An Introduction to Block Cipher Algorithms and

Their Applications in Communication Security

An Introduction to Block Cipher Algorithms and

Their Applications in Communication Security

"The price of freedom is eternal vigilance." [3] Thomas Jefferson said that in the early 1800's and it still applies today as much as it applied back then. The rapidly growing need for an "unbreakable" or end-all of all encryption algorithms has been sought after since 1900 BC when the art of Cryptography was first developed. So far, that search has been in vain. There has yet to be an algorithm that is considered unbreakable. However, an algorithm is considered to be secure as long as there has not been found vulnerability through cryptanalysis. [6]

Block Cipher algorithms are a type of Symmetric Key Encryption. Symmetric Key encryption is a key-based encryption in which the same key that is used to encrypt sensitive data is used to decrypt the sensitive data. [15] The disadvantage of Symmetric Key encryption is that it only requires the person wishing to break the encryption to obtain only one key. For this reason, the key must be protected and secured. The key is often called a secret key. [9]

The process of sending secure transmissions with Symmetric algorithms becomes tedious, because you can't let the key become known. You would have to get the key to the recipient of your secure transmissions in a secure fashion, such as hand delivering the key. Many times, public key encryption methods are used to send the secret key generated by Symmetric Key algorithms. When the recipient has the key, you can encrypt messages and the recipient can decrypt them using the key that you gave to them. When they wish to respond, they can use the same key to encrypt their message and then you can decrypt the message with your key.

Many symmetric key algorithms use a construct called a substitution box, also known as an "S-box". [1] The purpose of the S-box is to protect the algorithm from linear and differential cryptanalysis by hiding how the cipher text is obtained from the clear text. It also adds to the diffusion property of the algorithm. Diffusion is when you alter a bit in the input, and it changes a number of output bits. [6]

Symmetric key algorithms are broken down into Block Cipher and Stream Cipher algorithms. [10] Block Cipher algorithms work by breaking up the message into smaller blocks and encrypting each block individually. The block size is typically 64-bits long. [11] Stream Ciphers, on the other hand, encrypt data one bit at a time. Stream Ciphers advantage is that they are much faster than block cipher algorithms, often several times faster.

Block Cipher algorithms can operate in many modes. [5] A block cipher algorithm can be a:

- Iterative Block Cipher

- Electronic Code Book Cipher

- Cipher Block Chaining

- Cipher Feedback

- Output Feedback

Iterative Block Ciphers are block ciphers that work by performing the same transformation over the same blocks. The iterations are often called rounds. A subdivision of Iterative Block Ciphers is Feistel Ciphers. [2] Feistel Ciphers are ciphers that perform the same transformation over the same blocks to obtain the cipher text from the clear text. Feistel Ciphers are also known as "DES-Like" ciphers

because of the method the Data Encryption Standard uses for the algorithm. The strength of an Iterative Block Cipher can be increased by increasing the number of rounds. The cost of doing so is decreasing the performance in time to encrypt and decrypt the data. Often the tradeoff is not worth it, because for some algorithms it would take too many rounds to make it considerably more difficult to break the encryption, so the algorithm designers often to weigh the consequences of increasing speed at the cost of strength, or increase the strength at the cost of speed. [8]

Electronic Code Book ciphers are ciphers that encrypt each block independently of each other. Electronic Code Book ciphers are faster than Iterative Block Ciphers and Feistel Ciphers. The advantage of encrypting each block independently of each other means that you can encrypt and decrypt the data in parallel. [12][8]

Cipher Block Chaining starts by seeding a random value and XORing that with the first block. Then that value is encrypted, and becomes the first block of cipher text. That encrypted block is also used to XOR itself with the next block. Then that value is encrypted and the process continues until there are no more blocks. The advantage is that everything is concealed in the XOR'ing process. Any random block gives no indication on what the other blocks are. [13]
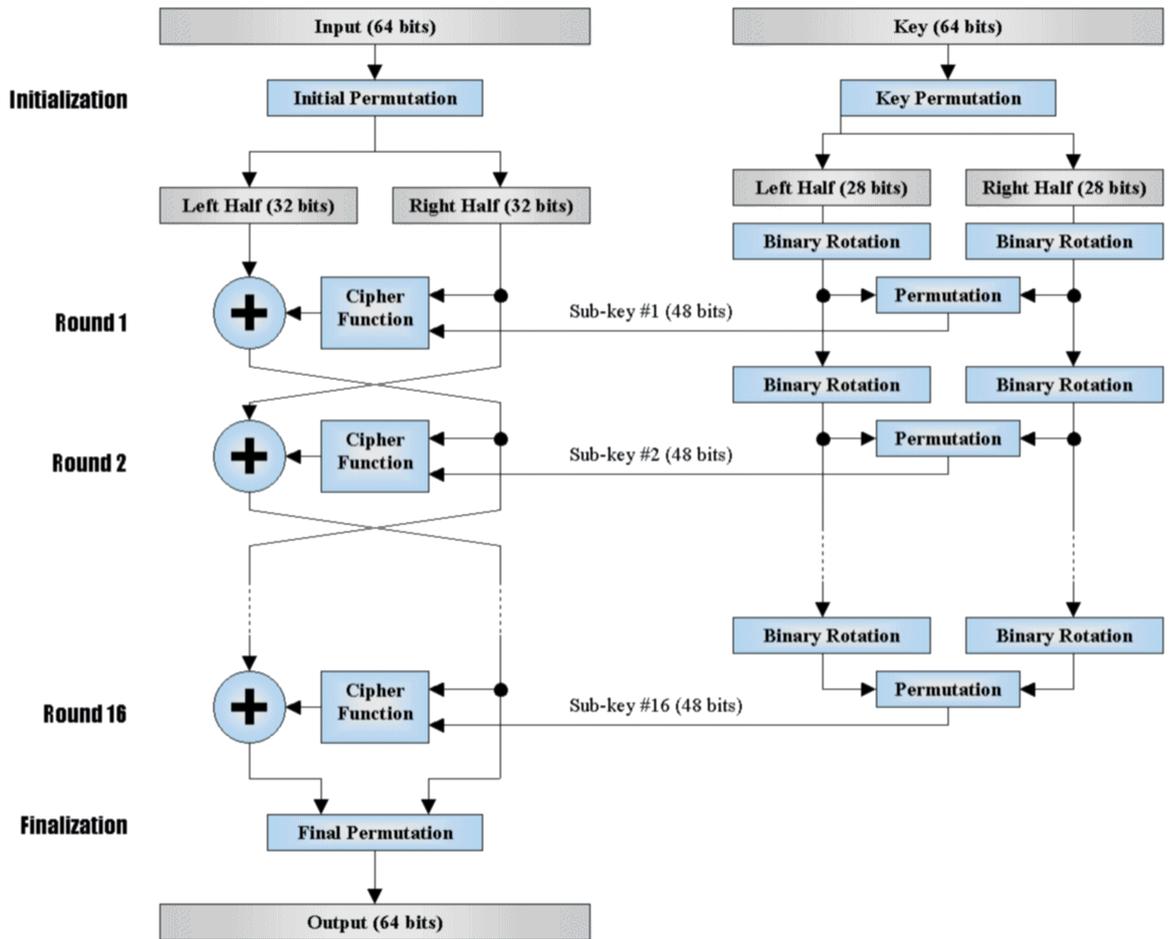
Cipher Feedback is similar to Cipher Block Chaining, but instead of encrypting the XORed block, it starts by encrypting the seeded value, and then XORing that with the first block. That becomes the first block of cipher text, and then that is encrypted and XORed with the second block. This process is repeated until there are no blocks. [8]

Output Feedback is similar to Cipher Feedback. Output Feedback begins by encrypting the seed and XORing that value with the first block of clear text to obtain

the first block of cipher text. The encrypted seed is then encrypted again, and then that value is used to XOR with the second block. This process is repeated until there are no more blocks. [8]

DES is one of the most popular encryption standards for Block Cipher encryption. DES stands for Data Encryption Standards and was released in 1974 by IBM when the Department of Commerce requested a general purpose encryption standard. DES works by breaking up the clear text into 64 bit blocks, and requires a 56-bit key. The block is then rearranged before it is sent through the algorithm. DES then starts on the first 64-bit input block and breaks it into 2 halves, a right and a left half.

The algorithm is a series of 16 transformations, which are called rounds. During the first round, the algorithm will transform the right half using a sub key generated by a series of operations that generates a 48-bit key from the original 56-bit key. Then it XORs the left half of the block with the new transformed block, and this becomes the new left half of the block. Then the algorithm swaps the left and right sides of the block and sends it through the next round. [14]

Input (64 bits) Key (64 bits)

Initialization Initial Permutation Key Permutation

Left Half (32 bits) Right Half (32 bits) Left Half (28 bits) Right Half (28 bits)

Binary Rotation Binary Rotation

Round 1 Cipher Function Sub-key #1 (48 bits) Permutation

Binary Rotation Binary Rotation

Round 2 Cipher Function Sub-key #2 (48 bits) Permutation

Binary Rotation Binary Rotation

Round 16 Cipher Function Sub-key #16 (48 bits) Permutation

Finalization Final Permutation

Output (64 bits)

DES was revised and then came Double-DES. Double-DES was found to be no more effective than DES, so Double-DES was revised and became Triple-DES. Triple-DES is performed by executing DES 3 times producing an effective key size of 168-bit. The vulnerability to DES become obvious when RSA Laboratories issued out a challenge entitled "DES Challenge II" and with a little over 56 hours and $250,000, DES was proven to be broken by the Electronic Frontier Foundation in 1998. [4] DES also has the vulnerability that the left side in a certain step is equal to the right side of the previous step. [7]

Block Cipher algorithms are subject to the same attacks that Symmetric Key algorithms are. Oddly enough, an encryption method is considered to be broken if it is

possible to derive the clear text in less than time than a brute force attack would. There are no limitations on the amount of storage that is required, the number of clear text and cipher text pairs you would need, or the time required, as long as it can complete the task faster than Brute Force, it will be considered to be broken.

Block Cipher algorithms are extremely important to Communication Security. Block Cipher algorithms are extremely simple to implement, relative to some Asymmetric algorithms. Block Cipher algorithms also have the advantage that it isn't difficult to encrypt and decrypt messages, because the same key is used to encrypt and decrypt. This is in comparison to asymmetric algorithms in which you have to have a separate public key for every person you wish to maintain secure transmissions with. The convenience, ease of use, and relatively secure algorithms are what make Block Cipher algorithms a good choice for Communication Security.

4/25/2005

Works Cited

1. http://en.wikipedia.org/wiki/S-box

2. http://www.freesoft.org/CIE/Topics/143.htm

3. http://www.samsimpson.com/quotes/cquotes.php

4. http://www.eff.org//Privacy/Crypto/Crypto_misc/DESCracker/

5. http://infosecuritymag.techtarget.com/2003/jan/algorithm.shtml

6. Katos, V., (2005). A Randomness Test for Block Ciphers. *Applied Mathematics*, Elsevier Publications.

7. Biham, Eli. (1997). An Improvement of Davies' Attack on DES. *Journal of Cryptology, 10*, 195-205.

8. http://www.rsasecurity.com/rsalabs/node.asp?id=2173

9. Whitman, Michael and Herbert Mattord. Principles of Information Security. Boston: Thomson Course Technology, 2005.

10. http://www.ssh.com/support/cryptography/introduction/algorithms.html

11. http://gnupg.unixsecurity.com.br/crypto-faq/Product_Ciphers.html

12. http://www.comp.mq.edu.au/units/itec855/lectures/03-secretkey-ovs.pdf

13. http://nexus.cs.usfca.edu/~brooks/S03classes/cs486/lectures/lecture-3.ppt

14. http://www.cs.usask.ca/grads/dtr467/400/

15. Campbell, Paul and Ben Calvert and Steven Boswell. Security+ Guide to Network Security Fundamentals. Boston: Thomson Course Technology, 2003.