ADVANCED ENCRYPTION STANDARD:

HOW DOES IT WORK?

Project Paper for
Information Systems Audit and Control

TABLE OF CONTENTS

1.Introduction

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including: Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.) Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Integrity: Assuring the receiver that the received message has not been altered in any way from the original. Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plain-text. It is encrypted into cipher-text, which will in turn (usually) be decrypted into usable plain-text.

2.Cryptography

If we follow the origin of the word Cryptography, crypt-ography, it basically means "burying" information. Practice is to transform the message into a form which is gibberish without the knowledge of the key. Original message, called plain-text, is encrypted under a key and the result is chiper-text. With the use of same key message can be retrieved. Transformation method used can be as simple as shifting the alphabet forward, writing C for A and D for B (Caesar Chiper). Of course this a very simple method and there are more secure and complex ones. Crypthograpic primitives are this tools used in encryption and decryption. Depending on the use and purpose there are several different kinds. Figure-1 below shows a classification of cryptographic primitives.

A message or data that can be read and understood without any special process is considered plain-text or otherwise referred to as clear-text. There are times when we need to protect sensitive messages or computer data, especially if it needs to travel across public networks. For example, an email message sent in plain-text through the Internet to a friend is like sending a postcard through the postal service. The message sent could be read by virtually anyone who cared to take a look. The email scenario might be worse than the postal service due to the speed of worldwide exposure that is possible with email. The postcard-like method may be fine for the casual message but what about sensitive or confidential messages? It is at times like these users may opt to protect their data through the use of a process that invokes encryption and decryption. Encryption is a method of converting plain-text into an unreadable an unintelligible format called cipher-text. The process of converting cipher-text back to a recognizable and readable format is call decryption. Using the process of encryption, a user can store or send sensitive information over public networks in a more secure manner than just sending or storing the data in plain-text. When intended viewers of the data wish to access the encrypted data, they use the process of decryption to convert the cipher-text back to a readable format.

Cryptography can be generally defined as the science of designing algorithms/chipers to encrypt and decrypt data enabling the storage and transmission of sensitive data in a secure manner. A crypto-system consists of a cryptographic algorithm, or cipher, which is a mathematical function to encrypt and decrypt data and all of the possible keys and protocols that make it work. Using a key, the cryptographic cipher can be used to convert plain-text to and from cipher-text.

An early example of a crypto-system is the Caesar cipher. The Caesar cipher, considered developed by Julius Caesar when he sent messages to his generals through untrusted messengers, can be classified as a substitution cipher, which replaces one piece of information with another. By substituting each letter in the message with the letter that corresponds to the letter 3 places forward in the alphabet from the original, Caesar was able to encrypt his messages. Basically, Caesar used a key of 3 and shifted the alphabet plus 3 when encrypting and minus three when decrypting. Thus, the message "SECRET" would become "VHFUHW" when encrypting by using a key of three and shifting the alphabet forward three letters. Decrypting "VHFUHW" would revert back to

"SECRET" by shifting the alphabet back three letters.

Obviously, these types of ciphers are considered weak using today's standards and the computing power that is available. The advancement of computing power is precisely the reason we must continuously evaluate our crypto-systems to ensure our sensitive data can be adequately protected while stored and/or sent over public networks.

3.Algorithms

As shown in the figure above there three types of algorithms. First type is unkeyed and there is no need for key this algorithms are used for one way encryption. Hash functions an Message authentication codes are examples of these. There is no decryption intended with this algorithms because they are used to identify files or authenticate messages.

3.1.Asymmetric Key Algorithms

Asymmetric key algorithms where a pair of keys-public and private- used. One key is used for each function and reverse operation can be done with the other key. So one part of the key pair can be made public. These algorithms have special uses in digital signatures and web of trust based applications.

3.2.Symmetric Key Algorithms

Than there is symmetric key algorithms where a single key is used for both encrypting and decrypting plain-text. These are also called secret key algorithms because the design of these algorithms require the key to be kept secret between exchanging parties.

Symmetric key chipers characterised by their use of a single key for both encryption and decryption. Advantage of a single key chiper is its efficiency. This type of crypto primitives are faster than public key algorithms. Because mathematical algorithms behind these chipers are linear and computational implementations of these chipers are fast in hardware and software.

3.3.Stream Chipers â€“ Block Chipers

A chiper operates on single bits (i.e. letters) or a block of bits (i.e. words). The type op operation characterises the chiper as a "Stream Chiper" or as a "Block Chiper" respectively. Well known block chipers are DES (Data Encryption standard), AES (Advanced Encryption Standard).

Nowadays cryptography is largely based on computers and for that reason most widely used algorithms are block chipers because implementing block chipers working on fixed length blocks of data in software is easier. Our main objective in this paper to analyse AES and it is a block chiper.

