Evaluation of Security Methods for Ensuring the Integrity of Digital Evidence

Shahzad Saleem
Digital Scene Investigation Lab
DSV, Stockholm University
Forum 100, SE-16440 Kista, Sweden
Email: shahzads@dsv.su.se

Oliver Popov
Digital Scene Investigation Lab
DSV, Stockholm University
Forum 100, SE-16440 Kista, Sweden
Email: popov@dsv.su.se

Rami Dahman
Department of Computer and Systems Sciences
DSV, Stockholm University
Forum 100, SE-16440 Kista, Sweden
Email: dhaman@dsv.su.se

Abstract—**The omnipresence of e-services running on various instances of pervasive e-infrastructures that are fundamental to the contemporary information society generates an abundance of digital evidence. The evidence in a digital form stems from a myriad of sources ranging from stand alone computers and their volatile and non-volatile storages, to mobile small scale digital devices, network traffic, ever-present applications comprising social networks, ISP records, logs, Web pages, databases and both global and local information systems. The acquisition and the analysis of this evidence is crucial to understanding and functioning of the digital world, regardless of the positive or negative implications of the actions and the activities that generated the evidence. In the case of the later, when the evidence comes from illegal, illicit and malicious activities, the protection of digital evidence is of major concern for the law enforcement and legal institutions, namely for investigators and prosecutors. To protect the integrity of the digital evidence, a number of security methods are used. These methods differ in terms of performance, accuracy, security levels, computational complexity, potential errors and the statistical admissibility of the produced results, as well as the vulnerabilities to accidental or malicious modifications. The work presented deals with the evaluation of these security methods in order to study and understand their "goodness" and suitability to protect the integrity of the digital evidence. The immediate outcome of the evaluation is a set of recommendations to be considered for selecting the right algorithm to protect integrity of the digital evidence in general.**

I. Introduction

The combinatorial explosion of the Internet, along with the number of users and applications which represent a global conglomeration termed as a cyber world and critical to the well functioning of governmental, business, educational, social, civic, entertainment institutions and organizations have also created a plethora of opportunities for abuse and crimes against the creative power of these digital resources. Usually qualified as cyber crimes, they have been increasing dramatically and include activities such as intrusion attempts, massive dynamic denial of service attacks, malware, identity thefts, large scale digital fraud and embezzlement, human and illicit materials trafficking, and violation of IPRs. In fact there is a spectrum of known and even unknown activities where the computer could be the subject or the object of the conduct constituting a crime [1] [2]. A cybercrime investigation takes place in the form of forensic investigation which can be defined as the science of acquiring, retrieving, preserving, and presenting data that has been processed digitally and stored on a computer media as specified by Douglas Schweitzer [3]. A successful forensic investigation requires protection of the collected evidence against potential attacks which may take advantage of the volatile nature of digital evidence. Therefore, several security methods are used in order to enforce the need for protecting the integrity of the digital evidence during various forensic investigations.

We have classified these security methods into three groups. The first group constitutes Checksums i.e. Cyclic Redundancy Check e.g. CRC-16 and CRD-32 that are primarily used for error detection. The second group comprises of Hash Functions where MDx and SHAx algorithms are dominant in detection of any possible errors and/or alterations. The third group encompasses Digital Signatures which rely upon public-key cryptography (PKI) to ensure data integrity and authenticity.

The integrity of the digital evidence is important so it can be qualified as probative or to be admissible in the court of law. The probative value requires reliability, completeness, and authenticity of digital evidence. Therefore, it is evident that deployment and maintenance of the integrity during and after forensic investigation is a major concern for forensic investigators. Our work evaluates security methods based upon ITSEC evaluation criteria [4] in order to know the efficiency of these methods, where the research methodology is depicted in Figure 1. Obviously, the idea is to determine the most appropriate and effective security methods for protecting the integrity of the digital evidence.

