A Survey about the Latest Trends and Research Issues of Cryptographic Elements

Ijaz Ali Shoukat[1, 2], Kamalrulnizam Abu Bakar[1] and Mohsin Iftikhar[2]

**[1] Department of Computer Systems and Communication, Universiti Teknologi Malaysia
81310, Johor Bahru, Malaysia**

**[2] College of Computer and Information Sciences, King Saud University
P. O. Box. 51178 Riyadh 11543, Saudi Arabia**

Abstract

Progression in computing powers and parallelism technology are creating obstruction for credible security especially in electronic information swapping under cryptosystems. An enormous set of cryptographic schemes persist in which each has its own affirmative and feeble characteristics. Some schemes carry the use of long bits key and some support the use of small key. Practical cryptosystems are either symmetric or asymmetric in nature. In this painstaking gaze, the accurate selection of right encryption scheme matters for desired information swap to meet enhanced security objectives. This survey compares trendy encryption techniques for convinced selection of both key and cryptographic scheme. In addition, this study introduces two new encryption selection constrains (section 4.1) which are neglected in previous studies. Finally this comprehensive survey thrash outs the latest trends and research issues upon cryptographic elements to conclude forthcoming necessities related to cryptographic key, algorithm structure and enhanced privacy especially in transferring the multimedia information.

Keywords: *Encryption schemes, symmetric vs. asymmetric, steganography, digital signature, hash functions, Cryptographic Issues*

1. Introduction

Cryptography can be categories as a branch of mathematics and computer science which further relates with information security and computer engineering. Krptōs ("hidden") is a Greek word gives birth to English word called cryptography- an art of changing the actual face look of information as well as converting it into unreadable form. Cryptography further relies on encryption techniques (symmetric and asymmetric) to encode the actual text message (Plain Text) with the use of secret code called key. The process of encoding or encrypting the plain text is referred as enciphering or encryption and the vise versed process is called deciphering or decryption. Symmetric encryption requires a single shared secret code known as private key and asymmetric encryption is based on two key(s); private key and public key where private key remains secret and public key is publically available. In asymmetric encryption public key is used to encrypt the message and private key is used to decrypt the same message.

Just to encrypt and decrypt the message cannot fulfill overall security requirements because the word *security* is itself relies on confidentially, integrity (authenticity, non-repudiation) and availability [1]. Confidentiality concerns with secrecy and privacy which means message should be visible to whom person for which it has been sent and integrity can be further classified into two terms: (1) authenticity – which means the identity of sender should be verified on delivering the message weather the information is coming from authentic sender, from whom we are expecting. (2) Non-repudiation – it means message should not be falsely modified with any kind of fake addition or deletion. Availability means information (message, key, Certificate Verification) and medium (Certification Authority Server, online services) should be timely available when needed. These security objectives births to key exchange methods (Diffie, Hellman, digital signature) and the asymmetric encryption which involves third trust party and the use of two key(s).

Cryptanalysis is art of breaking cryptographic algorithm using analytical reasoning, pattern locating, guessing and statistical analysis. The person who uses cryptanalysis science is called cryptanalyst or attacker where the both cryptography and cryptanalysis lie under cryptology [2]. Security is the major controlled factor now days mostly concerns with large information exchange system like Internet. Mostly users demand secure communication especially in case organizational linkage, Governmental communication and banking transactions. Cryptographic algorithms are reliable phenomena in this situation. Some cryptographic algorithms are symmetric and some are asymmetric in nature as summarized in table below.

Ijaz Ali Shoukat – PhD Student, Universiti Teknologi Malaysia
Assoc. Prof. Dr. Kamalrulnizam Bin Abu Bakar – Main Advisor/ Supervisor
Dr. Mohsin Iftikhar – Co-Supervisor

Table 1: Algorithm Categories [3]

Encryption Techniques	Algorithms	Country(s)
Symmetric	Data Encryption Standard (DES)	US(IBM)
	Advanced Encryption Standard(AES)	Belgium
	International encryption Standard (IDEA)	Switzerland
	Twofish	US (Counterpane)
	Blowfish	US (Counterpane)
	TEA (Tiny Encryption Algorithm	UK (Cambridge)
	Serpent	UK, Israel, Norway
	MARS US	US (IBM)
	Kasumi	Europe (ETSI)
	SEED	South Korea (Korea Information Security Agency)
	RC6	US (RSA)
Asymmetric	Rivest-Shamir-Adleman (RSA)	US (RSA)
	Diffie-Hellman	
	Digital Signature Algorithm (DSA)	
	EIGAMAl	
	XTR stands for ' ECSTR' Efficient and Compact Subgroup Trace Representation	

