Hao Dong

Professor Llesh Miraj

CS 608

08 May 2019

The introduction of different security algorithm

Nowadays, the internet technology has become extremely mature and popular. The convenience the internet brought to us is making our life colorful and bright, but meanwhile, the weak password made the hacker and people who want to steal the information from others easy to do illegal thing online. The security problem is getting more and more important to everyone right now.

There was a report talked about the number of the data breach in some big companies in the past. MySpace company had nearly 260 million accounts breach and Yahoo voice had nearly half of a million usernames and unencrypted passwords. In the case of the Yahoo data breach, 59% of users were using the exact same password in the Sony service too. These data made us the realize how strong and important passwords are in the internet world, the stronger password the users have, the safer the accounts they will have. Using leaked usernames and password from one service to other services are called credential stuffing. Thus, it’s really highly recommended that people should use different password for every website or service. However, it’s really complicated and cumbersome for the users to generate unique passwords for every website and app by using a password manager. That’s why there’s another better way to have unique passwords for every website and it is recommended by security experts, it is having a security algorithm when we are creating passwords. That strategy is making the password easy to remember but difficult to guess.

In this article I want to introduce several security algorithms based on what I researched and learned online. First, I want to talk about the security algorithms based on Symmetric-key algorithm which include DES, RC4, RC5, AES. Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. It means encryption keys can be inferred from decryption key and decryption key can be inferred from encryption keys too. This kind of algorithms require senders and receivers have to make an agreement to have a certain key before they have secure communication to each other. Hence, the security of this algorithm really depends on the key, leak the key means anyone is able to decrypt the message they send or receive. Everyone should realize secrecy of the key is extremely important to the communicativeness.

DES means Data Encryption Standard, it has three inlet parameters: key, data and mode. Key has 7 byte and 64 bits, it’s the working key for DES algorithm; Data has 8 byte and 64 bits, it’s the data foe being encrypted or decrypted; Mode is the way how the DES work: encrypt and decrypt. DES algorithm converts the plaintext of input block with 64 bits to the ciphertext of the output with 64 bits. There are two steps for the DES algorithm. The first step is called initial permutation. The function of the initial permutation makes the input data block with 64 bits re-combine together based on the bits, and then it splits the output data block into two parts which are L0 and R0. The length of L0 and R0 are both 32 bits. The rule of this permutation is put the 58th bit of the input into the first bit; put the 50th bit of the input into the second bit. So, based on this rule, the last bit after permutation will be the original 7th bit. L0 is the left 32 bits part and R0 is the right 32 bits part. Maybe it’s too abstract to understand it for the readers, don’t worry, I can put an example here to help understanding. Let’s assume the input data before the permutation are D1D2D3…D64, so the result after the permutation will be L0=D58D50…D8; R0=D57D49…D7. The whole table can be listed below like this:

58,50,42,34,26,18,10,2,60,52,44,36,28,20,12,4,

62,54,46,38,30,22,14,6,64,56,48,40,32,24,16,8,

57,49,41,33,25,17,9,1,59,51,43,35,27,19,11,3,

61,53,45,37,29,21,13,5,63,55,47,39,31,23,15,7,

Afterwards, it will be the second step of the DES algorithm which is called inverse permutation. It means the input data will be L16 and R16 after the iterated operation for 16 times, then through the inverse permutation, the result will be exactly same as the inverse operation of the initial permutation which means the output of the ciphertext.

After introduced DES, time to talk something about RC4 algorithm. The principle of RC4 is “disorder”, it includes Initialize the algorithm and pseudo-random generation algorithm. During the process of initializing, the main function of the key is making the cluster of the initial number with 256 bytes shuffle, the different clusters of numbers are able to get different subkey sequence after the pseudo-random generation algorithm process. Then the subkey sequence and plaintext get Exclusive OR(XOR), the ciphertext will be shown up eventually. Since RC4 algorithm is using the XOR method, once the subkey sequence has the repetition, the ciphertext might be able to be cracked, but people haven’t found any possibility to have the repetition of RC4 with 128 bits, thus, RC4 is still one of the safest Encryption Algorithm in the world.

