Kryptologie-Projekt

Dirk Kruse

BBS II Leer

03.11.2011

Gliederung

- Begriffe
- Historische Verfahren: Stabcode, Caesar, Vigenère, Enigma
- 100%ig sicher: One-Time-Pad
- Moderne Verfahren: DES, RSA, Hashing
- Anwendungen und Tipps
- Aufgaben zur Zusammenfassung

Begriffe (1)

- **Kryptographie**:
  - ist die Lehre der Absicherung von Nachrichten durch Verschlüsseln [1]
  - ist die Wissenschaft vom Design der Verschlüsselungsalgorithmen [2]
- **Kryptoanalyse**: ist die Kunst, einen chiffrierten Text ohne Kenntnis des Schlüssels zu lesen [2]
- **Kryptologie**: vereint Kryptographie und Kryptoanalyse

Folie 3

Begriffe (2)

- **Klartext** *(plaintext)*: ist der Originaltext, der verschlüsselt wird
- **Geheimtext** *(ciphertext)*: ist der verschlüsselte (chiffrierte) Text
- **Klartextangriff** *(plaintext attack)*: ist die Kryptoanalyse eines Geheimtextes, bei der Teile des Klartextes bekannt sind.
- **Alice, Bob, Charlie**: Personen, die an der Übertragung von verschlüsselten Nachrichten beteiligt sind (Charlie = Bösewicht)

Folie 4

Historische Verfahren
- Einführung -

„Denn es ist besser für den Schreiber, sich als Dummkopf ansehen zu lassen, als den Preis für die Aufdeckung seiner Pläne zu bezahlen.“

Giovanni Battista Porta
(1535 1615)

Chiffrierscheibe von Porta, 1563

5

Historische Verfahren
- Stabcode -

- Im 5. Jahrhundert v. u. Z. entwickelten die alten Griechen dieses ***Transpositions***verfahren.
- Transposition bedeutet „Vertauschung“, kein Zeichen wird verändert, es wechselt nur seinen Platz im Text.
- Die Dicke des Stabes bildet den Schlüssel.
- Verfahren ist (auch aus historischer Sicht) relativ unsicher, wenn man den Verschlüsselungsalgorithmus kennt.

Folie 6

Historische Verfahren - Caesar- Chiffrierung

- Julius Caesar (100 bis 44 v. Chr.) hat seine geheimen Nachrichten mit diesem ***monoalphabetischen Substitutions***verfahren verschlüsselt
- *Substitution* bedeutet „Ersetzung“, jedes Klartext-zeichen wird durch ein anderes Zeichen ersetzt
- *Monoalphabetisch* bedeutet, dass jedes Klartext-zeichen immer auf das gleiche Geheimtextzeichen abgebildet wird
- Der Schlüssel ist die Anzahl der Positionen, um die das Alphabet verschoben wurde, hier = 3

Folie 7

Historische Verfahren - Caesar- Chiffrierung – (2)

Beispiel: Wie lautet diese Nachricht im Klartext?

KDOOR ERE, KLHU LVW DOLFH!

↓

DEFGHIJKLMNOPQRSTUVWXYZABC

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

HALLO BOB, HIER IST ALICE!

Folie 8

Historische Verfahren - Caesar- Chiffrierung – (3)

Statistische Analyse einer monoalphabetischen Substitution:

Buchstabe	Häufigkeit [%]	Buchstabe	Häufigkeit [%]	Buchstabe	Häufigkeit [%]
A	6,51	J	0,27	S	7,27
B	1,89	K	1,21	T	6,15
C	3,06	L	3,44	U	4,35
D	5,08	M	2,53	V	0,67
E	17,40	N	9,78	W	1,89
F	1,66	O	2,51	X	0,03
G	3,01	P	0,79	Y	0,04
H	4,76	Q	0,02	Z	1,13
I	7,55	R	7,00		

