2020

CMPG215 ENCRYPTON PROGRAM

LECTURER: PROF. NEELS KRUGER

Janus Roestenburg 31611044

lLEWELLYN ANTHONY 32969694

dERICK FRITZ 30015219

FATHIMA DINDAR 31625185

DIRK STEYN 32521723

AAKIB PATEL 31825869

**Encryption algorithm**

The algorithm uses all the ASCII characters for encryption. The user enters a password, which will be used to encrypt a file. The program uses the length of the password to determine the ASCII combination to be used in the encryption. The key is then scrambled by an algorithm into different characters. The encryption program then runs through the bytes of the selected file changing the value of each byte by the length on the key on the ASCII table. The key determines the functional input and output of the cryptographic algorithm.

During the decryption process the same password must be used again in order to decrypt the content in a selected file. The program makes use of symmetric keys, thus if a different key is used to decrypt the data, plaintext file content will not be written to a decrypted file. The program then runs through all the bytes a file contains, changing characters back to their original position on the ASCII table.

A more in-depth explanation of how our program works:

1. Two methods named EncryptFile and DecryptFile are used to encrypt and decrypt files, respectively.
2. Each of the methods call another method named CryptFile, which is used to encrypt or decrypt a selected file, based on the Boolean parameter of the method (true encrypts a file, false vice versa).
3. The Cryptfile method also make use of byte arrays and hexadecimal strings to encrypt content in a file.
4. The method creates a new AesCryptoServiceProvider to use the AES encryption method.
5. This method creates input and output streams attached to the input and output files. It then passes them to the following CryptStream method to do all of the real work.
6. The CryptStream Method receives a key, input stream, output stream and a bool value determining whether the stream should be encrypted as arguments.
7. The encryption algorithm finds a valid key size for the stream. Then it finds the correct block size for the stream input.
8. An encryptor or decryptor object is created, depending on the type of stream used.
9. The stream allows content to be encrypted or decrypted and writes it to a file.
10. A stream reads all content from the files and display it in textboxes.

The program basically makes use of a cryptographic service provider and attach it to a stream. As you write into the stream, the provider automatically encrypts or decrypts the data. the program must make a key and initialization vector (IV) to initialize the service provider. It starts by finding a supported key size. It starts with a key size of 1,024 and reduces it until the provider’s ValidKeySize method returns true. The key size you get will depend on things such as which version of Windows you are using. The program then calls the MakeKeyAndIV method to create a key and IV. The salt is an array of pseudo-random bytes that you initialize to make breaking the code with a dictionary attack harder. This code creates a new Rfc2898DeriveBytes object, passing its constructor the entered password, salt, and an iteration number. The object applies its operation for the indicated number of iterations to make its result more random. The method then uses the object’s GetBytes methods to get the key and IV bytes that the program needs to initialize the cryptographic service provider. The user browses for a file to encrypt, the file content gets encrypted and stored to a new directory chosen by the user. The user can decrypt the file content if they want to and choose a new directory again to store the decrypted file content. All file content is read from a stream and displayed in textboxes, but the user can view the file content in the directories as well.

The program also uses a simplified version of the algorithm that only stores encrypted and decrypted files directly, without viewing any file content, to demonstrate the different ways AES can be implemented. A byte array is declared storing 256 values, after that a loop is executed converting each integer position of the array to its corresponding byte value. A byte matrix is initialized as well, each row of the matrix contains a character from the byte array, with each row beginning with a value in the corresponding index of the matrix. The program reads all byte content from the chosen file and password, a new key gets generated based on the byte values of the password. Based on whether the file should be encrypted or decrypted, the program loops through all the file content and assign the corresponding ASCII or byte value to each character in a file, based on the values of the byte array. All content is stored in the matrix and written to a new file stored in a directory chosen by the user. This part of the program makes no use of any input or output streams, as well as the AesCryptoServiceProvider.

**Salted Password**

The encryption program our group wrote makes use of a salted password. This means passwords are stored using a uniquely generated hash. Salted passwords are harder to acquire through potential attacks and hashed passwords ensure that no one gets access to a plaintext password in order to encrypt/decrypt files.

**Advantages**

The main strength of our algorithm is the salted password. Because the length of the password is changed when it is stored in a salted format, and due to the fact that hashing is a one-way function, potential attacks to gain access to passwords will not be of any use to hackers, since they don’t know the length or value of the password. Due to the length of AES key sizes, it makes the algorithm more robust against hacking. For a 128-bit key only, it takes about attempts to break a password. This makes it difficult to hack and as a result makes it a very safe algorithm to use to encrypt your data.

**Disadvantages**

Because the program uses the contents of the ASCII table to encrypt files it means that each file has 256 different code combinations it can use to encrypt files with. If potential threats were to gain access to encrypted files all they will have to do to decrypt the files is run a decryption algorithm using all 256 variations of key lengths to discover the true data. Besides the abovementioned, it uses a very simple algebraic structure and every block is encrypted in the same way. As one can see, within our program it was very hard to implement the AES algorithm.

**Reasons for the use of AES**

As a group we’ve decided to make use of the AES (Advanced Encryption Standard) algorithm as it is said to be the best encryption method due to the fact that it was created by the US National Institute of Standards and Security. Furthermore, when looking for confidentiality and integrity, AES is better than most other encryption algorithms and is considered impenetrable to all other attacks besides brute force.

**Difference Between AES and DES**

* DES was created during the 1970’s while AES, the successor to DES, was created in the 1990’s.
* While the normal text block is divided in half in DES before the main algorithm starts, in AES in order to obtain the cipher text the entire block is processed.
* DES has a smaller key size while AES has a larger key size.
* The plain text in DES is of 64 bits whereas the plain text in AES can be either 128, 192 or 256 bits.
* DES is generally slower than AES.
* DES has a smaller key while AES has a larger key which makes AES more secure.

**References**

Allan, M. 2019. *6 Types of Encryption that you must Know About*. Viewed 16 May 2020. <https://www.goodcore.co.uk/blog/types-of-encryption/>

Bradford, C. 2019. *5 Common Encryption Algorithms and the Unbreakables of the Future*. Viewed 16 May 2020. <https://blog.storagecraft.com/5-common-encryption-algorithms/>

Pornin, T. 2011. *Comparison of DES, Triple DES, AES, blowfish encryption for data.* Viewed15 May 2020. <https://stackoverflow.com/questions/5554526/comparison-of-des-triple-des-aes-blowfish-encryption-for-data>

RF Wireless World. s.a. Advantages of AES | disadvantages of AES. Viewed15 May 2020. <https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html>

Stephens, R. 2014. Encrypt or Decrypt Files in C#. Viewed15 May 2020.

<http://csharphelper.com/blog/2014/09/encrypt-or-decrypt-files-in-c/>

TECHDIFFERENCES. 2016. Difference Between DES (Data Encryption Standard) and AES (Advanced Encryption Standard). Viewed 17 May 2020.

<https://techdifferences.com/difference-between-des-and-aes.html>

Wahid, M.N.A. Ali A, Esparham, B. Marwan, M. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. *Journal of Computer Science Applications and Information Technology*, 3(2): 1-7.