International Journal of Computer Application Issue 3, Volume 2 (April 2013)
Available online on http://www.rspublication.com/ijca/ijca_index.htm ISSN: 2250-1797

LEGAL ISSUES INVOLVING CRYPTOGRAPHY IN INDIA

Parvathy.A[1], Ravi Shankar Choudhary[2], Dr. Vrijendra Singh[3]

1. MSCLIS, IIIT-A, UP, INDIA
2. MSCLIS, IIIT-A, UP, INDIA
3. Assistant Professor, Chief Proctor & Faculty In-charge(Ph.D Cell), IIIT-A, UP, INDIA,

ABSTRACT

The value of information is increasing day by day. Technological advancement had brought radical change in the exchange of information, which also gave birth to issues relating to freedom of information, the flow of information and the use of technology. Encryption and other advanced technologies can be use as a solution to these problems. But, the problem however, is to whether and to what extent the use of encryption techniques should be restricted by law. In most of the countries regulations on encryption techniques comes as a conflicting interest between the privacy rights of individuals and national security. By this paper we address major issues relating to the encryption laws in India namely issues relating to the commercial use of encryption software and hardware by private individuals and companies, credibility of the concept of key escrow or back door entry, and issues relating to the export of encryption software and hardware. And solutions are provided in the form of daft recommendations to the government.

Key words: Cryptography, IT Act, Key escrow, Key management, Lawful access, Quantum Cryptography, SCOMET Items, Self incrimination.

I. INTRODUCTION

Technological advancement had brought radical change in the exchange of information. One among such technological advancement is the advent of internet. Today people use internet for fulfilling their day to day activities such as booking air ticket, mobile recharge, purchasing books, clothes, for sending mails etc. Within micro seconds lots of critical information is exchanged over the internet, and the security of these critical information in transit is in question. Here comes the need of encryption techniques. The roots of the word encryption-crypt-comes from the Greek word Kryptos, meaning hidden or secret[1]. Cryptography is the process of translating data into an unreadable from. It is mainly used for protecting the confidentiality of data. Data is translated with the help of mathematical equations. The information used to decrypt the data is called a key. If same key is used for encryption and decryption then it is called single key system and if two keys i.e., public key and private key are used it is called dual-key system. The Strength of an encryption algorithm lies in the length of the key. Cryptography is an

effective tool for the secure use of information technology by ensuring the confidentiality integrity and availability of data and by providing authentication and non-repudiation mechanisms for that data[2]. It is a self-help mechanism against the newly emerging computer crimes. And it is necessary to protect the privacy rights of individuals, but at the same time it can be misused by the criminals to evade from law enforcement agencies. As encryption is a foundation for e-commerce and e-banking in our country, it is necessary to protect their information from being compromised. But the encryption regulations in India are weak to protect the privacy rights of the individuals.

II. MAJOR LAWS GOVERNING ENCRYPTION IN INDIA

History of Cryptography starts from the beginning of mankind. Ever since mankind started to communicate, the need to hide that communication also emerged. In ancient times cryptography has been considered vital in diplomatic and military secrecy. Cryptography techniques were used during the First and Second World War. As cryptography became more important and increasingly complicated, Government imposed restrictions on the use of cryptography. In India there is no specific law for encryption. Some of the provisions in Information Technology Act, Department of Telecommunication, SEBI, RBI, and TRAI etc provide guidelines for the use of encryption in India. In this section we will discuss these guidelines in detail:

2.1 THE INFORMATION TECHNOLOGY ACT, 2000

In India S. 84A of the Information Technology (Amendment) Act, 2008 empowers the Central Government to make a separate encryption policy independent of the guidelines issued by the Department of Telecommunications (DoT)[3]. And S.69 of the Information Technology (Amendment) Act, 2008 authorizes any Government Official or any policeman to listen into any phone calls, read any SMSs, and emails, and monitor the websites anyone visit[4]. They can perform it without obtaining any warrant from a Magistrate, which is a clear violation of Article 21 of the Constitution of India.

