Forum for information security

History

The attempt of a contemporary historical classification

c. 600 BC	Palestine encrypts text with the ATBASH.
c. 500 BC	The Greeks encrypt messages with the help of the SKYTALE
c. 200 BC	The Greek of Polybious for the first time describes its POLYBIOUS system...
c. 100 - 44 BC	Julius Caesar wrote confidential messages in the CAESAR CODE named after him.
c. 500 - 1400 ad	in Europe, the "dark time of Cryptography", begins i.e. it was associated with black magic, much knowledge about the Cryptography was lost during this time, on the other hand flourished the cryptography in the Persian room
855 ad	The first book on cryptology appears in the Arab region. Abu ' Abd al-Raham al-Khahil ibn Ahmad ibn'AMR ibn Tammam al Farahidi al-Zadi al Yahamadi proudly in his book describes among other things the successful deciphering a Greek code specific for the Byzantine Emperor
1412	a 14-volume Arabic encyclopedia also describes cryptographic methods, this is in addition to the substitution and the Transposition, for the first time the method of multiple substitution a plain-text characters mentioned
1397	Gabrieli di Lavinde invents the first desired Clemens of 7. Nomenclature (nomenclature code). This nomenclature code was due to its simplicity in the next 450 years, especially in diplomatic circles used.
1466	Leon Battista Alberti (1404-1472), one of the leading forces of the Italian Renaissance, published his book "Mode in ziferas" scribendi, by first mentioned the encryption plates invented by him. Albertis numerous CryptoLogic services are based on the fact that he was Secretary of authority, who studied with cryptology on the Roman Curia (papal court). He is known as the "Father of Cryptography".
1518	The first printed book on cryptology appears in German-speaking countries. The author is Johannes

	Trithemius. 1586 The book "Tractié de code" of French diplomat Blaise de Vigenère appears. His encryption method which was later named after him as Vigenere code is made available to the public. This code is the most famous among all poly alphabetischen algorithms.
1628	Antione Rissignol is the first full time employed Codebreaker after his deciphering of a hostile ciphered message ended the siege of Realmonts by the Huguenots. Since then, Cryptanalyst are an integral part of the military apparatus.
1700	Russian Tsar used a large code table of 2000-3000 syllables and words to his messages encryption
1795	Thomas Jefferson designed the first encryption cylinders called "wheel cypher". He never used it so that it was forgotten or never was open to the public. Thus the encryption engine was invented in parallel again to Jefferson's unknown invention in different places:
1854	the Englishman Charles Babbage invented a cipher cylinder, he was equal to the "wheel cypher"
1854	The English physicist Charles Wheatstone invented a cipher which matrix works with a 5 * 5. His friend Lord Lyon Playfair made Baron of St. Anrews this code in the higher military and diplomatic circles of Victorian England known, the code was so named "PLAYFAIR"-code.
1891	the French major Etienne Bazeries invented a cipher cylinder, his BAZERIES cylinder was similar to the "wheel cypher" in principle
1860	Friedrich Kasiski, and William F. Friedman develop statistical methods of cryptanalysis.
1863	The Prussian officer Friedrich Kasiski on the (1805-1881) published his kryptologisches work in Berlin with the title "The cryptology and the art of decoding", in which he proposed a method for the solution of poly alphabetischen ciphers first. Use this procedure, and the hitherto unsolvable Vigenere code could be cracked.
1883	"La Cryptographie militaire" by Auguste Kerkhoff of Nieuwendhoff appears.It is a milestone in the Telegraph time Cryptography. Includes the "principles of Kerkhoff" for the strategic Cryptology
1917	American Gilbert S. Vernam discovered and developed "ONE TIME PAD"
1918 April 15 [4)]	Arthur Scherbius offered prototype ENIGMA machine to German Navy
1921	The Californian Edward Hebern built the first machine

