Cracking Advanced Encryption Standard-A Review

Jashnil Kumar, Mohammed Farik

Abstract: Password protection is a major security concern the world is facing today. While there are many publications available that discuss ways to protect passwords and data, how widely user from around the world adhere to these rules are unknown. The novelty of this study is that this is the first time a review is done on software tools that can be used to crack Advanced Encryption Standards. Firstly, the study does a review on top 10 software tools that are available to crack Advanced Encryption Standards. After which an analysis on two software tools was performed to see how long each software tool took to crack a password. The result of the study gives Advanced Encryption Standard researcher, Network security researcher, and the general public helpful information on how to strengthen advanced encryption standards and strengthen passwords that are hard for the software tools discussed above to crack.

Index Terms: Advanced Encryption Standard, AES Cracking Software Tools, Brute-Force, Cracking Passwords, Password Cracking

1 Introduction

Computer security is a trending topic in the world today, millions of dollars are used every year to achieve the security goals, and hundreds of researches are currently underway to solve the problems of network security. According to Steve Morgan, the Founder, and CEO at Cybersecurity Ventures, by the year 2021, the amount wasted on cybercrime damages would be $6 Trillion [1]. One of the major way to safeguard network security is through Cryptography. Cryptography uses codes and ciphers to guard keys, messages, password, and other secret messages. The usage of cryptography began thousands of years ago, from classic cryptography to the recent modern cryptography [3]. Before the development of public-key encryption in the 1970s, symmetric encryption was the lone form of encryption in use [2]. At present Symmetric encryption and public key is mostly used [4]. Symmetric encryption is given several names such as secret-key, single-key encryption and conventional encryption [2]. Symmetric encryption has three chief block encryption algorithms, these are Data encryption standard (DES), Triple DES (3 DES), and Advanced Encryption Standard (AES) [2]. In this paper, we identified and reviewed available software tools that can crack AES. Section 2 of this paper will provide a brief explanation on symmetric encryption and Symmetric Encryption Model. Section 3 of this paper explains Advanced Encryption Standard. Moreover, Section 4 of this identifies and reviews the existing software tools that can crack Advanced Encryption Standards (AES) and provide a summary in the table. Section 6, of the research, focuses on the experiment of the software tools. Furthermore, section 6 of the paper provides recommendations of how to create a password that is hard to crack, and the paper concludes in Section 7.

- *Jashnil Kumar is currently pursuing post graduate diploma program in Information Technology in the School of Science and Technology at The University of Fiji. Email JashnilK@unifiji.ac.fj*
- *Mohammed Farik (Member IEEE) is a Lecturer in Information Technology in the School of Science and Technology at The University of Fiji. E-mail: MohammedF@unifiji.ac.fj*

2 Literature Review

2.1 What is Symmetric Encryption?

Symmetric Encryption basically consists for five (5) main components. These are Plaintext, Encryption algorithm, Secret Key, Ciphertext, and Decryption algorithm (See Fig. 1) [2] [9] [4].