In Symmetric cryptography, algorithms are either block cipher or stream cipher in block cipher plain text is converted into blocks (64 or 128 bits) and arithmetic operations (XOR, NOT, OR and etc.) are implemented on block level in such a way each block is encrypted separately. Each block can be encrypted either with a operation and the same operation may be repeated for any other next block but in stream cipher whole plain text is considered as single block and its every bit or byte (bit stream) relatively very small than block size is encrypted with different operation (may be repeated for any other bit or byte). The use of symmetric algorithms require that both parties have to share and agreed on same secret or private key before starting encryption procedure but in case of asymmetric algorithms public key is publically available to start encryption any time when needed before asking the other party and private key remains secret in both sides. Symmetric key length is shorter than asymmetric key length.

This survey does not concern with the issues of cryptographic algorithms but it mostly concerns the cryptographic primitives to point out the latest trends, research issues and future necessities. Cryptography is a secure technological phenomenon for information security. Prehistory of cryptography is reliant on message hiding art called steganography. Classical cryptography is based on information theory appeared in 1949 with the publication of “Communication Theory of Secrecy Systems” by C. Shannon. In classical cryptography both plain text and key were same length to support secrecy through encryption. New look of cryptography revolves around the some factors like confidentially, integrity (authenticity, non-repudiation) and availability to enhance security issues [4].

2. Cryptographic Types and Elements

These types and elements based on Encryption (symmetric and asymmetric) ,signature and key agreement where the signature can be further classified as Short Signature, Blind Signature, Multi signature, Aggregate Signature, Verifiably Encryption Signature, Ring Signature, Group Signature, Proxy Signature and Unique Signature /invariant signature Schemes[5]. Furthermore the survey [5] reported that the Identity base Public Key Cryptography (ID-PKC) scheme involves third trusted party to generate public and private key(s); due to the involvement of third party the following risks can be associated with this scheme.

1. Third party knows private key which may be risky.
2. To get private key once again person has to authenticate himself which require extra effort and loss of time.
3. Secure channel is required to transmit private key.
4. The both parties (sender and receiver) have to know and verify the public key of each other.

2.1 Comparison of Cryptographic Schemes

Generalized encryption schemes are symmetric encryption and asymmetric encryption but there are

some other cryptographic techniques are also the part of literature like Chaotic image encryption, Quantum cryptography, BioCryptosystems, Visual Cryptography, Elliptic Cryptography which lie under symmetric or asymmetric schemes. Table 2 shows the comparison of symmetric and asymmetric encryption scheme.

