ADVANCED ENCRYPTION STANDARD

Clemens Dubberke

Humboldt-Universität zu Berlin

Institut für Informatik

SE Geschichte der Verschlüsselung

Leitung: Constanze Kurz

WiSe 2006/2007

Übersicht

Die Historie

Der Algorithmus

Ausblick

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Historie I - DES

1977 Entwicklung des DES durch IBM

1994 Dechiffrierung von DES-Texten in < 5 Tagen

Ersetzen von DES durch 3DES

1997 Ausschreibung des AES als FIPS_197 durch das **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST)

1998 Entschlüsselung des DES in < 3 Tagen

1999 Entschlüsselung des DES in 22 Stunden

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Historie II - AES-Bedingungen

Symmetrische Blockchiffre

Verwendung von mind. 128 Bit Blöcken und Schlüsseln von 128, 192 und 256 Bit Länge

jeweils leichte Implementierung in Hard- und Software

überdurchschnittliche Performance in Hard- und Software

Widerstehen aller bekannten Methoden der Kryptonanalyse, insbesondere Power- und Timing-Attacken.

Erfordernis geringer Ressourcen

Keine patentrechtlichen Ansprüche, allgemeine unentgeltliche Nutzung

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Historie III- AES

15.06.1998 Deadline zur Abgabe der Algorithmen

08/1998 - 03/1999 Runde 1

Vorstellung aller Kandidaten
Vorstellung der Analyse aller Kandidaten

08/1999 – 11/2001 Runde 2

Vorstellung der 5 übrigen Kandidaten
ausgiebige Test- u. Analysverfahren

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Historie IV -AES-Kandidaten der 1. Runde

AES Round 1 Candidate Algorithms

Algorithm Name	*Submitter Name(s)*
CAST-256	Entrust Technologies, Inc. *(represented by Carlisle Adams)*
CRYPTON	Future Systems, Inc. *(represented by Chae Hoon Lim)*
DEAL	Richard Outerbridge, Lars Knudsen
DFC	CNRS - Centre National pour la Recherche Scientifique - Ecole Normale Superieure *(represented by Serge Vaudenay)*
E2	NTT - Nippon Telegraph and Telephone Corporation *(represented by Masayuki Kanda)*
FROG	TecApro Internacional S.A. *(represented by Dianelos Georgoudis)*
HPC	Rich Schroeppel
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
MAGENTA	Deutsche Telekom AG *(represented by Dr. Klaus Huber)*
MARS	IBM *(represented by Nevenko Zunic)*
RC6™	RSA Laboratories *(represented by Burt Kaliski)*
RIJNDAEL	Joan Daemen, Vincent Rijmen
SAFER+	Cylink Corporation *(represented by Charles Williams)*
SERPENT	Ross Anderson, Eli Biham, Lars Knudsen
TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

First AES Candidate Conference (AES1)

The First AES Candidate Conference (AES1) was held in Ventura, California on August 20-22, 1998 to announce the fifteen Round 1 AES candidates.

Quelle: http://csrc.nist.gov/CryptoToolkit/aes/

Historie V - AES-Kandidaten der 2. Runde

AES Round 2 Finalists

Algorithm Name	*Submitter Name(s)*
MARS	IBM *(represented by Nevenko Zunic)*
RC6™	RSA Laboratories *(represented by Burt Kaliski)*
Rijndael	Joan Daemen, Vincent Rijmen
Serpent	Ross Anderson, Eli Biham, Lars Knudsen
Twofish	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Quelle: http://csrc.nist.gov/CryptoToolkit/aes/

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

And the winner is…

What algorithm has been selected by NIST, and how do you pronounce it?

NIST has selected Rijndael as the proposed AES algorithm. The algorithm's developers have suggested the following pronunciation alternatives: "Reign Dahl", "Rain Doll", and "Rhine Dahl".

