**Security Technology Tools II**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**Case 04**

INTRODUCTION

Symmetric encryption is the first type of cryptographic techniques that is used to, securely, store and transmit data. Confidentiality is assured through the use of a secret key. This key combined with a mathematical algorithm converts data to an encrypted form which is unintelligible. The data can then be decrypted by applying the same key to a reversed version of the algorithm; thus, the resultant is the reconstitution of the original data. This algorithm is also known as a two-way algorithm (Slaviero, 2010).

Asymmetric encryption is also known as, public-key cryptography. This type of encryption is defined by a pair of secret keys that are used to encrypt, decrypt data and can be used interchangeably. This data can then be, securely, stored or transmitted over unsecured communication mediums like the internet (“What is asymmetric”, 2008).

One example of this type of encryption occurs when a user receives a public and private key pair from a certificate authority. In the instance that any other user chooses to send an encrypted message to the user, the public key can be obtained from a public directory. The message is then encrypted by the public key and the intended recipient has the message decrypted by the use of their private key (“What is asymmetric”, 2008).

DEFINITION OF ALGORITHMS

Skipjack is an algorithm that uses an 80-bit key and was designed to run on “tamper-proof” hardware (“Encryption And Its Importance To Device Networking”, n.d.). This algorithm is a classified symmetric key encryption algorithm that was developed by the National Security Agency (NSA). The intention of the NSA, in this regard, was to enable law enforcement to access secure voice and data communications that have been encrypted using Skipjack (“Safeguarding Networked Information”, 1994).

Data Encryption Standard (DES) is an algorithm that uses a 56-bit key to encrypt data. Because the 56-bit key is considered too small, it’s considered insecure for many applications. There or recordings of these keys being broken in less than 24 hours (“Encryption And Its Importance To Device Networking”, n.d.).

The DES cipher was published by the National Institute of Standards and Technology (NIST) and it’s an implementation of a Fiestel Cipher. It uses a 16 round Feistal structure with a block size of 64-bit. Since 8 of the 64 bits are not used by the encryption algorithm, the effective key length is 56 bits. The other 8 bits function as check bits (“Data Encryption Standard”, 2015).

Figure 1 depicts the general structure of DES.

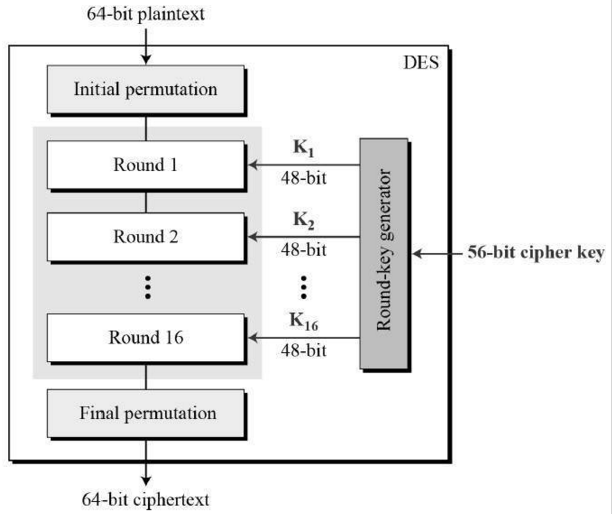


Figure 1: Data Encryption Standard (DES). Data Encryption Standard. (2015). Retrieved December 26, 2015, from http://www.tutorialspoint.com/cryptography/data\_encryption\_standard.htm

Triple-DES uses three successive DES operations to provide stronger encryption than DES. The algorithm is believed to be practically secure, although it is theoretically susceptible to some attacks. In recent years, Triple-DES has been superseded by the Advanced Encryption Standard (AES) (“Encryption And Its Importance To Device Networking”, n.d.).

“3 Key Triple DES (3TDES) also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES” (“Triple Data”, 2015). Longer key length is derived by the explicit meaning of 3TDES; in that, each key is made up of 56 bits resulting in a total of 168 bits. 2-Key TDES simply substitutes the 3rd key with the 1st key (“Cryptography Quick Guide”, 2015).

Figure 2 depicts the encryption scheme of Triple DES, the 2-Key variant.

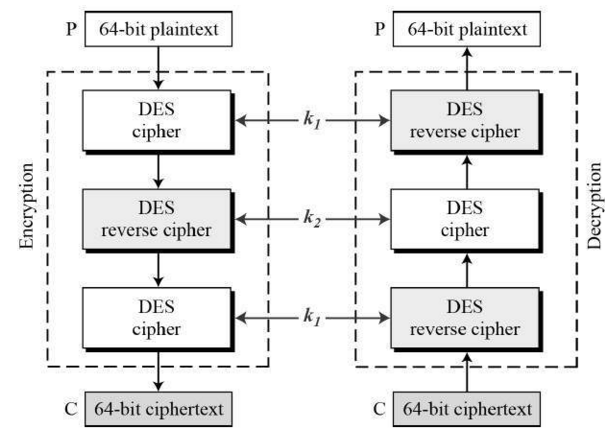


Figure 2 TDES Encryption Scheme Cryptography Quick Guide. (2015). Retrieved December 27, 2015, from http://www.tutorialspoint.com/cryptography/cryptography\_quick\_guide.htm

Advanced Encryption Standard (AES), also known as Rijndael, is a Federal Information Processing Standard (FIPS) approved cryptographic algorithm that can use 128, 192 or 256-bits to encrypt and decrypt data in blocks of 128 bits. As of 2004, there have been no successful attacks against AES (“Data Encryption Standard”, 2015).