	on the ROTOR principle.
1922	T.Jeffersons was "wheel cypher" discovered in the U.S.A., developed by the U.S. Navy and was used until in the World War II
1923	Idea developed rotor machine "ENIGMA" on the International Postal Congress of the German engineer of Arthur Scherbius Foundation of the "cipher AG", thus A. Scherbius marketed his Enigma throughout the world
1926	the German Reichsmarine introduces the radio key C (encoding of messages with a Enigma type C in the following years, a number of encryption modifications designed for Navy, air force, army, defense and other organizations.)
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
circa 1930 [5]	Betrayal material facts of the "Enigna" by the German encryption technician on the French secret service
from 1933	in the following years various encryption and encryption devices developed and introduced into practice: Key accessories SZ - 40 / SZ - 42-manufacturer; Standard electric Lorenz-(SZ key additional) Secret writer -T type 52 brand. Siemens; from this Verschlüsselumgsgerät there were multiple versions of A/B; C, CA, D and E. The version of A/B has been cracked by Prof, Arne Beurling / Sweden, also the following versions of C, CA and D had still cryptographic Schwachsteelen. The version of E could not be solved at that time. Report of the NSA on Swedish source material T-43 with absolutely secure key Strip -Key device 41 This group of encryption devices, they find detailed information on Wikipedia (cryptology) Secret writer (Siemens & Halske AG) use for the outbound links, such as embassies, as well as military institutions or so-called "leader commands" Full description
1934 [4]	Development of Soviet encryption technology M - 100/Crystal and M 101 Emerald not solved for military operations CryptoLogic in the 2. Weltkrig
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	Decoding of the Japanese attack message for the 2nd World War (many historians believe that world war one year has saved the Cryptology in the 2nd war). This decoding provided but not the target of the attack. These objectives could not be retrieved from the "prosaic text", although they have been decoded.
1942	Use the "Navajo code" by the American forces in World War II (detailed 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 December [6]	German radio monitoring manages the downturn in the US - Navy coastal message code. As a result, the coastal naval warfare of the United States in the far East gets Insightinto Germany.
1943/1944 [1]	Enigma - development with higher cryptographic strength introduced in late 1944 / early 1945 in use; This system is to be not unloading Bowl bar (by that time) gewessen
1944 February [4]	GC & CS activated COLOSSUS MK I for cryptanalysis of TUNNY; may be first computer
1945 May [4]	Intelligence teams find military Soviet codebooks in Saxony and Schleswig, Germany.
1940 - 1980	**Operation Venona** the double use of Soviet a one-time key managed the NSA the decryption of approximately 2,900 telegrams For details of the NSA
1939 - -1945	Solution a number of encoding method and encryption procedures and methods to spread transmission of information as well as other means and methods to protect of information from disclosure. There were won a whole range of information here. The successes have been achieved by a scientific burglary (decoding

	or decryption) as well as betrayal and also so-called "organisational weaknesses" in operation of board-systems. Supplement 1 Secret writer and "Fish" F 52 z (Germany) 2 cipher
1945 **New news**	The operation "TICOM" to solve all secrets in the field of cryptography of Germany in the years from 1933-1945
1950	Worldwide, every major country invents their own cipher: England: TYPEXJapan: PURPLEU.S.A.: SIGABA (M-134-C;)(ECM mark 2) T - 301, T - 304, T - 310, T - 312, as well as T - 314, as well as other various procedures (ex.) (DDR) [1]
1950	Key table or worm table into five groups with serial number/issue number and table number for the production of Geheimtextes. (Example source table) from the year 1960
1960	Substutionstabelle "Tapir" for the conversion of plain text in Zwischentext to link to the key text for the production of Geheimtextes. (Example source table)) from the year 1960
October 17, 1960	The "hot wire" between Washington and Moscow, and the solution of CryptoLogic connections between the two States during the cold war.
in 1966	**Operation Venona** II; real time intrusion in radio network of the Federal Republic of Germany (BND and others); caused by misapplication of CryptoLogic means, by the ZCO of ex. DDR. (Information)
in 1960	Start of the development of techniques of computer encryption. (Use of the cybernetic possibilities for the purposes of enciphering / quasi absolutely safe procedure)
1970 [3)]	Loss of encryption technology in military conflicts, as well as betrayal of key documents KG - 14 , KL - 47 ; KW-7 ; KW-37 ; KW-14; KY - 8, KY - 28 KY - 38,. Adonis , Nestor (Voice encryption machine)
1973 **New news**	The History of information security published by the NSA 1973
1975	Diffie and Hellmann show that PUBLIC-KEY method are theoretically possible, although they wanted to prove the opposite
1977	The 1975 IBM developed DES (data encryption standard) is chosen to standard procedure. approved for classified information
1980	"Documents of the Stasi documents authority shows that could decrypt the cryptologists and others - had broken down in the 1980s commonly used Vericrypt- and Cryptophon standards and conversations so that