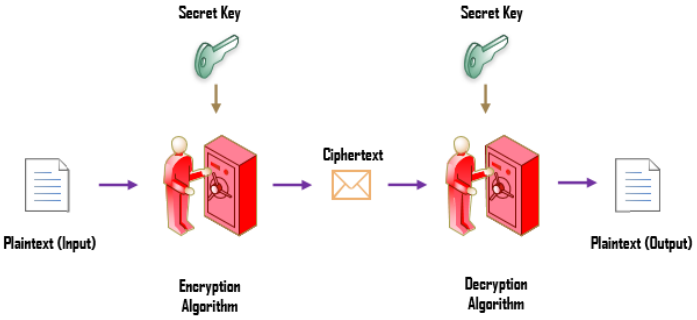

Fig.1 *Symmetric Encryption Model*

Firstly Plaintext, is an example of any data or message, that you would like to send or use, for example, a password. The Second component, the Encryption algorithm is a procedure that accomplishes a number of substitution and transformation onto the plaintext being used. The third and most vital component is the Secret Key, it is a contribution to the algorithm being used. The secret key is very vital as substitution and transformation solely depend on these keys. The fourth component is the Ciphertext, this is essentially the message formed as output once the substitution and transformation have occurred. The last component of symmetric encryption is the Decryption algorithm, this is basically the opposite of encryption algorithm. It takes into account the third and fourth component, Secret Key and Ciphertext respectively, to produce the original message as plaintext again [2] [9] [4]. In order to use symmetric encryption in a secure way, a user must keep in mind the two (2) requirements: these are, firstly, the need for a strong encrypting algorithm. The algorithm should be strong enough that even if another person may have access to the algorithm or ciphertext, he/she must not be able to decipher it, or even work out the key. Secondly, the secret key must be communicated by both the sender and received in a secure way, and kept in a safe place, where no one except the user has access [2] [9].

3 Advanced Encryption Standards

3.1 What is Advanced Encryption Standards (AES)?

Advanced Encryption Standards was introduced by United States National Institute of Standards and Technology in the year 2001 [2]. The main aim for the development of AES was to replace it with Triple DES (3 DES) [2]. This was because Triple DES (3 DES) uses 64- bit block size and was also slow. In the year 1997, United States National Institute of Standards and Technology issued a call for paper, after shortlisting 5 algorithms in August 1999, Rijndael algorithm was selected in 2000 [2] [8]. The Advanced Encryption Standards was developed by two Belgians cryptographers, Joan Daemen and Vincent Rijmen [5]. On November 26, 2001 Rijndael algorithm, was declared as the new standard for encryption by Federal Information Processing Standards Publication 197 Advanced Encryption Standards is grounded on the Rijndael Ciphers [2]. Advanced Encryption Standards has 128/192/256 keys and a block size of 128-bit compared to 64- bit block size of Triple DES (3 DES) [2] [8]. AES is now used worldwide and is also adopted by the US Government [5].

3.2 Cracking Advanced Encryption Standards (AES)

Avram Noam Chomsky, an American Philosopher, and Scientist argued that Somebody will be able to overcome any encryption technique you use [6]. At present, there are many free software tools that are available on the internet for cracking Advanced Encryption Standards. Using this software's anyone can crack an Advanced Encryption Standards; however cracking Advanced Encryption Standards may take time.

