ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

A Review to an Invincible Cryptographic Approach: DNA Cryptography

KamaljitKainth[1], Gurpreet Singh[2]

Department of Electronics and Communication, Guru Nanak Dev University Regional campus, Jalandhar, India[1,2]

Abstract: Cryptography is the oldest and effective way to provide security to computer networks and data. The very first cryptographic techniques were developed over 200 years ago. As technology grows there is an evolution in cryptographic techniques. A thorough understanding of cryptography and encryption will help people develop better ways to protect valuable information. In present scenario modern cryptographic techniques provides a better way of encryption. Algorithms like Symmetric and Asymmetric key, ECC cryptography techniques had tremendous advantages over classic techniques [1] but they are also having some drawbacks like security issues, hence did not provide full security to the network. The recent technique Quantum Cryptography is a solution to above problem but there are some issues regarding practical implantation of this approach. Bimolecular Computation has led to remarkable new dimension in secret communication i.e. DNA cryptography[2]. It is a novel field technology that brings forward a new hope for unbreakable algorithms. DNA cryptography has much more storage and computing capabilities than the traditional cryptographic algorithms. This paper will build a comparison between old cryptographic algorithms and their issues and it also provides an overview of different approaches used in DNA Cryptography.

Keywords: Symmetric key cryptography (SKC), Asymmetric key cryptography (AKC), Quantum cryptography (QC), DNA cryptograph

I. INTRODUCTION

Computer Security can be defined as protection yielded to an information system in order to achieve the desiredobjectives of maintaining the integrity, availability, and confidentiality hardware, firmware,software, and information(information system resources)[23].There are mainly three goals of data security namely as data confidently, its integrity and data availability. FIG.1 shows above three concepts which frequently referred as CIAtraid.The above goals of security are fulfilled when security engineering meets mathematics, i.e. cryptography.It provides us with the tools that underlie most modern security protocols.

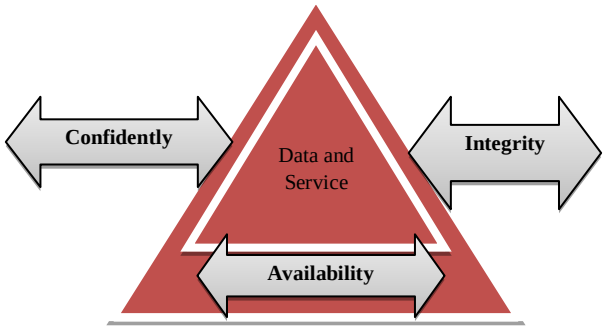

FIG.1.Security requirements triad [23]

II. CRYPTOGRAPHY (BACKGROUND WORK)

Cryptography refers to the science and art of planning ciphers. The study of ciphers and cryptanalysis is known as Cryptology, where cryptanalysis can be defined as art of breaking ciphers. An original message is known as plaintext, while the encryptedmessageis called the cipher text [6]. The process of converting from plaintext to cipher/encrypted text is known as encryption of the data and the very reverse process is known as decryption of the data.Thereexistmany algorithms of cryptography over 200 years old.This paper discusses only modern cryptographic techniques.Cryptography can be classified (on the basis of their encryption process) as Symmetric Key Cryptography (SKC) and Public key cryptography also known as Asymmetric Key Cryptography (AKC)[1].The latter one use different keys for encryption and decryption whereas symmetric key cryptography use same key for the encryption and decryption[5].A comparison between symmetric and asymmetric key cryptographic algorithms made.

A. Symmetric encryption

- Authentication: It did not provide origin authentication.
- Key Size:Symmetric key size and length is often smaller than asymmetric key.
- Size of cipher text :Usually the same or less than that of the plain text .
- Issue :Key exchange is a major problem (Discrete Logarithm Problem).

B. Asymmetric encryption

- Authentication:It provides origin authentication.Key Size:Symmetric key size and length is often smaller than asymmetric key .
- Size of cipher text :Cipher text size is greater than that of the plain text.
- Issue :There is no problem in key exchanging.

After comparing Symmetric and Asymmetric encryption ,let take a look of the discrete logarithm problem in brief .

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

C. The Discrete Logarithm Problem:

Let us consider some group G, suppose α, βϵ G. then if we solve for an integer y such that $\alpha^y = \beta$.This is known as the discrete logarithm problem [3]. Thediscrete logarithm probleminZg is considered difficult if g has at least 150 digits and g-1 has at least one large prime factor as close to g. These criteria for gare safeguards against the known attacks on discrete logarithm problem [7].Let consider there is sender Alice and on the other end BOB is the receiver's secure transmission of data has to be between these users. In finite fields consider a function F ={1,2,3,4,……p-1}Alice have to choose a secret key X (random) from F {} and similarly BOB have to choose Y (random) secret key from F{} .they will compute[$G=(g^y)^x = g^{xy} \bmod p$] and [$G= (g^x)^y = g^{xy} \bmod p$].

Now if there is an eavesdropper named kainth, he has to computeg^{xy} from g^xandg^yknowing x and y and there he will face the Discrete Logarithm Problem in finite fields. FIG.2 demonstrates the keyexchange model. So to defeat these issue Diffie-Hellman Key exchange algorithmis used in cryptography techniques. This allows two parties with no prior knowledge of each other to establish a shared secret key, which typically cipher.
DSA and RSA are thesubstitutefor the public key systems known as Elliptical Curve Cryptography.

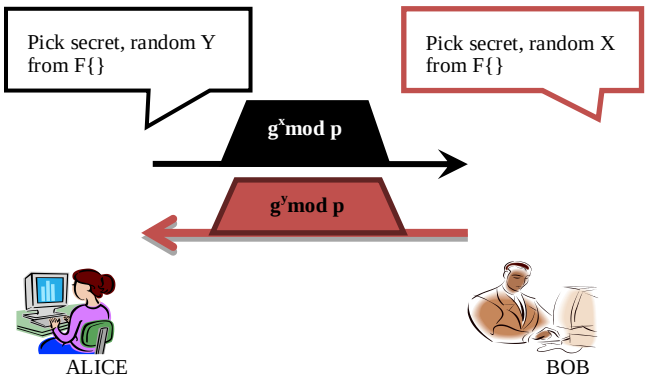

FIG.2.Secret Key echange model [3]

D. Elliptical Curve Cryptography (ECC)

ECC is an alternate for public-key that provides an analogous level of security and what is more of shorter keys than typical public-key algorithms. ECCwas brought in 1985 by Victor Miller [20] and Neal Koblitz [13]. ECC throughout binary field is of specific concern because the operations in binary field a time efficient and more spaced. There are unlike forms of ECC techniques that are sorted as:

- The Elliptic Curve Diffie-Hellman key agreement scheme (keyexchange approach) suggested by Diffie-Hellman scheme and it is based upon the public key cryptography [8].
- Elliptic Curve Digital Signature: This scheme was based upon the digital signature algorithm and is known as Elliptic Curve Digital Signature Algorithm.
- The Elliptic Curve Integrated Encryption Scheme in which encryption and key generation takes place in one step.

ECC is a type of public key cryptosystem in which secret key has to be shared because EEC deals with two points(x, y) which satisfied the curve equation ($y2 = x3 + ax + b$), and there exists different points on the elliptical curve including a point at ∞.General definition for an elliptic curve will be the Weierstrass equation applied condition that $47\ a^2 + 27\ b^2 \neq 0$.

Advantages:

- Key Size: The key size (160 bits) is small andmuch more secure than that of RSA with 1024 bits key.
- Robustness (memory and processing time): As ECC uses small length key pairs (Public and Private) .So it become robust in case of memory requirement and processing time as compared to RSA.[14]
- ECC is better decision for small devices with limited computational power and memory chip..
- Preferred for mobile devices.

*Issue:*ECC is slower just in case of enciphering method and signature verification than those of regular cryptography.

*One –Time Pad:*All cryptographic systems mentioned above are at risk of attacks. Thus there's need of secret writing technique that can't be cracked. This new technique is thought as one time pad. In cryptography it is a secret writing technique that can't be cracked if used properly. A plaintext is matched with random, secret key (or pad) every bit or character of the plaintext is encrypted by the combination it with the corresponding bit or character from the pad using modular addition as shown in FIG.3. [13].Itwas unreal within the early 1900's, and has since been evidenced as unbreakable. The unbreakable aspect of the one-time pad comes from two assumptions:

- The key used is completely random
- The key cannot be used more than once.

The security of the one-time pad relies on keeping the key 100% secret. It is implemented by using a modular addition (XOR) to combine plaintext elements with key elements. The key used for encryption is also used for decryption.

DOI 10.17148/IJARCCE.2015.4175

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

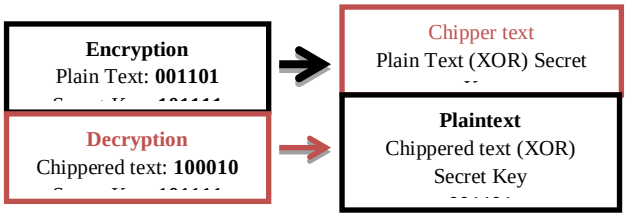

FIG.3. An example of a one-time pad implementation using modular addition.

E. Quantum Cryptography:

Quantum Cryptography: Modern Cryptography has certain limitations. Public key cryptography involves complex calculations which consume more time for encryption and decryption. Also these algorithms are applied to substitute keys rather than for the encryption of twisting amounts of date. RSA and therefore the Diffie-Hellman key schemes are usually utilized to distribute symmetric keys among remote parties as a results calculations area unit slow. As asymmetric encoding is slower than that of symmetric encoding, a brand new hybrid approaches a new reward of the speed of a shared key system. PKC systemssecurity for the initial exchange of the symmetric key [11]. There comes a new technology into existence known as Quantum cryptography. This algorithm is a combination of Quantum key distribution (QKC) and one time pad so that eavesdropping is not possible in this algorithm..

*Quantum key distribution*replace the traditional key distribution method .For example, Alice will send a particular key to Bob. Instead of this Alice and Bob initially generate their own, independent random number sets which contain more numbers than they need for the key material that they will share. Laws of quantum physics guarantied of secure communication. Alice begins by sending a message using a photon gun to send a stream of photons to Bob which is randomly chosen in one of the four polarizations that correspond to vertical, horizontal and diagonal in opposing directions.These polarization are 0, 45, 90 and135 degrees respectively [15][18]. Bob will randomly choose a filter and receive the message. Next by using out-of-band communication system it measure which photon is correct and inform Alice without telling correct measurements. Photos which are not measured correctly will be discarded and rest of photons converted into bits. If any eavesdropper tried to decode the information, he did not able to do so unless he knows the correct polarization of each particular photon. Hence it provides total security to the data [12].

Advantages:

- As photons cannot be duplicated because photons will be destroyed once they are measured or tampered, so it provides undefeated key security.[15]
- As encryption key predefines the length of the one-time pad will correspond to the length of the message, if transmitted message suffered much deviation than the original message receiver section will easily depict that there is loss of data.
- No cloning theory of photons provides better security as it is impossible to replace it without notifying the other related party [11] and less resources needed to maintain it

Issues

- In QKD the signal is currently limited to 90 miles.
- Quantum signature techniques provide only limited function such as verification that's why its practical use is limited to specified situations.
- QKC works upon quantum bits known as qubits, which are either 0 or 1.qubit will discard information which is in-between 0 and 1.This is a major issue of QKC [1].

F. Molecular computation

It is a collimate computation where data can be stored and processed inside objects of molecular size. Bimolecular Computation (BMC) is molecular computation which employs biotechnology techniques like recombinant DNA operations. BMC and therefore Quantum Computation are molecular computation. But they dissents each other by many parameters, few of them are listed in TABLE.2.

G. Hamiltonian path problem:

In graph theory the Hamiltonian path problem and the Hamiltonian cycle problem are problems of determining whether a Hamiltonian path which is defined as a path in an undirected or directed graph that visits each vertex exactly once or we can say that Hamiltonian cycle exists in a given graph is directed or undirected. There are n! different sequences of vertices that might be Hamiltonian paths in a given n-vertex graph so a brute force search algorithm that tests all possible sequences would be very slow. There are several faster approaches. First one is Frank Rubin that separates the edges of the graph into three different classes. Those must equal in the path, those that cannot equal in the path, and undetermined. The other one is dynamic programming algorithm of Bellman, Held, and Karp can be applied to solve the problem in time O (n2 2n).Else there is one more algorithm that provide solution to the above problem which is known as DNA computing. Given graph the problem asks if there exists a path that visits each vertex exactly once. Adelman carefully designed one set of DNA sequences to encode the vertices of the graph and another set of bridge DNA sequences to encode edges between these vertices [21].

TABLE.2.Comparision between Quantum Computation and Bimolecular Computation (BMC)[7]

Quantum Computation		Bimolecular Computation (BMC)
Parameters		
Process	Reversible	Reversible and Non-Reversible
Energy Consumption	1. Dissipate no energy or depend on the technology used.	1. Recombinant DNA operations (reversible) they require arbitrarily small energy. 2. Other recombinant DNA operations like separation (non-reversible), and use approx. 10^{-19}Joules per operation.

DOI 10.17148/IJARCCE.2015.4175

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Volume Bounds	Comparatively better as the volume is no more that the number of qubits.	Increase exponentially with the input size
Processing Rate Bounds	Can be execute at microsecond or even picosecond rates, but may be large as it depends upon the size of measuring apparatus	Vary within few seconds up to 100 min. as it depends upon temp. ,pH, solution concentration e.t.c
Data Storage	In the form of Atoms and photons	In the form of DNA and RNA
Examples	QKC	RNA

H. DNA Computing:

Adleman[20]proposed the DNA computing which give solution to the Hamiltonian path problem and to the others to combinatorial problems using molecular computation. DNA stands for Deoxyribo Nucleic Acid. It is also called as an information carrier. DNA is composed of two long strands of nucleotides, each containing one of four bases namely as (adenine (A), guanine (G), cytosine(C), thymine (T)) which are deoxyribose sugar and a phosphate group [19]. By using brute force method he solved the instance of graph containing seven vertices by encoding it into the molecular form algorithm and then different computational operations were performed with the help of some standard enzymes. Lipton[18] extended the work of Adleman by solving one more problem (NP-complete) called "satisfaction" by using DNA molecules in a test tube to encode the graph for 2 bit numbers.

*DNA Analysis and Storage Data:*There are different techniques to analyze DNA and it is possible to manipulate them only due to the important techniques that were designed and developed for this purpose. Some of them are mentioned here [24].

- DNA sequencing: It helps to determine the order of nucleotide's bases in a DNA sequence. Fluorescent tags can be used for the nucleotide bases and obtaining a fluorescent complementary.
- DNA recombination:. It is a technique for manipulating the genes. In this method certain proteins - enzymes are used to cut and paste parts of the DNA spiral.It is also named as gene splicing.
- Hybridization: It is a natural process in DNA molecules. Hybridization came into existence when two complementary strands of DNA come together to form a double-strand. This is a slow at the beginning, the rest of the matching process is fast if the strands are all complementary.
- DNA synthesis: It isprocess ofcreation of synthetic DNA molecules named oligonucleotides. Synthetic Oligonucleotides represent DNA strands usually10-100 nucleotides long.

DNA provides a medium for ultra-compact information storage In DNA large amounts of data can be stored in compress volume. DNA has much more storage capacity than that of conventional electronic, magnetic and optical media. Most recombinant DNA techniques are applied at concentrations of 5 grams of DNA per liter of water. Then a liter of water contains in solution about 1021 DNA bases. One liter of water provides an associative memory with 1019 to 1020 bytes, which is 107 to 108 tera-bytes, a very big amount of data[19].To store the same kind of data on hard drives the densest storage medium in use today one would need 233 pieces of three TB drives which weights a total of one hundred and fifty one kilos.

III. DNA CRYPTOGRAPHY (RELATED WORK)

An efficient direction of providing data security can be termed as DNA based Cryptography. In this plain text will be converted to the message which cannot be read by any eavesdropper. The encryption and decryption use DNA sequencing property of the DNA.DNA cryptography enhances the data security effective encryption algorithms by using DNA as a medium for large scale computation system. Biological properties of DNA sequences are used in almost of the cryptographic works.DNA cryptosystem use random one time methods These encryption method used mapping methods which include [21] (i).substitution method where encryption of message sequence is done by associated matching with corresponding section of one time DNA pad and the other method for encryption is (ii) The use of XOR computation and decryption is done by the same method, obviously in reverse manner.

TABLE.3. DNA ALGORITHMS BASED ON SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHIC APPROACH

Symmetric key Cryptographic Approach	Asymmetric key Cryptographic Approach
Algorithm :YAEA DNA Encryption *Technology* Substitution, one-time pad.	*Algorithm* : Public-key system using DNA *Technology*: Molecular
Algorithm : Secure routing in MANETs *Technology:* Central dogma of molecular biology, one-time pad.	*Algorithm* : Encryption Scheme Using DNA *Technology* : PCR amplification,DNA synthesis and DNA digital coding,
Algorithm: Secret Data Writing Using DNA Sequences, *Technology*:one-time pad.	*Algorithm*: Asymmetric Encryption and Signature with DNA
Security and Complexity of DNA Based Cipher *Technology* DNA Indexing, one-time pad	*Technology* :Hybridization,DNA chip technology,

Digital information storage in DNA: Small scale workresults in the difficulty in reading and writing faultless and long aDNA sequences. So it has a small spectrum of applications. Thisparticular issue led to encoding of digital information by using encoding schemes like base-2 and ASCII encodings with the help of next-generation DNA synthesis and sequencingtechniques[5]. These techniques have some advantages over the previous DNA storage approaches.

- Easy understanding of DNA sequences : Instead of two bits per base a new method which allows us to encode of one bit per base, i.e. A or C for 0, G or T for 1.It also providesencoding of messages different ways so that sequences can be read or write easily .

DOI 10.17148/IJARCCE.2015.4175

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

- Splitting: Splitting of the bit stream into addressed data blocks can be done so that we eliminate the need for long DNA constructs that are complex to assemble at this scale.
- Vitro approach:By using vitro approach we can avoid cloning and stability issues of in vivo approaches.

By using above new methods we can overcome with the issues of previous DNA storage approaches.

Advantages:

- DNA-Regeneration: By using this method one can generate binary random sequences of any length using DNA structures for public or private databases and the number of distinct random sequences is practically unlimited.[2]
- Security: DNA cryptography provides a better security to the encrypted data than that of previous cryptographic techniques.
- Storage:It provides security to large amount of data, i.e. it can store more information and data than the other cryptographic techniques.
- OTP cryptosystem: OTP system is unbreakable.The OTP key doesn't have to be transmitted entirely to the recipient. It can easily generate the key by using the same DNA database.
- Hence it provides an easy key management and this remove main drawback of symmetric cryptography: difficult key management when the number of users grows.

*Issue:*DNA cryptography has wide applications and far better than traditional cryptographic techniques. But beside all of these has it has some issues like implementation of this approach is quite difficult than the others technique.

IV. CONCLUSION

Symmetricand asymmetriccryptographic techniques provide more security to data then those of traditional cryptographic techniques, but it has certain issues like discrete logarithm problem. As technology grew, these approaches failed to provide security to the data. To overcome this ECC and Quantum Cryptographic came into existence. But these approaches also suffer from certain limitations as mentioned above in this paper. Finally DNA cryptography came into existence in recent years. Benefits of this technology are beyond our imagination,but this implementation of this technology is quite difficult as it requires. Asunderstanding of cryptography and encryption will help people develop better ways to protect valuable information as technology becomes faster and more efficient.

REFERENCES

[1] Ajay.Kakkar, M. L. Singh, P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in MultinodeNetwork",International Journal of Engineering and Technology ,Volume 2 No. 1,pp. 85-92,January 2012.

[2] Ashish. Gehani, Thomas. H. LaBean and John. H. Reif, "DNA-based Cryptography",5th Annual DIMACS Meeting on DNA Based Computers, MIT, Cambridge ,June , 1999.

[3] D. J. Bernstein. New Die-Hellman speed records. In M. Yung, Y. Dodis, A. Kiayias, andT. Malkin, editors, Public Key Cryptography (PKC 2006), volume 3958 of LNCS, Springer, pp. 207-228.

[4] G. JULIUS. CAESAR, JOHN. F. KENNEDY, "Cryptography, and Security Engineering: A Guide to Building Dependable Distributed Systems", pp. 73-81, Curve25519 (2006).

[5] Grasha. Jacob1, A. Murugan, "DNA based Cryptography AnOverview and Analysis", Int. J. Emerg. Sci., 3(1), 36-42ISSN: 2222-4254, pp. 36-42, March 2013.

[6] Ijaz. Ali.Shoukat, Kamalrulnizam. Abu. Bakar1 and MohsinIftikhar, "A Survey about the Latest Trends and Research Issues of Cryptographic Elements", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2,pp. 140-149,May 2011.

[7] John. H. Reif, "Alternative Computational Models: A Comparison of Bimolecular and Quantum Computation", pp. 1-16.

[8] Joppe. W. Bos1,J. Alex.Halderman, Nadia.Heninger, Jonathan. Moore, Michael. Naehrig, and Eric.Wustrow, "Elliptic Curve Cryptography in Practice", Microsoft Research University of Michigan, University of Pennsylvania .

[9] Mrs. Megha. Kolhekar, Mrs. Anita.Jadhav, "IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY ON TEXTAND IMAGE" ,International Journal of Enterprise Computing and Business Systems,Vol. 1 Issue 2, July 2011.

[10] Matthew. England, "Elliptic curve cryptography", Heriot-Watt University, pp. 47-58, summer 2006.

[11] MehrdadS.Sharbaf. & Associates, "Exploration of Quantum Cryptography in Network Security", 24th IEEE Annual Computer Communications Workshop (CCW).

[12] M. IndraSena. Reddy, K. Subba. Reddy, M. Purushotham. Reddy, P.J. Bhata, Rajeev, "Key Distillation Process on Quantum Cryptography Protocols in Network Security" ,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 6, , pp. 19-24, June 2012.

[13] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209.1999.

[14] Nicholas, G. McDonald, "PAST, PRESENT, AND FUTUREMETHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION". A Research Review, Department of Electrical and Computer Engineering University of Utah, pp. 1-22,

[15] Neal. R. Wagner, "The Laws of Cryptography Perfect Cryptography: The One-Time Pad", http://www.cs.utsa.edu/~wagner/laws/pad.html, 2002.

[16] Nirmalya. Kar, Atanu. Majumder, Ashim. Saha, Suman. Deb, "Data Security And Cryptography Based On DNA Sequencing", International Journal of Information Technology & Computer Science (IJITCS) (ISSN No : 2091-1610) Volume 10 , Issue No : 3,pp . 24-32, 2013.

[17] Piyush. Saxena, Amarpal. Singh, Sangeeta. Lalwani, "Use of DNA for Computation, Storage and Cryptography of Information" , International Journal of Innovative Technology and Exploring Engineering (IJITEE),ISSN: 2278-3075, Volume-3, Issue-2,pp. 26-30,July 2013 .

[18] Richard. J. Hughes, M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer, "Quantum Cryptography", University of California, LA-UR-95-806.

[19] Sanjeev.Dhawan, Alisha.Saini ,"Secure Data Transmission Techniques Based on DNA Cryptography", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), pp. 35-100,2012.

[20] Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology: proceedings Crypto'85, pp. 417-426

[21] http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Hamiltonian_path_problem.html

[22] [23] WILLIAM STALLINGS, "Cryptography and Network Security Principle and practice", Fifth edition, 2006 Pearson Education, Inc., publishing as Prentice Hall pp8-55, 2011.