RC5 algorithm is a type of new algorithm, it has a word oriented structure: RC5-w/r/b(w: word length, it can be 16, 32 or 64 bits, to different length of the plaintext and ciphertext, the word length will 2w bits; r: Encryption rounds; b: the length of the key byte). Here’s the whole process of RC5 about encryption and decryption below, since RC5 is a type of the password algorithm with the changeable packet length, I will explain how it works based on the 64 bits packet (w=32). The first step is creating a key group. Copy the byte of the key into array data structure L with 32-bit word, then use the linear congruential generator to initialize the array data structure S. Since if i=1 to 2(r+1-1) of RC5, when the 16 bits word and 32 bits group, P will be 0xb7e1 and Q will be 0x9e37; when the 32 bits word and 64 bits group, P will be 0xb7e15163 and Q will be 0x9e3779b9; when the 64 bits word and 128 bits group, P will be 0xb7151628aed2a6b and Q will be 0x9e3779b97f4a7c15. Eventually, mix L and S which means i=j=0; A=B=0 by processed 3n times (where n is the maximum value between 2(r+1) and c, c is the number of the input key words). After finishing creating a key group, we are going to move to the encryption process. This process is for encrypt plaintext, when it’s encrypting, we need split plaintext into two 32 bits words A and B so that the output ciphertext will be the content in register A and B. The last step will be decryption process and it has the same method as encrypt which is split plaintext into two 32 bits words A and B and get the ciphertext content from the register A and B.

The last important Symmetric-key algorithm I want to mention is AES algorithm. The full name of AES is Advanced Encryption Standard, it is a standard to replace the original DES and it has been analyzed and used world widely. Compare to the previous standard DES, AES is faster at encrypt and decrypt on both software and hardware. That means it’s easy to be used in the real life and it needs less registers. The block length is always 128 bits and the length of the key can be 128 or 192 or 256 bits. AES encryption has a lot of rounds to repeat and transform. The whole process from key Expansion, to initial round, to rounds (every round includes SubBytes, ShiftRows, MixColumns and AddRoundkey), then ends at final round but without any MixColumn. Maybe the readers are not familiar with the terms like AddRoundkey, SubBytes, ShiftRows and MixColumns, I will explain it. The process of the AES encryption is running on the 4x4 byte matrix, it can be called as state. Its initial value is a plaintext block, then when it’s encrypting, every round of AES encryption loop except the last round will have 4 steps: AddRoundKey is every byte in matrix will XOR with the round key and every sub key is generated by key generation protocol; SubBytes is looking up table(LUT) via nonlinear substitution function so that replacing every byte to the corresponding byte from the table; ShiftRows means circular shift every rows in the matrix; MixColumns means mix all the columns completely by using linear transformation to mix 4 bytes on every column.

Since I finished introducing Symmetric-key algorithms, it’s time to talk about the coolest security algorithm in the world so far. The name is called asymmetric algorithm and RSA is the most well-known security algorithm in asymmetric algorithm. The reason why I said it’s the coolest is because this method was created by three guys who were working in MIT and there’s still no reliable method to attack the RSA algorithm, only the short RSA key can be possibly cracked. RSA is based on the simple truth of number theory: It’s really easy to multiply prime numbers to each other but it’s extremely hard to factorize the product of two prime numbers, so they are smart to use the product as the encryption key. There are three main parameters n, e1, e2 we need to pay attention where n is the product of the primer numbers p and q, the number of bits in binary system is the key length. e1 and e2 are relative to each other, but e1 can be a random number but it’s required that e1 and (p-1）\*(q-1）are coprime to each other; then when we are picking e2, it’s require that (e2\*e1）mod((p-1）\*(q-1））=1. Eventually,（n，e1）,(n，e2）will be the key pair. (n，e1）is the public key and (n，e2) is the private key. The algorithm of the encryption and decryption will be the exactly same. Let’s assume A is plaintext and B is ciphertext, then A=B^e2 mod n and B=A^e1 mod n. e1 and e2 are exchangeable which means A=B^e1 mod n and B=A^e2 mod n.

Those stuff I wrote above are what I did research for the security algorithm. It’s a good chance to get to know more about the security stuff because I am interested in the cyber security. Also, it’s always good to learn how the security algorithm works, because everyone should realize the secrecy for prevent the data of the user got read by others, the data integrity for prevent the date got edited by others, the authentication for make sure all the data are sent from the certain side are important to care about, so that our privacy are able to be protected in 21 century when the internet technology is extremely mature nowadays.