It is important to note that this work is part of an ongoing project to evaluate a range of security algorithms employed to ensure integrity of digital evidence. This evaluation should be based on internationally acceptable standards such as ITSEC (Information Technology Security Evaluation Criteria) and CC (Common Criteria for Information Technology Security Evaluation). Inter alia, ITSEC is a set of criteria to evaluate security in products and systems [4]. Similarly, Similarly, CC can be used to evaluate security and assurance requirements in products and systems as well [5]. ITSEC precedes CC [6], and hence this fact may raise an argument concerning the validity of an evaluation by a standard that has been supplanted by a newer one. However, in view of the serious critique of CC

978-1-4577-0314-0/11/$26.00 ©2011 IEEE

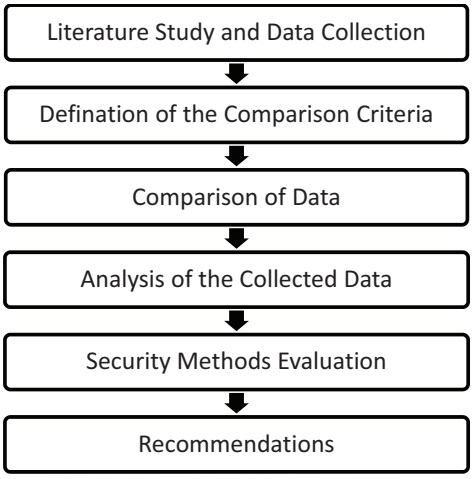

Fig. 1. Research Methodology

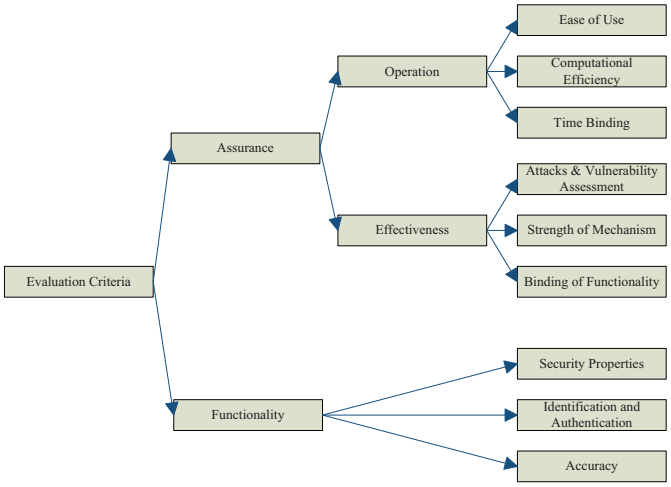

Fig. 2. Evaluation Criteria Model

by Jonathan Shapiro, Alan Paller and others [7] for being too complex, paperwork oriented, waste of time and resources, we decided to use both ITSEC and CC in the evaluation process, and then compare and contrast the results. This paper presents the results of the first phase of the project related to the evaluation of security algorithms based on ITSEC in the context of digital evidence integrity, which also provide us with the appropriate frame of reference. The second phase of the project deals with CC, and the final one will do the comparison and present the results and the recommendations.

As indicated in the model of research methodology Figure 1, the work started with the study of the three groups of security methods, proceeds with data collection and ends with recommendations through some intermediate activities such as identification of the comparison criteria, comparison of data, analysis of collected data and the evaluation of security methods.

This paper is organized in four sections, where Section I defines the problem and the motivation behind the research, as well as the general methodology. The issue of the evaluation and comparison criteria is addressed in Section II. The results from the evaluation and comparison of the security methods are presented in Section III, Section IV and V present the recommendations, conclusion and future work respectively.

II. Evaluation Criteria

We have used ITSEC evaluation criteria to evaluate security methods for protecting the integrity of digital evidence. ITSEC model is shown in Figure 2 and it consists of nine sub-criteria, used for the evaluation against the three categories of integrity protection mechanisms.

1) Security Properties: This criterion is about security properties of a security method such as data confidentiality, data integrity and non-repudiation.

2) Identification and Authentication: Relates to all functions intended to establish and verify a claimed identity.

