Forum für Informationssicherheit

Geschichte

Der Versuch einer zeitgeschichtlichen Einordnung

ca. 600 v. Chr	In Palästina werden Texte mit der ATBASH verschlüsselt.
ca. 500 v. Chr.	Die Griechen verschlüsseln Nachrichten mit Hilfe der SKYTALE
ca. 200 v. Chr.	Der Grieche Polybious beschreibt erstmals sein POLYBIOUS-System..
ca. 100 - 44 v. Chr.	Julius Caesar schrieb vertrauliche Botschaften in dem nach ihm benannten CAESAR-CODE.
ca. 500 - 1400 n. Chr.	in Europa beginnt die „Dunkle Zeit der Kryptographie“, d.h. sie wurde der schwarzen Magie zugeordnet, in dieser Zeit ging viel Wissen über die Kryptographie verloren, im Gegensatz dazu blühte die Kryptographie im persischen Raum auf
855 n. Chr	Im arabischen Raum erscheint das erste Buch über Kryptologie. Abu ‘Abd al-Raham al-Khahil ibn Ahmad ibn’Amr ibn Tammam al Farahidi al-Zadi al Yahamadi beschreibt stolz in seinem Buch unter anderem die geglückte Entschlüsselung eines für den byzantinischen Kaiser bestimmten griechischen Codes
1412	eine 14-bändige arabische Enzyklopädie beschreibt auch kryptographische Methoden, dabei wird neben der Substitution und der Transposition, erstmals die Methode der mehrmaligen Substitution an einem Klartextzeichen erwähnt
1397	Auf Wunsch Clemens des 7. erfindet Gabrieli di Lavinde die erste Nomenklatur (Nomenklatur-Code). Dieser Nomenklatur-Code wurde wegen seiner Einfachheit in den nächsten 450 Jahren vor allem in diplomatischen Kreisen verwendet.
1466	Leon Battista Alberti (1404 - 1472) , einer der führenden Kräfte der italienischen Renaissance, veröffentlicht sein Buch „Modus scribendi in ziferas“, indem erstmals die von ihm erfundenen Chiffrierscheiben erwähnt. Albertis zahlreiche kryptologischen Leistungen beruhen auf der Tatsache, das er Sekretär jener Behörde war, die sich an der römischen Kurie (päpstlicher Hof) mit Geheimschriften

	befasste. Er wird als „Vater der Kryptographie“ bezeichnet.
1518	Im deutschsprachigen Raum erscheint das erste gedruckte Buch über Kryptologie. Der Verfasser ist Johannes Trithemius. 1586 Das Buch „Tractié de Chiffre“ des französischen Diplomaten Blaise de Vigenère erscheint. Seine Verschlüsselungsmethode, die später nach ihm als Vigenère-Code benannt wurde, wird so der Öffentlichkeit zugänglich gemacht. Dieser Code ist der bekannteste unter allen polyalphabetischen Algorithmen.
1628	Antione Rissignol wird der erste vollzeitlich angestellte Kryptoanalytiker, nachdem seine Entschlüsselung einer feindlichen chiffrierten Botschaft die Belagerung Realmonts durch die Hugenotten beendete. Seitdem sind Kryptoanalytiker ein fester Bestandteil des militärischen Apparats.
1700	russischer Zar benutzte eine große Code-Tabelle von 2000-3000 Silben und Worten zur Chiffrierung seiner Botschaften
1795	Thomas Jefferson entwickelt den ersten Chiffrierzylinder namens „wheel cypher“. Er benutzte sie aber nie, so daß sie in Vergessenheit geriet bzw. nie der Öffentlichkeit zugänglich wurde. Somit wurde der Chiffrierzylinder parallel zu Jeffersons unbekannter Erfindung an unterschiedlichen Orten nochmals erfunden:
1854	der Engländer Charles Babbage erfindet einen Chiffrierzylinder, er war gleich der „wheel-cypher“
1854	Der englische Physiker Charles Wheatstone erfand einen Chiffre, der mit einer 5*5 Matrix arbeitet. Sein Freund Lord Lyon Playfair Baron von St. Anrews machte diesen Chiffre in den höheren militärischen und diplomatischen Kreisen des viktorianischen Englands bekannt, der Chiffre bekam so den Namen „PLAYFAIR“-Code.
1891	der französische Major Etienne Bazeries erfand einen Chiffrierzylinder, sein BAZERIES-Zylinder war der „wheel cypher“ im Prinzip ähnlich
1860	Friedrich Kasiski und William F. Friedmann entwickeln statistische Methoden zur Kryptoanalyse.
1863	Der preußische Offizier Friedrich Kasiski a.D. (1805-1881) veröffentlicht in Berlin sein kryptologisches Werk mit dem Titel „Die Geheimschriften und die Dechiffrierkunst“, in dem er als erster ein Verfahren zur Lösung von polyalphabetischen Chiffren vorschlug. Mit diesem Verfahren konnte auch der bis dahin unlösbare Vigenère-Code geknackt werden.

