Interested in learning more about security?

SANS Institute InfoSec Reading Room

One Fish, Two Fish, Red Fish, Blowfish A History of Cryptography and it's Application in Soci

Benign to the ordinary end user, crypto sciences are used in almost every electronic device to ordinary computer based software on the home personal computer. From PGP and SSL used in email and web browser packages to Elliptic Curve crypto used in the Palm pilots of tomorrow, the art of hiding messages in unreadable form has undoubtedly weaved its way into every technical facet of society. What will the future bring? Undoubtedly even longer key lengths and even more complex mathematical formulas used in symmetric algor...

One Fish, Twofish, Red Fish, Blowfish
A History of Cryptography and it's Application in Society

Joseph Kasten – 7/27/01 GSEC v1.2e

In the Beginning

On the sixth day, God created living creatures of every kind; and on the seventh day he rested [1]. Arguably millions of years later, approximately 2000 BC, cryptography was created; though not directly by God, but by ancient Egyptians writing hyroclifics on the walls of kings tombs. As times progressed, new applications were found and the art of enciphering messages evolved. From Greeks to Spartans to Julius Caesar employing character substitution, cryptography has continued to develop from an art of hiding messages in a secret language to the level of mathematical complexity it is today.

The Immaculate Conception

Some call James Lovell, a British immigrant to the colonies "the father of American cryptography," and yet others say it was Thomas Jefferson. Regardless, Lovell's contributions to deciphering British encryption led to the American victory of the Revolutionary war and paved the way for a new science in the New World. Lovell was subsequently followed in achievement by Jefferson, who created the "wheel cipher" in 1795; and Colonel Decius Wadsworth, who created a rotating disk cipher machine in 1817. By 1948, strong mathematical algorithms were being applied to the encoding of messages [4]. This year was recognized as a milestone due to the release of "A Communications Theory of Secrecy Systems" by Shannon, here the concept of unicity distance was introduced. Latter to be referred to as the Shannon Theories, "The unicity distance is a number that indicates the quantity of ciphertext required in order to uniquely determine the plaintext of a message." The computational analysis of unicity distance is $H(K)/(|M|-H(M))$ where $H(K)$ is the information content of the key, $H(M)$ is the information content per symbol of the message, and $|M|$ is the information content per symbol of the message assuming that all symbols are equally likely [5]. Although further mathematical analysis is beyond the scope of this paper, this demonstrates the beginning efforts to employ mathematical techniques to create ciphertext. It was 27 years later in 1975, that Whitfield Diffie and Martin Hellman developed a new key encryption with the help of a Berkley student named Ralph Merkle. Merkle saw the need to create a means in which the recipient of an encrypted set of key pairs could use that key pair with confidence even if the transmission of key pairs was intercepted. The problem existed that whomever intercepted the encrypted set would be able to decipher the encryption using the same amount of work as the intended recipient. When the recipient and the original sender of the key pairs decided on a particular key, the interceptor would also know the key. Merkles solution was to encrypt the sets of key pairs that were sent to the intended recipient individually. This differed from previous methods, which encrypted all keys sets with one encryption method. The benefit of this new method is that once the intended recipient chooses one particular key set and deciphers it, he can let the original sender know which key sets to use without the secret key being known to whomever

intercepted the individually encrypted key pairs. Now according to probability theory, if someone were to intercept this information they would have to decrypt half of the encrypted key pairs individually before discovering the one that was chosen by the sender and recipient. The table below is an illustration taken from "Pioneering Public Key: Public Exchange of Secret Keys" that describes this process where Alice is the sender and Bob is the recipient.