Quelle: http://csrc.nist.gov/CryptoToolkit/aes/

Quelle: http://www.pbcrypto.com/greatminds/rijndael.php

Joan Daemen und Vincent Rijmen

Algorithmus I

Blocklänge 128 (192 und 256) Bits
Schlüssellänge 128, 192 und 256 Bits

Referenz-Implementierung < 500 Zeilen C-Code

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Algorithmus II - Arbeitsweise

Blockzerlegung in 2D-Tabellen mit je 4 Zeilen und Spalten (Blocklänge 128)

rundenweise Transformation je Block (Runde r = 10, 12 oder 14) unter Anwendung eines Rundenschlüssels

Monoalphabetische Verschlüsselung per S-Box

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Algorithmus III - Ablauf

Schlüsselexpansion

Vorrunde

- KeyAddition ()

Verschlüsselungsrunden (r, r++, runde<r)

- ByteSub()
- ShiftRow()
- MixColumn()
- KeyAddition()

Schlussrunde

- Substitution()
- ShiftRow()
- KeyAddition()

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Algorithmus IV - Schlüsselexpansion

Schlüssel in r + 1 Teilschlüssel teilen
(r = rundenanzahl)

Rundenschlüssel müssen die gleiche Länge wie die Blöcke haben

Benutzerschlüssel auf die Länge b * (r + 1) expandieren, b = Blockgröße

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Algorithmus V - KeyAddition

bitweise XOR-Verknüpfung zwischen einem Block und dem aktuellen Rundenschlüssel

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Algorithmus VI - S-Box (Substitution)

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Quelle: http://realtec.dyndns.org/web/realtec/privat/files/AES_Krypto_Seminar.pdf

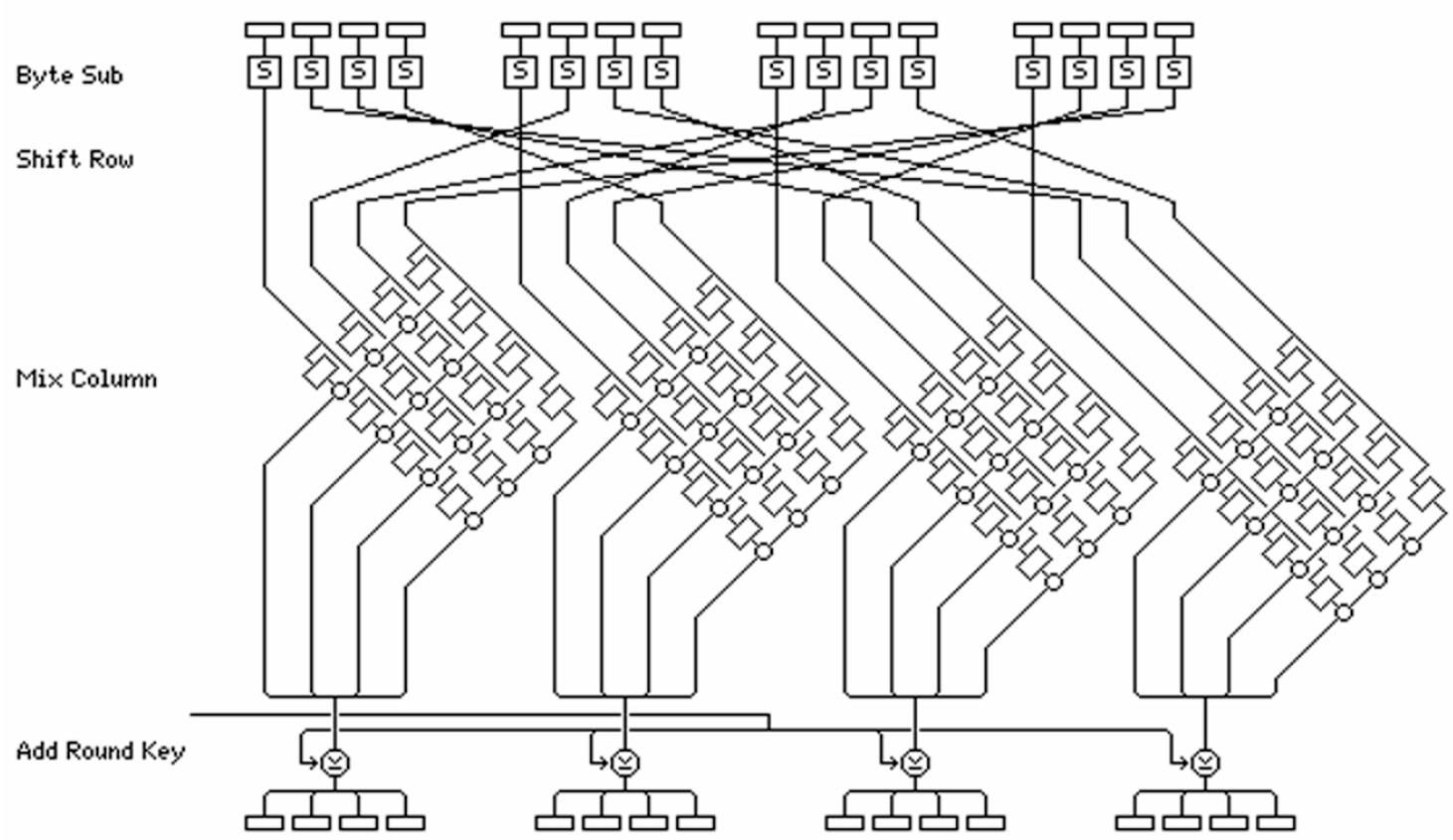
Algorithmus VII - ShiftRow und MixColumn

