlüsselverteilung

Lösung des Problems durch unterschiedliche Schlüssel:

Public key Öffentlicher Schlüssel kann überall hinterlegt werden und wird dazu benutzt, Nachrichten an Alice zu verschlüsseln.

Private key Geheimer Schlüssel kennt nur Alice und wird benutzt, um eingehende Nachrichten zu entschlüsseln.

Zur Geschichte

- entdeckt durch GCHQ (zufälliges Rauschen)
- öffentlich bekannt durch RIVEST, SHAMIR und ADLEMAN bzw. DIFFIE und HELLMAN
- Algorithmen: RSA, ElGamal etc.

Einwegfunktion

Definition

Seien X und Y Mengen. Eine injektive Funktion $f : X \to Y$ heißt *Einwegfunktion*, falls man für jedes $x \in X$ den Wert $y = f(x)$ schnell berechnen kann und für jedes beliebige $y \in \operatorname{Bld} f \subseteq Y$ das Urbild $f^{-1}(y) = x$ nicht in vertretbarer Zeit finden kann.

Public-Key-Kryptosystem

Definition

Ein Kryptosystem $\mathbb{K}$ heißt *Public-Key-Kryptosystem*, wenn jede Chiffrierfunktion $e_k : \mathcal{P} \to \mathcal{C}$ mit $k \in \mathcal{K}$ eine Einwegfunktion ist.

Public-Key-Kryptosystem

Beispiele

- Berechnung des diskreten Logarithmus
- Faktorisierung großer Zahlen

Der Algorithmus

1. Wähle $p, q \in \mathbb{P}$ mit $p \neq q$
2. Berechne $n = p \cdot q$ und $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$
3. Wähle $e \in \mathbb{N}$ mit $1 < e < \varphi(n)$ und $e \nmid \varphi(n)$
4. Berechne $d \in \mathbb{N}$ mit

$$ed \equiv 1 \mod \varphi(n)$$

5. Fertig ✓

Schlüssel

- öffentlicher Schlüssel: (n, e)
- privater Schlüssel: (n, d)
- Verschlüsseln:

$$e_B : \mathbb{Z}_n \to \mathbb{Z}_n \qquad x \mapsto y = x^e \mod n$$

- Entschlüsseln:

$$d_B : \mathbb{Z}_n \to \mathbb{Z}_n \qquad y \mapsto y^d \mod n$$

Funktioniert das?

Satz über die Entschlüsselung

Theorem (Satz)

Es gilt, $d_B(e_B(x)) = x$ *für alle* $x \in \mathbb{Z}_n$.

Kryptoanalyse

Dechiffrierung entspricht Lösung der Gleichung $x^e \equiv y \mod n$ bei gegebenem y.

Algorithmus

Alice und Bob wollen einen gemeinsamen Schlüssel vereinbaren. Sie legen eine Gruppe G mit einem $g \in G$ fest. Das Element g hat die Ordnung n.

1. Alice wählt $a \in \{2, \ldots, n-1\}$ und schickt g^a zu Bob
2. Bob wählt $b \in \{2, \ldots, n-1\}$ und schickt g^b zu Alice
3. Bob berechnet $(g^a)^b = g^{ab}$ und Alice berechnet $(g^b)^a = g^{ba}$. Das Ergebnis $g^{ab} = g^{ba}$ ist der Schlüssel.