4 Review On Software That Can Crack AES

To begin with, software programmers lately have been trying to generate algorithms that can crack the password in less possible duration. Dozens of algorithms or software tool have already been developed and is used for cracking encryptions [7]. However, each tool comes with its own pair of advantages and disadvantages. In this section of the paper, I will discuss ten (10) most popular cracking software tools. The software tool tagged as most popular is Brutus. Brutus is an online available cracking tool, marked as the fastest and most flexible tool, was released way back in October 2000, since then there was hardly any update done to the version of software. Brutus allows HTTP (Basic Authentication, HTML Form/CGI), POP3, FTP, SMB, Telnet, Brutus also allows to create an authentication type to suit your need. It also has an interesting feature that is the resume and load option, using this option a cracker pauses and resume the attack whenever he wants to. As of now, Brutus is only compatible with Windows System [7] [13]. The second software tool that I will discuss is Rainbow Crack. Rainbow Crack uses large-scale time- memory trade-off procedure for quicker password cracking compared to brute force. Hash Algorithm uses plain text and hash pairs to compute time- memory tradeoff. After this is computed all the results obtained are stored in a rainbow table. This is quite a long and time-consuming phase, however, once this is completed, cracking can be done much quicker [14]. Rainbow Crack is compatible to be used with Windows and Linux Systems [7]. The third software tool is Wfuzz. Wfuzz is also a free software tool that is available online to crack AES, it cracks passwords with the help of brute force. The software tool can also assist a user to recover or locate hidden resources, such as directories, files, and scripts. The software is also helpful in identifying injections in web applications [15]. The key features of Wfuzz cracking tool include: multi-threading, brute force HTTP Password, cookies fuzzing, and post, headers, and authentication data brute forcing. Wfuzz is compatible to be used on only Windows and Linux platform [7]. The fourth software tools that can crack Advanced Encryption Standards (AES) is Cain and Abel. Cain and Abel is a well-recognized cracking tool which is proficient in handling a lot of responsibilities. Cain and Abel work as sniffers in the network [17]. It cracks password using the dictionary attack, recording VoIP chats, brute force attacks, cryptanalysis attacks, revealing password boxes, discovery cached passwords, decrypting scrambled passwords, and examining routing procedures [7]. The software tool does not use any kind of a bug or viruses; however, it covers weakness in security, through which it grabs the passwords. This software is only available for Windows platform and can be downloaded free of cost [7]. Furthermore, another software tool which is well known and mostly used is John the Ripper. John the Ripper is a free software tool that can be downloaded from the internet. John the Ripper was initially designed for Unix platform, however today it can be used for windows, Mas OS X, Linux, and Unix. John the Ripper has many advanced features, it contains a number of password crackers [7] [17]. The sixth software tool I will discuss is THC Hydra. The program was developed by Van Hauser and supported by David Maciejak. It is known for fast network cracking tool. The tool is absolutely free and can be downloaded from the internet. THC Hydra is compatible with Linux, Solaris, Windows, OS X. The makers have also asked new developers to assist in making the current version more useful [7] [11] [12]. Moreover, the seventh software tool I will discuss is Medusa. Medusa is very much same as THC-Hydra. However, the software tool is command line, that is in order to fully use the tool you need to learn the commands that are to be used. Medusa has the capability to test around 2000 passwords in a minute, provided it is on a local system. The tools also have the feature to do parallel attacks, for instance, cracking passwords of a handful of emails at the same time. Medusa is compatible on Linux, Windows, Sun OS, Mac operating system [7] [17]. Medusa is a free software tool that is available on the internet, which can be downloaded by anyone [7]. The eight-software tool which I will discuss on is OphCrack. OphCrack bit similar to Rainbow crack, the reason because it is rainbow-table based. OphCrack is a windows software but it can also run on Linux and Mac System. The software tool together with a live CD (tutorial) is available on the internet to make the cracking procedure easier [7] [16]. The second last software tool that I will discuss is the LOphtCrack. LOphtCrack is a substitute of OphCrack. LOphtCrack uses active directory, primary domain controller, network servers and Windows workstation to crack. LOphtCrack was attained by Symantec and obsolete in 2006, however, Later LOpht inventors again re-acquired it and launched it again in the year 2009 [7] [17]. LOphtCrack is a free software tool that is available on the internet [7]. The last software which I will discuss is Aircrack-NG. Aircrack-NG is a Wi-Fi cracking tool, it is a free software tool to crack the password, it is capable of cracking WEP and WPA Passwords. It firstly analyses the encrypted packets before catching the passwords, by its algorithm. Aircrack-NG is a Linux and Windows based systems. A tutorial CD is also available on the internet to make the cracking procedures easier and quick [7].

So basically, these are the free software tools that can be used to crack Advanced Encryption Standard, however, the time limits are not guaranteed or but can always be predicted either manually or using the software.

TABLE 1

COMPARISON OF TOP TEN SOFTWARE CRACKING TOOLS

Software Tools	Free		Operating System			Tutorial Available	
	Yes	No	Windows	Linux	Mac	Yes	No
Brutus	☑		☑				☑
RainbowCrack	☑		☑	☑			☑
Wfuzz	☑		☑	☑			☑
Cain and Abel	☑		☑				☑
John the Ripper	☑		☑	☑	☑		☑
THC Hydra	☑		☑	☑	☑		☑
Medusa	☑		☑	☑	☑	☑	
OphCrack	☑		☑	☑	☑	☑	
L0phtCrack	☑		☑				☑
Aircrack-NG	☑		☑	☑		☑	

