Manuskript

radioWissen

SENDUNG: 03.08.2023
9.30 Uhr / B2

TITEL: Kryptographie – Die Geschichte der Verschlüsselung

AUTOR: Oliver Buschek
REDAKTION: Nicole Ruchlak
REGIE: Rainer Schaller
TECHNIK: Roland Böhm

SPRECHER: Sprecher/in Julia Fischer
Zitator Christian Schuler

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

Ansage Podcast

Wir sprechen, um uns anderen mitzuteilen. Und wenn wir uns nur ganz wenig Ausgewählten mitteilen wollen, müssen wir eine Geheimsprache benutzen. Davon gibt es unzählige. Kein Wunder – denn die erste Geheimsprache ist schon uralt….

Musik M01

Sprecher/in:
Wir schreiben das Jahr 404 vor Christus. Der Peloponnesische Krieg steht kurz vor dem Ende, den Spartanern ist der Sieg über die Athener nicht mehr zu nehmen. Nun planen die Perser, die Situation auszunutzen - und bereiten einen Angriff vor. Doch der spartanische Heerführer Lysander erfährt rechtzeitig davon – weil ihm die Regierungsbeamten aus der Heimat eine verschlüsselte Botschaft zukommen lassen.

Zitator
"...dem Lysander selbst schickten sie eine sogenannte Skytale mit dem Befehl zur Umkehr.“

Sprecher/in:
… berichtet der griechische Schriftsteller Plutarch und erklärt:

Zitator
„Mit der Skytale hatte es folgende Bewandtnis: Wenn die Ephoren einen Admiral oder General aussenden, so lassen sie zwei runde Stäbe von einer bis aufs Genaueste gleichen Länge und Dicke anfertigen.

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

Den einen behalten sie selbst, den anderen geben sie dem Abgehenden. Diese Stäbe nennt man Skytalen. Wenn sie nun etwas Geheimes und Wichtiges mitzuteilen wünschen, bringen sie ein Stück Papyrus in die Form eines langen schmalen Riemens, umwickeln damit die Skytale so, dass kein Zwischenraum übrigbleibt, sondern überall im Kreise herum seine Oberfläche mit dem Papier bedeckt erscheint.

Sprecher/in:
Auf diesen spiralförmig gewickelten Papyrus - so Plutarch – schrieb man die dann die geheime Botschaft. Zeile für Zeile, quer über die Wicklungen, immer über die gesamte Stablänge. Anschließend wurde der Papyrus abgewickelt und – ohne den Stab – an den Feldherrn geschickt.

Zitator
„Der Empfänger ist nun außer Stande, den Inhalt zu lesen, da die Buchstaben gar keinen Zusammenhang haben, sondern auseinandergerissen sind. Aber jetzt nimmt er seine eigene Skytale und zieht das Stück Papier rings an derselben auf, so dass die Windung wieder in die gleichmäßige Ordnung kommt, das Zweite sich an das Erste anschließt und hierdurch das Auge imstande ist, das Zusammengehörige aufzufinden."

Sprecher/in:
Plutarch schrieb diese Zeilen rund 500 Jahre nach den Ereignissen. Ob die „Skytalen“ in Sparta also wirklich die beschriebene Funktion von Geheimbotschaften hatten, ist keineswegs sicher. Bei anderen Autoren wird das Wort „Skytale“ als Synonym für Botschaft verwendet.
Doch man kann davon ausgehen: Schon in der Antike gab es das Bedürfnis, Nachrichten vor Unbefugten zu verschlüsseln.

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

ZSP Dahlke „Kryptologie ist so alt wie die Menschheit“

„Die Kryptologie ist wahrscheinlich genauso alt wie die Menschheit selbst.

Sprecher/in:

… erklärt die Museumspädagogin Carola Dahlke. Sie ist am Deutschen Museum in München als Kuratorin für den Bereich Kryptologie zuständig – also die Lehre vom Verschlüsseln und Entschlüsseln von Nachrichten. Und sie kennt noch mehr Beispiele dafür, wie man in der Antike versuchte, Informationen zu verbergen.