1883	„La Cryptographie militaire“ von Auguste Kerkhoff von Nieuwendhoff erscheint.Es gilt als Meilenstein in der Kryptographie der Telegraphenzeit. Beinhaltet die „Prinzipien von Kerkhoff“ für die strategische Kryptologie
1917	Der Amerikaner Gilbert S. Vernam entdeckt und entwickelt das „ONE-TIME-PAD“
1918 April 15 [4)]	Arthur Scherbius offered prototype ENIGMA machine to German Navy
1921	Der Kalifornier Edward Hebern baut die erste Chiffriermaschine nach dem ROTOR-Prinzip.
1922	wurde T.Jeffersons „wheel-cypher“ in den U.S.A. entdeckt, von der US-Marine weiterentwickelt und fand so bis in den 2.Weltkrieg Anwendung
1923	Vorstellung der vom dt. Ingenieur Arthur Scherbius entwickelten Rotormaschine „ENIGMA“ auf dem internationalen Postkongreß Gründung der „Chiffriermaschinen AG“, somit vermarktet A. Scherbius seine Enigma in alle Welt
1926	die deutsche Reichsmarine führt den Funkschlüssel C ein (Codierung der Nachrichten mit einer Enigma vom Typ C im Verlaufe der folgenden Jahre wurde eine ganze Reihe von Verschlüsselungsmodifikationen für Marine, Luftwaffe, Heer, Abwehr und andere Organisationen entwickelt.
1926 February 9 [4)]	German Navy introduced the ENIGMA machine as "Radio Key C" for communications security
1927 [4)]	Swedish businessman Boris Hagelin introduced A-22 machine
1928 July 15 [4)]	German Army introduced the ENIGMA machine for communications security
ca. 1930 [5)]	Verrat wesentlicher Tatsachen der "Enigna" durch einen deutschen Chiffriertechniker an den französischen Geheimdienst
ab 1933	in den folgenden Jahren wurden diverse Verschlüsselungs und Chiffriergeräte entwicklet und in die Praxis eingeführt: Schlüsselzusatzgerät SZ - 40/ SZ - 42- Hersteller ; Standard Electric Lorenz- (SZ Schlüsselzusatz) Geheimschreiber - T Typ- 52 Herstelller Fa. Siemens; von diesem Verschlüsselumgsgerät gab es mehrere Versionen A/B; C; CA,, D und E. Die Version A/B wurde durch Prof, Arne Beurling/ Schweden geknackt, Auch die folgenden Versionen C, CA und D wiesen noch kryptologische Schwachsteelen auf. Die Version E konnte zur damaligen Zeit nicht gelöst werden.

	Bericht der NSA auf schwedischem Quellenmaterial - T-43 mit absolut sicheren Schlüsselstreifen - Schlüsselgerät- 41 zu dieser Gruppe von Verschlüsselungsgeräten finden sie ausführliche Informationen bei Wikipedia (Kryptologie) -Geheimschreiber (Firma Siemens & Halske AG)Einsatz für die Auslandsverbindungen, wie Botschaften, sowie für militärischen Führungsstellen oder sogenannte "Führerbefehle" Umfassende Beschreibung
1934 [4)]	Entwicklung sowjetischer Verschlüsselungstechnik M - 100/Kristall und M 101 Smaragd für militärische Einsätze kryptologisch im 2. Weltkrig nicht gelöst
1937 February [4)]	U.S. Army SIS produced first translation of Japanese diplomatic "RED" machine
1937 February [4)]	Great Britain: Air Ministry adopted TYPEX MK 1 cipher machine
1938 June [4)]	Japanese Ministry of Foreign Affairs introduced "PURPLE" cipher machine
1939 June [4)]	Japanese Navy introduced code system known to the U.S. as JN-25
1939 September [4)]	U.S. Army SIS produced first translation of Japanese "PURPLE" machine
1940 September 11 [4)]	U.S. Army and Navy sign agreement on joint exploitation of Japanese "PURPLE" machine
1941	Decodierung der japanischen Angriffsmeldung für den 2. Weltkrieg (viele Historiker meinen, daß die Kryptologie im 2. Weltkrieg ein Jahr Krieg erspart hat). Diese Decodierung lieferte jedoch nicht das Angriffsziel des japanischen Angriffs. Diese Ziele konnten aus den "prosaischen Textteilen" nicht ermittelt werden, obwohl sie decodiert wurden.
1942	Einsatz des "Navajo Code" durch die amerikanischen Streitkräfte im 2. Weltkrieg (ausführliche Information)
1942 February 1 [4)]	German Navy introduced 4-rotor ENIGMA machine for U-boats
1942 March 15 [4)]	U.S. Navy began reading Japanese system JN-25
1943 March [4)]	German Navy adopted 4-rotor ENIGMA machine
1943 May [4)]	GC&CS activated HEATH ROBINSON machine for cryptanalysis of German TUNNY machine (Lorenz SZ 40/42)
1943 Dezember [6)]	Deutsche Funküberwachung gelingt der Einbruch in den Küstennachrichtencode der US - Navy. Dadurch bekommt Deutschland Einblickin die küstennahe Seekriegsführung der USA im ostasiatischen Raum.