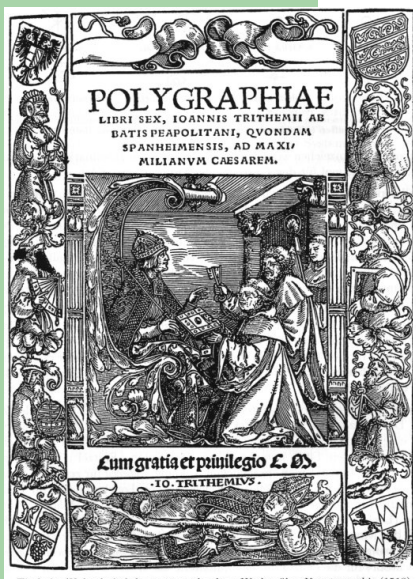
Folie 9

Historische Verfahren - Vigenère-Chiffrierung -

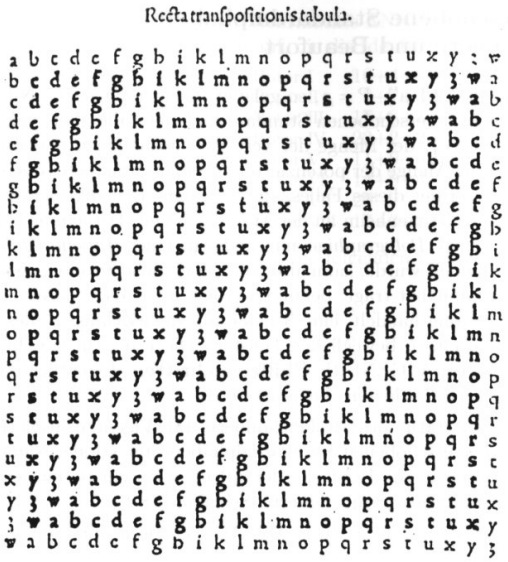
- Blaise de Vigenère (1523 – 1596) schlug 1585 ein spezielles polyalphabetisches Substitutionsverfahren vor, d. h. ein Buchstabe im Klartext kann durch verschiedene Buchstaben im Geheimtext dargestellt werden.
- Als Schlüssel dient eine beliebige Substitution des Alphabets. Dieses wird zudem noch zyklisch verschoben.
- Das Verfahren wurde in einer besonderen Form (geordnetes Alphabet wird verschoben) bereits 1518 in *Trithemius*‘ Buch „*Polygraphiae*“ dargestellt.

Folie 10

Folie 1: Titelseite und ‚tabula recta'-Abbildung



Titelseite (Holzschnitt) des ersten gedruckten Werkes über Kryptographie (1518)



(Original in der Bayrischen Staatsbibliothek München)

Folie 11

Historische Verfahren - Vigenère-Chiffrierung - (2)

Die einfachste Möglichkeit:

- Grundlage ist die bekannte Darstellung der Caesar-Methode: $c = (k + s) \bmod 26$
- Diesmal wird jedoch nicht einfach eine Verschiebung als Schlüssel gewählt, sondern ein Schlüsselwort, dass wiederholt über den Klartext geschrieben wird.
- Dann werden die übereinander stehenden Buchstaben addiert.

Folie 12

Historische Verfahren - Vigenère-Chiffrierung - (3)

Ein Beispiel:

das Schlüsselwort ist **„LIEBE“**

Der Klartext:	**TRIFFMICHHEUTEABEND**
	+
Schlüssel:	**LIEBELIEBELIEBELIEB**
Ergebnis der	**=**
Addition:	**EZMGJXQGILPCXFEMMRE**

Folie 13

Historische Verfahren - Vigenère-Chiffrierung - (4)

Die 2. Möglichkeit:

- Grundlage ist das „*Vigenère-Quadrat*“ (erfunden hat es jedoch J. Trithermius)
- Ganz oben in der 1. Zeile stehen die Klartextbuchstaben, in den Zeilen darunter die verschiedene Schlüsselalphabete der Verschiebechiffren.
- Um einen Text zu verschlüsseln, geht man der Reihe nach die Zeilen mit den Schlüsselalphabeten durch, für jeden Buchstaben ein neues Alphabet.

Folie 14

Folie 2: Das Vigenère-Quadrat

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

5

Historische Verfahren - Vigenère-Chiffrierung - (5)

Die 3. Möglichkeit:

- Grundlage ist wieder das „*Vigenère-Quadrat*“
- Ganz oben in der 1. Zeile stehen die Klartextbuchstaben, in den Zeilen darunter hier aber ein beliebiges Schlüsselalphabet und dieses in den weiteren Zeilen zyklisch verschoben.
- Die Verschlüsselung erfolgt mit dieser Matrix auf die bekannte Art und Weise.