3) Accuracy: Deals with the accuracy of security method which we evaluated by experiments to test three aspects of each security method which are errors, time and verification. Security methods were tested for (1) any errors while processing data, (2) the time taken by each security method to provide its intended security services and (3) the ability to verify security properties induced by security methods. The scenarios for the experiments to evaluate accuracy were based on the need to process 25MB of bulk data containing 20 files, and this has been repeated 15 times for each of the security methods under consideration.

4) Binding of functionality: Looks into the ability of a security method to work and bind with another security method so they can mutually support each other and thus provide more effective and stronger security solution.

5) Strength of Mechanisms : Defines the strength of a mechanism to withstand against potential attacks.

6) Attacks and Vulnerability Assessment: The criterion defines a database of all the potential vulnerabilities and attacks that the security method may detect, resist, and encounter.

7) Ease of Use/ Complexity or Simplicity : Measures and evaluates security methods for ease of use, complexity and simplicity.

8) Computational Efficiency: The criterion focuses on measuring computational efficiency of security method while processing the data. To evaluate the computational efficiency, experiments were based on various files with different sizes, represented in Table I.

TABLE I
Inputs for Computational Efficiency Experiments

Input Size	5MB	10MB	20MB	40MB	50MB	80MB	100MB	200MB	500MB

9) Time Binding: It is about the ability of a security method to bind time with the processed data. This capability of the method is important in the case of digital evidence since it may help to determine the validity and order of events during a forensic investigation.

III. Results Analysis: Comparison between Security Methods

The experiments and the subsequent results which were made by rigorously observing the behavior and studying the ITSEC model, as described in Section II, provide the basis for the analysis and the comparison.

However, in order to improve both the quantitative and the qualitative value of our analysis, we shall introduce a scale that actually reflects the degree of conformity or its absence to each of the enumerated criteria that belongs to the ITSEC model by every security method. We will use "+" sign to show that a particular security method establishes a specific criterion and a "-" sign to show its absence. The number of "+" signs will depict the degree to which a specific security method ascertains a particular criterion. Moreover, to the comparison and the evaluation of the security methods with respect to different criterion is placed in separate tables. Number of "+" signs in different cells of a specific comparison table should be used to compare security methods for one specific criterion in that particular table. For instance, the presence of two "+" signs relative to the confidentiality and integrity of MDx does not imply that MDx is equally dealing with these two different criteria. On the contrary, the presence of two "+" signs in confidentiality column for two different security methods means that both are equally good in dealing with confidentiality.

1) Security Properties: Table II shows that none of security methods provide confidentiality. Digital signatures are the only security method providing non-repudiation as it relies upon asymmetric cryptography and data is signed by a private key. The underlying assumption in this scenario is that private key will be kept safe and secure and will only be issued to a legitimate entity.

TABLE II
Algorithm's Security Properties

Algorithms	Security Properties		
	Confidentiality	Integrity	Non-Repudiation
CRC	-	+	-
MDx	-	++	-
SHAx	-	+++	-
Digital Signature	-	++++	+

CRCs provide integrity services, however they are mainly concerned with accidental error detection on bit level for blocks of data [8] [9]. Since they are weak in integrity protection their rank is the lowest. MDx is rated lower than SHAx because of reasons provided and discussed in [10] [11] [12] [13]. Digital Signatures are rated the highest as they leverage asymmetric cryptography in conjunction with digital hashes which are more powerful than hashes alone [14] [15] [16].

2) Identification and Authentication: Table III is the summary of the comparisons for the authentication criterion. Digital Signatures are the only security method which employees a private key tied to a specific entity hence provides identification and authentication.