Alice Makes and Keeps			Alice Sends to Bob
Pair Number	Plaintext of Secret Key / Serial Number (reproduced from Figure 9-1)	1,000,000 Different Secret Keys—One for Each Pair Number	Encrypted Text of Secret Key/Serial Number
1	aiet187f45 / # *1,287,341*	1	Ciphertext 1
2	9dsyh3701 / # *77,183,902*	2	Ciphertext 2
3	1yt8a42x35 / # ***500,121***	3	Ciphertext 3
. . .	. . .	. . .	. . .
900,000	43879d323 / # *10,100,001*	900,000	Ciphertext 900,000
. . .	. . .	. . .	. . .
1,000,000	25s42fds70 / # *95,428,385*	1,000,000	Ciphertext 1,000,000

Figure taken from "Pioneering Public Key: Public Exchange of Secret Keys"

In the example above, the sender Alice transmits 1,000,000 key pairs, this leaves approximately 500,000 for whoever intercepts the message to decipher. Now in the ever changing world of the information age, hardware and software is being developed that can cipher these faster and faster; hence the need for complex mathematical equations to encrypt the keys. Diffe-Hellman maintains Merkles original mindset of one way functioning and used modular arithmetic to encrypt keys but used a public means of transmitting them [6]. This DH method of encrypting information using a shared secret key came to be known as a symmetric cipher. A year later Diffe and Hellman discovered public key cryptography.

Bring me two of every kind…

As there are symmetric or conventional ciphers that are used primarily to encrypt data, there are asymmetric ciphers, which were pioneered by Diffie-Hellman that are used to manage the keys used by the conventionally encrypted data. Today's society calls for increasingly stronger encryption which can be accomplished by a longer key length. Today's proprietary information is at risk due to an ever-growing list of organizations with a mission to destroy or decrypt information for numerous reasons including industrial espionage and identity theft. New hardware developments such as Field Programmable Gate Array(FPGA) technology and Application Specific Integrated Circuits(ASIC) provide a base in which calculations required to break cryptographic systems can be accomplished faster than ever before [7]. In 1975 a 56 bit key length was sufficient to protect data for 20 years. However, 26 years later and significantly past its

prime, the Data Encryption Standard (DES) is still being utilized with its 56 bit key length in various processes around the world. The table below from 1996 shows how susceptible a 56 bit key length was five years ago. As shown, with an investment of $300,000 one would allow a DES cryptosystem to be broken in 19 days.

Investment	Time to Break
$10,000	18 months
$300,000	19 days
$300,000,000	12 seconds

Figure taken from Technical Discussion Key Lengths vs. Time to Break

This calls for a new breed of crypto systems that employed longer key lengths. This call has brought new products into the crypto arena such as triple DES (3DES), IDEA, and Blowfish. Triple DES simple runs the same 56-bit encryption put passes a block of data through 3 different keys. Blowfish, a 64 bit secret-key block cipher has a key length up to 448 bits. More recently, the National Institute of Standards and Technology endorsed a worldwide compitition to develop the next standard of encryption known as the Advanced Encryption Standard (AES). The four-year process reviewed many different submissions including Twofish, RC6, and Serpent. Twofish, a cipher build off the existing Blowfish block cipher is much faster and can operate on a smartcard with less than 64 bytes of RAM. This is increasingly more important as the market of portable electronic devices with little computing power continues to grow. However, it was a Belgian submission that ultimately won the compition. In October of 2000, an algorithm know as Rijndael was chosen to fulfill the standard. Rijndael, named after its conceivers, John Daemen and Vincinet Rijmen is available in three keylengths 128, 192, and 256 bit. It is published that "a hypothetical technology that could break the standard Rijndael will replace -- DES -- in one second. It would take that same technology 149 thousand-billion years to crack 128-bit AES." [9 Berinato] Further developments in the asymmetrical crypto environment have also transpired. As previously stated Diffe and Hellman conceived the public key or asymmetrical crypto system around 1976. At the same time across the Atlantic Ocean, British Intelligence was also working on the same theory. A group of individuals named James Ellis and Clifford Cocks discovered the mathematical computations required to make it work. However, what was secret government information in Britain, was a marketable technology in America. Aside from that, years before anyone else, the NSA claims to of already had such a cryto system although there is no documentation to either support or deny it [6]. Is there anything that MIT does not get involved in? Apparently not, later that year, Ronald Rivest from the institution sought the involvement of Adi Shamir and Leonard Adleman to form and create what is known today as RSA encryption, named after the last names of its designers. RSA "is based upon the relative ease of finding the product of two large prime numbers compared to finding the prime factors of a large number." [10 Kessler] These prime numbers are very large, more than 100 digits long. Today's computing power can now factor a number that is up to 140 digits long. RSA encryption maintains its integrity by the ability to increase the number of digits in its key, enabling it to stay just ahead of the current computing power. In early 2000, the patent expired on RSA encryption, of which many felt was entirely undeserved. Even the though the heading of this section is bring me two