Folie 16

Historische Verfahren
- Vigenère-Chiffrierung - (6)

Wo liegen die Schwachstellen:

- Alice und Bob müssen im Besitz der Vigenère-Quadrate sein und diese dürfen Charlie nicht bekannt werden.
- Das Brechen des Codes ist heute relativ einfach: Leicht nachvollziehbar ist das an der zuerst vorgestellten Variante: Man probiert verschiedene Schlüssellängen. Bei einer Schlüssellänge von 5 sind alle Zeichen an Pos. 1, 6, 11, 16, ... Caesar-chiffriert. Jetzt kann man in dieser Teilmenge Häufigkeits-untersuchungen vornehmen.

Folie 17

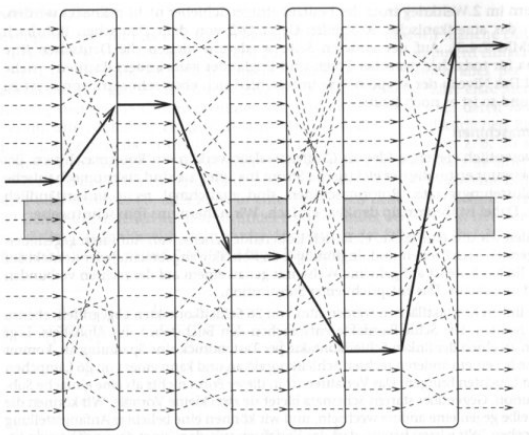
Historische Verfahren
- Die Enigma -

Folie 18

Historische Verfahren - Die Enigma - (2)

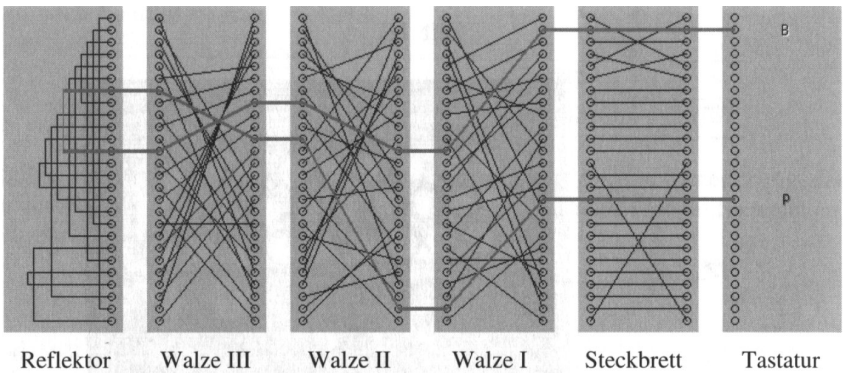
Dieser Stromlaufplan einer Rotormaschine zeigt, dargestellt durch die dicken Pfeile, den Stromverlauf von links nach rechts für ein zu verschlüsselndes Zeichen.

Verwendet werden insgesamt 4 Rotoren, man spricht auch von Walzen.



Stromlaufplan in einer Rotormaschine

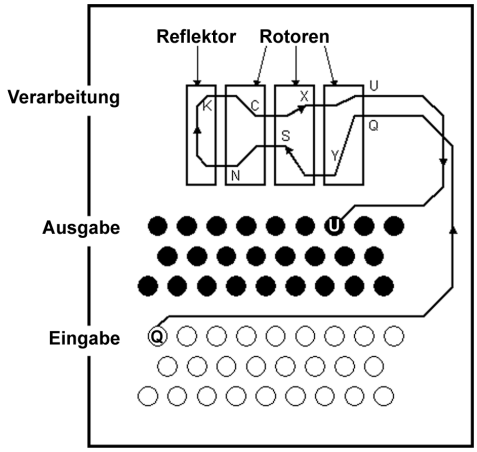
Historische Verfahren - Die Enigma - (3)



Der Verdrahtungsplan zeigt zusätzlich zu den 3 Rotoren ein Steckbrett (zur Erhöhung der Schlüsselanzahl) und den „problematischen“ Reflektor.