5 ANALYSIS OF SOFTWARE TOOLS

This research conducted an experiment based on two software tools that are widely used, these tools are Brutus and THC Hydra to crack an email. The research conducted a brute force attack using Brutus software, after which both software's were used to carry out an experiment using wordlist (rockyou.txt) downloaded from the web. Firstly, a Gmail account was created. The Username and password were noted down. Secondly, using Brutus software brute force was applied in order to crack the mail. The range specified for brute force attack was [qwertyuioplkjhgfdsazxcvbnmQWERTYUIOPASDFGHJKLMZXCVBN1234567890], the minimum character was set to 8 and the maximum character was set to 16. After which it was executed. As soon as it was executed the messaged showed that brute force will generate 981761686100049920 passwords (see Figure 2). After the message, the program halted, because it takes a lot of time, approximately some billion years.

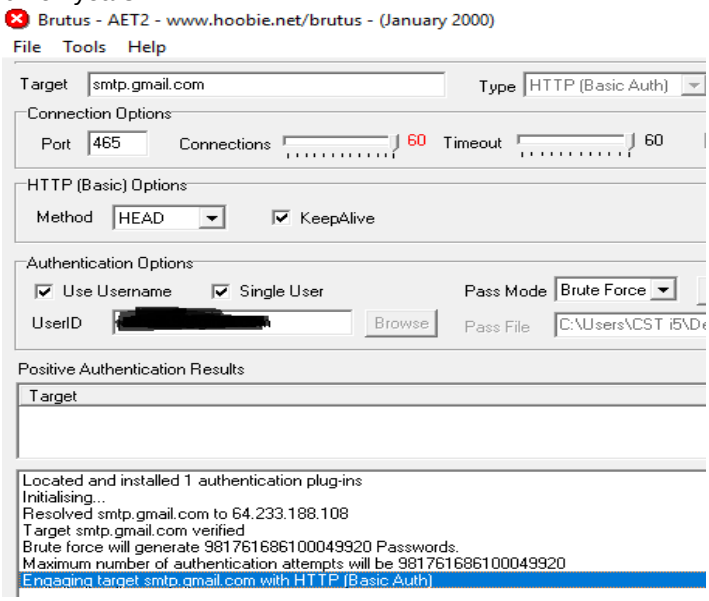

Fig.2 *Brute Force Result*

Moreover, another set of research was carried out this time with the help of wordlist (rockyou.txt). This text file was downloaded from the internet. First, the research was conducted using THC Hydra. Basically, this experiment was done in command prompt. After all the codes that were required were written in command prompt, execution began. Each password that is predefined in the text file were checked until the correct password was found. After this, the execution stopped (see Fig. 3 & Fig. 4).

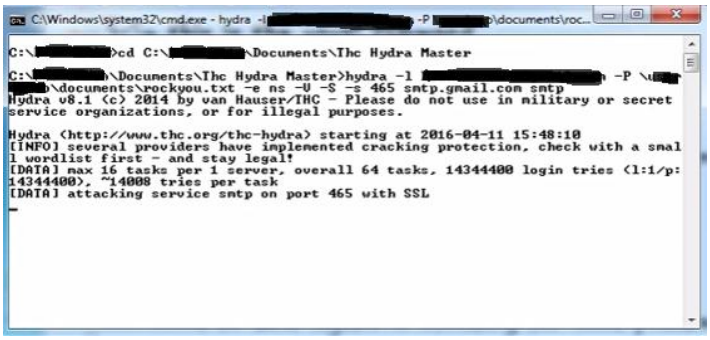

Fig.3 *THC Hydra Word List Approach Execution*

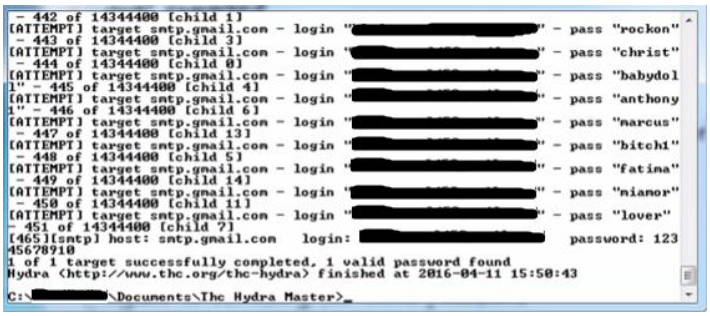

Fig.4 *THC Hydra Word List Approach Result*

Furthermore, using the same text file (rockyou.txt) the experiment was carried out with Brutus. Brutus did not require to use command prompt as it is a simple windows form application. All the necessary fields were entered, and execution began, however it took a lot of time, and at times the program stopped responding (See Fig. 5).