	encrypted protection of the Constitution, BND, and federal border police." "Even the BND - commands at the"Gladio"that should operate in an emergency under enemy occupation, underground force arrived in OST - Berlin in plain language." Excerpt from "Der Spiegel" No. 39 / 27.9.10
1978	The RSA procedure, named after its developers Ronald Rivest, Adi Shamir and Len Adleman is published. It is the first practically usable public key method and it is considered world's most innovative contribution of CryptoLogic research of our century
1980	Termination of the program of Venona, with the successful deciphering of Russian thousands Chiffretelegrammen from the time of war. Decryption of Russian one-time - key. This decryption managed so, because on russicher side against the principles of enciphering (see deadly sins of in Cryptology) has been grossly violated.This event reveals the importance of the Organization of CryptoLogic systems. This finding is also today still as up to date.The lessons of Venona 1985 Goldwasser, Micali and Racoff present so-called ZERO-KNOWLEDGE process
1980	There were a number of "non-industrial and security vulnerabilities" that required a fundamental new consideration of the problem in the development of programmatic encryption methods for the transfer of "classified information". The solution on the basis of einesr hardware and software was created as a result. One of the interesting Prüpdukte is the "hardened software" a solution from a hardware and software unit on the basis of a CryptoLogic system to protect of a number of threats or vulnerabilities of modern cybernetic Einheiten.offenbart the importance of the Organization of CryptoLogic systems.
1990	Xuejia develop the IDEA process 2840 used e.g. in the Kryptologiesoftware PGP (pretty good privacy) by Phillip Zimmermann Lai and James Massey.
2006 **New news**	The decryption of Enigma with latest findings from the world of intelligence services Written by a historian of the national security agency in the year 2006 "News about the story of how they have still not published."Solving the Enigma: "History of the Cryptanalytic bomb" by Jennifer Wilcox; Center for Cryptologic History;National security agency revised 2006.
2010	TDEA or TDES for classified information admitted Advavced encrytion standard 256 (AES 256) not for classified information admitted to see the appropriate information in the special reports, comments and

	recommendations of the NIST / United States to various encryption or signature process. (from 2010 only adequate cryptographic strength within the non-classified systems)
2010	At the beginning of modern cybernetic war (cyberwar) begins the use of modern means and methods of the cybernetic space based on new knowledge of computer science and of the ways "military scenarios" as the basis of cybernetic war.

This material has been prepared by a group of authors, list the name as well as rights and bibliographical references, see this link
The original material was continuously supplemented by more recent information
1) external information additions to the list of authors
(2) from various publications on the history of cryptography
(3) Publications from "NSA" Bramford (analysis by author of article)
(4) History of the NSA / United States this timeline contains only information up to the year 1952
(5) Publication "solving the Enigma: history of the Cryptoanalytic Bome" Wilcox, NSA 2006
(6) The publication of the sixties

Understandably, lineups to this specific nature suffer a lack of publicity way. Since you successes such as also failures not the general public would like to tell for understandable reasons.