4.Data Encrypting Standard (DES)

The Data Encryption Standard (DES) is an algorithm developed in the mid-1970s. It was turned into a standard by the US National Institute of Standards and Technology (NIST), and was also adopted by several other governments worldwide. It was widely used, especially in the financial industry. Many ATM machines today uses DES for example.

DES is a 16-round Feistel cipher and was originally designed for implementation in hardware. DES is a block cipher with a 64-bit block size. It uses 56-bit keys. This makes it suspect-able to exhaustive key search with modern computers and special-purpose hardware. DES is still strong enough against most of the attacks, but it is easily breakable with special hardware. During the design of the chiper NSA (National Security Agency of US) was consulted to make sure it was secure and strong enough. NSA convinced other parties to reduce the key Length to 64 bits and than 56 bits. many believe that was a deliberate move on the NSA part to reduce the strength of the chiper to their level of ability to crack it. It is even argued tat NSA made sure to put a "back door" for themselves to use.

Despite all this controversy the design was exceptionally good for a cipher that was meant to be used only a few years. DES proved to be a very strong cipher and it took over a decade for any interesting crypt-analytical attacks against it to develop. However most important thing about DES is the way it was designed. Before DES cryptography belonged to military circles and there wasn't much public research on the subject. Design process of DES helped developing a pub lic body of research on the subject. Also it proved the case for an open specification chiper which is the best way to make sure the security of the chiper. Therefore its successor AES was designed in the same way.

A variant of DES, Triple-DES (3DES) is based on using DES three times (normally in an encrypt-decrypt-encrypt sequence with three different, unrelated keys). The Triple-DES is arguably much stronger than (single) DES, however, it is rather slow compared to some new block ciphers.

5.Advanced Encryption Standard (AES)

The Advanced Encryption Standard is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard was found too weak because of its small key size and the technological advancements in processor power. Fifteen candidates were accepted in 1998 and based on public comments the pool was reduced to five finalists in 1999. In October 2000, one of these five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndael.

Rijndael (pronounced as in "rain doll" or "rhine dahl") is a block cipher designed by Joan Daemen and Vincent Rijmen, both cryptographers in Belgium. Rijndael can operate over a variable-length block using variable-length keys; the version 2 specification submitted to NIST describes use of a 128-, 192-, or 256-bit key to encrypt data blocks that are 128, 192, or 256 bits long; note that all nine combinations of key length and block length are possible. The algorithm is written in such a way that block length and/or key length can easily be extended in multiples of 32 bits and it is specifically designed for efficient implementation in hardware or software on a range of processors. The design of Rijndael was strongly influenced by the block cipher called Squa re, also designed by Daemen and Rijmen.

5.1.How AES works

After a brief introduction to cryptography and types of algorithms now it is time to explain how AES algorithm works. This paper aims to explain the inner workings of the chiper in plain English. AES algorithm â€“ as any other cryptographic algorithm- has non-trivial internal workings. There is a series of procedures to turn plaintext input into obscured chipertext. Some steps in these procedures are simple mixing and changing of values and some ot hers based on higher mathematics. However it is still possible to describe the workings of this algorithm in a non technical manner.

The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits.

The input converted to binary form before being encrypted. Each character is mapped to a decimal number by the help of ASCII table. ACSII stands for American Standard Code for Information Interchange. Computers can only understand numbers, so an ASCII code is the numerical representation of a character such as 'a' or '@' . For example letter â€œaâ€□ is denoted by the decimal number 65 , hexadecimal number â€œ41â€□ and in binary it is denoted by â€œ01000001â€□. Table below shows decimal, hexadecimal and binary conversions.

AES algorithm works on bytes and a byte is a sequence of eight bits treated as a single entity. The input, output and key bits are processed by grouping them into arrays of bytes. For example a 128 bit input is grouped into 16 bytes of 8 bits each. 5.1.1.The State

Internally, the AES algorithmâ€™s operations are performed on a two-dimensional array of bytes called the State. The State consists of four rows of bytes, each containing 4 bytes. At the start of the

Cipher , the input â€“ the array of bytes in0, in1, ... in15 â€“ is copied into the State array as illustrated in Figure 2 below. The Cipher operations are then conducted on this State array, after which its final value is copied to the output â€“ the array of bytes out0, out1, and out15.

5.1.2.Encryption Steps

AES algorithm takes three main steps and these are described in the figure below. After the input is copied into the state, a sub key is added to the state. Than a nine round of four different transformations performed and a final round with MixColumn transformation being omitted. Figur e 2 below briefly describes the routines in each of the four transformations. These are namely; SubBytes, ShiftRow, MixColumn and AddRoundKey.

