**Security Technology Tools II**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

INTRODUCTION

BODY

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.

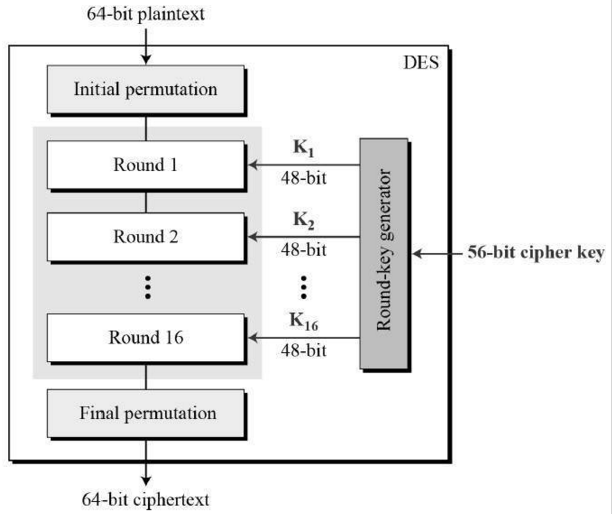


Figure 1: Data Encryption Standard (DES). Data Encryption Standard. (2015). Retrieved December 26, 2015, from http://www.tutorialspoint.com/cryptography/data\_encryption\_standard.htm

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.).

“Triple DES 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).

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.

ADVANTAGES AND DISADVANTAGES OF EACH ALGORITHM

EXAMPLES OF CHRIPTOGRAPHIC SYSTEMS THAT USE HYBRID TECHNOLOGIES

CONCLUSION

REFERENCES

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

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

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/

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