Folie 20

Funktionsweise der Enigma



Arthur Scherbius

Folie 21

Kryptoanalyse der Enigma

- 1927 fängt der polnische Zoll eine Enigma ab, die versehendlich an eine deutsche Firma geschickt wurde
- So war die Funktionsweise der Enigma den Alliierten schon früh bekannt. Auch die Walzen kannte man später zum Teil.
- Bei der Enigma galt erstmals das von *A. Kerkhoffs* bereits 1883 formulierte Prinzip:

Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels abhängen, nicht jedoch von der Geheimhaltung des Algorithmus.

Folie 22

Kryptoanalyse der Enigma (2)

- Klartextangriff mit negativer Mustersuche
- Analyse der Spruchschlüssel, die aus drei Buchstaben bestanden und am Anfang jeder Nachricht zwei mal gesendet wurden
- Spruchschlüssel waren häufig stereotyp gewählt

Marian Rejewski (1905–1980)

- Viele Nachrichten hatten gleichen Anfang („AN“) und stereotype Teile (z.B. „HEILHITLER“)
- Wetterberichte wurden nur mit 3-Rotor-Enigma übermittelt
- Enigma galt in Deutschland als vollkommen sicher

Folie 23

100% sicher? Das One-Time-Pad

- Einziges bewiesen sicheres Verfahren.
- Wurde vermutlich verwendet, um den heißen Draht zwischen Moskau und Washington zu schützen.
- Basiert meist auf XOR (⊕) Funktion.
- Text ⊕ Passwort = sichere Nachricht
- sichere Nachricht ⊕ Passwort = Text
- Passwort muss die gleiche Länge wie der Text haben, um Sicherheit zu gewährleisten.

Folie 24

100% sicher? Das One-Time-Pad (2)

- 1917 erfunden
- Schlüssel ist so lang wie die Nachricht
- Schlüssel muss echt zufällig sein
- Schlüssel darf nur einmal verwendet werden

Gilbert Vernam

Folie 25

100% sicher? Das One-Time-Pad (3)

Eine Zahlenfolge (a_n) mit $a_i \in \{0,1\}$ heißt **(echte) Zufallsbitfolge**, wenn die Werte 0 und 1 jeweils mit Wahrscheinlichkeit ½ vorkommen und wenn es keine Möglichkeit gibt, aus der Kenntnis eines beliebig langen Anfangsstücks der Folge Informationen über den Rest der Folge abzuleiten. (aus [1] S. 48)

Folie 26

Beispiel-Programme

- Verschlüsselungs-DEMO-Programme:
  - Crypto – Programm vom M. Roßberg (läuft ohne Installation)
  - „Cryptools“ der Deutschen Bank (mit vielen Möglichkeiten und umfangreicher Hilfe)

