

Michael Fritz

Kryptographisch sichere, tokenbasierte Datenarchivierung

Diplomarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 1999 Diplom.de
ISBN: 9783832421755

Michael Fritz

Kryptographisch sichere, tokenbasierte Datenarchivierung

Michael Fritz

Kryptographisch sichere, tokenbasierte Datenarchivierung

Diplomarbeit

an der Universität Klagenfurt, Österreich

Fachbereich Wirtschaftswissenschaften und Informatik

Prüfer O. Univ. Prof. Dr. Patrick Horster

Institut für Wirtschaftsinformatik und Anwendungssysteme

November 1999 Abgabe



Diplomarbeiten Agentur

Dipl. Kfm. Dipl. Hdl. Björn Bedey

Dipl. Wi.-Ing. Martin Haschke

und Guido Meyer GbR

Hermannstal 119 k

22119 Hamburg

agentur@diplom.de

www.diplom.de

ID 2175

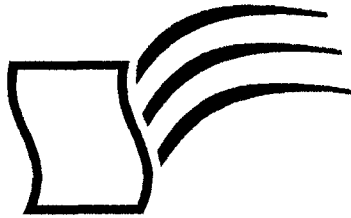
Fritz, Michael: Kryptographisch sichere, tokenbasierte Datenarchivierung/Michael Fritz -
Hamburg: Diplomarbeiten Agentur, 2000
Zugl.: Klagenfurt, Universität, Diplom, 1999

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Dipl. Kfm. Dipl. Hdl. Björn Bedey, Dipl. Wi.-Ing. Martin Haschke & Guido Meyer GbR
Diplomarbeiten Agentur, <http://www.diplom.de>, Hamburg
Printed in Germany



Diplomarbeiten Agentur

Wissensquellen gewinnbringend nutzen

Qualität, Praxisrelevanz und Aktualität zeichnen unsere Studien aus. Wir bieten Ihnen im Auftrag unserer Autorinnen und Autoren Wirtschaftsstudien und wissenschaftliche Abschlussarbeiten – Dissertationen, Diplomarbeiten, Magisterarbeiten, Staatsexamensarbeiten und Studienarbeiten zum Kauf. Sie wurden an deutschen Universitäten, Fachhochschulen, Akademien oder vergleichbaren Institutionen der Europäischen Union geschrieben. Der Notendurchschnitt liegt bei 1,5.

Wettbewerbsvorteile verschaffen – Vergleichen Sie den Preis unserer Studien mit den Honoraren externer Berater. Um dieses Wissen selbst zusammenzutragen, müssten Sie viel Zeit und Geld aufbringen.

<http://www.diplom.de> bietet Ihnen unser vollständiges Lieferprogramm mit mehreren tausend Studien im Internet. Neben dem Online-Katalog und der Online-Suchmaschine für Ihre Recherche steht Ihnen auch eine Online-Bestellfunktion zur Verfügung. Inhaltliche Zusammenfassungen und Inhaltsverzeichnisse zu jeder Studie sind im Internet einsehbar.

Individueller Service – Gerne senden wir Ihnen auch unseren Papierkatalog zu. Bitte fordern Sie Ihr individuelles Exemplar bei uns an. Für Fragen, Anregungen und individuelle Anfragen stehen wir Ihnen gerne zur Verfügung. Wir freuen uns auf eine gute Zusammenarbeit

Ihr Team der Diplomarbeiten Agentur

Dipl. Kfm. Dipl. Hdl. Björn Bedey –
Dipl. Wi.-Ing. Martin Haschke —
und Guido Meyer GbR —————

Hermannstal 119 k —————
22119 Hamburg —————

Fon: 040 / 655 99 20 —————
Fax: 040 / 655 99 222 —————

agentur@diplom.de —————
www.diplom.de —————

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre hiermit ehrenwörtlich, daß ich die vorliegende Arbeit vollkommen selbständig verfaßt und außer dem im Literaturverzeichnis angeführten Schrifttum bei der Abfassung keine andere Unterstützung in Anspruch genommen und genossen habe. Die Arbeit ist noch keiner anderen Prüfungsbehörde vorgelegt worden.

Klagenfurt, am 5. November 1999

A handwritten signature in black ink, appearing to read "Fritz Michael". The signature is written in a cursive style with a large, sweeping initial "F".

Für Eva,
durch die ich die nötige seelische Stärke erhalten habe.

"Any sufficiently advanced technology is indistinguishable from magic."

Arthur C. Clarke's Third Law

"The only way of discovering the limits of the possible is to venture a little way past them into the impossible."