1943/1944 [1)]	Enigma - Weiterentwicklung mit höherer kryptologischer Festigkeit Einführung Ende 1944/ Anfang 1945 in den Einsatz eingeführt; dieses System soll nicht entschüsselbar gewessen sein (bezogen auf die damalige Zeit)
1944 February [4)]	GC&CS activated COLOSSUS MK I for cryptanalysis of TUNNY; may be first computer
1945 May [4)]	Military intelligence teams find Soviet codebooks in Saxony and Schleswig, Germany.
1940 - 1980	**Operation Venona** die doppelte Verwendung sowjetischer Einmalschlüssel gelang der NSA die Entschlüsselung von ca. 2.900 Telegrammen Ausführliche Informationen der NSA
1939 - -1945	Lösung einer ganzen Reihe von Codierverfahren und Verschlüsselungsverfahren sowie Methoden zur gespreizten Übermittlung von Informationen sowie anderer Mittel und Methoden zum Schutz der Informationen vor Offenbarung. Es wurden dabei eine ganze Reihe von Informationen gewonnen. Die Erfolge wurden erzielt durch einen wissenschaftlichen Einbruch (Decodierung oder Dechiffrierung) sowie durch Verrat sowie auch sogenannter "organisatorischer Schwächen" bei Betrieb deratiger Systeme. Ergänzung 1 Geheimschreiber und "Fisch" F 52 z (Deutschland)2 Chiffriermaschinen
1945 **Neu News**	Die Operation "TICOM" zur Lösung aller Geheimnisse auf dem Gebiet der Kryptologie Deutschlands in den Jahren von 1933 - 1945
1950	Weltweit erfindet jedes größere Land eigene Chiffriermaschinen:England: TYPEXJapan: PURPLEU.S.A.: SIGABA (M-134-C;ECM Mark 2) T - 301, T - 304, T - 310, T - 312 sowie T - 314 sowie weitere diverse Verfahren (ex. DDR)[1]
1950	Schlüsseltabelle oder Wurmtabelle in Fünfer-Gruppen mit Seriennummer/Heftnummer und Tabellennummer zur Erzeugung des Geheimtextes. (Beispiel Originaltabelle) aus dem Jahre 1960
1960	Substutionstabelle "Tapir" zur Umwandlung von Klartext in Zwischentext zur Verknüpfung mit dem Schlüsseltext zur Erzeugung des Geheimtextes. (Beispiel Originaltabelle)) aus dem Jahre 1960
Oktober 1960	Der "heiße Draht" zwischen Washington und Moskau und die Lösung der kryptologischen Verbindungen zwischen den beiden Staaten während des kalten Krieges.
ab 1966	**Operation Venona** II; Echtzeiteinbruch in Funknetz der BRD (BND u.a.); verursacht durch fehlerhafte Anwendung von kryptologischen Mitteln; durch das