TABLE III
Authentication Analysis

Criterion	Security Methods			
	CRC	MDx	SHAx	Digital Signatures
Identification and Authentication	-	-	-	+

3) Accuracy: Table IV shows that no errors occurred while processing the same data 15 times which indicates the accuracy of security methods. Time accuracy is established by all the security methods at slightly different levels as depicted in Table IV. It is interesting to note that all security methods detected modifications with a hundred percent success rate. In a descending order, the list of security algorithms with respect to vulnerabilities as indicated in [8] [10] [11] [12] [17], is CRC, MD, SHA-1, SHA-512. Since CRC is most vulnerable to attacks, it is consequently the least accurate in terms of verification and on the other hand, SHA-512 is the most accurate in terms of verification accuracy. One can modify the original data, recalculate hash, and then swap the original hash with the recalculated one, which obviously subverts integrity service. However, in the case of digital signatures no one without a correct private key is able to do the same. Hence digital signatures [15] are the most reliable algorithms when it comes to verify data integrity and thus their ranking is the highest with respect to verification accuracy.

TABLE IV
Algorithm's Accuracy Analysis

Method	Directory Size	Number of Files	Number of Executions	Errors Reported	Time Accuracy	Errors Detection
CRC-32	25 MB	20	15 Times	No	98.35%	100%
MD5	25 MB	20	15 Times	No	99.7%	100%
SHA-1	25 MB	20	15 Times	No	99.1%	100%
SHA-512	25 MB	20	15 Times	No	97.98%	100%

4) Binding of Functionality: Row 6 of Table VII shows that ability to work in conjunction with other security methods is supported by all. CRC is rated lowest as it is barely supplemented with other security methods to muster up security. MDx and SHAx supplement other security methods such as asymmetric cryptography to enhance security, however SHAx is more secure than MDx, and consequently rated higher [10] [11] [12] [17] [18] [19].

5) Attacks and Vulnerability Assessment: Since CRC algorithms are vulnerable to attacks [20] [21], data integrity can be easily violated. Several successful attempts and vulnerabilities have been reported against MDx and SHAx. The need for more resources to break SHAx than MDx ranks SHAx higher than MDx [10] [11] [12] [17] [18] [19], as indicated in Row 11 of Table VII.

6) Strength of Mechanisms: Row 7 of Table VII is a summary of comparisons for the strength of mechanism criterion. The strength of a security method depends upon its effectiveness to resist different attacks. CRC is placed at the lowest rank because the output of the CRC is either 16-bit or

32-bit long which is too small for low collision rate [20] [21]. It also does not fulfill the three properties of the cryptographic hashes such as pre-image resistance, second-image resistance and collision resistance. MDx and SHAx are better than CRC, but inferior to digital signatures. However, SHAx is ranked higher than MDx because SHA provides a range of 80, 128, 192, and 256 bit security for 160, 256, 384 and 512 bits digest length respectively. This means that SHA provides at least 32 bits more security than MD5 [10] [11] [12] [17] [18] [19]. When compared to other algorithms. Digital Signatures use asymmetric cryptography with keys having greater key space along with digital hashes. This indicates more robustness when compared with other algorithms.

7) Ease of Use/ Complexity or Simplicity: Table V is a summary of the comparisons for the ease of use and complexity criterion.

TABLE V
EASE OF USE AND COMPLEXITY ANALYSIS

Criteria	Security Methods			
	CRC	MDx	SHAx	Digital Signature
Ease of Use	+	+	+	+++
Complexity	+	++	+++	++++

Since CRC, MDx and SHAx algorithms are built in to the digital forensic tools, so they require least intervention from a user. The user has only to configure the tool according to his preferences. This automatically generates message authentication codes based upon the security algorithm selected during configuration. So they are equally easy to use. On the other hand, digital signatures require private key of a user. This indicates the need for more user involvement, while getting ready to use the forensic tool, which makes Digital Signatures less easy to use in comparison with other security methods.

For measuring complexity we rely on the information provided in Figure 3 that shows the times required by different algorithms for providing their services. From Figure 3 it is evident that there is slight difference in all security algorithms with an exception of SHA-256. If we group SHAx algorithms together and take an average of their time from Figure 3 then the ascending order with respect to complexity will be CRC, MD5 and SHAx. Clearly, Digital Signatures are the most complex of all, as they are based upon expensive asymmetric cryptography and require PKI as well.