Table 2: Symmetric vs. Asymmetric Encryption Schemes

Symmetric Encryption OR Private-Key Cryptosystems	Asymmetric Encryption OR Public-Key Cryptosystems
It is based on single secret key to encrypt and decrypt data. Key is called share, secret or private key [6].	It deals with pair of key(s) Public key and Private key. Public key is used to encrypt the message and private key is used to decrypt the message [6].
Symmetric key size and length is often smaller than asymmetric key(s).	Key size and length is often larger than symmetric key
In symmetric encryption process there is need to agree on same secret key before starting encryption [6].	There is no need to agree on same secret key before starting encryption process [6]. Because public key is publically available but the verification of public is required.
It deals with operations like XOR, OR NOT, OR, substitution etc. [6].	It deals with nontrivial mathematical computations, modular arithmetic functions, huge integers (512- 2048 bits) [6].
The symmetric based algorithms are 100 times faster than asymmetric ones [23].	Asymmetric based methods are 100 times slower than symmetric ones [23].
It requires less processing and electric power than asymmetric algorithms of equal length and complexity [6].	It requires more processing and electric power than symmetric algorithm of equal length and complexity [6].
It provides confidentiality [7].	It provides confidentiality [7].
It did not provide integrity by itself [7].	It did not provide integrity by itself because it also relies on message digest and digital signature for this purpose [7].
It did not provide origin authentication [7].	It provides origin authentication [7] as it uses digital signature for this purpose.
Key must be remained secret in both sides because there is need to share private key.	Public key is publically available and each part has its own private key which needs not to be shared.
The life of key is not longer because it has shared with the other person so in case of any future secret transaction for any other person there is need to be changed it for security reasons.	The life time of key is longer because each party has its own private key which needs not be shared and it remains secret for both parties.
Group key generation formula for symmetric encryption scheme is n(n-1)/2 = ? keys is used to calculate required key(s) for n users. So this approach is less feasible in case of mutual communication of a group of n users because if there are 5 users in a group then total key(s) required to exchange for whole group will be 5(5-1)/2 = 10 keys. This situation will result more load on network. Similarly if a user wants to communicate with 8 different users then against each user the same sender will require to select and share another secret key which is difficult to remember.	There is no need to get and remember more and more secret keys because it has only 2 keys for any no. of users.
It did not involve third party.	It involves third party called Certification Authority (CA).
There is only one key which results less hedge to manage.	Managing of key(s) and certificate is complex and it is also time consuming to get touch with the trusted party.
It did not need any kind of certificate or extra registration charges because it did not deal with third party.	It requires extra registration charges due to third party involvement and renewal of certificates.
It did not share any other personal information except the secret key. So it has no miss use information vulnerabilities.	The public key contains much information about the person which may be wrongly used by the other person(s) to whom we are going to share it.
It did not require any extra validation time like client validation in asymmetric scheme.	Each time there is needs to validate the client's certificate which may be stopped or delayed if the CA's server is damaged or down.
It has not any danger of third party related political or spy miss use.	In case of highly secret information related to Governmental plans or any country's defense the involvement of third party may be risky due to political or spy based attack especially in case of Identity based Public Key Cryptography (ID-PKC) due to private key escrow problem which means third party knows the private keys of registered users.
It did not require any extra space to store or manage digital certificates like asymmetric scheme.	For third trusted party the storage and management of certificates is becoming critical due to the increase of large no. of demands.

Symmetric encryption often referred as secret-key cryptosystems and asymmetric encryption is the same name as public-key cryptosystems. Public-key cryptosystems further birth to digital signature in

which verification is done with public key and signing is performed with private key [7]. Moreover, the study [7] reported that digital signatures are slow in processing but it can be improved by combing it to hash functions that are fast in speed and also known as message digest or deletion codes but another technique called authentication codes is also available to provide message integrity. The benefits to authentication codes are same as hash function with additional characteristic of producing shorter length message. Table 3 reports the comparison of digital signature, hash functions and Message Authentication Code (MAC).

Table 3: Comparison of Digital Signature, Hash Functions and Message Authentication Code [7]

Digital Signatures	Hash Functions	Authentication codes (MACs)
They deal with 1024 bit minimum key length [3] and have not been patented or licensed yet.	Has functions mostly deals with 128 to 256 bit key. examples: MD5, RFC, SHA1, RACE	MACs are able to reduce message into short length. It is typically 32 or 64 bit long and key is 56 bit long. MAC= hash value+ Public Key
Digital signatures rely on public key cryptography; where verification key is public and signing key is referred as secret or private key.		MACs are based on secret key or private key.
As a prerequisite, parties did not need to agree on shared key before starting encryption.	As a prerequisite, parties did not need to agree on shared key before starting encryption.	As a prerequisite, a secret key needs to be shared therefore both parties need to agree on same key before starting the encryption through authentication code.
Digital signatures are slow in processing than hash function and symmetric encryption scheme.	Fast in processing speed.	Quite fast in processing.
Did not provide confidentiality.	Did not provide confidentiality.	Did not provide confidentially.
Digital signatures provide origin authentication.	They did not provide origin authentication.	They provide origin authentication.
Digital signatures provide integrity.	They provide integrity.	They provide integrity.

Electronic passport scheme primarily relies on, Public Key Infrastructures (PKI), Biometrics and Radio Frequency Identification (RFID) to avoid unfair means of authentication. The purpose of RFID wireless system with 13.56MHz frequency is to extract biometric identity (natural physiological characteristics) and PKI is the process of document verification through Country Verifying Certificate Authorities (CVCA) which deals with public and private key(s) [8].