of every kind, referring to asymmetrical and symmetrical crypto systems; it would be relevant to mention the third. The third breed of cryptosystem is known as hashing. Hashing simply takes a value or compilation of a string of bits and assigns it a value. This value can be packaged with the sting of data and the package encrypted and sent off for the recipient's eyes-only. Once the information is received it can be decrypted and again a hash can be run on the string of data. If the two values match, than it is safe to say that the information has not been tampered with in transit. This is a similar process in the accounting world known as a check sum. No one form of cipher system need be used independently from one another. In essence all three can work well together in practice, from hashing information being sent encrypting the information and hash with a conventional cryptosystem and using a public key system for the key pairs. Wouldn't Thomas Jefferson be proud, or perhaps he would say "I helped invent Crypto… and all I got was this stupid wheel."

New Testament?

Elliptic Curve Cryptography (ECC) was introduced in 1985 by Neil Koblitz and Victor

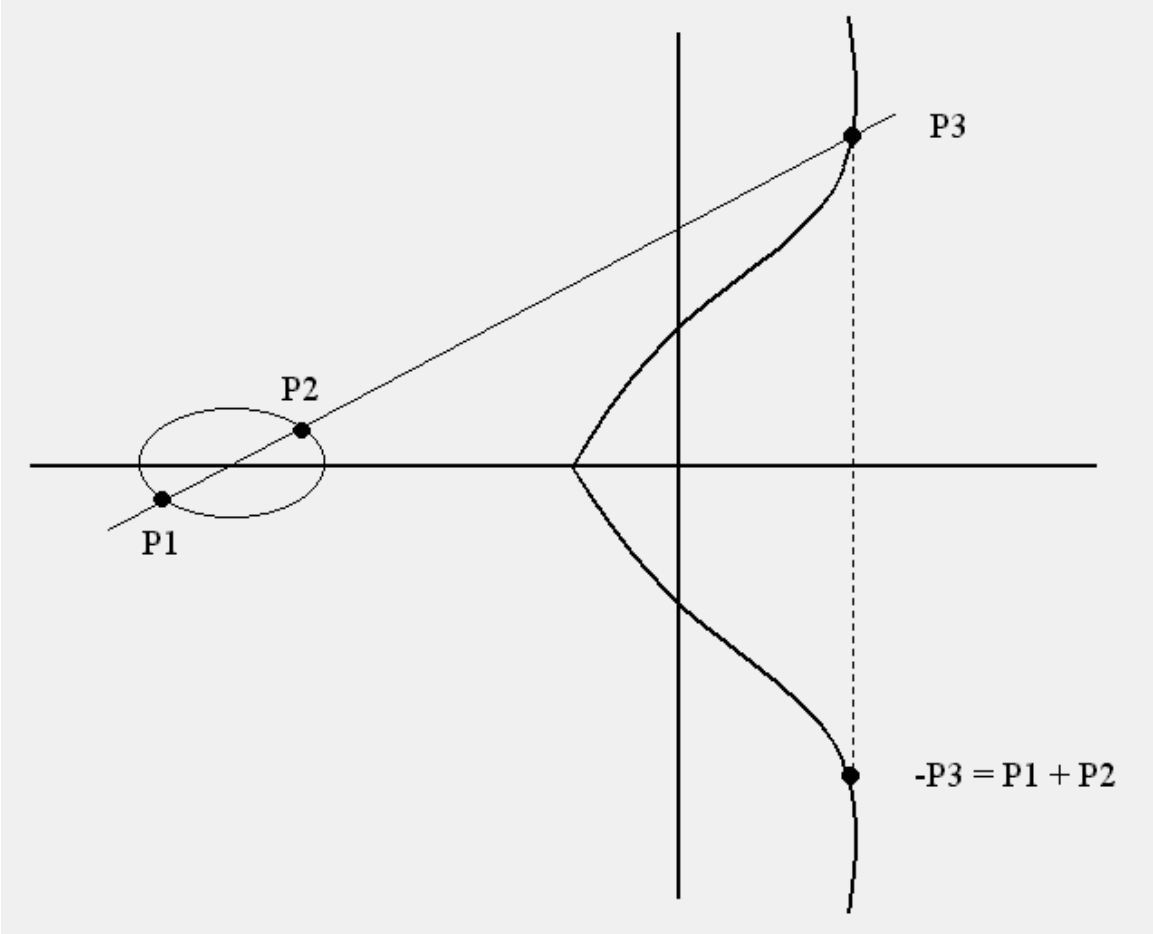

Figure taken from "An Overview of Cryptography"

Miller, the method utilizes discrete logarithmic problem over the points of an elliptic curve. The benefit to ECC is that the mathematics are so difficult to crack enabling the keys to be dropped in size. In comparison, to achieve the same level of protection RSA encryption would require a 1024 bit key where Elliptic Curve would require only a 160 bit key.

The figure above "shows the addition of two points on an elliptic curve, which is defined according to a set of simple rules: point P1 plus point P2 is equal to point -P3 = (x,-y), where (x,y) = P3 and P3 is the intersection of the elliptic curve and a line going through P1 and P2. As shown, small changes in P1 or P2 can cause a large change in the position of P3." [10 Kessler]

A Place for Cryptography in every Business (ok, so its not a biblical reference)