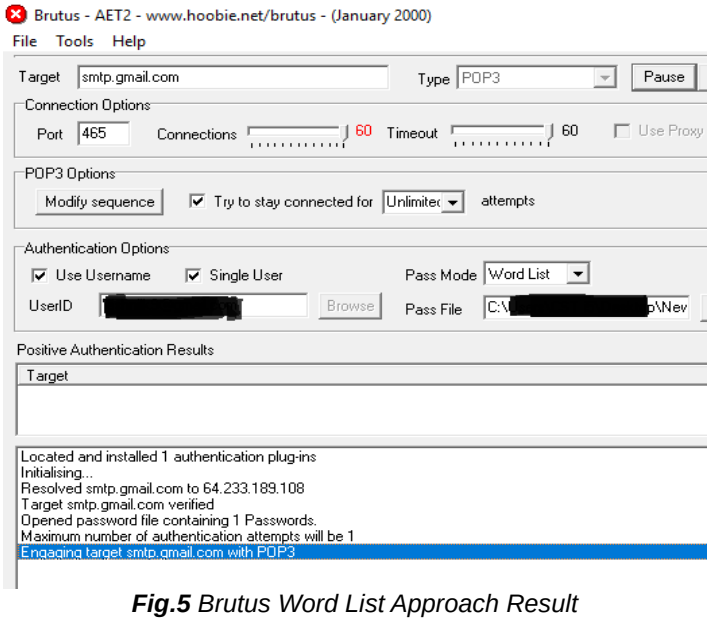

Fig.5 *Brutus Word List Approach Result*

THC Hydra is better software to use while comparing the two, even though you need to use the command prompt, it is simple provided you know the syntax of code. THC Hydra is fast and as well as convenient to use, and cracks password more quickly, provided the password is available in the word list, compared to Brutus. Brutus on the other hand is an outdated version with no update since 2000, this may be cause of software rapidly not responding.

5.1 Systems Used for Experiment

For experiment purpose, Intel® Core™ i5-6600K CPU @ 3.50GHz was used. The operating system used for the experiment was Windows 10 64-bit (See Fig. 6).

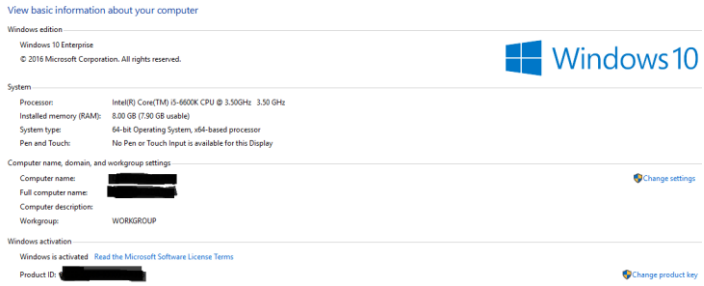

Fig.6 *System Used for Experiment*

6 Recommendation

There are many ways in which you can make you password safe and hard to crack. Firstly, there are many online available tools to check the strength of the password. Make use of that and always check the strength of the password, if they are weak change it. Secondly, keep a long password, the length of the password is very vital. If the password is short the cracking time will be less, however, if the length of the password is big, the cracking time increases [7]. Thirdly, try to use combinations of numbers, special characters, and characters when setting up a password [10]. While cracking software tools check combination, suppose if you have alphabetical character only in password, the tool only needs a combination from a-z, however if you use different characters the combination to guess will increase making it hard to crack the password, moreover there are many things to avoid while setting up a password, these are: never use word that is directly from the dictionary, avoid the usage of sequence and patterns, and avoid using names of families and relatives [7].

