GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

History of Encryption:
Version 2.

Introduction:

Encryption, process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The root of the word encryption—*crypt*—comes from the Greek word *kryptos*, meaning hidden or secret. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures, this paper highlights in chronology the history of Cryptography throughout centuries. For different reason humans have been interested in protecting their messages. The Assyrians were interested in protecting their trade secret of manufacturing of the pottery. The Chinese were interested in protecting their trade secret of manufacturing silk. The Germans were interested in protecting their military secrets by using their famous Enigma machine. With the advancement of computers and interconnectivity, the United States governmental institutions and industries are subject to cyber attacks, intrusion and industrial espionage. The following are chronological history of cryptography:

About 1900 BC An Egyptian scribe used non-standard hieroglyphs in an inscription. Kahn lists this as the first documented example of written cryptography.

1500 BC ancient Assyrian merchants used intaglio, a piece of flat stone carved into a collage of images and some writing to identify themselves in trading transactions. Using this mechanism, they are producing what today we know as 'digital signature.' The public knew that a particular 'signature' belonged to this trader, but only he had the intaglio to produce that signature. Using this mechanism, they are producing what today we know as 'digital signature.' The public knew that a particular 'signature' belonged to this trader, but only he had the intaglio to

© SANS Institute 2000 - 2005 Author retains full rights.

produce that signature.

500-600 BC Hebrew scribes writing down the book of Jeremiah used a reversed-alphabet simple substitution cipher known as ATBASH. (Jeremiah started dictating to Baruch in 605 BC but the chapters containing these bits of cipher are attributed to a source labeled ``C'' (believed not to be Baruch) which could be an editor writing after the Babylonian exile in 587 BC, someone contemporaneous with Baruch or even Jeremiah himself.) ATBASH was one of a few Hebrew ciphers of the time.

487 BC The Greeks used a device called the ``skytale'' -- a staff around which a long, thin strip of leather was wrapped and written on. The leather was taken off and worn as a belt. Presumably, the recipient would have a matching staff and the encrypting staff would be left home.

Julius Caesar (100-44 BC) used a simple substitution with the normal alphabet (just shifting the letters a fixed amount) in government communications. This cipher was less strong than ATBASH, by a small amount, but in a day when few people read in the first place, it was good enough. He also used transliteration of Latin into Greek letters and a number of other simple ciphers. When Julius Caesar sent messages to his trusted acquaintances, he didn't trust the messengers. So he replaced every A by a D, every B by an E, and so on through the alphabet. Only someone who knew the ``shift by 3'' rule could decipher his messages

725-790 A.D Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn `Amr ibn Tammam al Farahidi al-Zadi al Yahmadi wrote a (now lost) book on cryptography, inspired by his solution of a cryptogram in Greek for the Byzantine emperor. His solution was based on known (correctly guessed) plaintext at the message start -- a standard cryptanalytic method, used even in WW-II against Enigma messages.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1379 Gabrieli di Lavinde at the request of Clement VII, compiled a combination substitution alphabet and small code -- the first example of the *nomenclator* Kahn has found. This class of code/cipher was to remain in general use among diplomats and some civilians for the next 450 years, in spite of the fact that there were stronger ciphers being invented in the meantime, possibly because of its relative convenience.

1466 Leon Battista Alberti (a friend of Leonardo Dato, a potifical secretary who might have instructed Alberti in the state of the art in cryptology) invented and published the first polyalphabetic cipher, designing a cipher disk (known to us as the Captain Midnight Decoder Badge) to simplify the process. This class of cipher was apparently not broken until the 1800's. Alberti also wrote extensively on the state of the art in ciphers, besides his own invention. Alberti also used his disk for enciphered code. These systems were much stronger than the nomenclature in use by the diplomats of the day and for centuries to come.

1518 Johannes Trithemius wrote the first printed book on cryptology. He invented a steganographic cipher in which each letter was represented as a word taken from a succession of columns. The resulting series of words would be a legitimate prayer. He also described polyalphabetic ciphers in the now-standard form of rectangular substitution tables. He introduced the notion of changing alphabets with each letter.

1553 Giovan Batista Belaso introduced the notion of using a passphrase as the key for a repeated polyalphabetic cipher. (This is the standard polyalphabetic cipher operation miss-named ``Vigenère'' by most writers to this day.)

1563 Giovanni Battista Porta wrote a text on ciphers, introducing the digraphic cipher. He classified ciphers as transposition, substitution and symbol substitution (use of a strange alphabet). He suggested use of synonyms and misspellings to confuse the cryptanalyst. He apparently introduced the notion of a mixed alphabet in a polyalphabetic tableau.

© SANS Institute 2000 - 2005 Author retains full rights.

1585 Blaise de Vigenère wrote a book on ciphers, including the first authentic plaintext and ciphertext autokey systems (in which previous plaintext or ciphertext letters are used for the current letter's key).

1623 Sir Francis Bacon described a cipher which now bears his name -- a biliteral cipher, known today as a 5-bit binary encoding. He advanced it as a steganographic device -- by using variation in type face to carry each bit of the encoding.

1790 Thomas Jefferson, possibly aided by Dr. Robert Patterson (a mathematician at U. Penn.), invented his wheel cipher. This was re-invented in several forms later and used in WW-II by the US Navy as the Strip Cipher, M-138-A.

1917 William Frederick Friedman, later to be honored as the father of US cryptanalysis (and the man who coined that term), was employed as a civilian cryptanalyst (along with his wife Elizebeth) at Riverbank Laboratories and performed cryptanalysis for the US Government, which had no cryptanalytic expertise of its own. WFF went on to start a school for military cryptanalysts at Riverbank -- later taking that work to Washington and leaving Riverbank

1933-1945 The Enigma machine was not a commercial success but it was taken over and improved upon to become the cryptographic workhorse of Nazi Germany. [It was broken by the Polish mathematician, Marian Rejewski, based only on captured ciphertext and one list of three months worth of daily keys obtained through a spy. Continued breaks were based on developments during the war by Alan Turing, Gordon Welchman and others at Bletchley Park in England.]