ZSP Dahlke „Verschlüsselungsscheibe“

„Da gibt es zum Beispiel die Schriften von einem sogenannten Aenaeas Tacticus, 400 v. Christus, der hat ein Pergament hinterlassen über die Belagerung von Städten, und da gibt es zum Beispiel die Möglichkeit, dass man Wörter auf Metallscheiben schreibt mit einer Schnur.“

Sprecher/in:

Für das Deutsche Museum hat Carola Dahlke eine solche Metallscheibe anfertigen lassen. Sie ist etwa so groß wie ein Handteller, am Rand sind ringsum Löcher gebohrt – insgesamt 26 Stück. Jedes Loch steht dabei für einen Buchstaben – die allerdings nicht eingezeichnet sind; nur der Sender und der Empfänger kannten die Zuordnung.

ZSP Dahlke „Verschlüsselungsscheibe (Forts.)“

Also das ist jetzt hier diese Scheibe mit den Löchern, wie sie Aenaeas Tacticus sich vorgestellt hat und sie sieht ja aus wie eine schöne Gürtelschnalle. Wenn man jetzt nicht weiß, dass da ein verschlüsselter Text drauf wäre, könnte man das nicht ahnen. Und man kann jetzt da durch dieses Fädeln sich ein Wort überlegen, was man vielleicht senden möchte, das ganz wichtig ist, zum Beispiel hat man vielleicht in der belagerten Stadt ein Essensproblem und schreibt „Mehr Essen“ drauf.

Sprecher/in:

Und zwar indem man die Schnur Buchstabe für Buchstabe durch die zugehörigen Löcher fädelt. Erst durch das M, dann das E, das H, das R … und so weiter.

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

ZSP Dahlke „Verschlüsselungsscheibe (Forts. 2)“

Und der Empfänger hat die gleiche Scheibe, hat aber auch bei jedem Loch die Information, welcher Buchstabe das ist, und wenn er jetzt die Schnur ausfädelt, erhält er rückwärts die Geheimbotschaft.“

Musiktrenner 02

ZSP Beutelspacher „Kopfhaut des Sklaven“

„Es gab auch so ganz skurrile Dinge, dass man einem Sklaven den Kopf kahlgeschoren hat, dann die Nachricht auf die Kopfhaut geschrieben hat, gewartet hat, bis die Haare wieder gewachsen sind, ihn irgendwo hingeschickt und dann wurde er wieder rasiert. Das ist sicher das kryptografische Verfahren mit der schlechtesten Performance überhaupt, aber es wurde jedenfalls so darüber berichtet, dass es mehrfach angewandt wurde, das heißt, manchmal hat es auch funktioniert.“

Sprecher/in:

… erzählt der Mathematiker Professor Albrecht Beutelspacher, Verfasser eines viel gelesenen Lehrwerks über Kryptologie. Darin erfährt man zum Beispiel, dass in der Antike drei verschiedene Arten von Verschlüsselungsverfahren existierten: Erstens, die Transposition, bei der – wie im Fall der Skytale – die Buchstaben eines Textes gründlich durcheinandergewirbelt werden. Zweitens, die Steganografie, bei der für Außenstehende nicht erkennbar ist, dass es sich um eine Botschaft handelt – wie im Fall der Gürtelschnalle oder des Sklavenkopfes. Und drittens: Die Substitution – bei der jeder Buchstabe durch einen anderen ersetzt wird.

ZSP Beutelspacher „Julius Cäsar“

„Eine Idee geht auf Julius Cäsar zurück. Der hat gesagt, ich verschlüssele ein Wort so, indem ich jeden Buchstaben verschlüssele, und zwar jeden Buchstaben ersetze ich durch einen anderen Buchstaben – soweit allgemein – er sagte: ich zähle jeweils um eine gewisse Anzahl von Buchstaben weiter. Also wenn ich zum Beispiel den nächsten Buchstaben nehme, würde aus A B werden, aus B C aus X Y, aus Z würde dann wieder A werden usw. Und wenn man das macht, sieht man, dass aus einem vernünftigen Satz, aus vernünftigen Wörtern scheinbar unleserliches Zeug entsteht.“

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

Sprecher/in:

Die Idee von Julius Cäsar prägt die Kryptologie über Jahrhunderte. Kinder wenden sie heute noch an, wenn sie – vielleicht im Grundschulalter – zum ersten Mal mit Geheimbotschaften experimentieren. Doch bis zum Beginn der Neuzeit verbreitet sich allmählich die Erkenntnis, dass dieses Ersetzen von Buchstaben nur einen schwachen Schutz bietet.

ZSP Beutelspacher „Häufigkeitsanalyse“

„Weil nämlich zum Beispiel im Deutschen – aber auch in anderen Sprachen – ein Buchstabe besonders häufig ist. Im Deutschen ist es das E, das fast 20 Prozent aller Buchstaben ausmacht. Und bei allen solchen Verfahren wird das E in den gleichen Buchstaben ersetzt, und ich muss nur nach dem häufigsten Buchstaben suchen und dann habe ich schon das E entschlüsselt. Und bei einfachen Verfahren habe ich dann fast alles entschlüsselt.

ZSP Dahlke „Polyalphabetische Verschlüsselung“

„Und das war der Beginn, wo man nicht mehr einen Buchstaben durch einen anderen ersetzt hat, sondern durch ganz viele verschiedene. Und das war ungefähr 1490.“

Musiktrenner M03

ZSP Dahlke „Fortschritte zum Beginn der Neuzeit“

„Allgemein muss, man sagen, dass dieser Beginn der Neuzeit um 1500 – da entstanden eben diese diplomatischen Beziehungen, da entstand das Postwesen, da hat die Menschheit begonnen, Bücher zu drucken, da wurde Information plötzlich etwas, was allen zugänglich war. Da wurde die Wichtigkeit, dass man etwas verschlüsselt – dass man es aufschreibt und verschlüsselt – die wurde so viel größer als vorher, dass sich da unglaublich viel getan hat.

Sprecher/in:

Zur erfolgreichsten Verschlüsselungsmethode der Neuzeit wird bald die sogenannte Vigenère-Chiffre. Benannt nach Blaise de Vigenère, einem französischen Diplomaten des 16. Jahrhunderts, der in Rom mit der Kryptologie in Kontakt kommt. Diese Methode beruht auf einem Schlüsselwort,

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

das nur dem Sender und dem Empfänger bekannt ist. Dieses Wort wird an den zu verschlüsselnden Text angelegt – und zwar so oft, bis die ganze Länge des Textes abgedeckt ist, erklärt Carola Dahlke.

ZSP Dahlke „Vigenère-Chiffre Eule “

Also wenn wir jetzt ein ganz einfaches Schlüsselwort nehmen, zum Beispiel EULE, dann schreiben wir unter den Geheimtext, den ich jetzt schreiben will, also weiß nicht, „Lieber Freund“, dann schreibe ich unter das L also das E. Dann unter das I von Lieber schreibe ich dann das U von der Eule. Unter das E schreibe ich dann das L und so weiter, also dass wirklich – EULEEULEEULE schreibe ich so unter diesen Geheimtext drunter.

Sprecher/in:

So entstehen Buchstabenpaare: Der Original-Buchstabe des Geheimtextes und der zugeordnete Buchstabe des Schlüsselwortes. Mit diesen Paaren geht es nun zum Herzstück der Vigenere-Chiffre: Ein Koordinatensystem, befüllt mit den Buchstaben des Alphabets.

