**Annotated Bibliography**

**Biryukov, Alex, & Khovratovich, Dmitry. “Related-key Cryptanalysis of the Full AES-192 and AES-256.”**

***Advances in Cryptology - ASIACRYPT 2009 15th International Confernece on the Theory and Application of Cryptology and Information Security Tokyo, Japan, December 2009.* Ed. Mitsuru Matsui. Springer, 2009. 1-18. Print.**

This paper gives the most recent and currently only attack on the full AES encryption algorithm key space. The paper shows how using related encryption keys (the secret used by the algorithm to make encrypted data) can be used to simplify the complexity of guessing the key to decrypt data in a smaller time frame. This effectively weakens the encryption algorithm, but still does not completely break the protection offered by it.

Dmitry Khovratovich was a PhD student under Alex Biryukov who both studied cryptanalysis at the University of Luxembourg and published multiple papers on the AES algorithm. This is a continuation on previous work done by them on them on breaking the algorithm. The paper is targeted at those with a strong background in mathematics and a deep understanding of the AES algorithm. It assumes that the reader is already familiar with their previous work as well. The paper is theoretical in nature, but the concepts used are explained in an objective manner with statistical comparison to other previous methods. This paper is cited by many other scholarly papers in cryptography as well.

The most useful aspect of this source for our work is that it eliminates attempting to brute force the entire AES key space as a possibility since it shows that the complexity is still infeasible in terms of time.

**Pkware.com. “APPNOTE.TXT - .ZIP File Format Specification Version: 6.3.2.” 2007. Web.**

**12 March 2011 < http://www.pkware.com/documents/casestudies/APPNOTE.TXT>**

This document describes the technical details of the zip file format. The company, called PKWARE, that originally invented this file format in 1989 maintains this specification which is used not only in their products but many other compression archive products as well. The zip format was released into the public domain and additions to the standard since then have been published here. Other entities have also developed their own software tools for creating and reading zip files based on this standard. Since we must decrypt the zip file in our implementation having this specification will be of great help in understanding the format and how the decryption should be applied.

**United States. National Institute of Standards and Technology. *Announcing the ADVANCED***

***ENCRYPTION STANDARD (AES).* Maryland: NIST. 2001. Web.**

**<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>**

The NIST is an authoritative source for many computing standards used in both the U.S. government and academic worlds. This document provides the complete AES encryption algorithm specification which was chosen as a standard in 2001 by the United States government for protecting confidential data. Since our project involves decrypting AES encoded data this document will help us to implement the decryption code.

**Le Deguang, Jinyi Chang, Xingdou Gou, Ankang Zhang, Conglan Lu. *Parallel AES Algorithm for Fast Data Encryption on GPU.***

**Changshu: Changshu Institute of Technology, China, 2010.**

**<**[**http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5486259**](http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5486259)**>**

This paper is from 2nd International Conference on Computer Engineering and Technology, 2010. The paper introduces the traditional algorithm of AES encryption and then explains the technologies of general-purpose computation of GPU.

The authors propose the parallelized algorithm of AES encryption and analyze its principle of AES parallelism. Then, they detail the implementation of a fast encryption system for accelerating the AES encryption on GPU. Furthermore, they test and analyze the performance of their approach by comparing with the traditional approach, which shows the advantage and higher performance of their approach.

In our project we can make use of this approach for fast decryption of zipped files.

**Passware, Inc. *Password Recovery Attacks*. Web.**

**<**[**http://www.lostpassword.com/attacks.htm**](http://www.lostpassword.com/attacks.htm)**>**

Passware, Inc. was founded in 1998 and it is the maker of password recovery and e-Discovery software for Federal and State agencies, law enforcement and military organizations. An overview of the software made by Passware will be very useful for our project. The website describes 8 possible attacks for recovery of password. It describes how the attacks are implemented and how they can be used.

**Matt Bishop & Daniel V.Klein. “Improving System Security via Proactive Password Checking.”**

***Computers and Security 14(3), May/June 1995.***

This paper outlines some of the problems of password security by demonstrating the ease by which individual accounts may be broken. Various techniques used by crackers are outlined, and finally one solution to this point of system vulnerability, a proactive password checker, is documented.

Dr. Matt Bishop is a professor at the University of California at Davis. His research area is computer security in which he has been active since 1979. He has also worked extensively on the security of various forms of the UNIX operating system. His textbook, *Computer Security: Art and Science*, was published by Addison-Wesley in December 2002.

The paper first presents experimental results which expose the fact that the passwords selected by users are often weak and can lead to security breaches. To overcome these breaches the authors propose a scheme that checks the password entered by the user against a dictionary of words. Forming this dictionary of words thus becomes the major aspect of this system. The paper gives implementation details for the UNIX systems, but does not provide any results conforming improvement in security by using proaction. Also since the paper is quite old most of the flaws mentioned in security do not exist now.

In spite of these weaknesses, the paper does give useful insight as to how to build a dictionary of possible passwords, which is very useful for our project.

**Pfleeger, Charles & Shari Lawrence Pfleeger, Paul Petralia ed. “Security in Computing.”**

***New Jersey: Upper Saddle River, 2003. Print.***

This book is intended for study of computer security. The book is targeted at college and university students, computing professionals, managers, and users of all kinds of computer-based systems. It covers various aspects of computer security like cryptography, program security, operating system security, network security, database security, etc. It is a useful source for our project since it places the problem of security in an empirical context and also gives insight on AES algorithm as well the various password selection criteria that users should follow.