1976 A design by IBM based on the Lucifer cipher and with changes (including both S-box improvements and reduction of key size) by the US NSA, was chosen to be the U.S. Data Encryption Standard. It has since found worldwide acceptance, largely because it has shown itself strong against 20 years of attacks. Even some who believe it is past its useful life use it as a component -- e.g., of 3-key triple-DES.

© SANS Institute 2000 - 2005 Author retains full rights.

1976 Whitfield Diffie and Martin Hellman published ``New Directions in Cryptography'', introducing the idea of public key cryptography. They also put forth the idea of authentication by powers of a one way function, now used in the S/Key challenge/response utility. They closed their paper with an observation for which this timeline web page gives detailed evidence: ``Skill in production cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from amateurs."

1977 Inspired by the Diffie-Hellman paper and acting as complete novices in cryptography, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman had been discussing how to make a practical public key system. One night in April, Ron Rivest was laid up with a massive headache and the RSA algorithm came to him. He wrote it up for Shamir and Adleman and sent it to them the next morning. It was a practical public-key cipher for both confidentiality and digital signatures, based on the difficulty of factoring large numbers. They submitted this to Martin Gardner on April 4 for publication in Scientific American. It appeared in the September, 1977 issue. The Scientific American article included an offer to send the full technical report to anyone submitting a self-addressed, stamped envelope. There were thousands of such requests, from all over the world.

1990 Xuejia Lai and James Massey in Switzerland published ``A Proposal for a New Block Encryption Standard'', a proposed International Data Encryption Algorithm (IDEA) -- to replace DES. IDEA uses a 128-bit key and employs operations which are convenient for general purpose computers, therefore making software implementations more efficient.

1991 Phil Zimmermann released his first version of PGP (Pretty Good Privacy) in response to the threat by the FBI to demand access to the cleartext of the communications of citizens. PGP offered high security to the general citizen and as such could have been seen as a competitor to commercial products like Mailsafe from RSADSI. However, PGP is especially notable because it was released as freeware and has become a worldwide standard as a result while its competitors of the time remain effectively

© SANS Institute 2000 - 2005 Author retains full rights.

unknown.

1994 Professor Ron Rivest, author of the earlier RC2 and RC4 algorithms included in RSADSI's BSAFE cryptographic library, published a proposed algorithm, RC5, on the Internet. This algorithm uses data-dependent rotation as its non-linear operation and is parameterized so that the user can vary the block size, number of rounds and key length. It is still too new to have been analyzed enough to enable one to know what parameters to use for a desired strength -- although an analysis by RSA Labs, reported at CRYPTO'95, suggests that w=32, r=12 gives strength superior to DES. It should be remembered, however, that this is just a first analysis.

© SANS Institute 2000 - 2005, Author retains full rights.

Summary:

Cryptanalysis is the art of breaking cryptosystems---seeing through the disguise even when you're not supposed to be able to. Cryptology is the study of both cryptography and cryptanalysis. Today's cryptosystems are divided into two categories: ***symmetric*** and ***asymmetric***. Symmetric crypto systems use the same key (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it and all of today's algorithms fit within those two categories. Asymmetric cryptosystems are also called *public key* cryptosystems. We have shown that the field of Cryptography has evolved tremendously since the Assyrian and Egyptian time, and as the technology progresses and computers become faster and advanced, it will be easier to cultivate the power of distributed processing and break the different encryption algorithms such DES or triple DES, thus Cryptology is an evolving field.

© SANS Institute 2000 - 2005 Author retains full rights.

References:

The British Museum

Bacon: Sir Francis Bacon, ``De Augmentis Scientarum'', Book 6, Chapter i. [as quoted in C. Stopes, ``Bacon-Shakspere Question'', 1889]

Deavours: Cipher A. Deavours and Louis Kruh, ``Machine Cryptography and Modern
Cryptanalysis'', Artech House, 1985.

Diffie: Whitfield Diffie and Martin Hellman, ``New Directions in Cryptography'', IEEE Transactions on Information Theory, Nov 1976.

Garfinkel: Simson Garfinkel, ``PGP: Pretty Good Privacy'', O'Reilly & Associates, Inc., 1995.

Kahn: David Kahn, ``The Codebreakers'', Macmillan, 1967.
Price: Derek J. Price, ``The Equatorie of the Planetis'', edited from Peterhouse MS 75.I, Cambridge University Press, 1955.

Rivest: Ronald L. Rivest, ``The RC5 Encryption Algorithm'', document made available by FTP and World Wide Web, 1994.

ROT13: Steve Bellovin and Marcus Ranum, individual personal communications, July 1995.

RSA: Rivest, Shamir and Adleman, ``A method for obtaining digital signatures and public key cryptosystems'', Communications of the ACM, Feb. 1978, pp. 120-126.

Shamir: Adi Shamir, ``Myths and Realities'', invited talk at CRYPTO '95, Santa Barbara, CA; August 1995.

http://all.net/books/ip/Chap2-1.html
http://www.wakecomp.com/josh/history.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.cybercrimes.net/Cryptography/Articles/Hebert.html
http://www.massconfusion.com/crypto/Lecture/intro2.shtml
http://www.massconfusion.com/crypto/Lecture/intro3.shtml
http://home.us.net/~encore/Enigma/text.html
http://bucket.ualr.edu/~spirit/crypto/what.html

© SANS Institute 2000 - 2005, Author retains full rights.