ZSP Dahlke „Vigenère-Chiffre Chaos“

Und jetzt gehe ich zu meinem Koordinatensystem und schaue den Schnittpunkt an zwischen dem L und dem E. Und da könnte jetzt zum Beispiel ein B stehen oder ein T. Und das ist jetzt mein Geheimtextbuchstabe. Und dadurch dass ich eben bei jedem einzelnen Buchstaben meines Geheimtextes im Koordinatensystem mir eine andere Stelle auswähle, kommt eine sehr chaotische Verschlüsselung raus.“

MUSIK m04

Sprecher/in:

Erst im 19. Jahrhundert veröffentlicht der preußische Infanteriemajor und Kryptoanalytiker Friedrich Wilhelm Kasiski ein allgemeingültiges Verfahren, mit dem sich Texte, die nach der Vigenére-Chiffre verschlüsselt sind, entziffern lassen. Beinahe 300 Jahre lang hat sie Stand gehalten. Damit bewährt sich ein Prinzip, das noch heute die Kryptologie prägt: Nicht das

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

Verschlüsselungsverfahren muss geheim sein, sondern nur der verwendete Schlüssel – erklärt der Mathematiker Albrecht Beutelspacher.

ZSP Beutelspacher „Verfahren dürfen öffentlich sein“

„Das ist so ein Grundprinzip, dass wir die Sicherheit nicht darauf bauen können, dass das Verfahren geheim bleibt. Nicht alle Verfahren sind öffentlich, also die Geheimdienste auf der ganzen Welt haben Verfahren, die sie in der Regel nicht veröffentlichen, aber auch die würden sagen: wenn unser Verfahren irgendwie bekannt wird, ist die Sicherheit nicht gefährdet. Ihre Furcht ist nur, dass die jeweiligen Gegner dann diese wunderbaren Verfahren auch nutzen können. Und das wäre vielleicht schlecht.“

Musiktrenner m05

Sprecher/in:

Vom 19. Jahrhundert an ist es vor allem die Technik, die die Kryptografie vorantreibt. Zunächst die Telegrafie, erfunden 1837 von Samuel Morse. Die drahtlose Übertragung von Botschaften – die von jedem mit entsprechenden Empfangsgeräten abgefangen werden können – macht Verschlüsselung wichtiger denn je, erst recht im Kriegseinsatz. Daneben findet aber auch eine ganz andere Art von Codes Verwendung, erklärt Carola Dahlke vom Deutschen Museum.

ZSP Dahlke „Codebücher – öffentlich und geheim“

„Da wurden dann die Codebücher interessant. Ein Codebuch bedeutet im Grund nichts anderes als ein Lexikon, dass zum Beispiel ein A immer ersetzt wird durch eine Ziffernfolge oder dass ein ganzes Wort ersetzt wird, denn in der Telegraphie wird ja buchstabenweise abgerechnet, das ist teuer, also versucht man natürlich eher kürzer zu werden. Wenn ich jetzt sage „Guten Tag“ – ist sehr lang, hat sehr viele Buchstaben, das ersetze ich jetzt durch ein X. Dadurch wird’s viel billiger und man muss aber im Codebuch hinterlegen, dass das X „Guten Tag“ bedeutet. Diese Codebücher gab es öffentlich, damit konnte man eben telegrafieren, es gab aber auch streng geheime Bücher, die hat man auch Schlüsselbücher genannt. Und die wurden vor allen Dingen im Ersten Weltkrieg eingesetzt.“

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

Geräusch m06

Sprecher/in:

Doch das Verwenden von Schlüsselbüchern gehört bald der Vergangenheit an. Die Berechnungen, die für sichere Verschlüsselungen nötig sind, werden immer komplexer, und nach dem Ersten Weltkrieg konstruieren Ingenieure Maschinen, die diese Aufgabe übernehmen können.

