Global Information Assurance Certification Paper

An Introduction to Modern Cryptosystems

By Andrew Zwicke

GIAC Version 1.4b, option 1

Abstract:

Organizations with a need for intense information security, such as government agencies, law enforcement, financial institutions, businesses, and health care facilities, can leverage strong, modern cryptosystems to help ensure that their data is not accessible to outsiders. All cryptosystems use either asymmetric or symmetric encryption. Symmetric key systems typically operate more quickly than asymmetric systems, but they require a highly secure means of exchanging keys between users. Major symmetric systems include DES, Triple DES, AES, Blowfish, and SkipJack. Major asymmetric systems include elliptic curve systems, RSA, and their associated authentication and repudiation technologies.

There are important strengths and weaknesses of both types of cryptosystems that must be understood before selecting a solution. Performance, data type, data access, cost, community acceptance, strength of algorithm, and key management should all be determined in order to select the most appropriate solution. After a cryptosystem has been selected and implemented, it is critical that users understand how to safeguard their encryption keys. A strong key management process is essential to prevent unauthorized access to sensitive information. The strength of most current encryption algorithms is far beyond the ability of computing technology to defeat, so the preferred method of attacking a cryptosystem is key theft.

Selecting a cryptosystem that provides a high level of security while meeting the business requirements of an organization is extremely important. Knowing the types of systems that are available, their strengths and weaknesses, and how to evaluate a system are key considerations when evaluating cryptographic technologies for an organization.

Introduction:

For thousands of years, the written word has served humankind by conveying meaning under circumstances where spoken communication is either not practical or not possible. The deliberate act of committing language to print or electronic media preserves a tangible, transferable record of an author's message. The human want or need of secrecy certainly predates written language itself. Inevitably, the desire for privacy inspired the authors of sensitive messages to derive methods of disguising their texts soon after the development of written language. Ciphers were created to obscure the meaning of messages, rendering their content useless to any party other than the message's intended recipient.

The need to establish secure and reliable methods of communication is at least as important now as it was when the first attempts to encrypt text were made. A high premium is placed on confidentiality when information regarding state secrets, war strategy, business plans, financial transactions, and medical records needs to be stored or transmitted. Since its inception, the Internet has enabled unprecedented levels of communication. The author of a message can now type on a machine on one side of the world, and the message recipient can receive that message on the other side of the world in a matter of minutes. The Internet is a convenient and effective communication channel, but it is not a secure one. Modern cryptosystems provide a powerful method of ensuring the privacy, integrity, and validity of messages that are transmitted across the Internet.

The Need for Private Communications

To gain perspective, consider the discovery of "a Mesopotamian tablet in 1500 B.C. containing an enciphered formula for making pottery glazes…" (Schneier, p. 86) The need for business secrecy is nothing new. Individuals, in their personal lives and their professional lives, have many needs for privacy in their communications with one another. At the most basic level, a person sending an email to a friend or family member would like to know that their message is received by that person alone, and that the message has not been intercepted by a third party or altered from its original form in any way. The privacy of this message is made possible through the use of cryptosystems. In fact, "Email was the first use of cryptography on the Internet." (Schneier, p. 112)

There are organizations that depend on the ability to safeguard their information while it is in storage and while it is transmitted between parties. Government agencies, law enforcement agencies, financial institutions, businesses, and health care organizations all require the ability to communicate securely over the Internet. If information is intercepted or altered, the consequences could be severe. State secrets could be passed to a hostile government. Lives could be

lost. Financial data could be stolen. Business secrets could benefit competitors. Clearly, there is much at risk, and a method of protecting data is critical.

Introduction to Cryptosystems

Cryptosystems are complex combinations of hardware and software that are used to transform plaintext messages into a series of unintelligible characters, known as cipher text, then back to their original plaintext form. "An encryption algorithm scrambles data by combining the bits in the key with the data bits; in decryption, the algorithm unscrambles data by separating the data bits from the key bits." [1, NetAction] Encryption is at the heart of secure electronic communication, however it does not guarantee that a message will remain completely safe. The authenticity and integrity of an encrypted message requires the use of digital signatures and one-way hashes.

The two types of cryptosystems in use, symmetric and asymmetric, rely on the responsible use of keys and sound key management practices to preserve their security. The easiest way for an attacker to decrypt a private message is by obtaining a copy of the key used to encrypt it, since the strength of modern cryptosystems makes code-breaking computationally unfeasible using today's technology. "It should be emphasized that the strength of a cryptographic system is usually equal to its weakest link. No aspect of the system design should be overlooked, from the choice of algorithms to the key distribution and usage policies." [2, SSH]

Symmetric Cryptosystems

Symmetric key systems, or secret key systems, rely on the same key to encrypt and decrypt cipher text, so ensuring that the secret key is not compromised is extremely important. The length of the keys used by different systems varies. Symmetric cryptosystems either encrypt data in a stream, bit by bit, or in block form, usually 64 bits at a time. Symmetric key systems generally use shorter key lengths, and provide faster rates of data manipulation than asymmetric key systems.

