Reynaldo Ortiz

Module Four Algorithm Ciphers

CS-305 Software Security

1. **Algorithm Cipher**:
   1. Consider security protection best practices to defend against various types of security attacks.
      * My recommendation would be the use of the Advance Encryption Standard (AES) since it is the most well-known method of security when involving the internet since it can protect against well-known security risks.
   2. Consider and identify all the risks in your recommendation.
      * Although AES is a symmetric encryption that large companies widely use because it is hard to crack, it has some shortcomings. This means the system uses one key to encrypt and decrypt. The key could be stolen by using an unsecured network by being intercepted through your phone or your PC, allowing them to decrypt any files.
   3. Consider the most current government regulations and how they will be met.
      * The government has established regulations that are in place, providing standardization for corporations that they must meet to protect their data and clients' data. This is not 100 % secure; however, it has saved the industry billions of dollars in liability fees. This is why the government requires secure AES since it is currently what large corporations, groups, and organizations use.
   4. How will this algorithm cipher be used?
      * This algorithm cipher can be used to send or receive files of information, pictures, and documents to another person while connected to a secure network, allowing the receiver to view the report. This also will not allow anyone that can intercept the information to be able to view the data without the key.
   5. What is the best cipher, and why?
      * In my opinion, AES is the best cipher out there today since it is considered one of the most difficult to break, making it efficient against all forms of attack.
   6. What are the reasons why you might not choose the most secure cipher?
      * There is no reason not to choose the most secure cipher. However, we need to keep in mind as computers become a lot more sophisticated and faster, intercepting data becomes more effortless. Therefore, the need to update the cipher or develop a better alternative will always be in demand.
2. **Justification**:
   1. What is the purpose of the cipher's hash functions and bit levels?
      * Hashing is a one-way process where the input is digitized and then disarranged using an algorithm. Due to that, it is known as a one-way algorithm since once it is disarranged, it is nearly impossible to re-arrange even with the algorithm. On the other hand, Bit-level encryptions are a two-way process. This means that the correct algorithm can decode the information, allowing a safe and secure sharing of information between two parties.
   2. Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.
      * While symmetric uses a private key to encrypt and decrypt any message, the key is shared. While non-symmetric or Asymmetric encryption uses a public key from the receiver to encrypt the message.
   3. Describe the history and current state of encryption algorithms.
      * One of the first known proofs of using cryptography was found in an inscription carved in the tomb's main chamber of the nobleman Khnumhotep II in Egypt around 1900 BC. Julius Caesar, back in 100 BC, was known to use a form of encryption to send secret messages to his Generals on the war front. Caesar’s cipher is the most mentioned in cipher history. The first cipher to use an encryption key was invented in the 16 century by Blaise de Vigenère. In the 19th century, Edward Hebern designed an electro-mechanic contraption called the Hebern rotor machine. The machine used a single rotor, with the secret key embedded in a rotating disc. This way, the key encoded a substitution table, where pressing from the keyboard resulted in the output of the cipher text. The Germans invented the enigma machine during WW1 and used it during WW2. The machine used various rotors to rotate at different rates as the user typed on the keyboard, outputting appropriate cipher letters. In the 70s, IBM formed the crypto group due to the demands of customers who were looking for some type of encryption. They designed a cipher called Lucifer. In 1973, the Nation Bureau of Standards (now called the National Institute of Standards and Technology) requested proposals for a block cipher that would become a national standard. They went with Lucifer which then was called Data Encryption Standard or DES. In 1997 and forward, DES was broken by extensive attacks, the problem being the small size of the encryption key. As computers became more sophisticated, it became easy to break all different combinations of keys to get a plain text message. Because of it the NIST in 1997 again put out a request for proposal for a new block cipher, which received over 50 entries. In 2000, they accepted Rijndael’s cipher and renamed it the Advanced Encryption Standard or AES. AES is still today a widely accepted standard used for symmetric encryption.