7 Conclusion

As I discussed earlier in the paper, the quote from Avram Noam Chomsky, explained somebody will be able to overcome any encryption technique you use. In this paper, I discussed several software tools that are available on the internet for free to use and crack Advance Encryption Standards (AES), therefore, to some extend the quote seems to be true, as these software's can easily crack password and obtain data and information that do not belong to them, for instance stealing credit card details from banks and then using the credit card information (PIN Number) to do shopping without the bank and the credit card holder having knowledge about it. However, there are always several measures that could be taken to overcome this problem and also secure your data from intruders.

References

[1] IDG Communications, Inc., (2017). Cybersecurity Business Report. Top 5 cybersecurity facts, figures, and statistics for 2017. [online] Available at: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html [Accessed 30 Mar. 2017].

[2] Stallings, W. (2011). Network security essentials. 4th ed. Boston27-55: Prentice Hall, pp.27-55.

[3] En.wikipedia.org. (2017). History of cryptography. [online] Available at https://en.wikipedia.org/wiki/History_of_cryptography [Accessed 30 Mar. 2017].

[4] Docs.aws.amazon.com. (2017). How Symmetric Key Cryptography Works - AWS Key Management Service. [online] Available at: http://docs.aws.amazon.com/kms/latest/developerguide/crypto_overview.html [Accessed 30 Mar. 2017].

[5] Rijmen, V. and Daemen, J., 2001. Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, pp.19-22.

[6] BrainyQuote. (2017). Encryption Quotes - BrainyQuote. [online] Available at: https://www.brainyquote.com/quotes/keywords/encryption.html [Accessed 31 Mar. 2017].

[7] Shankdar, P. (2016). 10 Most Popular Password Cracking Tools. [online] Infosec Institute. Available at: http://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref [Accessed 30 Mar. 2017].

[8] Kotfu.net. (2017). What does it take to hack AES? | kotfu.net. [online] Available at: https://www.kotfu.net/2011/08/what-does-it-take-to-hack-aes/ [Accessed 30 Mar. 2017].

[9] Techopedia.com. (2017). What is Symmetric Encryption? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/1789/symmetric-encryption [Accessed 30 Mar. 2017].

[10] Farik, M. and Ali, S., 2015. Analysis Of Default Passwords In Routers Against Brute-Force Attack. *International Journal of Scientific and Technology Research, 4*(9)

[11] Tools.kali.org. (2017). THC-Hydra | Penetration Testing Tools. [online] Available at: http://tools.kali.org/password-attacks/hydra [Accessed 30 Mar. 2017].

[12] Concise Courses. (2017). THC Hydra Password Cracking/ Hacking Tool - Concise Courses. [online] Available at: https://www.concise-courses.com/hacking-tools/password-crackers/thc-hydra/ [Accessed 30 Mar. 2017].

[13] Salunkhe, S. (2017). [Blog] Download Password Cracker : Brutus. Available at: http://technosnoop.com/2016/03/download-password-

cracker-brutus/# [Accessed 30 Mar. 2017].

[14] Project-rainbowcrack.com. (2017). RainbowCrack - Crack Hashes with Rainbow Tables. [online] Available at: http://project-rainbowcrack.com/ [Accessed 30 Mar. 2017].

[15] Anon, (2017). [Blog] Wfuzz- A Web Application Password Cracking Tool. Available at: https://latesthackingnews.com/2017/01/14/wfuzz-web-application-password-cracking-tool/ [Accessed 30 Mar. 2017].

[16] Ophcrack.sourceforge.net. (2017). Ophcrack. [online] Available at: http://ophcrack.sourceforge.net/ [Accessed 30 Mar. 2017].

[17] Wondershare.com. (2017). Top 10 Password Cracking Tools. [online] Available at: https://www.wondershare.com/password/password-cracker-tools.html [Accessed 30 Mar. 2017].