8) Computational Efficiency: The execution results on the inputs presented in Table I for testing computational efficiency of the hash functions are shown in Figure 3.

The results of experiments conducted in [22] to evaluate the performance of RSA, DSA and Fractal Digital Signature algorithms in terms of key size and their execution time are given in Figures 4, 5 and 6 respectively.

Table VI is a summary of comparisons for the computational efficiency criterion.

CRC-32 algorithm is based on a simple mathematics which makes it the fastest one. It can be seen that SHA256 is the slowest where average time is 42992 ms. Digital signature algorithms are also fast in generating keys (one time process), signing and verification. The average time needed for key generation and signing using DSA and RSA is illustrated in Figure 5. It is evident that DSA algorithm is faster than RSA relative to key generation and signing, where the average time needed to perform these operations is 1923.7 ms for DSA and

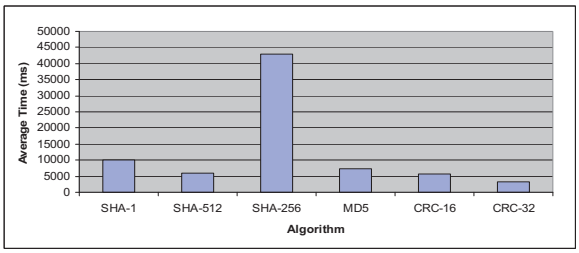

Fig. 3. Average Time to Compute Message Digests

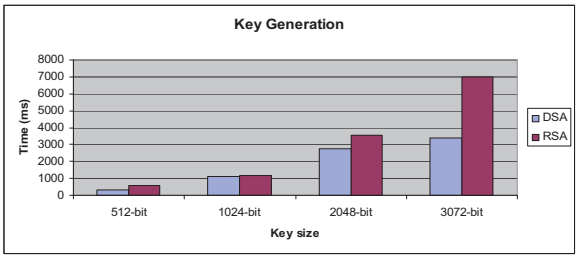

Fig. 4. Average Time for Key Generation Using DSA and RSA [22]

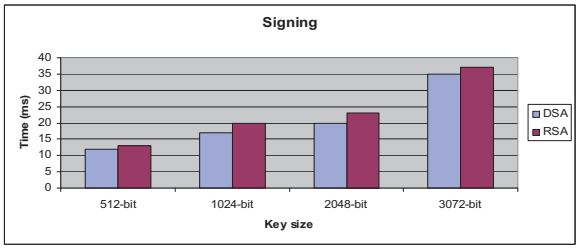

Fig. 5. Average Time for Signing Using DSA and RSA [22]

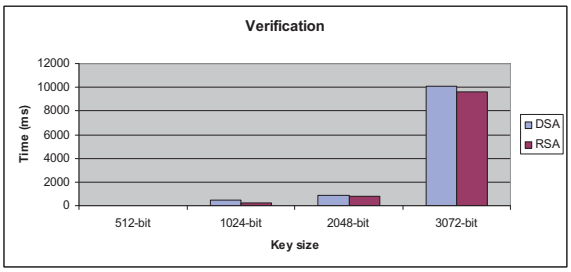

Fig. 6. Average Time for Varification Using DSA and RSA [22]

TABLE VI
COMPUTATIONAL EFFICIENCY ANALYSIS

Criteria	Security Methods						
	CRC-16	CRC-32	MD-5	SHA-1	SHA-256	SHA-512	Digital Signature
Computational Efficiency	+++	++++	+++	++	+	++++	+++

TABLE VII
ANALYSIS AND EVALUATION SUMMARY

Criteria			Security Methods			
			CRC	MDx	SHAx	Digital Signature
Functionality Criteria	Security Properties	Data Integrity	+	++	+++	++++
		Confidentiality	-	-	-	-
		Non-Repudiation	-	-	-	+
	Identification and Authentication		-	-	-	+
	Accuracy		+	++	+++	++++
Assurance Evaluation Effectiveness	Binding of Functionality		+	++	+++	
	Strength of Mechanism		+	++	+++	++++
	Attacks and Vulnerabilities		++++	+++	++	+
Effectiveness Criteria Operation	Ease of Use		+	+	++	+++
	Computational Efficiency		+++	++	+	++
	Time Binding		-	-	-	-

3090.3 for the RSA.

9) Time binding: Row 11 in Table VII is a summary of comparisons for the time binding criterion which shows that none of the security methods have the ability of binding the time with the processed digital evidence. Having the time associated with the outputs of the security methods while processing the digital evidence would have been advantageous because time is an important and crucial factor in proving the integrity of the digital evidence. It is beneficial to know when the digital evidence was processed by the security method, and for how long after the preservation of the evidence, the integrity of the evidence was protected. Some forensics tools such as EnCase and AccessData Forensic Tool Kit provide a facility to save time with the collected digital evidence.

Table VII is a summary of what we have discussed in this section.

IV. RECOMMENDATIONS

Based upon the results and the analysis in Section III, we will give some recommendations which should be helpful in making the right decision when selecting a security algorithm for integrity protection of digital evidence. Table VIII is a summary of our recommendations.

TABLE VIII
RECOMMENDATIONS

Recommendations	Security Algorithms
High Level of Data Integrity	Digital Signature with SHAx
Data Confidentiality	....
Non-Repudiation	Digital Signature
Identification and Authentication	Digital Signature
High Level of Accuracy	Digital Signature with SHAx
Binding of Functionality at High Level	SHAx
High Level of Strength/Security	Digital Signature with SHAx
High Computational Efficiency	CRC
Least Attacks	SHAx, Digital Signature
Time Binding	....

A brief description of the recommendations based upon the results of our experiments, analysis and evaluation follows:

(a) High Level of Data Integrity: Use either SAH-512 or/and Digital Signatures.
(b) Non-Repudiation: Digital Signature is the only security method which can provide non-repudiation.
(c) Authentication and Identification: Again, Digital Signature is the only security method capable of providing this service.
(d) Accuracy: Digital Signature with SHAx algorithm for hashing is recommended over others.
(e) Binding of Functionality: It is recommended to use SHAx hash functions due to the strength and security levels associated with these algorithms.
(f) High level of strength: Digital Signature along with SHAx in general should be selected if one wants higher level of strength.
(g) Easy to Use/ Low complexity supported: CRCs and digital hashes have advantage over others since they require least user intervention and are usually built in by default. In the case of digital signatures, a little more effort from user and PKI infrastructure is required, which adds up to the degree of difficulty when compared to other security mechanism.
(h) Computationally efficient-fast: CRC is fastest when it comes to computational efficiency. According to our findings in Figure 3, SHA-512 is not that far from CRC-16 in terms of computational efficiency. But CRC is really very weak when compared with SHA-512, hence one should prefer SHA-512 over CRC in this area too.
(i) Lesser number of attacks reported: With respect to this objective, SHAx and Digital Signature are way ahead from others so they should be a choice of preference.

V. CONCLUSION AND FUTURE WORK

Based on our experiments and evaluation in the framework of ITSEC standard, we would suggest that SHA-512 should be considered for integrity protection since it is (1) computationally very fast, (2) least vulnerable, (3) easy to use, (4) has high strength, and (5) higher levels of accuracy and capability

to provide higher levels of data integrity. But if one can afford expensive operations of asymmetric cryptography along with PKI then SHA-512 with Digital Signatures should be preferred for integrity protection. Since risks, stakes and outfall of digital evidence with weak integrity protection are generally high so we would conclude with a recommendation to use, whenever possible, Digital Signatures with SHA512 for protecting the integrity of digital evidence.

We have evaluated security methods used to protect integrity of digital evidence based upon the criteria enumerated in ITSEC. During this process we have ranked different alternative security methods which provide us with the sound indication for using decision analysis techniques described in [23]. Hence, there are plans to create a decision tree from the information presented in [23] and thus have th possibility to analyze different alternatives.

Moreover, as mentioned in the Introduction Section i.e. Section I, the work in the second phase of this project deals with the evaluation of these security methods based on the Common Criteria (CC), model. This would eventually enable us to compare and contrast the results of both the phases and to develop a deeper insight into this area. The intention of the project is to provide (as its final output) a formal basis for ensuring integrity of digital evidence for all the individuals working in the area of digital forensics and related disciplines.

REFERENCES

[1] B. Nikkel, "Improving evidence acquisition from live network sources," *Digital Investigation*, vol. 3, no. 2, pp. 89–96, 2006.

[2] T. A. Johnson, *Forensic Computer Crime Investigation*. CRC Press, 2006.

[3] D. Schweitzer, *Incident Response: Computer Forensics Toolkit*. Wiley Publishing, 2003.

[4] O. for Official Publications of the European Communities. (2010, January). [Online]. Available: www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

[5] C. C. D. Board. (2010, November) Common criteria for information technology security evaluation. [Online]. Available: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

[6] T. N. T. A. for Information Assurance. (2010, November) Common criteria & itsec. [Online]. Available: http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/index.shtml

[7] W. Jackson. (2010, November) Under attack. [Online]. Available: http://gcn.com/articles/2007/08/10/under-attack.aspx

[8] W. Peterson and D. Brown, "Cyclic codes for error detection," *Proceedings of the IRE*, vol. 49, no. 1, pp. 228–235, 1961.

[9] T. Ritter. (2010, January) The great crc mystery. [Online]. Available: http://www.ciphersbyritter.com/ARTS/CRCMYST.HTM

[10] AccessData. (2010, January) Official webpage of access data. [Online]. Available: http://www.accessdata.com/media/en_us/print/papers/wp.md5_collisions.en_us.pdf

[11] M. Stevens, "Fast collision attack on MD5," *IACR ePrint archive Report*, vol. 104, p. 17, 2006.

[12] M. Robshaw, "On recent results for MD2, MD4 and MD5," *RSA Laboratories Bulletin*, vol. 4, 1996.

[13] X. Wang, Y. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Advances in Cryptology–CRYPTO 2005*. Springer, 2005, pp. 17–36.

[14] M. Raheem, "Evaluation of Cryptographic Packages," *Statistics*, pp. 03–27, 2009.

[15] G. Locke and P. Gallagher. (2010, January) Fips publications. [Online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

[16] R. S. EL-SAYED, M. A. EL-AZIEM, and M. A. GOMAA. (2010, January) Reference repository. [Online]. Available: http://eref.uqu.edu.sa/files/eref2/folder6/f69.pdf

[17] X. Wang and H. Yu, "How to break MD5 and other hash functions," *Advances in Cryptology–EUROCRYPT 2005*, pp. 19–35, 2005.

[18] K. Aoki, J. Guo, K. Matusiewicz, Y. Sasaki, and L. Wang, "Preimages for Step-Reduced SHA-2," *Advances in Cryptology–ASIACRYPT 2009*, pp. 578–597, 2009.

[19] S. Sanadhya and P. Sarkar, "New collision attacks against up to 24-step SHA-2," *Progress in Cryptology-INDOCRYPT 2008*, pp. 91–103, 2008.

[20] Anarchriz, "Crc and how to reverse it," vol. 1, no. 1, 2004.

[21] M. Stigge, H. Pl
"otz, W. M
"uller, and J. Redlich, "Reversing CRC–theory and practice," Technical Report SAR-PR-2006-05, Humboldt University Berlin, Tech. Rep., 2006.

[22] M. Alia and A. Samsudin, "A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Sets." *American Journal of Applied Sciences*, vol. 4, no. 11, pp. 850–858, 2007.

[23] R. Clemen and T. Reilly, *Making hard decisions with DecisionTools Suite*. Duxbury, 1999.