The following major symmetric systems are detailed alphabetically below: AES, Blowfish, DES, IDEA, RC4, Skipjack, and Triple DES.

AES (Advanced Encryption Standard):

- Rijndael, pronounced Rain Doll, was selected as the AES algorithm in October 2000.
- AES is extremely secure, and its performance is excellent.

- DES encryption resisted attacks for more than 20 years, and AES should surpass that time frame.
- Rijndael was officially ratified in November 2001.
- "When considered together, Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility make it an appropriate selection for the AES." [3, NIST]
- "Rijndael's very low memory requirements make it very well suited for restricted-space environments, in which it also demonstrates excellent performance." [3, NIST]
- Rijndael uses key sizes of 128, 192, or 256 bits.
- AES encryption executes much faster than DES and Triple DES.
- "In comparison, DES keys are 56 bits long, which means there are approximately 7.2×10^{16} possible DES keys. Thus, there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys." [3, NIST]
- "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key." [3, NIST]

Blowfish:

- Blowfish was developed by Bruce Schneier in 1993.
- Blowfish was conceived as a replacement for DES or IDEA.
- Blowfish uses a variable-length key, from 32 bits to 448 bits, and is appropriate for both domestic and international use. [3]
- "Blowfish does not meet all the requirements for a new cryptographic standard…it is only suitable for applications where the key does not change often, like a communications link or an automatic file encryptor." [4, Schneier]
- Blowfish is significantly faster than DES. [4]
- It is very time consuming to initialize the algorithm with a new key. [5, XILINX]

Data Encryption Standard (DES):

- "Developed in the United States during the 1970s by the National Bureau of Standards and the National Security Agency…to provide a standard method for protecting sensitive commercial and unclassified data." [6, Lay Networks]
- DES officially became a federal standard in November of 1976. [6]
- DES is no longer considered secure, and the algorithm can be broken in a matter of hours or days.

- DES was replaced by Triple DES, which is still considered secure and is in wide use.
- "There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys." [6, Lay Networks]
- "DES takes as input a 64 bit key, of which only 56 bits are used. From these 56 bits, 16 48 bit sub keys are created. The message is split into 64 bit chunks, and a complex series of steps enciphers the message using each subkey." [6, Lay Networks]

International Data Encryption Algorithm (IDEA):

- The same algorithm is used to do the encryption and decryption.
- Used by Pretty Good Privacy (PGP) software.
- IDEA operates on 64-bit plaintext block, and uses a 128-bit key. [7]
- Software implementation speeds are comparable with those for DES. [7]

RC4:

- Stream cipher that encrypts data bit by bit.
- RC4 uses a variable key-size.
- The algorithm is owned by RSA Security, Inc. and requires a license.
- "Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software." [8, RSA Securities]
- Used in SSL and WEP (IEEE 802.11 WLAN standard) [5]

SkipJack:

- Skipjack was developed by the National Security Agency (NSA).
- The algorithm was declassified and made publicly available in 1998.
- Skipjack has four different modes of operation: ECB, CBC, CFB, and OFB.
- Skipjack was used to encrypt sensitive, but not classified, government data. It was implemented in two government encryption devices: the Clipper chip and Fortezza PC card. [9]
- SkipJack is currently one of the preferred cryptosystems, and it has not been broken.
- "Skipjack encrypts and decrypts data in 64-bit blocks, using an 80-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext." [9, Tropical Software]

- "Skipjack has 32 rounds, meaning the main algorithm is repeated 32 times to produce the ciphertext." [9, Tropical Software]

Triple-DES:

- Triple DES has two modes of operation. Triple ECB is the most commonly used mode, however Triple CBC provides an additional layer of security.
- Triple DES performs much more slowly than AES.
- Triple DES can provide greater security than AES.
- Uses a block cipher for encryption.
- Developed due to concerns about the weakness of the DES algorithm due to advances in computer processing power.
- It is important to use different keys during the encryption process.
- The data is encrypted with the first key, decrypted with the second key, and then encrypted again with the third key. [10]
- Data is encrypted and decrypted in 64-bit chunks. [10]
- Uses a 112 or 168-bit key. [5]

Asymmetric Cryptosystems

Asymmetric key systems, or public key systems, use both a private and public key for encrypting and decrypting cipher text. "The beauty of public key cryptography is that the public keys can be freely distributed. Encrypted communication can be established between any two parties once the public keys are shared between them." [11, Meyer] These are much slower than symmetric systems, and are usually used only to exchange keys initially. After this exchange, encryption is often performed symmetrically.