The Information Technology (Intermediaries Guidelines) Rules, 2011 require an intermediary to provide information to Government agencies those are lawfully authorized for investigative and other purposes (Rule 7)[5]. The information shall be provided for the purpose of verifying the identity of and individual. And for such other purposes like preventing, detecting, investigating and prosecution of cyber security incidents and for the punishment of offences committed under any law for the time being in force[6]. Therefore as per Rule 7, ISPs will be required to disclose the content to the authorities even if encrypted. Information Technology Act, 2000 does not specifically prohibit the commercial use of encryption by individuals or companies. It means the commercial use of encryption by individuals or companies are allowed.

2.2 DEPARTMENT OF TELECOMMUNICATION (DoT)

Without obtaining any prior permission from the DoT, ISP license holders such as individuals, groups, and organizations are permitted to freely utilize the encryption levels up to 40 bit key length[7]. And it is mandatory for such ISPs to obtain a written permission if the encryption exceeds the limit of 40 bit and they are required to deposit the decryption key with the DoT. The ISPs are further entrusted with an obligation to ensure that no bulk encryption is deployed[8].

2.3 TRAI Regulations on Encryption

As per the TRAI Draft Recommendation on Growth of Value Added Services and Regulatory Services, VASP registered as OSP are prevented from the employment of bulk encryption equipment[9]. A written approval from the concerned access service provider is required for the use of encryption algorithm and algorithms higher than 40 bit key length. Such VASP must deposit the decryption key with the access service provider or DoT. The Draft Recommendation authorizes DoT the right to modify these conditions or incorporate new conditions if it necessary[10].

2.4 SEBI

SEBI Master Circular for Stock Exchange or Cash Market issued on April 13, 2012 for Operation and System Requirement states that it is the responsibility of the Stock Exchange to ensure that the system used by the broker has provision for protecting the reliability and confidentiality of data through use of encryption technology[11]. It also provides guidelines for securities trading through wireless medium on Wireless Application Protocol platform. The requirements states that for secure data transmission from the WAP Gateway server to the Internet server should be secured using SSL security, and for server access through Internet it is preferable to use 128 bit encryption techniques. It also states that the level of encryption is subject to the DoT regulations. Additional requirements for Internet Based Trading (IBT) and Securities trading using Wireless Technology (STWT) states that there should be secure end-to-end encryption for all data transmission between the client and the broker through a Secure Standardized Protocol.

2.5 RBI

RBI has issued on 14th June 2001, "Guidelines for Internet Banking" which has to be implemented by Banks in India. The Guidelines required the use of at least 128-bit SSL for securing browser to web server communication and require for the encryption of sensitive data within the organization[12]. RBI on 8th October 2008 issued Operating Guidelines for Mobile Banking transactions in India, which requires the implementation of strong encryption techniques to protect all stages of the transaction processing[13].

2.6 EXPORT CONTROLS

Foreign Trade (Development & Regulation) Act, 1992 as amended in the year 2010 has included a new Chapter IV A which deals with the controls on export of specified goods, services and technologies i.e. Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET). In India the dual-use items are popularly known as Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) items[14]. Export of SCOMET items is either prohibited or permitted under a licence. Category 7 deals with the export of Electronics, computers and information technology including information security equipments, which includes cryptography. Under Category 7, 7D001 specifically mentions about the use of ciphering processes. But it does not specify the types of encryption products that will be subject to the export restrictions.

III. BLACKBERRY ISSUE

BlackBerry is a brand of wireless handheld devices and services developed by the Canadian telecommunications company BlackBerry Limited- known as Research In Motion (RIM)[15]. BlackBerry service provides high level of encryption on data transfers, which is one of its biggest advantages and a threat to security for many countries. BlackBerry phones can be misused by terrorist people, with BlackBerry a user can have instant and encryption communication to another party by calling the other parties unique four character number. The licensing norms require the telecom companies to put a mechanism in place to allow security agencies to intercept any conversation or message of a subscriber. In India for the purpose of national security India Government required BlackBerry to allow monitoring of its e-mails and SMS. But the security architecture designed for encryption is in such as way that it excludes RIM/ any third party to gain an unauthorized access to the key or corporate data. To handle the surveillance request from Indian authorities BlackBerry had set up domestic office with a server capable of performing interception in Mumbai. In BlackBerry case Government of India demanded the RIM to build a self-escrow system within its organization and they have to submit the keys on government demand.