ZSP Beutelspacher „Mechanische Maschinen“

Die frühen Maschinen waren natürlich mechanische Maschinen, ne Kombination von Zahnrädern, von Walzen, die komplex zusammengearbeitet haben, die berühmteste ist die Enigma, deren Grundprinzip auf Walzen beruht, die wie so ein Kilometerzähler hintereinander geschaltet sind.“

MUSIK m07

Sprecher/in:

Im Februar 1918 erhält der deutsche Elektroingenieur Arthur Scherbius das Patent auf einen neuartigen „Chiffrierapparat“. Kurz darauf bietet er ihn der kaiserlichen Marine an, doch diese lehnt dankend ab. Der Einsatz maschineller Verschlüsselung sei nicht erforderlich. Einige Jahre später stellt sich heraus: Die deutsche Niederlage im Ersten Weltkrieg war auch darauf zurückzuführen, dass es Franzosen und Briten gelungen war, Codes des deutschen Militärs zu entziffern. So steigt das Interesse von Heer und Marine an Scherbius‘ Erfindung. Und als später die Nationalsozialisten die massive Aufrüstung der Wehrmacht betreiben, wird der Apparat unter dem Namen „Enigma“ zum Herzstück der militärischen Kommunikation. Insgesamt etwa 40.000 dieser Maschinen gab es – in unterschiedlichen Ausfertigungen für die einzelnen Teilstreitkräfte.

ZSP Dahlke „Erklärung Enigma“

„Das ist jetzt eine klassische Heeres-Enigma, die wir hier sehen können, das heißt sie hat drei Walzen.“

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

MUSIK m08

Sprecher/in:

… erklärt Carola Dahlke, während sie in einer Werkstatt des Deutschen Museums vor einer aufgeklappten Holzkiste steht, wenig größer als ein Schuhkarton. Darin: Eine anthrazitgraue Metallapparatur mit Tasten und Buchstabenfeldern, die durch darunterliegende Glühbirnen zum Aufleuchten gebracht werden können. Unter einer Abdeckung befinden sich drei rotierende Walzen.

ZSP Dahlke „Erklärung Enigma (Forts.)“

„Also wir haben den Walzensatz, eine Tastatur, sieht aus wie eine Schreibmaschine im Endeffekt und hat auch schon diese klassische QWERTZ-Anordnung der Tasten. Dann haben wir ein Glühlämpchen-Feld, also wenn ich jetzt einen Buchstaben drücke, wird er verschlüsselt und leuchtet dann in der verschlüsselten Version auf dem Glühlämpchen-Feld auf. Und man hat noch hier vorne, wenn man sie aufklappt, ein sogenanntes Stecker-Brett. Da wurden nochmal extra – um sozusagen die tägliche Verschlüsselungseinstellung zu komplizieren – wurden hier nochmal Buchstaben extra vertauscht. Und wie man das eingestellt hat, also welche Walze wo gelegen hat, welcher Buchstabe nach oben gezeigt hat oder in dem Fall, bei der Heeres-Enigma, welche Zahl nach oben geguckt hat und welche Buchstaben auf diesem Steckerbrett miteinander vertauscht wurden – stand eben in einer monatlich ausgegebenen Maschinentabelle, also die nannte sich Maschinenschlüssel, und da stand eben für jeden Tag die genaue Aufstellung drin, wie man die Maschine einstellen muss, für diesen Tag, um zu verschlüsseln.“

Sprecher/in:

Das Geheimnis der Enigma besteht in der Rotation der Walzen. Wird eine Taste gedrückt, um den Code für den entsprechenden Buchstaben zu erhalten, dreht sich der Walzensatz weiter. Der nächste Buchstabe wird also nach einer anderen Chiffre kodiert. Dabei leistet die Enigma nicht mehr als die Verschlüsselung selbst. Der kodierte Text muss Buchstabe für Buchstabe notiert und danach zum Funker gebracht werden. Umgekehrt muss man eine empfangene Botschaft in die Enigma eingegeben, um den Originaltext zu erhalten. Ein System, das lange Zeit gut funktionierte – auch wenn die Nachrichtendienste anderer Staaten der Enigma bald auf der Spur waren.