Another important advantage to asymmetric systems is that they provide enhanced security in the form of digital signatures and strong key management. "As a consequence of the encryption key and the decryption key being different, public key cryptography makes possible digital signatures…" [12, Network Computing] Using public and private keys in asymmetric encryption assists a message recipient in verifying the authenticity of the sender because the recipient's private key and the sender's public key are both used to decrypt the message.

Message Algorithms: Secure Hash Algorithm (SHA-1) and MD5

- SHA-1 is a hashing algorithm, ideal for proving message integrity.
- Hashes are a compressed form of data that reveals whether the contents of a message have been altered during transmission.

- SHA-1 is used in SSL and IPSec.
- "SHA-1 accepts a message of up to 2^{64} bits in length (processed in 512-bit blocks) and produces a 160-bit message digest." [5]
- "Mathematical algorithms that take any amount of data as their input and produce a fixed-size result that is a "signature," or a "fingerprint" of the data." [12, Network Computing]
- MD5 is generally felt to not be as strong as SH-1.

Digital Certificates

- Certificates are available for individuals, organizations, servers, and software developers.
- Used to establish message authenticity by preventing online imposters.
- Available in "classes", based on the amount of identification information provided by the certificate requestor, the higher the certificate level, the more trust-worthy the certificate. [13]
- A respected organization will take a key pair from a user and use it's own private key to encrypt the message. The organization's public key and a certificate are sent to the message recipient to verify that the sender is valid.
- "Digital certificates that are trusted by Web browsers and mail clients allow users to digitally sign e-mails and encrypt their contents and attachments, protecting messages from being read or tampered with by online intruders." [14, Verisign]

Elliptic Curves:

- Not widely in use, but support is growing.
- Low resource requirements make it attractive to organizations with limited processing power.
- Algorithm uses a different mathematical problem than the use of massive numbers that require factoring.
- "At a high level, they are analogs of existing public-key cryptosystems in which modular arithmetic is replaced by operations defined over elliptic curves." [15, RSA Securities]
- Shorter key sizes can be used to achieve the same security of conventional public-key cryptosystems. [16]

RSA:

- The RSA system is currently used in a wide variety of products, platforms, and industries. The RSA algorithm is built into current operating systems by Microsoft, Apple, Sun, and Novell. [17]

- The RSA cryptosystem provides both encryption and authentication functions.
- RSA is included in S/MIME and Secure Sockets Layer (SSL).
- "[RSA is] very slow in software, and at least 1000 times slower in hardware than DES or AES." [5]

Key Considerations in Selecting a Cryptosystem

There are many cryptosystems available to organizations that require secure communication methods across insecure media. Careful consideration of the strengths and weaknesses of the available cryptosystems is essential in choosing a solution that best meets the needs of the user. When choosing an appropriate cryptosystem, the following evaluation criteria can help determine which to implement.

Performance: Performance varies among cryptosystems due to many factors. The length of the key used influences the speed of the system; longer keys require greater computing time and resources. The cipher mode, block encryption or stream encryption, also affects system performance. The complexity of the encryption algorithm and the number of times that encryption is performed will also control the performance. One of the main reasons that AES was developed was as a secure alternative to the slow, resource intensive Triple DES.

Key Management: Symmetric cryptosystems generally provide faster throughput, but require a secure means of exchanging a secret key, such as Diffie-Hellman or RC4/RC5. Asymmetric systems using a public key do not have this limitation, however their throughput is often much slower then symmetric systems. Consider which key management schema is most appropriate for the users of the cryptosystem.

Data Type: The sensitivity of the data that needs protection should be one of the primary determining factors in selecting a cryptosystem.

Data Access: Identify the approximate number of system users that will need access to the cryptosystem. The locations of the users and the frequency of their access will also help determine an appropriate solution.

Community Acceptance: One of the most important considerations in selecting a cryptosystem is acceptance by the cryptanalyst community. Select a cryptosystem that has been available for several years. The only true way to judge the security of an algorithm is by exposing it to the cryptanalytic community for their testing and scrutiny. These time-tested systems are far superior than any proprietary encryption algorithm offered by a software vendor. [Schneier, p. 119]

Strength of Algorithm: Choose a cryptosystem that uses a powerful algorithm. The DES cryptosystem may now be defeated in a short time using modern computers.

