Güclü, am 31.03.2022

AES / DES

AES

AES (Advanced Encryption Standard) ist ein symmetrisches Verschlüsselungsverfahren und der Nachführer des DES (Data Encryption Standard). Symmetrisches Verschlüsselungsverfahren bedeutet, dass im Gegensatz zur asymmetrischen Verschlüsselung nur einen Schlüssel zum Verschlüsseln und zum Entschlüsseln gibt.

AES setzt man häufig ein, um Daten verschlüsselt zu übertragen. [0]
Beim AES sind mögliche Schlüssellängen gegeben durch 128, 192 oder 256 Bit, weshalb man diese AES Varianten dann mit AES-128, AES-192 und AES-256 bezeichnet (z.B. 256-Bit ist dabei die Schlüssellänge). [0]

Anwendungsbereiche:

Die AES Verschlüsselung findet in den verschiedensten Bereichen Anwendung, wie z.B. bei WLAN oder WAP2, sowie SSH.
Es ist bisher keine Schwäche von AES bekannt, die auch nur annähernd eine praktische Bedeutung hat. [1]

Durchführung

Das Verfahren wechselt bei jedem Schritt zwischen Substitution und Permutation (SP-Netzwerk). Man spricht von AES auch als SP-Chiffre. Der Klartext wird dabei nicht als Ganzes, sondern in Blöcken verarbeitet. Hierbei wird unter anderem die Beziehung zwischen Klar- und Geheimtext verwischt, was man in der kryptologischen Fachsprache als Konfusion bezeichnet. [1]

Ein SP-Netzwerk (Substitution-Permutation-Netzwerk) besteht aus einer Anzahl von Runden gleichen Aufbaus. In jeder Runde wird zuerst ein Rundenschlüssel auf die Eingabe addiert. Dann wird das Ergebnis in mehrere Blöcke aufgeteilt, und jeder Block mittels der Substitutionsbox (S-Box) durch einen anderen Block ersetzt. Diese Blöcke werden wiederum durch eine Permutationsbox (P-Box) vermischt.

Konfusion ist in der Kryptologie eines der beiden zentralen Prinzipien zur Verschleierung von Strukturen eines Klartextes im Zuge einer Verschlüsselung oder beim Hashen. Um Konfusion zu erreichen, muss ein kryptografisches Verfahren nichtlineare Operationen enthalten. [2]

(Hinweis: Eine lineare Operation wäre z.B.: Wenn das Ergebnis, als Polynom 1.Grades ausgedrückt werden kann.)

Beispiel [3]

„Two One Nine Two“ muss verschlüsselt werden.

In HEX sind diese Buchstaben folgendes:

Buchstaben	T	h	a	t	s		m	y		K	u	n	g		F	u
HEX	54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

1.Runde:

HEX wird in 4 Blöcke unterteilt:
w(0): (54, 68, 61, 74)
w(1): (73, 20, 6D, 79)
w(2): (20, 4B, 75, 6E)
w(3): (67, 20, 46, 75)

g(3):

1. Schritt -> Byte left shift. Resultat = (20, 46, 75, 67)
2. Schritt -> Byte Substitution. Resultat = (B7, 5A, 9D, 85)
3. Konstante hinzufügen: (01, 00, 00, 00) -> (B6, 5A, 9D, 85)

w(4): w(0) + g(3) = (E2, 32, FC, F1)
w[5] = w[4] + w[1] = (91, 12, 91, 88)
w[6] = w[5] + w[2] = (B1, 59, E4, E6)
w[7] = w[6] + w[3] = (D6, 79, A2, 93)

Endresultat für die erste Runde: (E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93)

Insgesamt: 10 Runden.
Am Ende der 10. Runde kommt der tatsächlich verschlüsselte und nach-außen-geschickte Schlüssel heraus.

DES

Aufgrund der kurzen Schlüssellänge von 56 Bit müsste diese Verschlüsselungstechnik weiterentwickelt werden (siehe AES). Man muss auch sagen, dass 56-Bit-Schlüsseln jetzt von Computern in paar Minuten/Stunden geknackt werden können -> Mit einem Brute-Force-Angriff ließe sich der geheime Schlüssel sehr einfach entschlüsseln, indem man alle möglichen Schlüsselkombinationen durchprobiert.