3.1 KEY ESCROW

The concept of key-escrow came into being with the advent of Clipper Chip a proposal made by the Clinton Administration in 1993 in US[16]. People who wish to encrypt their messages are required to use the Clipper Chip which will help the law enforcement officials to easily tap the Clipper encrypted messages, using the copies of the Clipper decoding keys. The law enforcement officials were allowed to access to the keys only with a court- approved warrant. But due to public agitations the administration withdrew the proposal. Thereafter a second proposal came in which individuals are free to use encryption greater than 40- bit but they have to leave their decryption key with a government approved escrow agent. As it was government intrusion on individuals privacy rights public agitation was high and the administration was forced to withdraw the proposal. In 1999 the crypto wars in US come to an end with the liberalization of encryption laws.

The concept of key escrow is prevalent in India in the name of back door entry which is clear from the BlackBerry Case. S.69 of the Act empowers the Central Government or a State Government to direct an agency to decrypt information. Failure to comply is punishable by imprisonment up to seven years and or fine. Department of Telecommunication "License agreement for provision of internet service" also mandates the submission of decryption key if the encryption exceeds the limit of 40 bit. TRAI regulation also requires the same.

The major drawbacks of key escrow system are the effective maintenance of keys in a central database for a stipulated time period. If the central database is compromised all the recoverable keys in the system could be compromised. If the keys went into wrong hands what will be the consequences i.e., difficulty in ensuring the confidentiality and integrity of data. There is no proper mechanism for ensuring the authority of the enforcement officials. The high cost of building, maintaining and operating a self-escrowed system within the organization (BlackBerry Case).

3.2 SELF INCRIMINATION

Self-incrimination is the act of accusing oneself of a crime for which a person can then be prosecuted. Self-incrimination can occur either directly or indirectly. In India Article 20(3) of the Constitution provides the protection against self incrimination. In addition to that S.161 of the Cr.P.C 1973 and S.132 of the Indian Evidence Act, 1872 also provides the same protection. It prevents government officials from compelling a person to testify against himself. Right against self incrimination is an implied right conferred under Article 6 of the European Convention on Human Rights. Article 8 of the European Convention on Human Rights guarantees limits the amount of monitoring and intercepting the private life of an individual by a public authority.

IV. INTERNATIONAL LAWS:

OECD Guidelines for Cryptography Policy

In March 1997, the Organization for Economic Cooperation and Development laid down Guidelines on Cryptography Policy for the formulation of a suitable cryptography policy by a country. It contains eight principles such as trust in cryptographic methods, choice of cryptographic methods, market driven development of cryptographic method, standards for cryptographic methods, protection of privacy and personal data, lawful access, liability and international cooperation[17].

V. QUANTUM CRYPTOGRAPHY

At present public key cryptosystems such as RSA & Diffie-Helman are considered to be the secure cryptosystems against all known attacks. But the advancement in computer processing will be able to defeat these cryptosystems in future. Technology has given a solution for this in the form of quantum cryptography. A Quantum Key Distribution application has been developed for this purpose. Quantum Cryptography relies on physics rather than mathematics. In this any attempt to eavesdropping will be detectable. The current encryption policy will not be sufficient enough to address this new concept. Export policies do not apply. Key escrow/ recovery policy will not apply. The future of cryptography will change drastically with new technologies such as quantum cryptography, which brings aspects that current policies and standards cannot address.