ShiftRow: Verschiebung der Zeilen
um 0, 1, 2 oder 3 Spalten

MixColumn: Jede Zelle wird mit
einer Konstanten multpliziert, dann die Ergebnisse
XOR verknüpft

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Algorithmus VIII - Rundenübersicht



Quelle: http://realtec.dyndns.org/web/realtec/privat/files/AES_Krypto_Seminar.pdf

Algorithmus IX - Dechiffrierung

Vorrunde

KeyAddition (State, Roundkey)

InvVerschlüsselungsrunden (State, Roundkey)

InvByteSub(State)
InvShiftRow(State)
InvMixColumn(State)
KeyAddition(State, InvMixColumn(Roundkey))

Schlussrunde

InvByteSub(State)
InvShiftRow(State)
KeyAddition (State, Roundkey)

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Ausblick I - Kryptographische Stärke von AES

6 Runden ($6*2^{32}$ ausgewählte Klartextblöcke)=ca.400 GB Klartext

2^{44} komp. Op. je 1 ms = 200 Tage

7 Runden (2^{128} Klartext)= $5*10^{39}$ Byte

2^{120} komp. Op. Je 1 ns = 40 Trill. Jahre

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Ausblick II Angriffe

AES gilt bisher als weitgehend unbrechbar bzw. nur als theoretisch brechbar

Osvik, Shamir und Tromer beschreiben auf der RSA-Conference 2006 Angriffe und Gegenmaßnahmen auf den AES

Institut für Informatik
Informatik in Bildung und Gesellschaft
Constanze Kurz
Referent: Clemens Dubberke

Quellenverzeichnis

Osvik, Dag Arne/Shamir, Adi/Tromer, Eran: Cache Attacks and Countermeasures: The Case of AES. In: Pointcheval, David (Hrg.): Topics in Cryptology – CT-RSA 2006. Berlin: Springer, 2006, S. 1-20.

Linke, Achim: The Advanced Encryption Standard (Rijndael). Seminararbeit zum Hauptseminar Kryptographische Protokolle (SoSe 2005) der Abteilung Sichere und Zuverlässige Softwaresysteme an der Universität Stuttgart. Internet: www.informatik.uni-stuttgart.de/fmi/szs/teaching/ss2005/krypto/Linke.pdf [09.01.07].

NIST: C S R C-Cryptographic Toolkit. Internet: http://csrc.nist.gov/CryptoToolkit/aes/ [09.01.07].

Renz, Christian: Advanced Encryption Standard. Hauptseminar Internet-Technologien der nächsten Generation (WiSe 2003/2004) der Fakultät Informatik der Universität Stuttgart. Internet: www.web42.com/crenz/en/data/aes.html [09.01.07].

Wilkin, Christian: Der Algorithmus des „Advanced Encryption Standard“. Seminararbeit zum Seminar Kryptographie (WiSe 2004/2005) des Fachbereiches Design und Informatik an der Fachhochschule Trier. Intenet: http://realtec.dyndns.org/web/realtec/privat/files/AES_Krypto_Seminar.pdf [09.01.07].