Because 2/3TDES was slow and becoming vulnerable as computing power became greater, AES was created and found to be faster and stronger. As opposed to being a Feistel cipher like DES, AES is an iterative cipher. It’s comprised of a series of linked operations using substitutions and permutations (“Advanced Encryption Standard”, 2015).

Figure 3 depicts the schematic of AES.

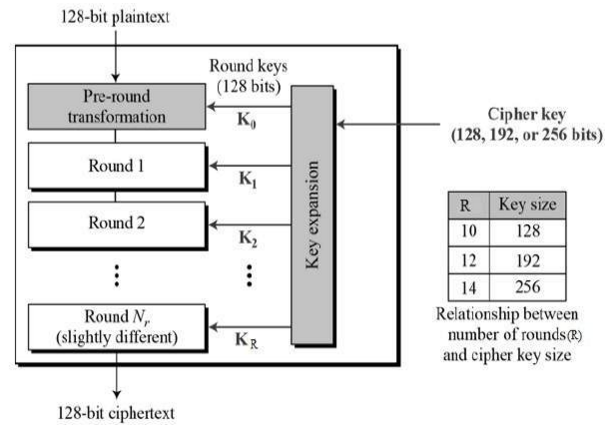


Figure 3: AES Schematic Advanced Encryption Standard. (2015). Retrieved December 27, 2015, from http://www.tutorialspoint.com/cryptography/advanced\_encryption\_standard.htm

Pretty Good Privacy (PGP) is a cryptographic system that uses a hybrid of symmetric and asymmetric cryptography. In this system, each user has a publically known or shared encryption key and their own private keys. The data being transmitted is encrypted with the public key and the receiving user decrypts the data with their private key. To help with the efficiency of this process, PGP uses a faster encryption algorithm to encrypt the message and the public key to encrypt the shorter key that was passed to the algorithm to encrypt all the data. The receiver then receives both, the encrypted message and the short key. The receiving user then uses their private key to first decrypt the short key and then use that decrypted short key to decrypt the data (“What is pretty”, 2015).

TRADITIONAL & COMPUTER FORENSICS

Traditional forensics is a domain of investigative practices performed by highly trained practitioners that use, tangible, physical items found, in, on, or around, a person’s body at a crime scene. The results of these efforts are typically used to support law enforcement and various courts as needed (Foster et al, 1997).

Traditional forensics analysis methods reside within a number of different disciplines to include, physics, chemistry, and biology. Within physics, behavioral patterns revealed by tests (polygraph, psychological exams) are focused on for the, recognition, identification, and evaluation, of physical evidence. Within chemistry, chromatography, spectroscopy, hair and fiber analysis, and serology, are focused on for the, recognition, identification, and evaluation, of physical evidence. Within biology, pathology, anthropology, odontology, toxicology, structural engineering, and examination of questionable documents, are focused on for the, recognition, identification, and evaluation, of physical evidence (Foster et al, 1997).

Computer forensics or cyber forensics is the application of investigative and analytical techniques. This measure is taken in order to, gather, preserve, and present, evidence from a particular computing device that is suitable preceding, during a legal bout in a court of law. The goal of cyber forensics is create a chain of documented evidence, during the structured investigation process; thereby, exposing exactly what happened and who was responsible for it on a particular computing device (“What is computer”, 2015).

To ensure the security, validity of evidence that will need to be used in court, there are basic criteria that need to be met. Any and all evidence must be kept free from being, damaged, destroyed, or otherwise compromised, during any of the processes, procedures used to investigate the computing device in question. Any and all extracted or possibly relevant data that is or can be construed as evidence is properly handled and protected from mechanical or electromechanical damage. The establishment and maintenance of thorough, proper documentation to include procedures and findings; such as, a chain of custody (Tsoutsouris, 2001).

The first step to take to ensure any and all evidence is kept free from being, damaged, destroyed, or otherwise compromised, during the investigation of a computing device is to create a back-up of the subject drive. This must be done prior to turning the machine on as there is a, potential, risk to data; such as, erasing file slack or swap files. This back-up is also known as, a clone, a bit-stream backup, or a mirror image. This type of back-up involves “the backup of all areas of a computer hard disk drive or another type of storage media (“Bitstream Copy”, 2015).