Today, the practice of cryptography is abundant. IT departments have most undoubtedly used passwords for years and years to protect "sensitive" information. However, in today's technically advanced world, adequate passwords only makes up one piece of the Information Security puzzle. For example, more information is sent electronically than in any other format, mail service, telegraph, pigeon… So, much like a bank uses armored trucks to move money, we turn to Cryptography to be our armored truck of information. This is prodomantely displayed in the transfer of messages via email. Protected email using an encryption package allows business' to transfer information without having to worry about how it will be intercepted. This also offers a feature in which the armored truck does not, non-repudiation. By the use of digital signatures, it is easy to identify who the sender of a message is. With an armored car, who knows who put the money in and if they conveniently left some out. Pretty Good Privacy (PGP), a tool for this purpose is not uncommon to today's market place. PGP is a cryptosystem that was developed in the early 90s by Phil Zimmerman. Zimmerman and his cryptosystem have been the topic of many policy conversations and legal proceedings since he refused to program in a back door and due to export regulations and his failure to abide by them.

Another arena that has fallen into the laps of today's corporate America is the challenge of allowing users to work from home. The days of a single income family have long ago passed. Today, two working parents are common place and in many instances require one of these individuals to work from home. Most companies find that employees can achieve the same productivity they other wise would in the work place while working at home. Remote logon allows the employer to offer a fringe benefit while saving the cost of leasing office space. The challenge however, is to allow employees to logon to trusted networks remotely while doing it securely. Enter the smart card. The token card produces a randomly generated number which is synchronized with a vendors listing of card serial numbers. This randomly generated number or token in conjunction with a known passphrase can allow remote users to remotely access proprietary information. Companies such as SecurID and TREK produce these devices using an RSA encryption algorithm.

As the technology continues to progress and years pass, the costs of these levels of security decrease. It is now not only Fortune 500 companies that employ cyber policing of information but…. almost everyone. Where once school children used two cups and string to communicate, now they use laptops with cellular modems.

The New Millenium brings?