5.1.2.1.SubBytes

Byte substitution in AES algorithm is equivalent of S-Box of other algorithms. S-Box or substitution box is basically a lookup table used as reference in replacing individual bytes with transformed values. S-Box design is the hearth of a chiper. Because this is the part of the chiper providing non-linearity of algorithm. This lookup table is calcula ted by polynomial algebra over a Galois Field. Mathematical details of this calculation is beyond the limits of this paper. However we suffice to state that this finite field operation has very good non-linear properties. So that AES is strong against linear algebraic attacks.

5.1.2.2.ShiftRow

ShiftRow transformation shifts the individual bytes in the state array by a certain offset. This offset is the index number of the row. Row zero is left unchanged, row one bytes shifted one to their left, row two bytes two and row three bytes three. Result is shown in Figure 5, effects of this shifting can be seen by index number of each byte and also colours of bytes.

5.1.2.3.MixColumn

The MixColumn transformation operates on the columns of the state, providing int ra-column diffusion. In this step, the bytes in the columns are linearly combined, and matrix multiplication is performed over the same Galois Filed as used in the design of the S-box. This transformation causes every byte in a column to modify every other byte in that same column. Both the MixColumn and ShiftRow transformations are linear operations that work together to ensure that all of the bytes in a block affect each other, thereby generating high diffusion over many rounds of same operations.

5.1.2.4.AddRoundKey

AES encryption starts and ends with key addition. In each round of operation a sub key is added to the state array by XOR operation. This means every round is key dependent. A special key schedule is used to generate all the sub keys from the original key. Standard 128 bit encryption requires initial key addition, nine regular rounds and a slightly modified last round. Therefore 11 sub keys are needed. Key schedule uses same S-Box in the SubBytes transformation to expand the key.

5.2.Strengths of AES

In evaluating AES security it is natural to compare it to its predecessor DES. They both, are block chipers with similar designs. For example every encryption step of AES has a corresponding mechanism in DES. Despite the similarities fundamental differences between these to chipers. First of all AES has different S-Box design. Feistel network used in DES owes its security to block size, key size and number of rounds. DES key size being too short for contemporary computing power AES brings enhancements. Because AES doesn't rely on more round operations for extra security it requires few less rounds than DES. That translates into speed on hardware and software.

AES design includes mainly symmetrical, linear operations. However its S-Box design and variable key size and requisite number of rounds give it asymmetrical properties. Another Advantage of the chiper is the key schedule. AES has good resistance to weak keys because key schedule uses the same S-Box design to XOR the keys and it provides non-linearity. It is also worth noting that the chiper was designed to be resistant to cryptanalytic attacks. Requirements for the S-Box, and in-round transformations are supposed to provide this property.

5.3.Attacks on AES

Attacks against a chiper is always expected. First of all it is an academic study by experts aiming to improve security of the chiper. In modern day cryptography chiper procedures open and known by everybody. So that chiper is under constant scrutiny to ensure its security. Cryptanalysis or plainly put code breaking activity is traditionally targeted against the chiper itself, trying to conceal the secret information which is the encryption key. Described this way chiper is taken as a piece of mathematical function and than tried to solve. So far AES algorithm resistant to this type of attacks.

As for brute force attacks, trying all possible keys by the help of computing, 128 AES is quite secure for the foreseeable future. Because it requires 2^127 permutations which would take several millennia. However it is worth noting that foreseeable future in computing terms can be far less than it would mean.

So far only successful attacks against the AES chiper are side channel attacks. Side channel attacks are targeted not against the chiper itself but its various implementations. In 2005 D. J. Bernstein published timing attacks against AES (http://cr.yp.to/antiforgery/cachetiming-20050414.pdf) This attack required 200 million chosen plaintexts and may not be considered practical. Another group of researchers mounted a successful side channel attack and this attack requires that the attacker be able to run programs on the same system that is performing AES encryption(http://www.wisdom.weizmann.ac.il/~tromer/papers/cache.pdf) Finally T. Kohno presents possible attacks against the WinZip implementation of the AES (http://www.cs.washington.edu/homes/yoshi/papers/WinZip/winzip.pdf)

6.Summary

AES is an iterated block chiper with 128 bit block size and variable key lengths. It is known to be secure against linear and differential cryptanalysis It has sufficient key size to resist the brute force attacks

AES design is based on carefully constructed mathematical principles. However very design of the chiper makes it quite fast on hardware and software. Its internal structure can be described as card shuffling. But this shuffling operations are carefully designed so the chiper is easy to implement and secure.

7.Bibliography

1- FIPS-197: Advanced Encryption Standard National Institute of Standards and Technology (NIST) 2001

2- The Design of Rijndael Joan Daemen and Vincent Rijmen Springer, ISBN 3 -540-42580-2 2002

3- Applied Cryptography, Second Edition, Bruce Schneier, Wiley Computer Publishing, 1996

4- Wright, M. A. (Oct. 2001). The Advanced Encryptio n Standard. Network Security, 2001(10), 11 -13

5- Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, S. Vanstone, 1996