VI. FINDINGS AND ANALYSIS

In India individuals regularly use wide range of encryption products such as SSL, HTTPS, VPN, voice communication such as Skype, mobile email communication etc., for data protection and privacy protection. But current laws in India limits encryption to 40 bit key which is outdated and easy to break. Only for the purpose of easy monitoring the level of encryption is limited to 40 bit, which is far below international standards. All 40-bit and 56-bit encryption algorithms are out of date, because they are vulnerable to brute force attacks, and therefore cannot be treated as secure. As a result, virtually all web browsers now use 128-bit keys, which are considered

Issue 3, Volume 2 (April 2013)
ISSN: 2250-1797

strong. Some web servers will not communicate with a client unless it has a 128-bit encryption capability installed on it.

Time to Crack Messages Encrypted with Various Key sizes	
Number of Bits	Time to Crack the message
40	78 seconds
48	5 hours
56	59 days
64	41 years
72	10,696 years
80	2,738,199 years
88	700,978,948 years
96	179,450,610,898 years
112	11,760,475,235,863,837 years
128	770,734,505,057,572,442,069 years

Fig 1: Message Cracking Time

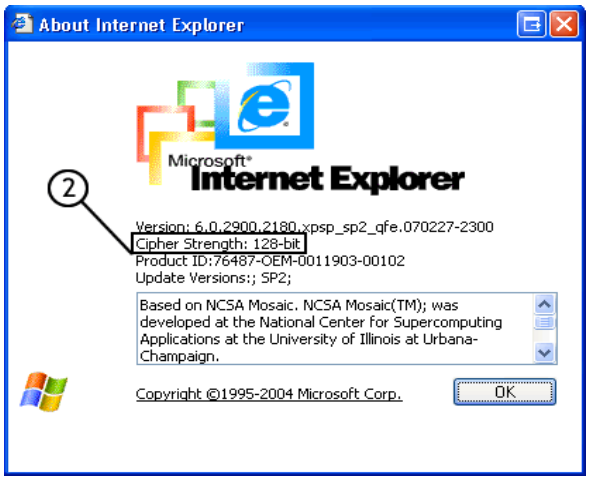

Fig 2: Key size used by IE

The Electronic Frontier Foundation's Deep Crack, built by a group of enthusiasts for US$250,000 in 1998, could break a 56-bit Data Encryption Standard (DES) key in days, and would be able to break 40-bit DES encryption in about two seconds[18].

In order to generate confidence in the mind of the people while dealing with e-transactions strong encryption techniques should be used. Absence of strong encryption techniques will give birth to the presumption that the data will be easily compromised. As per the SEBI and RBI guidelines 128 bit encryption is required to protect internet banking and stock exchange transactions. These varying standards demands for a uniform national encryption policy. Government can formulate a separate encryption policy with the powers conferred under S.84A of the Information Technology (Amendment) Act, 2008. The OECD Guidelines on

Cryptography Policy can be taken as a road map for developing the nation policy. Under which an authority must be constituted with powers to formulate, adjust and publish relevant rules and regulation relating to encryption products and technology. Policy must ensure the use of a global standard for encryption that would be maximal for the prevention of data leakage. Provisions must be included for ensuring the authority of the enforcement officials, mechanism for securely storing the keys, specifying the time period for how long they have to protect the keys etc.

Law enforcement authorities are under fear that encryption would block their ability to protect public safety and national security. But in reality strong encryption techniques is already widely available from all over the world, and that terrorist can get it whether or not the government regulates the export. Law enforcement agencies should develop better capability to crack encrypted communications such as in China they are using "Great Firewall" by which they can discover and block encrypted communications. Liberalization of crypto laws also is a solution for all these controversies.

S43A of the IT (Amendment) Act, 2008 deals with the compensation for failure to protect data. As per this it is the responsibility of the body corporate that possesses, deal or handles data, has to protect such data and may therefore be responsible for using appropriate cryptographic methods. But for this purpose the government should give a right to choose any cryptographic method to fulfill different data security requirements. It is therefore clear from the above facts that an encryption policy should address various issues such as technical, national security, and business privacy. Disparities in policy may create obstacles to the evolution of national and global information and communications networks and hinder the development of international trade.

VII. PROPOSED ENCRYPTION LAW:

From the above finding and as per the powers conferred under S.84 A of the IT (Amendment) Act 2008 we are suggesting some of the following recommendations for the enactment of an Encryption Legislation in India.

7.1 SCOPE

Applicable within the territory of India except Jammu and Kashmir

7.2 DEFINITIONS: See Annexure 1

7.3 LAWFUL ACCESS

- Clearly specify the provisions for lawful access
- Such provisions must be beneficial for public safety, law enforcement and national safety
- It must address the risk of misuse
- Specify the expense of supporting infrastructure, prospects of technical failure & other cost
- The authority must have a legal right to possess the plaintext
- Once obtained the data must only be used for lawful purpose

- A log must be maintained for recording the process through which the lawful access is obtained.
- Time limit should be kept for granting the access
- The lawful access provisions should be stated clearly and published in a way that they are easily available to users, key holders and providers of cryptographic methods.

7.4 KEY MANAGEMENT SYSTEM

- A key management system should be developed in such a way that it could balance the interests of users and enforcement authorities.
- Key management system should contain a mechanism for key recovery if the keys are lost.
- Separate procedure for obtaining keys which are used to protect confidentiality and keys which are used for other purposes only.
- Secure storage of keys
- Time period for keeping the keys.
- Or provisions for the preservation and retention of such information must be clearly specified.

7.5 LIABILITY

Liability of individual (such as ISPs) / entity (such as companies, government etc) that offers cryptographic services / holds/ has access to cryptographic keys should be made clear.

7.6 PUNISHMENT

Punishment shall be prescribed for misuse of keys obtained through lawful access.

7.7 EXEMPTION

Key holder is exempted from liability if he/she is providing cryptographic keys/plaintext of encrypted data in accordance with lawful access provisions.

VIII. CONCLUSION

It is the responsibility of the government to protect the privacy of individuals, facilitating information and communications systems security, promoting commerce, maintaining public safety and national security. And at the same time it is the responsibility of the government to take necessary steps against the use of cryptographic techniques by individuals or entities for illegal activities, therefore governments, however has to develop a balanced encryption policy. By combining and amending the existing provision for encryption which are mentioned in IT Act, DoT, SEBI, RBI, & TRAI the India government can formulate a new Encryption Regulation.

ANNEXURE 1

AUTHENTICATION: - "Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.

AVAILABILITY: - "Availability" means the property that data, information and communications systems are accessible and usable on a timely basis in the required manner

CRYPTOGRAPHY: - "Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.

CRYPTOGRAPHIC KEY:-"Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

CRYPTOGRAPHIC METHODS: - "Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems

DATA: - "Data" means the representation of information in a manner suitable for communication, interpretation, storage, or processing.

DECRYPTION: - "Decryption" means the inverse function of encryption

ENCRYPTION: - "Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

INTEGRITY: - "Integrity" means the property that data or information has not been modified or altered in an unauthorized manner.

INTEROPERABILITY: - "Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.

KEY ESCROW: - A controversial arrangement where the keys needed to decrypt encrypted data must be held in escrow by a third party so that government agencies can obtain them to decrypt messages which they suspect to be relevant to national security[19].

KEY MANAGEMENT SYSTEM: - "Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.

KEY HOLDER: - "Key holder" means an individual or entity in possession or control of cryptographic keys. A key holder is not necessarily a user of the key.

LAW ENFORCEMENT: - "Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter

LAWFUL ACCESS: - "Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.

MOBILITY: - "Mobility" of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.

NON-REPUDIATION:- "Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).

PERSONAL DATA: - "Personal data" means any information relating to an identified or identifiable individual

PLAINTEXT: - "Plaintext" means intelligible data.

TRUSTED THIRD PARTY:- In cryptography, a trusted third party (TTP) is an entity which facilitates interactions between two parties who both trust the third party; The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content.

AUTHORITY

Establishment- Central Government shall, by notification, establish one Central Encryption Board, named as Encryption Administration Board.