OK, so now it's the new millenium, 2001 even. When do we start using this technology to maximum capacity in every day products that has taken so long to refine? This is a question probably asked by more than one not so technical savvy consumers; that is unless they have seen the movie Swordfish and see how glamorous the Information Security profession can truly be. Benign to the ordinary end user, crypto sciences are used in almost every electronic device to ordinary computer based software on the home personal computer. From PGP and SSL used in email and web browser packages to Elliptic Curve crypto used in the Palm pilots of tomorrow, the art of hiding messages in unreadable form has undoubtedly weaved its way into every technical facet of society. What will the future bring? Undoubtedly even longer key lengths and even more complex mathematical formulas used in symmetric algorithms. One thing is for certain, eventually there will be a certification offered by some corporation that helps endorse their own particular brand of cipher products, its only a matter of time.

References/Bibliography

[1] Bible Text: New Revised Standard Edition; Division of Christian Education of the National Council of the Churches of Christ in the United States of America

[2] Cohen, Fred "A Short History of Cryptography"; 1995 http://all.net/books/ip/Chap2-1.html

[3] Electronic Frontiers Australia (EFA) "Introduction to Cryptography", http://www.efa.org.au/Issues/Crypto/crypto1.html

[4] Ritter, Terry "Learning about Cryptography: A Basic Introduction to Crypto", May 27, 2001; http://www.io.com/~ritter/LEARNING.HTM#Fundamental

[5] Salviander, Sami Anton, "THE HISTORY OF ENCRYPTION AND CRYPTOLOGY" CS407 Seminar http://cs.eou.edu/~slipknot/Papers/CS407.html

[6] H.X. Mel, Baker, Doris M., "Pioneering Public Key: Public Exchange of Secret Keys" May 8, 2001 http://www.informit.com/newsletter.asp?link=338

[7] Blaze, Matt Diffe, Whitfield: "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" 1996 http://www.counterpane.com/keylength.html

[8] Technical Communications Corporation: "Technical Discussion on Key Lengths vs. Time to Break" 1996 http://www.tccsecure.com/keyleng.htm

[9] Berinato, Scott "'Rijndael' proposed as government encryption standard" eweek; 10/02/2000 http://www8.zdnet.com:80/eweek/stories/general/0,11011,2638138,00.html

[10] Kessler, Gary "An Overview of Cryptography" 9 Jul 2001 http://www.garykessler.net/library/crypto.html#pkc

[11] Southern, Richard "Elliptic Curve Cryptosystems: The Future of Public Key Encryption?" April 20, 1998. http://www.cs.uct.ac.za/courses/CS400W/NIS/papers98/rsouther/ecc.html

[12] Heath, Jim "How electronic encryption works and how it will change your business." May 2001 ViaCorp http://www.viacorp.com/crypto.html

Last Updated: June 29th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Cyber Defence Japan 2017	**Tokyo, JP**	**Jul 05, 2017 - Jul 15, 2017**	**Live Event**
SANS Cyber Defence Singapore 2017	**Singapore, SG**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS ICS & Energy-Houston 2017	**Houston, TXUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Los Angeles - Long Beach 2017	**Long Beach, CAUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Munich Summer 2017	**Munich, DE**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DCUS**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
Security Awareness Summit & Training 2017	**Nashville, TNUS**	**Jul 31, 2017 - Aug 09, 2017**	**Live Event**
SANS San Antonio 2017	**San Antonio, TXUS**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Boston 2017	**Boston, MAUS**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Prague 2017	**Prague, CZ**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Hyderabad 2017	**Hyderabad, IN**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Salt Lake City 2017	**Salt Lake City, UTUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS New York City 2017	**New York City, NYUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Adelaide 2017	**Adelaide, AU**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Chicago 2017	**Chicago, ILUS**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VAUS**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS San Francisco Fall 2017	**San Francisco, CAUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Tampa - Clearwater 2017	**Clearwater, FLUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NVUS**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS Dublin 2017	**Dublin, IE**	**Sep 11, 2017 - Sep 16, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**The Hague, NL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London July 2017	**OnlineGB**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**