2.2 Performance Factors of Chaotic Image encryption

General cryptographic methods are based on algebraic notations and number theory but Chaotic methods rely on large numbers (chaos) belong to nonlinear dynamics field. Chaotic based cryptographic functions follow deterministic dynamics, non guessable behavior with non-linear functions and chao's properties. Most significantly for any cryptographic method the performance is major factor. The notable issue is that different authors have different opinions for evaluating chaotic encryption methods even the no. of factors and their nature is also vary from person to person. A survey [9] for comparing the performance metric of chaotic based image encryption has been conducted in 2011 which reported following findings as summarized in a Table 4 below.

Table 4: Performance Factors of Chaotic Image Encryption

Performance metrics for performance analysis of chaotic Image encryption	Year	By
▪ Simplicity ▪ Security	2001	Goce Jakimoski and Ljup˘ co Kocarev [10]
▪ Speed ▪ Resistance ▪ Key space ▪ Key sensitivity	2004	Yaobin Mao, Guanrong Chen and Shiguo Lian [11]

▪ Speed, ▪ Key space, ▪ Key sensitivity, ▪ Histogram, ▪ Pixel correlation ▪ Resistance to known attacks.	2006	Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li [12]
▪ Confusion ▪ Diffusion properties, ▪ Correlation coefficient ▪ Histogram.	2008	Su Su Maung, and Myitnt Myint Sein [13]
▪ Key space, ▪ Correlation coefficient ▪ Information entropy	2009	Musheer Ahmad and M Shamsher Alam [14]
▪ Probability distribution, ▪ Complexity ▪ Cipher sensitivity	2009	Wang, Yongping Zhang, Tianjie Cao [15]

2.3 Characteristics of Visual Cryptography

An easy kind of cryptographic technique relies on hiding information by utilizing overlying method of a single or multiple images. Overlying method consists of preparing the two layers where one contains secret information in visual form and other did not contain any secret information. By utilization of pixel expansion and pixel merging schemes the encryption is implemented on secret visual information (printed text, image, handwritten notes). It was firstly designed by Naor and Shamir in 1994 [28]. It does not require complex mathematical computations [29] for decryption process. Following characteristics are associated with visual cryptography [16].

1. Computations are avoided.
2. Encryption time is small because no complex algorithm is available in visual cryptography
3. To avoid extra disk space for encrypted data, compression techniques are needed.
4. Compressed data takes more time to transmit in visual cryptography rather than other cryptography.

2.4 Quantum Cryptography and its Issues [17]

The high performance computers are called quantum machines which necessitate the use of quantum cryptography that restricts the attacker under the implementation of polarization properties of quantum mechanics. In both cryptographic techniques (symmetric and asymmetric) the sender and receiver cannot rely the interception of key by attacker but in quantum cryptography it is possible because it uses an invisible photon. This invisible photo based on no cloning theory which means it impossible to replace it without notifying the other related party. Quantum cryptography creates more processing efforts for attackers rather to general cryptography in case of brute force attack (plain text attack) but two other attacks like man in middle and denial of service (DoS) which both rely on network structure are still possible to implement them in quantum cryptography. Recently Quantum Cryptography does facilitate reliable digital signature because it relies on public key cryptography for integrity and authentication. Moreover, the available quantum signature techniques provide only limited function such as verification that's why its practical use is limited to specified situations [18].

2.5 Elliptic Curve Cryptography (ECC) and its Characteristics [19]

IBM cryptographer Victor Miller and Neal Koblitz from Washington University firstly proposed Elliptic Curve Cryptography as a combined fashion of number theory and algebraic geometry in 1985. It is a type of public key cryptosystem in which there is need to share secret key because EEC deals with two points(x, y) which satisfied the curve equation $\mathbf{y^2 = x^3 + ax + b}$ with particular condition $\mathbf{(4a^3 + 27b^2 \neq 0)}$. Points on curve behave as a Public key and a randomly selected number is considered as private key. Its key size (160 bits) is small and considered as much secure as RSA with 1024 bits key. On the other hand ECC uses small length key pairs (Public and Private) to make it robust in case of memory requirement and processing time as compared to RSA but the issue with ECC is that it is slower in case of signature verification and enciphering process than symmetric encryption [20]. ECC is better decision for small devices with limited computational power and memory chip.

2.6 Bio Cryptosystems [27]

It is based on biometric key and restricts the user to be present at the time of authentication to avoid duplication. Cryptographic key(s) are often large and difficult to remember. On the other hand password codes are mostly short and relies on a common habit to use them repeatedly therefore rather to password code and cryptographic key

(public, private) biometric key is considered as superior because it needs not to be remembered. The other benefits of biometric key are that it provides grunted identification and privacy while authenticating the user. But the major issue with BioCrytosystems is the high variability of biometric traits which creates fuzziness problems.

2.7 Steganography

It is the art of hiding information. Steganography has two types that differ with the usage of mediums. First type is *Physical steganography*- it use physical mediums to hide the message like Invisible Links, Microdots, Puzzles, Spam messages and selection of characters from string (first one or last one). The other one is *Electronic Steganography*- it deals with the following mediums like Image, Audio and Video to hide information. We can store and hide the message in image bits or in audio/video bits. Mostly message is stored in video or audio file where there are inter-bit delays. In audio file if only first or last bit is changed within each byte then the audio and video become out of understand. But the significance issue is that by applying statistical and Radiofrequency methods, like Measurement and Signature Intelligence Technique (MASINT), the inter– bit delays can be realized. The comparison of steganography and cryptography is described in Table 5 below.

Table 5 : Steganography Vs. Cryptography

Steganography	Cryptography
Process of hiding information on digital media through concealing the existence of information. Its motive is to keep secret the presence of message to fool the attacker in order to prevent the detection of the hidden message [21].	Its motive is to obscure the message so that it could not readable with its original meanings.
Message cannot be seen.	Message cannot be understood and remains visible to attacker in encrypted form.
It is hard to guess that whether message is private or ordinary or is it contains secret information behind it or not which minimize the unwanted attentions of attackers.	In case of secure governmental or country secret communication from country to country the encrypted message may attract unwanted attentions of cracker to realize it. **Issue:** In many countries the use of cryptography is prohibited. It can provide enhanced privacy between parties but it is negotiable incase of protection while communicating the highly secret information about criminal shifting or transferring times from one location to other.
If we hide the message under the image may it is possible some important data is altered or lost automatically while communicating the image over internet. This change is minor like change in color (grey or white pixel) which does not detectable by human eye in case of seeing the image but a single bit change may effected the loss of those bit(s) which is the part of secret message.	No such case
The size is major problem because if we conceal the message with image; its size becomes large and in case of large data this is more notable problem.	Size remains consistent or bearable.
It cannot provide most of security objectives (Integrity, authenticity, non repudiation) by itself without using the cryptographic techniques. However it provides confidentiality by itself because mostly, the concerning person knows that the message is hidden in what kind of medium.	It can provide complete security objectives by implementing the public and private key(s) with hash functions or authentication codes or digital signatures.

3. Research Issues and Problems in Cryptography

The existence of high computing power processors are the creating diversified situation for symmetric encryption that relies on small length of key because distributed computation methods can broke small key easily. 56 bits symmetric key of Data Encryption Standard (DES) has already been cracked practically by Electronic Frontier Foundation in 1998 within the duration of less than 3 days [22]. Other problem of symmetric encryption is the key exchange because without secret and secure key exchange, symmetric encryption becomes unconfident. Origin authentication and group based secure information exchange under symmetric approach are the big issues. It cannot be assured at the time of exchanging secret key, either the received key is not falsely modified by hacker and it is really send by the authentic sender from whom we are expecting? Similarly, if a person P wants to send 50 different secret messages to 50 group members then P required to generate 50 secret key(s) for completing this task under symmetric

encryption scheme which is difficult to remember; moreover, in this case if each user wants to communicate with each other user of the same group then the total no. of key(s) required to exchange for whole group can be calculated as follows

Let "G" is the no. of group members
So G = 50
Total Key(s) required for mutual communication of whole group = G(G-1) / 2
= 50(50-1) / 2
= 50(49)/2
= 1225 keys

It means for mutual communication of all group members; 1225 secret keys will be required to exchange and this situation will result extra load on the network. Asymmetric scheme is 100 times slower than symmetric one [23]. It deals with large key(s) and involvement of third trusted party which may be risky from country to country communication due to spy attacks or political reasons. Issuing and renewing of certificate requires cost and extra penalty of time consumption. In case of large data it is not feasible due to laziness of encrypting process that requires more Random Access Memory (RAM) and electric power. Certification Authority behaves like a central server so the central point of failure is another notable issue that may leads the situation to large penalty of waiting time due to load or failure. Furthermore, the increasing demand of public key cryptosystem is creating problem for managing and storing of large no. of certificates. Natural disasters, security threats and vulnerabilities may lead the Certification Authority to a critical situation. It means sufficient backup and enhanced security plans are required for central point authority.

Origin authentication is necessary for security and this objective can be achieved with digital signature but the minimum key size is 1024 bit [3] for digital signature that is the greatest hurdle in processing speed. Hash functions are fast in processing but hash function did not provide origin authentication [7]. Message authentication codes are quite fast and based on symmetric key, so these are required to share and agreed on single key as a prerequisite of encryption; moreover, key is small as compared to public key that makes the user unconfident due to large computation power processors that can act in distributed fashion with parallelism to break the security of small length key.

For chaotic image encryption there is no standard criteria to measure performance as different authors have different opinions. Quantum cryptography does not provide reliable signature scheme for authentication and integrity; furthermore, it associates the possibility of man-in-middle attack and Denial of Service attack. Elliptic Curve Cryptography is slow in signature verification and enciphering process than symmetric encryption. NIST and ISO do not recommend quantum cryptography and elliptic cryptography. Steganography itself is just process of hiding information but it cannot provide required security objectives and concealing process with image results the large size of message. The critical issue with steganography is the implementation of statistical and Radiofrequency methods like Measurement and Signature intelligence (MASINT) to realize the inter–bit delays for cracking the information.

4. Latest Trends and Analysis

Symmetric scheme associates probability of happening many things for the cracker where the asymmetric scheme is based on factorization of large no. with large mathematical functions but it can be determined mathematically that means asymmetric technique is just increasing the processing time but lacked to confuse the cracker with randomness. A study [6] conducted in 2007 that claims; the practical encryption scheme should be probabilistic like symmetric encryption rather than deterministic scheme like a symmetric encryption. In 2009, Perlner. R. A. and Cooper. D. A. said, there is no particular need to replace symmetric encryption with quantum cryptographic methods [24]. In 2007 study [25] reported that the International Standard Organization ISO 9564-1 recommends that the minimum key length for symmetric scheme should be 112 bits for sufficient security. In 2008, Cryptographic Key Injection Facility: Auditor's Guide Version 1.0 reported the following key lengths for following cryptographic algorithms as shown in Table 6.

Table 6: Minimum Key lengths

Cryptographic Schemes	Minimum Key Length
Symmetric Cipher (DES)	112 bits
Asymmetric Elliptic Cryptography	160 bits
Asymmetric RSA and DSA	1024 bits

Studies [25] and [26] reported that National Institute of Standard and Technology (SP800-57, NIST [2005a]) recommends the follow key sizes as summarized in Table 7.

Table 7: Minimum Recommend Key Length by NIST and ISO

Cryptographic Schemes	Minimum Key lengths	Year	Practical Attacks
(2DEA)	80 bits	2007- 2010	Sound assumption of practical Attack is reported
Symmetric Cipher	112 bits	Up to 2030	No practical attack is reported yet.

(3DES)	128 bits	Beyond 2030	No practical attack is reported yet.
Asymmetric Cipher	1024 bits	2007- 2010	No practical attack is reported yet.
	2048 bits	Up to 2030	No practical attack is reported yet.
	3072 bits	Beyond 2030	No practical attack is reported yet.
Elliptic Curve Cryptography	160 bits	2007 -2010	No practical attack is reported yet.
	224 bits	Up to 2030	No practical attack is reported yet.
	256	Beyond 2030	No practical attack is reported yet.

In the light of above discussion and analysis it is clear that Public key cryptography is not feasible in case large data. For asymmetric encryption Large key(s) are based on complex factorization where the diversified situation with large factorization is that 663 bits and 911 bits composite number has been practically factorized in 2005 and 2006 respectively [25]. NIST supports the use of symmetric encryption scheme DES and AES up to 2030 as mentioned in NIST stranded (SP800-57, 2005a). Still symmetric and asymmetric schemes are latest trends and most widely used in all over the world. Key size should be optimal which means not too long but not too small because large key creates problems for small computing devices having low memory and *extra ordinary small* key is not sufficient for brute force attacks. Our analysis founds that the data block length should not be fixed; it should be more than 64 bits long in such a way some blocks length should be more than 128 bits long but should be less than 512 bits long for creating difficulties for cracker at the time of block matching. This objective requires change in the structure of cryptographic algorithms.

4.1 Selection of Right Cryptographic Scheme

The selection of right cryptographic technique relies on time, memory and security where memory constraint is highly significant in case of small devices as they have low memory where the time is most important for processing speed [6]. In this paper we introduced two new constraints as discussed at no. 4 and 5.

1. **Time:** How much time will be needed for encrypting and decrypting the data and how much time is need to fulfill the pre-requisites before starting an encryption.
2. **Memory:** How much memory will be need especially in case of small devices like PDAs, smart cards, RFID tags.
3. **Security:** Selected encryption scheme should meet the confidentiality, integrity (authentication, non-repudiation) and availability.

According to our opinion, the above selection constraints are not enough for the selection of sufficient encryption scheme. We introduced two new worth full constraints in this regard as stated below.

4. **Nature of data:** Nature of data means the communicating information is how much confidential or important. If the information is small in size and not too much important; then any encryption scheme is suitable. If information is highly secret or important then joint hybrid combination of symmetric + asymmetric scheme will be suitable.
5. **Type of Data:** In case of video data the privacy is more valuable and considerable constraint. If the data is small and in video format the previous described constrains (Time, memory, security) suggest the use of asymmetric scheme but this selection is not sufficient because the third party especially in case of Identity based Public Key Cryptography (ID-PKC) can view the video clip as they have all information (key(s), encrypted data). So in this case the privacy is nothing. That's why the *type of data* constraint is highly important constraint which should not be neglected in case of right selection of cryptographic scheme. If data type is confidential multimedia (personal video clip) then the symmetric scheme is good but hybrid encryption method (symmetric + asymmetric) can provide all security objectives.

5. Conclusion

In the light of all above debate and analysis, this study suggests the necessity of randomness in both key and data blocking to get optimal encryption security. To select lengthy key means just to increase the processing time, wastages of extra memory and electric power. So selection of extended bits key is not a confident verdict to achieve optimal performance. Furthermore to presume outsized key with complex factorization is not an adequate solution against brute force attack especially in the presence of parallelism capabilities of super and quantum computers of current era. Actual need is to revise the structure of cryptographic algorithms by creating large number of random probabilities under optimal key length (not too long, nor too small). Symmetric scheme is still a good decision with at least 112 bits key if it is combined with public key cryptography in such a way, for encrypting the data, algorithm should be symmetric in nature and for getting complete security objectives the key (symmetric secret key) should be exchange under public key infrastructure (PKI) having third trusted party. Therefore, hybrid encryption scheme (symmetric + asymmetric) can

provide more secure satisfaction against the hypothetical feelings of miss use or spy attempts of third party. Too meet this satisfaction we support to exchange just symmetric secret key under the involvement of third party by using PKI but the encrypted data should be exchanged separately within sender and receiver only as compared to Identity based Public Key Cryptography (ID-PKC). In this way third party cannot view our data and the confidentiality of communicated information will remain 100%. On the other hand if we use only ID-PKC to encrypt and exchange small video clip then it does not mean the privacy is there because the third party can view the personal video clip which means privacy will be nothing in this case. Our newly proposed two constrains (nature of data and type of data) are really worth full in selection of right encryption scheme for proper data.

References

[1] Bement A. L. et. al. (2004), Standards for Security Categorization of Federal Information and Information Systems, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900.

[2] Ayushi, (2010), A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications (0975 - 8887) Volume 1. No. 15.

[3] CCSDS. (2008), Authentication/Integrity Algorithm Issues Survey, Informational Report, CCSDS 350.3-G-1.

[4] Kramer. S. (2007), Logical Concepts in Cryptography, À La Faculté Informatique Et Communications, Laboratoire de modèles et théorie de calculs.

[5] Dutta R. and Barua. R. et al. (2003), Pairing-Based Cryptographic Protocols : A Survey, Cryptology Research Group Stat-Math and Applied Statistics Unit 203, B. T. Road, Kolkata India 700108

[6] Fontaine. C. and Galand. F. (2007), A Survey of Homomorphic Encryption for Nonspecialists, EURASIP Journal on Information Security Volume 2007, Article ID 13801, 10 pages, doi:10.1155/2007/13801, Hindawi Publishing Corporation.

[7] Kaliski. B. (1993), A Survey of Encryption Standards, *IEEE Micro*, 0272-1732/93/1200-0074$03.*00* 1993 IEEE

[8] Nithyanand. R., A Survey on the Evolution of Cryptographic Protocols in ePassports, University of California – Irvine.

[9] Philip. M. and Das. A. (2011), Survey: Image Encryption using Chaotic Cryptography Schemes, *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011*

[10] Jakimoski, G. and Kocarev L., (2001), Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications. 48(2): 163-169.

[11] Mao Y.B. and Chen G. et. al. (2004), A novel fast image Encryption scheme based on the 3D chaotic baker map, International Journal of Bifurcate Chaos, vol. 14, pp. 3613–3624, 2004.

[12] Gao H. and Zhang. Y. et. al. (2006), A new chaotic algorithm for image encryption, Chaos, Solutions &Fractals, vol. 29, no. 2, pp. 393–399, 2006.

[13] Maung. S. S. and Sein M. M. (2008), A Fast Encryption Scheme Based on Chaotic Maps, GMSARN International Conference on Sustainable Development: Issues and Prospects for the GMS, 2008.

[14] Ahmad. M. and Alam M. S. (2009), A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping, International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[15] Wang. F. and Zhang. Y. et. al. (2009), Research of chaotic block cipher algorithm based on Logistic map, 2009 Second International Conference on Intelligent Computation Technology and Automation, 2009: 678 – 681.

[16] Hawkes L. W. and Yasinsac A. et. al. An Application of Visual Cryptography To Financial Documents, Security and Assurance in Information Technology Laboratory, Computer Science Department, Florida State University Tallahassee, FL 32306-4530

[17] Techateerawat. P. (2010), A Review on Quantum Cryptography Technology, published in International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, Volume 1 No. 1. eISSN: 1906-9642

[18] Moses. T. (2009), Quantum Computing and Cryptography-Their impact on cryptographic practice, Advanced Security Technology, Entrust, Inc.

[19] Muyinda. N. (2009), Elliptic Curve Cryptography, African Institute for Mathematical Sciences (AIMS).

[20] *Kessler. G. C. (1999),* An overview of cryptography in Sloan, J. (Ed.) *Handbook on Local Area Networks, Published by Boston* Auerbach.

[21] Pfitzmann. B. (1996), Information hiding terminology - results of an informal plenary meeting and additional proposals. In *Proceedings of the First International Workshop on Information Hiding*, volume 1174 of *LNCS*, pages 347{350. Springer, 1996}.

[22] Abuzineh. S. (2005), The Data Encryption Standard and It's Problems, ISAC project paper, Program of Advanced Financial Information System.

[23] Schneier. B. (1996), Book- Applied cryptography: Protocols, algorithms, and source code in c, second edition.

[24] Perlner. R. A. and Cooper. D. A. (2009), Quantum Resistant Public Key Cryptography: A Survey, in proceedsing of IDtrust '09, April (14-16), 2009, Gaithersburg, MD. ACM 978-1-60558-474.

[25] Une. M. and Kanda. M. (2007), Year 2010 Issues on Cryptographic Algorithms, Institute for Monetary and Economic Studies, Japan. Vol.25,No.1 / March 2007. Cited at: http://www.imes.boj.or.jp

[26] Giry. D. (2010), Cryptographic Key Length Recommendations, BlueKrypt - v 25.2: - July 7, 2010. Cited at: http://www.keylength.com/en/4/

[27] Saraswathi. K. and Balasubramaniam. R. (2010), BioCryptosystems for Authentication and Network Security-A Survey, Global Journal of Computer Science and Technology, Vol. 10 Issue 3 (Ver 1.0), April 2010.

[28] Naor. M. and Adi Shamir. A. (1995), "Visual Cryptography", advances in cryptology– Eurocrypt, pages (1-12),1995.

[29] Revenkar. P. S. and Anjum. A. (2010), Survey of Visual Cryptography Schemes, published in International Journal of Security and Its Applications, Vol. 4, No. 2, April 2010