Composition of Encryption Administration Board- Encryption Administration Body should consist of five members, two of them must be from law background, and three of them must be of the technical background.

Qualifications- (i) The Law background person must possess the Bachelor of Law, and Master's in Cyber Law.

(ii) Technical background person must possess the degree of B.Tech (IT/CS), as well as Master's in Cyber Law.

Powers and Rights- Board must have powers to formulate, adjust and publish relevant rules and regulation relating to encryption products and technology.

Tenure- Board members must be appointed for the term of three years at first time and the same person may be re-appointed for a term of ten years, until he attends the age of sixty-five years, whichever is earlier.

Salary, allowances and other terms and conditions of service - The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of the members shall be such as may be prescribed: Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

Removal- The member of the board may, by notice in writing under his hand addressed to the senior member (if available) or Central Government, resign his office:

Provided that the said member shall, unless he is permitted by the senior member (if available) or Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

REFERENCE

1) SANS Institute InfoSec Reading Room; "**History of Encryption**"; Retrieved on 4th March, 2013, from http://www.sans.org/reading_room/whitepapers/vpns/history-encryption_730.
2) Head of Publications Services, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France; "CRYPTOGRAPHY POLICY: THE GUIDELINES AND THE ISSUES"; Retrieved on 4th March, 2013, from http://encryption_policies.tripod.com/international/oecd_1997_guidelines.pdf
3) Information Technology (Amendment) Act, 2008; Section 84A.
4) Information Technology (Amendment) Act, 2008; Section 69.
5) THE GAZETTE OF INDIA; NOTIFICATION G.S.R. 314(E), New Delhi, the 11th April, 2011; Information Technology (Intermediaries guidelines) Rules, 2011 Retrieved on 4th March, 2013.
6) Ibid

7) Department of Telecommunications (DoT), "Guidelines and General Information for setting up of international gateways for internet", Part II, Retrieved on 4th March, 2013, from http://www.dot.gov.in/isp/guide_international_gateway.htm,
8) Department of Telecommunications (DoT); License Agreement for provision of Internet Services; Retrieved on March 5th, 2013, from http://www.dot.gov.in/isp/licence_agreement.htm
9) TRAI; "Draft Recommendations on Growth of Value Added Services and Regulatory Issues"; Retrieved on 5th March, 2013.
10) Ibid "Page 11"; Retrieved on 5th March, 2013.
11) SEBI; "Master Circular for Stock Exchange / Cash Market"; Retrieved 5th on March, 2013, from http://www.sebi.gov.in/cms/sebi_data/attachdocs/1334312676570.pdf
12) RBI; "' Internet Banking in India – Guidelines"; Retrieved on 5th March, 2013 from http://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf
13) RBI; "Mobile Payment in India- Operative Guidelines for Banks"; Retrieved on 5th March, 2013, from http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=18432
14) http://dgft.gov.in/exim/2000/download/Appe&ANF/38D.pdf Retrieved on 20th February 2013.
15) http://en.wikipedia.org/wiki/BlackBerry Retrieved on 4th March, 2013.
16) Brookings Institution; "Deciphering the Cryptography Debate" by "Kenneth Flamm"; "; Retrieved on 6th March, 2013, from; http://www.brookings.edu/research/papers/1997/07/technology-flamm
17) OECD BETTER POLICIES FOR BETTER LIVES, " OECD Guidelines for Cryptography Policy", Retrieved on 16th February 2013 from : http://www.oecd.org/internet/ieconomy/guidelinesforcryptographypolicy.htm
18) Wikipedia; " 40-bit-encryption" ; Retrieved on 6th March, 2013, from; http://en.wikipedia.org/wiki/40-bit_encryption
19) http://dictionary.reference.com/browse/key+escrow Retrieved on 17th March 2013

Picture 1: http://www.p2pnet.net/images/tkx.gif

Picture 2: http://support.transact.wa.gov/taw_user/images/tw72/tw72_02.gif