Cost: As with any technology, consider the cost of implementing a cryptosystem compared to the benefits provided by the enhanced security. Not all data is critical enough to justify the purchase of a cryptosystem that provides massive key length and multiple modes of encryption.

Summary

For individuals and organizations that require privacy and secrecy, a strong cryptosystem is an essential component of the overall security framework. Government, law enforcement, financial, and health care organizations possess data that must remain secure to avoid damaging consequences. Cryptosystems provide the power to secure communications and safeguard data. Symmetric systems typically provide the best performance, but they require a secure method of exchanging keys between users. Asymmetric systems do not need users to exchange keys, but their performance may be many times less than secret key systems.

Cryptosystems are powerful tools, but they are not the final answer to the threats related to security. Modern algorithms are so strong that attackers typically focus their efforts on obtaining a copy of a key used for decryption. Safeguarding these keys by implementing an effective key management plan is critical, as is educating the system users. Cryptosystems should be used in conjunction with other security technologies such as firewalls, intrusion detection systems, virtual private networks, and access controls.

The strength of a cryptosystem is based largely on its release to the cryptanalytic community, where it may be rigorously tested for flaws. Purchasing a proprietary, "secret" encryption product is not recommended. Other factors that can influence the selection of a cryptosystem include data type, speed, key length, encryption mode (stream or block), and cost.

References:

1. NetAction. "NetAction's Guide to Using Encryption Software." http://www.netaction.org/encrypt/intro.html. 17 Dec. 2002.

2. SSH. "Strength of Cryptographic Algorithms." http://www.ssh.com/support/cryptography/introduction/strength.html. 20 Dec. 2002.

3. National Institute of Standards and Technology (NIST). "Advanced Encryption Standard (AES) Fact Sheet." 19 Jan. 2001. http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html. 4 Jan. 2003.

3. Counterpane Internet Security, Inc. "The Blowfish Encryption Algorithm." http://www.counterpane.com/blowfish.html. 16 Jan. 2003.

4. Schneier, Bruce. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)." http://www.counterpane.com/bfsverlag.html. 16 Jan. 2003.

5. XILINX. "Network Security." 5 Jan. 2003. http://www.zilinx.com/esp/optical/collateral/network_security.pdf 12 Jan. 2003.

6. Lay Networks. "DES Explanation." 2 May 2002. http://www.laynetworks.com/users/webs/des.htm. 10 Jan 2003.

7. Naval Postgraduate School: IDEA http://www.cs.nps.navy.mil/curricula/tracks/security/notes/chap04_43.html

8. RSA Securities. "What is RC4?" http://www.rsasecurity.com/rsalabs/faq/3-6-3.html. 15 Jan. 2003.

9. Tropical Software. "Skipjack Encryption." http://www.tropsoft.com/strongenc/skipjack.htm. 10 Jan. 2003.

10. Tropical Software. "Triple DES Encryption." http://www.tropsoft.com/strongenc/des3.htm. 10 Jan. 2003.

11. Meyer, Peter. "An Introduction to the Use of Encryption." July 1997. http://serendipity.magnet.ch/hermetic/crypto/intro.htm. 17 Dec. 2002.

12. Network Computing. "Web Proxy Servers, 1/e: Encryption and Authentication Security." 2 Apr. 1999. http://www.networkcomputing.com/netdesign/1007part2a.html. 18 Dec. 2002.

13. Comodo Group. “Introduction to Digital Certificates: Enrolling for a Digital Certificate.” http://www.comodogroup.com/support/learning/digital_certs_intro/index5.html. 29 Jan. 2003.

14. Verisign. “Secure Messaging.” http://www.verisign.com/products/email/index.html. 29 Jan. 2003.

15. RSA Security. “What are elliptic curve cryptosystems?” http://www.rsasecurity.com/rsalabs/faq/3-5-1.html. 15 Jan. 2003.

16. RSA Security. “How do elliptic curve cryptosystems compare with other cryptosystems?” http://www.rsasecurity.com/rsalabs/faq/3-5-4.html. 15 Jan. 2003.

17. RSA Security. “Is the RSA cryptosystem currently in use?” http://www.rsasecurity.com/rsalabs/faq/3-1-9.html. 15 Jan. 2003.

18. Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, Inc., 2000.

Further Reading:

Cryptanalysis and Attacks on Cryptosystems:
http://www.ssh.com/support/cryptography/introduction/cryptanalysis.html

Cryptographic Protocols and Standards
http://www.ssh.com/support/cryptography/protocols/

Encryption Software to Avoid
http://www.interhack.net/people/cmcurtin/snake-oil-faq.html

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor