Encryption

Throughout the development of technology, the world has changed in numerous ways. Rise of technology provided convenience and enabled humans to use precise techniques in a way that they earn profit. Especially the development of computer changed the entire human society. Back in the days, people did not worry much about protecting their privacy since privacy could be protected easily unless they spread out their own information. Now, most of our information is saved online for example, home addresses, credit card information and also personal information. It is aggravated to say that most of the information is exposed in the air in the cyber world. Users in the cyber world are easy to access to the information anytime they want unless it is being secured or protected.

In cyber security, database security is considered to be most important because information regarding person, credit card and communication are all included in the data. Database security share different characteristic: confidentiality, availability and integrity. Confidentiality prevents illegal access to the data and preserve the sender and the recipient, where availability determines the property of databases. Thus, integrity indicates that the data will not be contaminated in any situation. In the database security, there are four control systems that are tolerated by security which are: access control, information flow control, cryptographic flow control and inference control. Access control deals with all the accesses to the database, whether the access is illegal or authorized. Moreover, the access control regulates over internal or external attacks, and it also points out minor errors to fix the problem at its first place before the error turns into a major problem. Thus, it reduces the risk of main server to be disturbed or attacked. Information flow control is about the accuracy of information, if the data contains false information, it is leaded to high occurrence of data being disturbed or misused. Cryptographic control secures the data from a plain text to cipher text.

The most famous and efficient technique in order to protect information is by encryption. Encryption allows user to keep their messages secured and if desired it could be decrypted by the third user. Nowadays, data exchange and communication has been occurring in the cyber world more than it was used to be and cryptography with the certain key is being more practical. An original message is called a plain text, and when the plain text is encrypted with the
key it becomes a cipher text. Cipher text is not readable unless the user knows the key to decryption. When the cipher text is revealed or decrypted, it shows the original plain text. There are two types of cipher algorithms; block ciphers that are formed with fixed size block and stream ciphers which stream flows repeatedly for encryption and decryption. Fixed size of a block in a block cipher determines the size of n-bits of data, and the usual sizes of each block are 64 bits, 128 bits, and 256 bits. In a stream cipher, its algorithm encrypts a bit or byte of plaintext at a time using infinite stream from pseudorandom generator. In cryptography, symmetric encryption algorithm shares a single key between the sender and the receiver. The key is kept secret in order to prevent other user to decrypt the cipher text. In the other hand, asymmetric encryption algorithm shares two keys which are: private key and public key. Only the recipient knows the private key and the public key is shared to everyone.

There are three types of encryption level: storage-level encryption, database-level encryption and application-level encryption. Storage level encryption allows user to encrypt the data which already exists in the storage to be secured and prevent intruders from illegally reading the data. It is important to have every single data to be encrypted in order to reduce the risk of data being selectively encrypted. After the storage-level encryption, the database-level encryption is performed. It takes charge of database design and the encryption is done by tables, rows and column. Lastly, application-level encryption is done in the application, providing full resilience to the algorithm.

According to the reading passage, out of many encrypting techniques, mixed cryptography technique based on data classification methods has showed strength on protecting attacks at multiple levels due to containing multiples of keys to different users. Its technique also allowed user to secure data and as well as sensitive data. However, the access control was not defined in the technique causing minor confusion. Hash Security module encryption strategy can occur at both database level and storage level, containing stable security server. Also, there is a low chance of key being revealed to the public. However, hash security module encryption has a problem of being complex since users rarely use them as their encryption method.

In cryptography, there are total of 12 algorithms that are developed in encryption. DES(Data Encryption Standard) is a symmetric encryption algorithm that uses 64-bit blocks. Out of 64-bit keys, only 56-bit keys are the real key and remaining 8-bit key verify the integrity of the key. It was once the dominant symmetric-key algorithm however it is now outdated symmetric key algorithm. DES also doubles the length of the key which is 128-bit, and uses a decimal number to a modified algorithm. There are total of 16 rounds of repeating encryption progress and each round
contains ‘transportation’ and ‘substitution’ that will outcome the cipher text. DES is confirmed not to be safe as an encryption method because of rapid development of computer. DES was tested every 5 years for its stability until the suggestion of AES in year of 2000. 3DES(Triple Data Encryption Standard) is a method that applies DES algorithm three times to encryption using the same data. It is basically a Block cipher that uses 48 rounds, containing a key length of 168 bits. This technique is known to be slow in software because it requires three times of DES algorithm. Its algorithm contains two keys as an encryption key and used temporarily until the development of AES and. Instead of figuring out a single key, user needs to figure out two keys in order to decrypt the message.

The RSA is known to be the most important technique in public key algorithms. RSA is developed by three mathematician(Ron Rivest, Adi Shamir, and Leonard Adleman) and is named after the first letter of their last name (R, S, A). This system made it available to connect to Microsoft Window, Netscape, Lotus and many other software and has become the encryption standard of international institutes. Using asymmetric algorithm, it is formed with a block cipher which is composed of large integers like 1,024. Its technique is also known as public key encryption because a chosen integer gives outcome of two keys: public and private key. The reason why it comes with two outcomes is because even super computers takes more than a decade in order to encrypt the data with private key. In the other hand, public key can be used in most of the encryption in every aspect. In RSA algorithm, every user are to have the given value N(two multiples of integer)and the value of the public key is exposed to every user to be decrypted. Even though the RSA algorithm provides decent security, it consumes a lot of time for a system to encrypt or decrypt the data.

AES(Advanced Encryption Standard) is a symmetric key algorithm which is formed with three block cipher. It has replaced both DES and 3DES techniques and been recommended to be used for securing both data and information. AES was actually intended to be developed due to the weak security of DES. Developed by IBM, AES algorithm does not contain Feistel Cipher and the size of each block is 128-bit. Moreover, without a change in algorithm, the size of the block can increase to 192-bit, and 256-bit. During the encryption, the algorithm uses different round keys and the round transfers to every round until it reaches the desired value of a plain text. The purpose of the algorithm was to provide security within it could perform for 30 years, and 128-bit encryption block, and having a variety of key length.
ECC (Elliptic Curve Cryptography) is a new technique which applies the public key encryption. Its technique is based on the mathematical bond of elliptic curve and it provides keys that are more fast and efficient. ECC technique was developed by Victor Miller at the IBM lab and the decrypting method is still not defined. It provides high security with key that is lengthy short, calculates the signature rapidly and suitable for electronic devices that contains IC smart card. ECC can perform with the least bit which allows less energy with best performance. According to the reading passage, “an elliptic curve is a plane curve over a finite field (rather than the real numbers)” [1].

Following method is the Blowfish algorithm. Blowfish was the outcome by Bruce Schneier. Blowfish algorithm is a symmetric algorithm forming a block cipher with various length key from 32 bits up to 448 bits. The size of the block is 64-bits, and contains 16-round Feistel cipher. The algorithm has two parts: key expansion data encryption. Its algorithm came up instead of DES and IDEA algorithm, and because the algorithm contains wide range of key lengths, it has never exposed to an illegal attack.

Similar algorithm addresses the technique of Twofish technique. Twofish is the final version of DES algorithm which relies on Blowfish. The Twofish algorithm is also formed with block cipher and shares the key sizes of 128-bit, 192-bit and 256-bit. It is best performed when encrypting small data that has small capacity. Sometimes it is also used in the small processor such as smart card and it is also available to be chipped in the software and hardware. Despite of the fact that it provides decent security, the speed lacks compare to the blowfish.

Threefish algorithm is directly related to both Blowfish and Twofish algorithm, and it encrypts every single block of encrypted data. Threefish algorithm is developed in 2008, and it is a symmetric key block cipher. Because the key size shares the same size as the block size, there are three block sizes of 256-bits, 512-bits and 1024 bits. It applies 72 rounds in encryption.

RC5 (Rivest Cipher 5) is an algorithm designed by Ronal Rivest and it is directly related to the AES. It provides simple calculation to encrypt/decrypt messages and it is suitable for most of the hardware. RC5 algorithm consist of 32-bit, 64-bit and 128-bit and it is 10 times faster than the DES. Total of 12 rounds are suggested but maximum of 255 encryption rounds is available. It is a symmetric key block cipher that changes the plain text to cipher text within block sizes.
IDEA (International Data Encryption algorithm) was developed by James Massey and his student Xuejia Lai in 1991. IDEA algorithm has 64-bit block cipher and key length is 128-bit and consists of 8 rounds to outcome the result of 64-bit encryption. Every calculation is formed with 16-bit and since its algorithm is efficient in 16-bit processor it is often used in the key exchange. IDEA algorithm is confirmed to be the most secured and the fastest algorithm, it transfers blocks 177mb/s. However, it is found that IDEA algorithm has weakness in a typical keys that contains a lot of 0s causing an error.

Despite the fact of existence of many encryption algorithm techniques, there are always a risk of security being disturbed and illegally exposed. For example, a DoS attack (Denial of Service) shut downs the server and breaks the code itself to retrieve information. DoS attack is also known as the “Smurf Attack”, and it uses ICMP (Internet Control Message Protocol) Packet. The attacker aims the target IP address as a start-up point (IP Spoofing) and announced to the whole network with ICMP Request Packet. In other word, an excessive quantity of information is requested repeatedly without authority of administrators, confusing computer to work on the request but does not perform on other elements. Moreover, Dos attack can be powerful when there are more than a single host, allowing each hosts remote control their victims. Anonymity are very practical and many fake IP addresses allow attackers to be concealed and not be revealed. DoS attack consists short attack duration because the actual attack makes the server crash or fall within short period of time. Also, the attack is most likely happening to send more packets to the minorities, the individuals due to its popularity.

Also there are threat such as weak authentication strategy which allows data to be more exposed to the risk of attack. When there is weak authentication and there is no existence of certain administrator to the data, attackers find really easy to steal one’s data by breaking the code. There is also incident where the backup data is exposed to the threat of the attackers. This could be a major problem because once the data is stored in the data it becomes the original file and once the original data is stolen there is no way to retrieve it unless the user owns the copy of the original data. Database communication protocol is to perform to vary illegal access and data exploitation. It is critical to have the protocol perform vulnerable in order to determine different type of accesses whether it is authenticated or unauthenticated.