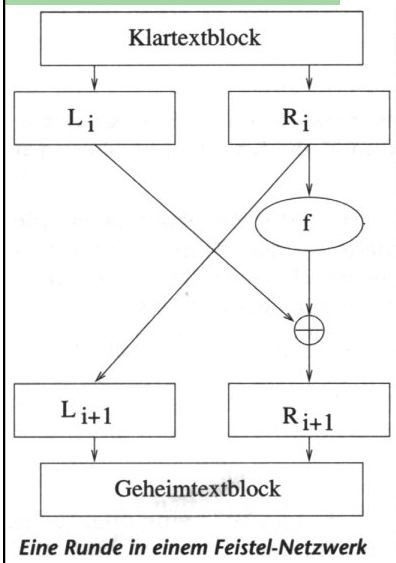
Folie 27

Moderne Verfahren - DES -

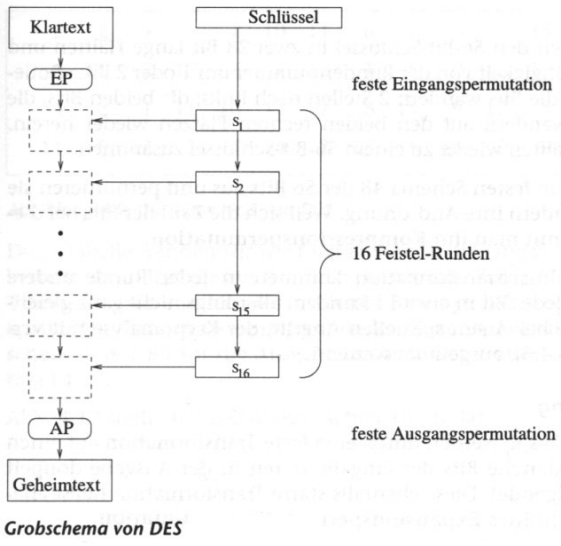
- Der ***D**ata **E**ncrytion **S**tandard* ist das am besten untersuchte kryptografische Verfahren
- Wurde nach einer 2. öffentlichen Ausschreibung 1974 von einem IBM-Team eingereicht
- Wurde 1976 zum offiziellen Verschlüsselungsstandard erklärt
- Verfahren ist für „normale“ Geheimhaltung gedacht, nicht zum Schutz von Informationen höchster Sicherheitskategorie

Folie 28

Folie 3: Funktionsweise von DES (grob)



Eine Runde in einem Feistel-Netzwerk



Grobschema von DES

Folie 29

Moderne Verfahren - DES - (3)

Wie sicher ist DES?

Es sind nur drei Angriffsmöglichkeiten bekannt:

- Brute Force
- differentielle und
- lineare Kryptoanalyse

Folie 30

Moderne Verfahren
- RSA -

- Asymmetrisches Verfahren, „das Beste was wir haben“.
- Von Ron **R**ivest, Adi **S**hamir, und Leonard **A**dleman 1978 entwickelt
- Gut verstanden und relativ sicher für große Schlüssel (mehr als 2048 Bit).

Folie 31

Moderne Verfahren
- RSA - (2)

- Schwierigkeit ist die Primfaktorzerlegung
  einfach: 250=5*5*5*2
  schwierig: 247=(?)
  hart: 256793=(?)
- RSA in 3 Zeilen Perl Code:
  print pack"C*",split/\D+/,`echo "16iII*o\U@ {$/=
  $z;[(pop,pop,unpack"H*",<>)]}\EsMsKsN0[lN*1
  lK[d2%Sa2/d0

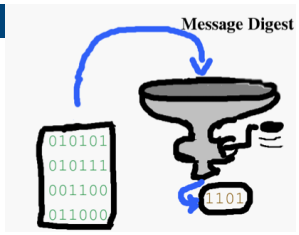
Folie 32

Hashing in der Natur

- Nehmen wir als Beispiel zur Erklärung des Hashing einen kleinen Hasen.
- Wenn der Hase gefressen hat, wird das Futter im Magen zer-hackt (hash = hacken), vermischt, zerrührt, verdaut, entwässert und ausgestoßen.
- Das Resultat ist ein kleiner Haufen. Das Endprodukt lässt sich der Eingabe, dem Futter, zuordnen. Hierbei geht natürlich eine ganze Menge an Information verloren; die Zuordnung zum Futter und sogar zu einem ganz bestimmten Hasen ist aber (z. B. durch DNS-Analyse) immer noch möglich.

Folie 33

Hashing in der Informatik



- Dasselbe lässt sich auch mit digitalen Dokumenten, wie Text-Dokumenten, Musik-Dateien und Film- Dateien durchführen.
- Für einen Informatiker sind das einfach Folgen von Nullen und Einsen.
- Hierzu wird das Originaldokument durch eine Folge von Operationen vermengt, vermischt und verdichtet, bis eine Bit- folge fester Länge „ausgeschieden“ wird.
- Ein bekannter Algorithmus, der diesen Vorgang durchführt, ist MD-5 (*Message Digest 5), was soviel wie Nachrichtenverdauer Version 5 heißt.*

Folie 34

MD-5 Hash-Algorithmus

- wurde 1991 von Ronald Rivest (der auch an der Entwicklung des RSA-Algorithmus beteiligt war) entwickelt
- Die genaue Beschreibung des Algorithmus kann bei Wikipedia nachgelesen werden.
- Andere bekannte Algorithmen sind SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512
- Übersetzt sind das ”sichere Hack-Algorithmen“ (*Secure Hash-Algorithm).*
- *MD-5 ist als Standardfunktion in PHP enthalten und kann deshalb einfach eingesetzt werden.*
- *Java: Klasse String: enthält die Methode „hashCode“*

Folie 35

MD-5 im Detail

- MD5 (Message-Digest Algorithm 5) erzeugt aus einer beliebigen Nachricht einen 128-Bit langen Hashwert.
- 1996 fand Hans Dobbertin zwei speziell präparierte Nachrichten, die sich unterscheiden, aber dennoch denselben Hashwert ergeben. Dieses war allerdings ohne praktische Auswirkungen auf die Sicherheit von MD5, denn die beiden kollidierenden Nachrichten ergaben keinen Sinn.
- 2008 wurde mit einem Cluster von 200 Sony Playstation 3 gezeigt, wie man für jede beliebige URL ein SSL-Zertifikalt fälschen kann.
- Da der Rechenaufwand seit dem noch gesunken ist, wird MD-5 für sicherheitsrelevante Anwendungen nicht mehr empfohlen.

Folie 36

Was leisten MD-5 und Co.? (1)

- Sie bilden Dateien unterschiedlicher Länge auf Bitfolgen fester Länge ab.
- Aus dem Ergebnis lassen sich die ursprünglichen Dateien identifizieren, aber nicht unbedingt rekonstruieren.
- Das bedeutet: Wenn die Hash-Werte zweier Nachrichten gleich sind, ist die Wahrscheinlichkeit hoch, dass auch die Nachrichten gleich sind.

Folie 37

Was leisten MD-5 und Co.? (2)

- Eine 100%ige Sicherheit gibt es aber nicht, dass dies so ist.
- Zum Beispiel galt lange MD-5 als praktisch sicher.
- Heute kennt man Methoden zur Konstruktion von beliebig vielen Übereinstimmungen der Hash-Werte bei ungleichen Nachrichten.
- Derzeit gilt SHA-512 (mit 512 Bits für den Hash-Wert) als sehr sicher.
- Die Bedeutung des Hashing in der praktischen Informatik ist groß.

Folie 38

Anwendungsbeispiel für Hashing (1)

- Alice möchte an Bob eine E-Mail schicken. Bob soll prüfen können, ob der Inhalt der Mail nicht verändert wurde.
- Alice schreibt die E-Mail und bildet daraus mit einem Hash-Algorithmus einen Hash-Wert.
- Alice überträgt die E-Mail und in einer Extra-Nachricht (möglichst über einen anderen Kanal) den Hash-Wert.

Folie 39

Anwendungsbeispiel für Hashing (2)

- Bob empfängt die E-Mail und liest sie. Jetzt bildet er mit dem gleichen Hash-Algorithmus (z. B. MD-5) den Hash-Wert der Nachricht, die er gelesen hat.
- Bob empfängt den Hash-Wert von Alice und vergleicht ihn mit seinem ermittelten Wert.
- Wenn beide Hash-Werte gleich sind, kann Bob davon ausgehen, das die E-Mail unverfälscht bei ihm angekommen ist.

Folie 40

Zusammenfassung:
Was sollte jeder beachten?

- Einsatz von Open Source (Software) lohnt sich
- Ältere, aber nicht alte Algorithmen verwenden
- Nur gut bekannte Algorithmen verwenden
- Sichere Speicherung von Schlüsseln.
- Nicht davon ausgehen, dass man nichts zu verbergen hat

Folie 41

Einteilung der Verschl.verfahren

Man unterscheidet prinzipiell 3 Gruppen:

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hash-Verfahren

Aufgaben:

- Worin unterscheiden sich symetrische und asymmetrische Verschlüsselungsverfahren?
- Ordnen Sie die genannten Verfahren den Gruppen zu!

Folie 42

Literaturverzeichnis

[1] Ertel, Wolfgang: Angewandte Kryptographie, Leipzig: Fachbuchverlag im Carl Hanser Verlag, 2001

[2] Wobst, Reinhard: Abenteuer Kryptologie, 3., überarb. Aufl. - München: Addison-Wesley Verlag, 2001

[3] Bauer, Friedrich L.: Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie. – 3., überarb. u. erw. Aufl. – Berlin; Heidelberg; New York: Springer-Verlag, 2000