Arthur C. Clarke's Second Law

Inhaltsverzeichnis

0	EINLEITUNG	1
1	PROBLEMSTELLUNG UND PROGRAMMENTWICKLUNG	3
2	CHIPKARTEN	7
2.1	SPEICHERKARTEN (MEMORY CARDS).....	8
2.2	INTELLIGENTE SPEICHERKARTEN (INTELLIGENT/PROTECTED MEMORY CARDS)....	9
2.3	MIKROPROZESSOR (CPU) KARTEN (SMARTCARDS).....	9
2.4	CO-PROZESSOR CHIPKARTEN	10
2.5	KONTAKTLOSE CHIPKARTEN	10
2.6	ZUR WAHL DER VERWENDETEN CHIPKARTEN	10
2.7	ATTACKEN AUF CHIPKARTEN	11
3	SYMMETRISCHE CHIFFREN	12
3.1	BLOCKCHIFFREN	12
3.2	STANDARD - BETRIEBSARTEN	13
3.3	DATA ENCRYPTION STANDARD (DES).....	18
3.3.1	Geschichte	19
3.3.2	Aufbau des DES Algorithmus	20
3.3.3	DES Eigenschaften und Schwächen	26
3.4	TRIPLE - DES	27
3.5	ADVANCED ENCRYPTION STANDARD (AES)	29
3.6	ATTACKEN AUF SYMMETRISCHE BLOCKCHIFFREN	31
4	HASHFUNKTIONEN	34
4.1	MDx	35
4.2	SECURE HASH ALGORITHM - 1 (SHA-1).....	38
4.3	RIPEMD	40
4.3.1	RIPEMD-160	40
4.3.2	Erweiterung auf RIPEMD-256 und RIPEMD-320	45
4.4	LITTLE-ENDIAN VERSUS BIG-ENDIAN	45
4.5	PERFORMANCE	45
4.6	ATTACKEN AUF HASHFUNKTIONEN	46

5	ASYMMETRISCHE CHIFFREN	47
5.1	PUBLIC-KEY-KRYPTOSYSTEME	47
5.2	DIGITALE SIGNATUREN	48
5.2.1	Geschichte	49
5.2.2	Eigenschaften	49
5.2.3	Vorgehensweise	50
5.2.4	Mögliche Attacken	51
5.2.5	Das Digitale Signaturen Gesetz	51
5.3	RSA - VERFAHREN	52
5.3.1	Verschlüsselungsverfahren	54
5.3.2	Digitale Signatur Verfahren	55
5.3.3	Kombinationen der beiden Verfahren	55
5.3.4	Attacken auf RSA Signaturen	56
5.3.5	Mathematische Anmerkungen	57
5.4	DIGITAL SIGNATURE STANDARD (DSS)	60
5.5	ZERTIFIKATE	63
5.6	ENVELOPE SYSTEME	64
6	DIE KRYPTOGRAPHISCHE LIBRARY	65
6.1	KEY CONTAINER	65
6.2	ALGORITHMEN	66
6.3	BEGRÜNDUNG DER AUSWAHL	67
7	SCHLÜSSELMANAGEMENT	69
7.1	ALLGEMEIN	69
7.2	SCHLÜSSELMANAGEMENT IM ASE PAKET	69
7.3	ANSI X9.17 GENERATOR	71
8	PROGRAMM	72
8.1	VERWALTUNG DER SCHLÜSSEL	72
8.2	ERZEUGUNG DER SCHLÜSSEL	73
8.3	ZUGRIFF AUF DEN KEY CONTAINER	74
8.4	DATEISTRUKTUR	75
8.5	VERSCHLÜSSELUNG	77
8.6	ENTSCHLÜSSELUNG	79
8.7	GENERIERUNG DER DIGITALEN SIGNATUR	81
8.8	VERIFIZIERUNG DER DIGITALEN SIGNATUR	82
8.9	OPTIONEN	83
8.10	LÖSCHEN EINZELNER DATEIEN AUS DEM DATENFILE	84
9	BRENNEN AUF EINE CD	86
9.1	VERWENDUNG DES PROGRAMMS	86
9.2	DATEISYSTEME	88
9.3	"TRACK-AT-ONCE" VERSUS "DISC-AT-ONCE"	89
9.4	MULTISESSION-CDS	89
9.5	WISSENSWERTES UND INTERESSANTES	90

10	SCHLUSSFOLGERUNGEN UND AUSBLICK.....	92
11	ANHANG.....	93
11.1	PERFORMANCE TESTS MIT VERSCHIEDENEN PUFFERGRÖSSEN	93
11.2	ABBILDUNGSVERZEICHNIS.....	95
11.3	TABELLENVERZEICHNIS	96
12	LITERATURVERZEICHNIS	97