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

ZSP Dahlke „Entschlüsselung der Enigma“

„Das Dechiffrierbüro in Warschau hat große Anstrengungen unternommen und geniale Ergebnisse erzielt mit den ersten Enigma-verschlüsselten Nachrichten, die eben da bis 1938 abgefangen werden konnten. Dann hat Deutschland zu Beginn des Kriegs allerdings zwei weitere Walzen eingeführt, und es wurde so schwierig mit dem manuellen Aufwand, die zu entschlüsseln, dass sich Polen entschlossen hat, ihre Informationen zu teilen mit Frankreich und England. Und die Franzosen und Engländer sind bei diesem Treffen wohl aus allen Wolken gefallen, weil sie gedacht haben, die Enigma ist nicht entzifferbar. Und haben auch zuerst das gar nicht glauben können.

MUSIK m07

Sprecher/in:

In England arbeitet von 1939 an eine Spezialeinheit von Kryptoanalytikern daran, den geheimen Nachrichtenverkehr der deutschen Wehrmacht zu entziffern. In der Barackensiedlung mit dem Namen „Bletchley Park“ sind zeitweise bis zu 10.000 Personen beschäftigt, darunter brilliante Mathematiker wie Alan Turing und – die Männer sind an der Front – zahlreiche Frauen.

ZSP Dahlke „Entschlüsselung der Enigma (Forts.)“

„Mit dieser Vorarbeit der Polen konnten viele Nachrichten entziffert werden, die mit der Heeresenigma verschlüsselt worden sind. Die Marine-Enigma allerdings hat sehr viel Kopfzerbrechen bereitet, wurde dann auch noch mal umgebaut, da kam dann die vierte Walze dazu, dann gab es den sogenannten „Blackout“, also Bletchley Park hat das so genannt, Blackout bedeutet: Man kann nichts entziffern, und das hat viele Monate gedauert, es gab da große Anstrengungen aus gekaperten U-Booten und Schiffen die Enigmas auszubauen und das hat auch geklappt, und dadurch hat England Informationen über die Walzen erhalten und über die Maschinenschlüssel, und konnte so dann auch ab 1942 die Marine-Enigma auch mitlesen.“

Musiktrenner m07

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

Sprecher/in:

Noch während des Zweiten Weltkriegs, im Jahr 1941, baut der deutsche Ingenieur Konrad Zuse den ersten funktionstüchtigen Computer der Welt, den Z3. Die Erfindung läutet auch für die Kryptografie ein neues Zeitalter ein.

ZSP Beutelspacher „Treibende Kraft Computer“

„Wir können heute Verfahren realisieren, die man mechanisch nie realisieren könnte, also haben eine riesige Komplexität erreicht, auf der einen Seite. Aber die Angreifer haben natürlich auch Computer zur Verfügung und können statistische Analysen und irgendwelche Durchläufe natürlich auch in einer Zahl und einer Performance machen, die mechanisch oder gar von Hand undenkbar gewesen wäre. Also der Computer ist ein Movens, ein treibendes Element bei der Entwicklung der Kryptografie.“

Sprecher/in:

Im Computer- und Internet-Zeitalter gilt es plötzlich nicht mehr nur die Botschaften von Militärs, Diplomaten und Geheimdiensten zu verbergen. Auch Unternehmen und Privatleute haben plötzlich Bedarf, ihre Daten und ihre Kommunikation zu schützen. In den 70er Jahren wird dazu bei IBM der „Data Encryption Standard“ entwickelt – kurz: DES. Ein Verfahren, dessen Nachfolger bis heute verwendet werden. Und doch hat es für den Gebrauch im Internet einen Haken.

ZSP Beutelspacher „Archillesferse Schlüssel“

„Das ist das unlösbare Grundproblem der klassischen Kryptografie. Man hat einen Schlüssel – „man“ ist sowohl der Sender als auch der Empfänger, der Sender benutzt ihn zum Verschlüsseln, der Empfänger zum Entschlüsseln. Das heißt, der Schlüssel, das wirklich absolut geheime Stück, muss irgendwann vom Sender zum Empfänger oder von einer dritten Instanz an beide geschickt werden. Das ist die Archillesferse der klassischen Verfahren.“

Sprecher/in:

Die Lösung für dieses Problem finden – ebenfalls schon in den 70er Jahren – die beiden Amerikaner Whitfield Diffie und Martin Hellman. Ihr Konzept ist eine Sensation:

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

ZSP „Asymmetrische Verfahren“

„Die Grundidee war zu sagen: Verschlüsselung müsste doch eigentlich so einfach funktionieren wie telefonieren. Ich muss nur den Namen meines Partners wissen, dann kann ich die Telefonnummer nachschauen, kann ihn anrufen. Wir müssen nicht vorher irgendwelche Daten austauschen, um überhaupt telefonieren zu können. Und sie sagten: Kryptografie heißt dann auch – das ist die sogenannte „Public Key“-Kryptografie, also Kryptografie mit öffentlichen Schlüsseln – heißt: Ich weiß den Namen meines Partners, und kann seinen öffentlichen Schlüssel, der irgendwo veröffentlicht ist, nachschauen, und dann kann ich ihm eine verschlüsselte Nachricht schicken. Und nur er kann mit seinem privaten Schlüssel diese entschlüsseln.

MUSIK m09

Sprecher/in:

Ein öffentlicher Schlüssel zum Verschlüsseln und ein geheimer, privater Schlüssel zum Dechiffrieren. Beide hängen miteinander zusammen, und dennoch lässt sich der eine kaum aus dem anderen errechnen. Denn das Public-Key-Verfahren basiert darauf, dass es für einen Computer leicht ist, zwei Primzahlen miteinander zu multiplizieren. Dass es aber bedeutend aufwändiger ist, ein solches Produkt in seine zwei Primfaktoren zu zerlegen – wenn denn diese Zahl nur groß genug ist. Das führt etwa dazu, dass sich gut geschützte E-Mails nicht einmal mit Großrechnern dechiffrieren lassen. Häufiger als im E-Mail-Verkehr trifft man Public-Key-Kryptografie allerdings dort an, wo man sie gar nicht bemerkt.

ZSP Beutelspacher „Kryptografie im Alltag“

„Es gibt ganz viele Bereiche, in denen das wirklich automatisch funktioniert. Wann immer Sie mit Ihrer Chipkarte irgendetwas machen, gibt es da Algorithmen, die die Authentizität nachweisen und die auch Verschlüsselung machen. Bei der Einkommensteuer-Erklärung über ELSTER wird man immer nach Zertifikaten gefragt, das ist sozusagen ein Herzstück der modernen Public-Key-Kryptografie, die hier angewandt wird. Und auch im Internet wird automatisch verschlüsselt, und die Schlüssel werden mit diesen Public-Key-Verfahren ausgetauscht. Also das begegnet uns überall, wenn Sie ins Auto gehen, mit ihrer Fernbedienung die Türe aufmachen, ist auch wichtig, dass nicht der andere Ihr Auto aufmachen kann – auch das ist Kryptografie, gibt es an ganz vielen Stellen verborgen, und deswegen funktioniert’s auch so gut.“

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de

MUSIK m10

Sprecher/in:

Wie lange Public Key Verfahren noch sicher sein werden – das ist kaum abzusehen. Schon morgen könnte ein genialer Mathematiker ein Verfahren ersinnen, mit dem sich Primfaktoren viel einfacher erre chnen lassen als bisher. Und sogenannte Quantencomputer, die sich bereits in der Entwicklung befinden, werden im Faktorisieren viel besser sein als heutige Systeme. Doch die Geschichte der Kryptografie zeigt auch: Für jedes geknackte Verfahren hat sich stets ein besseres gefunden.

Absage:

Sie hörten
Kryptographie – Die Geschichte der Verschlüsselung
von Oliver Buschek
Es sprachen: Julia Fischer und Christian Schuler
Regie hatte: Rainer Schaller
Technik: Roland Böhm
Redaktion: Nicole Ruchlak
Das war eine weitere Episode unseres radioWissen-Podcast.

Bayern 2-Hörerservice
Bayerischer Rundfunk, 80300 München; Service-Nr.: 0800-5900222 (kostenfrei); Fax: 089/5900-46258
service@bayern2.de; www.bayern2.de