Prior to data-mining the back-up drive by the investigation team, they must ensure the media to which the data is being copied to (the clone) is free of any previous data and viruses. Some best practices include using anti-virus tools and then utilizing a secure delete program to ensure the media being cloned is empty and free of malicious software (Tsoutsouris, 2001).

Properly storing evidence in, evidence rooms, evidence lockers, or large evidence storage facilities, aids in keeping evidence free from mechanical or electromagnetic damages. Any of these storage mechanisms have proven to be well, maintained, documented, and orderly, and have helped keep criminals in prison (Marks, 2013).

The chain of custody is an essential step in ensuring the integrity and validity of evidence. The purpose of the methods established in the chain of custody is to trace the evidence from the crime scene to the courtroom and everywhere in between. Chain of custody is also known as maintaining the continuity of evidence. The tests for validity, of such a mechanism, is to prove that that a particular piece of evidence was at a particular place at a particular time in a particular condition. These tests not only apply to the hardware or physical evidence, but to the documentation as well. If at any point the chain of custody fails, the entire validity of the evidence could be compromised or found inadmissible in court (Ryder, 2002).

“The final step of documentation is simple to follow and crucial to a successful investigation and subsequent successful prosecution. Without it, the best evidence tools and experts will not be able to convince a judge and or jury that the evidence is sound. Once again, the Solitaire comes in handy as it prints a report at the conclusion of the cloning process which details the types of drives used as well as the confirming CRC check, the date of backup and the success of the backup. NTI and Encase also have similar utilities and reports are available in each of these software’s tools detailing times, dates and specifics of findings. The more documentation there is, the less likely that human intervention could alter data and corrupt evidence” (Tsoutsouris, 2001).

CONCLUSION

REFERENCES

Advanced Encryption Standard. (2015). Retrieved December 27, 2015, from <http://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm>

Bitstream Copy. (2015). Retrieved December 29, 2015, from http://www.edrm.net/resources/glossaries/glossary/b/bitstream-copy

Cryptography Quick Guide. (2015). Retrieved December 27, 2015, from http://www.tutorialspoint.com/cryptography/cryptography\_quick\_guide.htm

Data Encryption Standard. (2015). Retrieved December 26, 2015, from http://www.tutorialspoint.com/cryptography/data\_encryption\_standard.htm

Eckert, W. G. (n.d.). Introduction to Forensic Sciences, 1997, CRC Press.

Encryption And Its Importance To Device Networking. (n.d.). Retrieved December 23, 2015, from <http://www.lantronix.com/wp-content/uploads/pdf/Encryption-and-Device-> Networking\_WP.pdf

Federal Rules of Evidence, Article VII. (n.d.). Opinion and Expert Testimony, Rule 702 & Rule 703. Retrieved December 28, 2015, from [www.house.gov/judiciary/evid00.pdf](http://www.house.gov/judiciary/evid00.pdf)

Foster, K., R Huber. (1997). Judging Science: Scientific Knowledge and the Federal Courts, MIT Press.

Koehler, J. J., A. Chia, S. Lindsey. (1995). “The Random Match Probability in DNA evidence: Irrelevant or Prejudicial,” Jurimetrics Journal, Winter, pp. 201-219.

Marks, K. (2013, February 1). The Magazine for Police Management. Retrieved December 29, 2015, from <http://www.hendonpub.com/law_and_order/articles/2013/02/the_modern_police_evidenc> e\_room

Ryder, K. (2002). Computer Forensics – We’ve had an incident, who do we get to investigate? Retrieved December 29, 2015, from <https://www.sans.org/reading-> room/whitepapers/incident/computer-forensics-weve-incident-investigate-652

Safeguarding Networked Information. (1994). In Information Security and Privacy in Network Environments (p. 64). Diane Publishing Company.

Slaviero, M. (2010, January 4). Symmetric Encryption. Retrieved December 23, 2015, from <https://www.simple-talk.com/dotnet/.net-framework/symmetric-encryption/>

Triple Data Encryption Standard (Triple-DES). (2015). Retrieved December 26, 2015, from <http://www.vocal.com/cryptography/tdes/>

Tsoutsouris, D. (2001). Computer Forensic Legal Standards and Equipment. Retrieved December 29, 2015, from <https://www.sans.org/reading-> room/whitepapers/incident/computer-forensic-legal-standards-equipment-648

What is asymmetric cryptography (public-key cryptography)? - Definition from WhatIs.com. (2008, June 1). Retrieved December 23, 2015, from <http://searchsecurity.techtarget.com/definition/asymmetric-cryptography>

What is computer forensics (cyber forensics)? - Definition from WhatIs.com. (2015). Retrieved December 28, 2015, from <http://searchsecurity.techtarget.com/definition/computer-> forensics

What is Forensics? (2015). Retrieved December 28, 2015, from http://www.crimesceneinvestigatoredu.org/what-is-forensic-science/

What is Pretty Good Privacy (PGP)? - Definition from WhatIs.com. (2015). Retrieved December 28, 2015, from http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy