2 Research Methodology & Review of Literature

“All progress is born of inquiry, Doubt is often better than overconfidence, for it leads to inquiry, and inquiry leads to invention”
-Hudson Maxim.

2.1 Research Methodology

Research methodology is a way to systematically and scientifically solve the research problem. It may be understood as a science of studying how research is done scientifically. In it we study the various steps that are generally adopted by a researcher in studying his research problem along with the logic behind them. It is necessary for the researcher to know not only the research methods/techniques but also the methodology.

As the name my research work entitled “An Analytical Study of Hybrid Cryptography and Implementation of RSA with Hash Functions” suggests that it has two parts, one is analytical study part and other is implementation part. So the methodologies used for those parts are described as follows –

(i) Methodology for Analytical Study part of my research work

First part of my research work is analytical research in which the researcher use facts or information already available, and analyse these to make a critical evaluation of the material. Two types of methods used in the analytical research for gathering data as well as subject-related matter are Primary Source Method and Secondary Source Method.
Primary Source Method means to collect, tabulate and analyze data. A primary source provides direct or firsthand evidence about an event, object, person, or work of art. Primary sources include historical and legal documents, eyewitness accounts, results of experiments, statistical data, pieces of creative writing, audio and video recordings, speeches, and art objects. Interviews, surveys, fieldwork, and Internet communications via email, blogs, listservs, and newsgroups are also primary sources. In the natural and social sciences, primary sources are often empirical studies—research where an experiment was performed or a direct observation was made. The results of empirical studies are typically found in scholarly articles or papers delivered at conferences [21]. In this process the researcher collects data from various authentic sources to study the problem and tests the hypothesis on/from statistical techniques, formula and tools. After the collection of data researcher analyses and summaries them and finally completes his research work. It is a theoretical approach of research work.

Secondary sources describe, discuss, interpret, comment upon, analyze, evaluate, summarize, and process primary sources. Secondary source materials can be articles in newspapers or popular magazines, book or movie reviews, or articles found in scholarly journals that discuss or evaluate someone else's original research [21]. In Secondary Source Method, the use of secondary source material is helpful in discerning variety of views and options that can be relied upon either for substantiating or facilitating rebuttal of the arguments. It is a theoretical approach of research work.

To collect data and information for my research work, I have gone through the text books of renowned authors and articles published in well reputed national and international journals; participated in several conferences; refer libraries; and surf the net to gather the relevant information. Hence, I have adopted both of the methods of research methodology to make my
research more authentic and relevant and useful in this era of high technological innovations.

(ii) Methodology for Implementation Part of my research work

Software Development Life Cycle (SDLC) is a sequence of events carried out by analyst or designer to improve or develop and implement an information system. It is layered technique whose main focus is on quality. Software Methodology, step-by-step plan some desired results, is usually identifies the major activities to be carried out and indicates which people should be involved in each activity and what role they play. Methodologies often describe entry criteria, exit criteria and checkpoints for each of the activities/stages. The term Life-Cycle can be used synonymously with the term methodology [22]. Various processes and methodologies have been developed over the last few decades to improve software quality, with varying degrees of success. Any model is chosen on the nature of the project, the method & tools and the controls.

My research work is focused on hybrid cryptosystem and to research, design, develop and implement a GUI-based easy to use RSA-based software tool named “RSAAPP” which provides facilities of RSA key generation (512 bit, 1024 bit and 2048 bit), encrypt private key with DES by 8 character password then save encrypted private key which provides enhanced security level with the application of hybrid cryptosystems, encryption of any file, decryption of encrypted file, digital signature generation using MD5, SHA1, SHA2 three different hash functions and digital signature verification. Keeping in view of my research work, Iterative Waterfall model has been chosen for development of RSAAPP. Iterative Waterfall Model provides faster results, require less up-front information and offer greater flexibility. In this model, the project is divided into small parts. This allows the development team to demonstrate results earlier on in the process and obtain valuable feedback from system users. Each iteration of this model is a mini-waterfall
process with the feedback from one phase providing vital information for the design of the next phase.

The proposed system RSAAPP is implemented in ANSI C with windows APIs using structured programming methodologies. These methodology techniques are best suited for process-oriented systems i.e. they that are driven by the functionality of the system rather than by the data used in the system. Structured analysis and design tools were originally characterised by graphical modelling tool called data flow diagrams (DFD). Feasibility study, system analysis, requirement analysis system design and detailed DFDs of the RSAAPP are explained in chapter 5 of the thesis.

The developed and implement a GUI-based software tool named “RSAAPP”, for the security purposes not only in electronic file transactions and EDI for a specific user but also for local storage of confidential data. The application is to be geared towards low-end processors despite the high computational costs involved in the RSA algorithm. At the same time it should be ensured that all the computation done by the application and the resulting output are reasonably secure. The software shall be developed in a modular format with each module performing a separate function which would ensure reusability of the software.

2.2 Review of literature

The quest for a reliable means of keeping information completely secure is a troubling enigma that reaches far back into the history of mankind. From the concealment of top-secret military files, to the protection of private notes between friends, various entities over the years have found themselves in need of disguises for their transmissions for many different reasons. This practice of disguising or scrambling messages is called encryption, and in these days of ever-improving network technology, its importance is becoming more and more apparent. Information security is the fundamental goal for
secured exchange of information. Cryptographic tools or primitives should be evaluated with respect to various criteria such as level of security, functionality, methods of operation, performance etc.

This literature review looks at the research works that has been published in the field of cryptography specially DES, RSA, hybrid cryptography, Hash functions, Digital Signature etc. It compares and contrasts the research pointing out overall trends in what has already been published on this subject. It analyzes the role that cryptography has played and will play in the future relative to security. A cryptographic algorithm is said to be more secure, if it provides the capability to resist the attacks. Similarly, the operational speed of the most public-key algorithms fully depends on modular exponentiation which plays a vital role in both encryption and decryption process and performing such exponentiation is a time consuming operation, if it is not properly implemented. This review addresses cryptography around the central theme of the security that it provides or should provide individuals, corporations, and others in the modern age of computing technology, networking, and Web-based ecommerce.

By reviewing both scholarly and non-scholarly works, it is our objective to make a case that continuing research into the use of cryptography is paramount in preserving the future of electronic data security and privacy as well as the continuing development of Web-based applications that will permit the growth of ecommerce business worldwide to be conducted over the Internet.

The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. The most striking development in the history of cryptography came in 1970s when Feistel at IBM and culminating in 1977 with the adoption as a U. S. Federal information processing standards for encrypting unclassified information, DES [23]. In
1976, Diffie and Hellman [5] introduced the concept of public key cryptography and intractability of the discrete logarithm problem. In 1978 Rivest, Shamir, and Adleman [24] discovered the first practical public key encryption and signature scheme, 1985 major advances in public key schemes by ElGamal [25]. One of the most significant contributions provided by public key cryptography is the digital signature [26].

Hybrid Cryptography

Dr. Mahmoud T. El-Hadidi et al [27] presented a software-based implementation of a hybrid encryption scheme for Ethernet LAN. It used a DES-type symmetric key for information exchange between communicating users. In addition, a Diffie-Hellman method is adopted for key distribution which incorporates an RSA-type public key scheme for securing the exchange of the symmetric key components. The disadvantage was that it is believed that by using hardware implementation for certain parts of the proposed encryption scheme, a much faster operation could be obtained.

Cramer and Shoup [28] proposed the first hybrid encryption scheme that was practical, and is provably secure against adaptive chosen ciphertext attack under standard intractability assumptions.

Louis Granboulan [29] compared the two published RSA-based hybrid encryption schemes having linear reduction in their security proof: RSA-KEM with DEM1 and RSA-REACT and showed that RSA-KEM+DEM1 should be preferred to RSA-REACT. He also proposed some changes to RSA-REACT to improve its efficiency without changing its security, and conclude that this new RSA-REACT is a generalisation of RSA-KEM+DEM1, with at most the same security, and with possibly worse performance.
Kaoru Kurosawa and Yvo Desmedt [30] used a variant of Cramer-Shoup and obtained a very efficient IND-CCA secured hybrid encryption scheme by using a KEM which is not necessarily IND-CCA secure. This scheme was also secure in the sense of IND-CCA under the DDH assumption in the standard model. The result is further generalized to universal projective hash families.

The ISO/IEC JTC1/SC27 standardization committee suggest [31] that hybrid cryptography can be defined as the branch of asymmetric cryptography that makes use of convenient symmetric techniques to remove some of the problems inherent in normal asymmetric cryptosystems. Then Alexander W. Dent [32,33,34] explained hybrid cryptography ad shown that the KEM-DEM approach to hybrid cryptography can be used for more than just encryption particularly for constructing signcryption schemes (although it is not very useful for constructing signature schemes). Perhaps the most intriguing aspect of this work is the potential for a streamlined piece of software that allows a user to choose between encryption, signcryption with outsider security and signcryption with insider security by just changing the nature of the KEM and DEM that are being used. Of course, in such a case, care would have to be taken to ensure that suitably independent public/private key pairs were used for each possible KEM/DEM pair.

M. Ayoub Khan and Y.P. Singh [35] presented the security of joint signature and hybrid encryption. The proposed scheme combines the security of a document by hybrid encryption method and authenticity by digital signatures. IDEA-RSA algorithm is used for hybrid encryption and RSA digital signature algorithm is used to obtain digital signature (D). The effectiveness and correctness of the proposed scheme is illustrated through implementation and its results. The proposed scheme achieved a speed of 2.8 Mbps.
A. Al Hasib and A. A. Md. M. Haque [36] besides analyzing different kinds of attacks on AES and RSA for security purpose, a solution for the limitations is also provided.

Y. Wang, and M. Hu [37] under the same key length and for the same size of the processed data, RSA is about several hundred times slower than AES, triple-DES is about three times slower than AES, and there are other runtime characteristics which further highlights the difference between these three cryptographic algorithm and provides a reference value of for people’s rational using. The increasing key length in case of RSA and triple-DES when projected against key length used in AES, result show significant increase in AVL factor.

W. Xing-hui, and M. Xiu-jun [38] discussed the technique problem of key management and database encryption in the implementation process of database encryption system, some difficult technology of encrypt/decrypt engine in the implementation process are discussed, the hybrid cryptography encryption program is presented based on IDEA combined with RSA, and the encryption system is designed and realized.

W. Ren, and Z. Miao [39] proposed hybrid encryption algorithm, instead of the E0 encryption, DES algorithm is used for data transmission because of its higher efficiency in block encryption, and RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission in the Bluetooth system will be more secure. Meanwhile, it is clear that the procedure of the entire encryption is still simple and efficient as ever. In addition, the confidentiality of the hybrid encryption algorithm is also discussed.

Y. Li, Q. Liu, and T. Li [40] aims at speeding up Batch RSA decryption. BEARSA (Batch Encrypt Assistant RSA) and BEAMRSA (Batch
Encrypt Assistant Multi-Prime RSA) are proposed to improve Batch RSA decryption performance. Two variants of Batch RSA speed up decryption by reducing modules in modular exponentiation and shifting some decryption work to encryption. The experimental results and the theoretical values show that the speed of the decryption has been substantially improved.

A. A. Gutub, and F. A. Khan [41] proposes a hybrid crypto system that utilizes benefits of both symmetric key and public key cryptographic methods. Symmetric key algorithms (DES and AES) are used in the crypto system to perform data encryption. Public key algorithm (RSA) is used in the crypto system to provide key encryption before key exchange. All the hardware modules are designed by Register Transfer Level (RTL) modeling of Verilog HDL using Model Sim SE 5.7e showed interesting promising results.

S. P. Bansod, V. M. Mane, and L. R. Ragha [42] presented a paper on hybrid cryptographic techniques based on DES and RSA algorithms to achieve data encryption and compression technique to store large amount of data. A combination of both provides superior security control. The suggested algorithm is modified BPCS (Bit Plane Complexity Segmentation) steganography technique that can replace all the “noise-like” regions in all the bit-planes of the cover image with secret data without deteriorating the image quality. It allows for a large capacity of embedded secret data and can be extracted from stego-image without the assistance of original image.

According to A. Chitra and T. B. Sheeba [43], to achieve the maximum security required a Parallel Processing, User Reconfigurable Cryptographic RISC Microprocessor is proposed in our paper. Rather than protecting the data using tools and external codes, a microprocessor is specially designed in our project to offer maximum digital security. They proposed a hybrid architecture in which both the advantage of asymmetric and symmetric cryptographies are combined. For implementation, Asymmetric RSA cryptography and a
symmetric lightweight SEA encryption is combined to mutate a reconfigurable Cryptographic processor.

S. A. Nagar, and S. Alshamma [44] aimed to speed up the implementation of the RSA algorithm during data transmission between different communication networks and Internet. Also proposed a new method to exchange the values of the keys between gateways, which are exchanged indexes (Indexes Exchange) refers to the fields that contain the values of public and private keys that are stored in the tables inside the database before starting to use RSA algorithm to encrypt and decrypt the data, rather than using the exchange of real values n, e, and d.

According to R. S. Dhakar, A. K. Gupta, and P. Sharma [45], The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. So to improve the security, this scheme presents a new cryptography algorithm based on additive homomorphic properties called Modified RSA Encryption Algorithm (MREA). MREA is secure as compared to RSA as it is based on the factoring problem as well as decisional composite residuosity assumptions which is the intractability hypothesis. The scheme is an additive homomorphic cryptosystem which means that given only the public-key and the encryption of m1 and m2, one can compute the encryption of m1 + m2.

P. S. Rasmi, and Dr. V. Paul [46] designed a new paired cipher text public key System based on RSA is designed, which incorporates two hard mathematical problems (Both Discrete logarithms and Factoring) to make the algorithm too secure.

J. Zhang, and X. Jin [47] developed a system of wide range of practicality, triple DES used for data encryption and RSA for key management and SHA-1 for validating data integrity.
Ijaz Ali Shoukat et al [48] proposed a Generic Hybrid Encryption System (HES) under mutual committee of symmetric and asymmetric cryptosystems. They have done some functional and design related changes in existing Public Key Infrastructure (PKI) to achieve simplicity, optimal privacy and more customer satisfaction to fulfill all set of standardized security constraints.

Y. L. Huang, et al [49] presented a new scheme for 4G environment provides secure data transmission, privacy preservation and reduced processing time for key exchange. It also enhances key exchange security and provided a new method for message digest calculation.

H. Wang et. al. [50] introduced the basic number theories of RSA cryptosystem and applies t to key algorithm of RSA cryptosystem, such as Euclidean and its extension theorem, square-multiply algorithm and prime number testing. At last, provides a description of Matlab simulation of key algorithm and RSA encryption and decryption. The result shows that the whole simulation took 0.140176s, and solves the problem of key transmission.

Colin D. Walter [51] has proposed an algorithm based on ‘Division Chain’ to minimize the number of multiplications involved in computing the exponent. The main advantage of this scheme is that almost no extra memory is required. Furthermore, the method is adaptable to a wide range of space and time resources, providing a variable search space from which better evaluation order can be found. Noboru Kunihiro and Hirasuke Yamamoto [52] have proposed two methods viz., a run-length method and a hybrid method to generate a short addition chain for the given exponent $e$.

C. K. Koc [53] presented a report which includes RSA algorithm, the Diffe-Hellman key exchange scheme, the ElGamal algorithm, and the recently proposed Digital Signature Standard (DSS) of the National Institute for
Standards and Technology. The emphasis of the report is on the underlying mathematics, algorithms, and their running time analyses. The aim of the report is to bridge the gap between the mathematics of the modular exponentiation operation and its actual implementation on a general purpose processor. In another report he suggested RSA hardware implementation [54].

Knuth [55] gives the history of binary method and it is one of the oldest method as it was introduced before 200 B.C in Pingala’s Hindu classic Chandah-sutra. This method is also called ‘square and multiply method’. To compute $x^e$ using binary method, binary representation of $e$ is used and it is given as: $e = c_{n-1}2^{n-1} + c_{n-2}2^{n-2} + ... + c_12^1 + c_02^0$, where $c_i$ is either 0 or 1. The idea is based on ‘square and multiply’ technique for efficient computation of exponentiation to be used in any public-key algorithm like RSA. He Debiao et al. [56] have proposed a new algorithm using the concept of square root (sqrt) and multiply and all other accelerating tricks over square-and-multiply algorithm such as m-ary method, recording method, look-up-table method for modular exponentiation over $GF(2^m)$, and its implementation. The result has proved that to compute modular exponentiation, it uses lesser modular multiplication in most cases when it is compared with classical square-and-multiply algorithm. But a little pre-computation is necessary.

A. Young [57] demonstrated the limitations in computer platform security in the use of cryptography. This study showed the experimental results of launching a crypto-viral payload on the Microsoft Windows platform, specifically on the Microsoft Cryptographic API. The study revealed that using eight types of API calls and 72 lines of C code, the payload was able to hybrid encrypt sensitive data and hold it hostage. The researchers in this study were able to develop a countermeasure to the crypto-viral attack, which forces the API caller to show that an authorized party can successfully recover the asymmetrically encrypted data.
Riemann hypothesis [58] solution is a very major threat to RSA. Thus a solution has neither been proven to exist nor to not exist. However, if a solution were found, prime numbers would be too easy to find, and RSA would fall apart.

Michael J. Wiener [59] proposed an attack on RSA and it is termed as Wiener’s low decryption exponent attack. It is noted that to reduce the workload of the exponentiation, normally small value is used for private-key rather than random value. It is important that the private key d be large enough. Wiener showed that if p is between q and 2q and d < $n^{1/3}$, then d can be computed efficiently from n and e.

Boneh and Durfee [60] show that as long as $d < n^{0.292}$ an attacker can efficiently recover $d$ from $(n, e)$. In order to reduce the encryption time, it is customary to use a small public exponent e. The common choices of a public exponent e are 3 or $2^{16} + 1$. If the public exponent is small and the plaintext m is very short, then the RSA function may easy to invert. If this concept is adapted, the RSA algorithm could be easily be broken.

Imad Khaled Salah et al [61] have proposed various mathematical attacks on RSA cryptosystem. They indicated integer factoring attacks on RSA. The factoring algorithms come in two parts: general purpose and special purpose algorithms. The efficiency of the general purpose depends on the number to be factored whereas the efficiency of the latter depends on the unknown factor. Special purpose algorithms are best for factoring small numbers with small factors, but the numbers used for the modulus in the RSA do not have any small factors. Hence, general purpose factoring algorithms are more important ones in the context of cryptographic algorithms and their security.

Several authors have illustrated in the literature on low public exponent attacks. J. Hasted [62] showed that small public exponents can be dangerous
when the same plaintext is sent to many different recipients. This attack was later improved by Don Coppersmith [63]. Wei-Hua He et al [64] have given a counterexample to J. Hasted [62] to show the Lee-Chang [65] RSA-based cryptosystem cannot withstand the low exponent attack with respect to their suggested lower boundary for the size of the public encryption key. Our suggested new lower boundary for the size of the public encryption key depends not only on the number of recipients, but also on the size of the message to be encrypted. Furthermore, our suggested new lower boundary is always larger than that suggested by Lee and Chang when the number of recipients is larger than two. It can be easily verified that our suggested new lower boundary actually minimizes the size of the public encryption key required in the RSA-based cryptosystem when a low exponent is used, while still enforcing secrecy.

Kocher [66] explained the timing attack on the basis of Square-and-Multiply exponentiation carried out. In that, the attacker can determine the particular sequence of squaring and multiplications that the program went through. Based on the outcome, the attacker can simply compute the secret exponent d stored on the card.

In a study conducted by Pistoia, Chandra, Fink, & Yahav [67], three areas of security vulnerability in software systems were analyzed. These were: access-control, information flow, and application-programming interface conformance. Static analysis techniques were used to analyze two major areas of access-control: stack-based and role-based access control. Static analysis techniques were also used to address integrity violations and confidentiality violations, which comprise information flow. The study also discussed how static analysis could be used to verify the correct usage of security libraries and interfaces for component-based systems.

Studies conducted by Schneier [68,69,70], the researchers concluded that the argument that secrecy is good for security is a myth and worthy of
rebuttal. They further demonstrated that secrecy is especially not good for security with respect for vulnerability and reliability information. They also show that security that relies totally on secrecy is extremely fragile, and once it is lost, there is no way to regain it. Schneier goes on to make a case that cryptography—since it is based on secret keys that are short, easy to transfer, and easy to change—must rely on one of its basic principles that the cryptographic algorithm be made public if it is to remain strong and offer good security. Using the public key system avoids the fallacy in the argument that secrecy works. Those who oppose secrecy ignore the security value of openness. The only reliable means to improve security is to embrace public scrutiny.

Digital Signature and hash functions

In 1978, R.L. Rivest, A. Shamir, and L. Adleman [24] proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers to permit secure communications without the use of couriers to carry keys, and it also permits one to “sign” digitized documents.

In 1984, D. E. Denning [71] identified several properties that should be satisfied by any signature system; in particular, it should destroy any homographic structure in the underlying public-key algorithm. They also described a signature scheme which satisfies these properties.

In 1990, Ivan Bjerre Damgård [72] showed that if there exists a computationally collision free function $f$ from $m$ bits to $t$ bits where $m > t$, then there exists a computationally collision free function $h$ mapping messages of arbitrary polynomial lengths to $t$-bit strings. Let $n$ be the length of the message. $h$ can be constructed either such that it can be evaluated in time linear in $n$ using 1 processor, or such that it takes time $O(\log(n))$ using $O(n)$ processors, counting evaluations of $f$ as one step. Finally, for any constant $k$
and large $n$, a speedup by a factor of $k$ over the first construction is available using $k$ processors. Also suggested changes to other proposed constructions to make a proof of security potentially easier. They gave three concrete examples of constructions, based on modular squaring, on Wolfram’s pseudorandom bit generator [Wo], and on the knapsack problem.

In 2001, Burton S. Kaliski [73] explained the RSA Digital Signature Scheme and its legal issues in detail. Also advised developers to make a planned, gradual migration to an RSA digital signature scheme offering several compelling benefits, most notably provable security, continued use of existing RSA keys and hardware accelerators, and straightforward, localized software changes.

In 2002, W. C. Cheng, C. F. Chou and L. Golubchik [74] proposed a simple way to improve the performance of the server is to reduce the number of computed digital signatures by combining a set of documents into a batch in a smart way and signing each batch only once. This reduces the demand on the CPU but requires extra information to be sent to clients. They investigated the performance characteristics of online digital signature batching schemes and presented a semi-Markov model of a gated batch-based digital signature server and its approximate solution and also validate the solutions of the analytical model through both emulation and simulation. The study shows that significant computational benefits can be obtained from batching without significant increases in the amount of additional information that needs to be sent to the clients.

In 2002, P. Kitos et al [75] proposed a VLSI implementation of the digital signature scheme for efficient usage in any cryptographic protocol. This architecture is based on Secure Hash Function and the 512-bit RSA cryptographic algorithm. The whole design was captured by using VHDL language and a FPGA device was used for the hardware implementation of the architecture. A method to reduce the switching activity of the overall design is
introduced. The proposed VLSI implementation of the Digital Signature scheme achieves a data throughput up to 32 Kbit/sec.

In 2005, C. Dods, N. P. Smart and M. Stam [76] discussed various issues associated with signature schemes based solely upon hash functions. Such schemes are currently attractive in some limited applications, but their importance may increase if ever a practical quantum computer was built. They also discussed issues related to both their implementation and their security and provide the first complete treatment of practical implementations of hash based signature schemes in the literature.

In 2005, Z. Shao [77] proposed a new digital signature scheme based on the difficulties of simultaneously solving the factoring and discrete logarithm problems has been proposed by Tzeng et al. in 2004. In the proposed scheme, each user uses a common arithmetic modulus and only owns one private key and one public key. Although Tzeng and colleagues claimed that their scheme cannot be overruled by some possible limitations, they showed that their scheme is not secure if attackers can solve discrete logarithm problems or factoring composite numbers.

In 2005, Ilya Mirnov [78] surveyed theory and applications of cryptographic hash functions, such as MD5 and SHA-1, especially their resistance to collision-finding attacks and reviewed definitions, design principles, trace genealogy of standard hash functions, discuss generic attacks, attacks on iterative hash functions, and recent attacks on specific functions.

In 2005, Xiaoyun Wang and Hongbo Yu [79] discussed how to break MD5 and other hash functions. In their paper they presented a new powerful attack on MD5 which allows finding collisions efficiently. The attack is a differential attack, which unlike most differential attacks, does not use the exclusive-or as a measure of difference, but instead uses modular integer
subtraction as the measure. This attack is also applicable to other hash functions, such as RIPEMD and HAVAL.

In 2006, S. R. Subramanya and Byung K. Yi [80] explained digital signature, hash functions and its importance and also said that this technology is rather new and emerging and is expected to experience growth and widespread use in the coming years.

In 2006, D. R. Stinson [81] studied issues related to the notion of “secure” hash functions. Several necessary conditions are considered, as well as a popular sufficient condition (the so-called random oracle model). In particular, he considered the important question “does collision resistance imply preimage resistance?” and provided partial answers to this question – both positive and negative! – based on uniformity properties of the hash function under consideration.

In 2006, Carlos Cid [82] emphasized on cryptographic hash functions. His paper provides an overview of cryptographic hash functions and some of the recent developments affecting their security, namely the discovery of efficient methods for constructing collisions for algorithms such as MD5 and SHA-1. We also discuss the many implications of these recent attacks, and the possible directions for the development of the theory of hash functions.

In 2007, Zanin, Di Pietro, & Mancini [83] in their study presented a new distributed signature protocol based on the RSA cryptographic algorithm, which is suitable for large-scale ad-hoc networks. This signature protocol is shown to be distributed, adaptive, and robust while remaining subject to tight security and architectural constraints. The study reveals that the robustness of this protocol scheme can be enhanced by involving only a fraction of the nodes on the network. Zanin et al. demonstrated that their protocol scheme is correct, because it allows a chosen number of nodes to produce a valid cryptographic signature; it is secure, because an attacker who compromises
fewer than the given number of nodes is unable to disrupt the service or produce a bogus signature; and it is efficient, because of the low overhead in comparison to the number of features provided.

In 2008, Joseph Sterling Grah [84] researched on the application of hash functions in cryptography and presented standard cryptographic hash functions in detail.

In 2008, Ying-yu Cao and Chong Fu [26] proposed a carry array based large integer denotation approach to speed up the large integer calculation in RSA key generation and data encryption/decryption process, so as to improve the efficiency of a RSA system. The RSA digital signature algorithm and its mathematic foundation are discussed in detail and the feasibility of RSA algorithm is proved. An integrated large integer library is built by using C++ and the implementations of Miller-Rabin, extended Euclid and Montgomery algorithms for complex numeric operations in RSA are given.

In 2010, Xinli Hu & Lianjie Ma [85] described a hybrid encryption technology which involves encryption technology, digital digest, digital authentication and digital signature. Encryption technology is to ensure the confidentiality of information, digital digest to ensure the integrity of information, while digital authentication and digital signature technology can be certified to protect the Authentication identity, non-repudiation and non-counterfeit. By using of hybrid encryption technology, that is, the above four kinds technology of integration application, the security of electronic documents will be greatly improved.

In 2011, Erfaneh Noorouzi et al [86] introduced a new digital signature which works very well for such applications which have low file size for sending. The new hash function generates dynamic and smaller size of bits which depends on each bytes of message. A simple mechanism for hashing the
message and encryption is one of advantages of suggestive algorithms. The main function which is used for hashing is bitwise OR and Multiply functions. Testing new algorithms showed that its hashed file size is 4% of the original file in messages with size lower than 1600 bytes. This algorithm can be used in applications which have low file size for sending and want simple and fast algorithms for generating digital signature.

In 2012, Prakash Kuppuswamy, Peer Mohammad Appa and Saeed Q. Y. Al-Khalidi [87] presents a new variant of digital signature algorithm which is based on linear block cipher or Hill cipher initiate with Asymmetric algorithm using mod 37 which is faster and highly secured.

In 2012, Hemant Kumar and Ajit Singh [88] presented an architecture is related with Secure Hash Function and 512-bit SRNN cryptographic algorithm. SRNN algorithm is based on RSA algorithm with some modification and included more security. They also designed a new algorithm for generating signature that overcomes the shortcomings of the RSA system.

In 2013, Zhang Hairong, Li Rong, Li Ling and Dong Ying [89] presented an improved speed algorithm isDSA (Improved Speed DSA), which is based on the idea of avoiding the complex and time-consuming modular inverse. In isDSA, it modifies the component $s$ of the signature, cancels $w$ of the verification, modifies $u_1$ and $u_2$ of the verification, and in the meantime the independent messages operations are pre-computed and saved. Using the same fast algorithm for large numbers, isDSA and DSA are simulated. Setting the length of modulus $p$ 1024bits, the simulation result shows that the signature speeds of isDSA and DSA with pre-computation are same - less than 1ms because of no complicated operations. And the verification speed of isDSA is increased by 25.40% than DSA. And the security of isDSA and DSA is compared and analyzed, it proves that isDSA has the same security strength with DSA.
Finally, a variety of existing scholarly and non-scholarly works related to enhancement of security, increasing operational speed, and generation of key-stream, attacks, hash functions, digital signature for cryptographic algorithms and techniques have been studied. Their relevance to the existing cryptographic algorithms is also analyzed. These ideas are useful to develop various mathematical models so that they could be stored as components in the proposed application framework. Any user can use these components as methods for runtime optimization and for increasing the operational speed of the cryptographic algorithms.