DES basiert auf einer monoalphabetischen Substitutionschiffre. Die Funktionsweise der Verschlüsselung von DES entspricht einer Kombination aus One-Time-Pad, Permutations- und Substitutionschiffre, die auf Bitfolgen angewendet werden. [4]

Monoalphabetisch = Dabei wird jedes Zeichen des Klartextes nach einem festgelegten Schema, der Verschlüsselungsvorschrift, durch ein anderes, ihm zugeordnetes Zeichen ersetzt (substituiert).

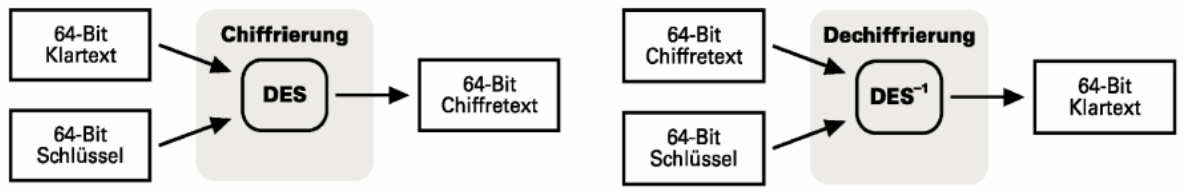


Abb 1: Chiffrierung und Dechriffierung beim DES [5]

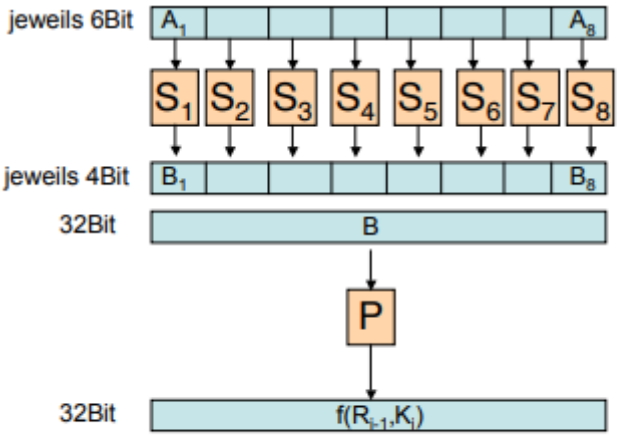
Anwendungsbereiche:
Gibt fast keine mehr, da es sehr unsicher ist.

Durchführung

Beim DES-Verfahren wird 16-mal verschlüsselt. Es kann in vier verschiedenen Modi ablaufen, wobei die Blöcke einzeln verschlüsselt werden oder jeder Chiffrierblock von allen vorangegangenen Blöcken abhängig gemacht wird.

Normalerweise verwendet DES einen 64-Bit-Schlüssel, aber da 8 dieser Bits für Paritätsprüfungen verwendet werden, beträgt die effektive Schlüssellänge nur noch 56-Bit.

(Paritätsprüfung ist ein relativ einfaches Verfahren zur Fehlererkennung von Bits.)



Permutation P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Abb 2: Durchführung: DES [6]

Ich konnte kein **einfaches** Beispiel finden! Da diese Methode veraltet ist, halte ich ein Beispiel für irrelevant

Literaturverzeichnis

[0] ‚AES Verschlüsselung' https://studyflix.de/informatik/aes-verschlusselung-1611, 2019, Abgerufen am 29.03.2022

[1] ‚AES – Advanced Encryption Standard' https://www.elektronik-kompendium.de/sites/net/1901171.htm 2021, Elektronik-Kompendium, Abgerufen am 29.03.2022

[2] ‚Konfusion' https://de.wikipedia.org/wiki/Konfusion_(Kryptologie), Wikipedia, Abgerufen am 29.03.2022

[3] ‚AES Example - Input ‘https://www.kavaliro.com/wp-content/uploads/2014/03/AES.pdf‘, März 2014, kavaliro, Abgerufen am 29.03.2022

[4] ‚DES‘ https://www.elektronik-kompendium.de/sites/net/1901161.htm#:~:text=Funktionsweise%20von%20DES&text=Die%20Funktionsweise%20der%20Verschl%C3%BCsselung%20von,Bit%20als%20Pr%C3%BCfsumme%20verwendet%20werden, 2022, Abgerufen am 31.03.2022

[5] Hai Anh Pham. ‚AES – DES‘ https://www.cs.uni-potsdam.de/ti/lehre/04-Kryptographie/slides/DES-AES, 2021, Abgerufen am 31.03.2022

[6] ‚Kryptopgrafie‘ http://www.inf.fu-berlin.de/lehre/SS04/SySi/folien/KryptografieTeil1.pdf, 2021, Abgerufen am 31.03.2022