	ZCO der ex. DDR. (Information)
ab 1960	Beginn der Entwicklung von Verfahren der Computerchiffrierung. Nutzung der kybernetischen Möglichkeiten für die Zwecke der Chiffrierung /quasi absolut sichere Verfahren)
1970 [3)]	Verluste an Chiffriertechnik bei militärischen Auseinandersetzungen sowie Verrat von Schlüsselunterlagen KG - 14, KL - 47; KW-7; KW-37; KW-14; KY - 8, KY - 28, KY - 38, . Adonis, Nestor (Sprachverschlüsselungsmaschine)
1973 **Neu News**	Die Geschichte der Informationssicherheit veröffentlicht durch die NSA 1973
1975	Diffie und Hellmann zeigen, daß PUBLIC-KEY-Verfahren theoretisch möglich sind, obwohl sie das Gegenteil beweisen wollten
1977	Das ab 1975 von IBM entwickelte DES (Data Encryption Standard) wird zum Standardverfahren auserkoren. nicht für klassifizierte Informationen zugelassen
1980	"Aus Dokumenten der Stasi-Unterlagen-Behörde geht hervor, das die Kryptologen u.a. die bis in die achtziger Jahre gebräuchlichen Vericrypt- und Cryptophon-Standards gebrochen hatten - und damit verschlüsselte Funksprüche von Verfassungsschutz, BND und Bundesgrenzschutz dechiffrieren konnten. Sogar BND - Befehle an die Untergrundtruppe "Gladio" die im Ernstfall unter feindlichen Besetzung operieren sollte, kamen in Ost - Berlin im Klartext an." Auszug aus "Der Spiegel"Nr. 39/27.9.10
1978	Das nach seinen Entwicklern Ronald Rivest, Adi Shamir und Leonard Adleman benannte RSA-Verfahren wird veröffentlicht. Es ist das erste praktisch einsetzbare Public-Key-Verfahren und es gilt als innovativster Beitrag der kryptologischen Forschung unseres Jahrhunderts
1980	Beendigung des Programmes Venona mit der erfolgreichen Dechiffrierung von russichen tausenden Chiffretelegrammen aus der Zeit des 2.Weltkrieges. Dechiffrierung von russischen Einmal - Schlüssel. Diese Dechiffrierung gelang deshalb, weil auf russicher Seite gegen die Grundsätze der Chiffrierung (siehe Todsünden der Kryptologie) grob verstossen wurde.Dieses Ereignis offenbart die Bedeutung der Organisation von kryptologischen Systemen. Diese Erkenntnis sind auch heute noch genauso aktuell.Die Lehren aus Venona 1985 Goldwasser, Micali und Racoff stellen sog. ZERO-KNOWLEDGE-Verfahren vor

1980	Bei der Entwicklung von programmgesteuerten Chiffrierverfahren für die Übertragung "klassifizierter Informationen" ergaben sich eine Reihe von "sicherheitsmäßigen Schwachstellen" die eine grundsätzliche neue Betrachtung des Problems erforderten. Im Ergebnis entstand die Lösung auf der Grundlage einesr Hard- und Software. Eines der interessanten Prüpdukte ist die "gehärtete Software" eine Lösung aus einer Hard- und Software-Einheit auf der Grundlage eines kryptologischen System zum Schutz einer ganzen Reihe von Gefährdungen oder Schwachstellen moderner kybernetischer Einheiten.offenbart die Bedeutung der Organisation von kryptologischen Systemen.
1990	Xueija Lai und James Massey entwickeln das IDEA-Verfahren, das z.B. in der Kryptologiesoftware PGP (Pretty Good Privacy)2840 von Phillip Zimmermann eingesetzt wird.
2006 **Neu News**	Die Entschlüsselung der Enigma mit neuesten Erkenntnissen aus der Welt der Nachrichtendienste Geschrieben von einem Historiker der NSA im Jahre 2006 Neuigkeiten zur Geschichte, wie sie bisher noch nicht veröffentlicht wurden."Solving the Enigma: History of the Cryptanalytic Bombe" von Jennifer Wilcox; Center for Cryptologic History;National Security Agency Revised 2006.
2010	TDEA oder TDES nicht für klassifizierte Informationen zugelassen Advavced Encrytion Standard 256 (AES 256) nicht für klassifizierte Informationen zugelassen siehe hierzu die entsprechenden Informationen in den Fachberichten Bemerkungen und Empfehlungen der NIST / USA zu diversen Verschlüsselungs oder Signaturverfahren. (ab 2010 nur ausreichende kryptologische Festigkeit innerhalb der nichtklassifizierten Systeme)
2010	Beginn des modernen kybernetischen Krieges (Cyberwar) Beginn des Einsatzes moderner Mittel und Methoden des kybernetischen Raumes auf der Grundlage neuer Erkenntnisse der Informatik und der Möglichkeiten "militärischer Szenarien" als Grundlage des kybernetischen Krieges.

Dieses Material wurde erarbeitet von einer Gruppe von Autoren, Aufstellung der Namen sowie Rechte und Quellenangaben finden Sie unter diesem Link
Das Ursprungsmaterial wurde fortlaufend durch neuere Informationen ergänzt
1) externe Informationen Ergänzungen zu der Aufstellung der Autoren
2) aus verschiedenen Veröffentlichungen zur Geschichte der Kryptologie

3) Veröffentlichungen aus "NSA" Bramford (Analyse durch Autor des Artikels)
4) Zeittafel der NSA / USA Diese Zeittafel enthält nur Angaben bis zum Jahre 1952
5) Veröffentlichung "Solving the Enigma : History of the Cryptoanalytic Bome" Wilcox, NSA 2006
6) Veröffentlichung aus den sechziger Jahren

Aufstellungen zu dieser Spezifik leiden verständlicherweise Weise an einem Mangel an Publizität. Da man aus verständlichen Gründen Erfolge wie auch Mißerfolge nicht der Allgemeinheit mitteilen möchte.