# How India Regulates Encryption

*Centre for Internet and Society* | 2015-10-30

Pranesh Prakash

*Governments across the globe have been arguing for the need to regulate the use of encryption for law enforcement and national security purposes. Various means of regulation such as backdoors, weak encryption standards and key escrows have been widely employed which has left the information of online users vulnerable not only to uncontrolled access by governments but also to cyber-criminals.*

---

Governments across the globe have been arguing for the need to regulate the use of encryption for law enforcement and national security purposes. Various means of regulation such as backdoors, weak encryption standards and key escrows have been widely employed which has left the information of online users vulnerable not only to uncontrolled access by governments but also to cyber-criminals. The Indian regulatory space has not been untouched by this practice and constitutes laws and policies to control encryption. The regulatory requirements in relation to the use of encryption are fragmented across legislations such as the Indian Telegraph Act, 1885 (Telegraph Act) and the Information Technology Act, 2000 (IT Act) and several sector-specific regulations. The regulatory framework is designed to either *limit encryption or gain access to the means of decryption or decrypted information.*

**Limiting encryption**

The IT Act does not prescribe the level or type of encryption to be used by online users. Under Section 84A, it grants the Government the authority to prescribe modes and methods of encryption. The Government has not issued any rules in exercise of these powers so far but had released a draft encryption policy on September 21, 2015. Under the draft policy, only those encryption algorithms and key sizes were permitted to be used as were to be notified by the Government. The draft policy was withdrawn due to widespread criticism of various requirements under the policy of which retention of unencrypted user information for 90 days and mandatory registration of all encryption products offered in the country were noteworthy.

The Internet Service Providers License Agreement (ISP License), entered between the Department of Telecommunication (DoT) and an Internet Service Provider (ISP) to provide internet services (i.e. internet access and internet telephony services), permits the use of encryption up to 40 bit key length in

the symmetric algorithms or its equivalent in others.[1] The restriction applies not only to the ISPs but also to individuals, groups and organisations that use encryption. In the event an individual, group or organisation decides to deploy encryption that is higher than 40 bits, prior permission from the DoT must be obtained and the decryption key must be deposited with the DoT. There are, however no parameters laid down for use of the decryption key by the Government. Several issues arise in relation enforcement of these license conditions.

1. While this requirement is applicable to all individuals, groups and organisations using encryption it is difficult to enforce it as the ISP License only binds DoT and the ISP and cannot be enforced against third parties.
2. Further, a 40 bit symmetric key length is considered to be an extremely weak standard[2] and is inadequate for protection of data stored or communicated online. Various sector-specific regulations that are already in place in India prescribe encryption of more than 40 bits.

- The Reserve Bank of India has issued guidelines for Internet banking[3] where it prescribes 128-bit as the minimum level of encryption and acknowledges that constant advances in computer hardware and cryptanalysis may induce use of larger key lengths. The Securities and Exchange Board of India also prescribes[4] a 64-bit/128-bit encryption for standard network security and use of secured socket layer security preferably with 128-bit encryption, for securities trading over a mobile phone or a wireless application platform. Further, under Rule 19 (2) of the Information Technology (Certifying Authorities) Rules, 2000 (CA Rules), the Government has prescribed security guidelines for management and implementation of information technology security of the certifying authorities. Under these guidelines, the Government has suggested *the use of suitable security software or even encryption software* to protect sensitive information and devices that are used to transmit or store sensitive information such as routers, switches, network devices and computers (also called information assets). The guidelines acknowledge the need to use *internationally proven encryption techniques* to encrypt stored passwords *such as PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit), PKCS#5 Password Based Encryption Standard or PKCS#7 Cryptographic Message Syntax Standard* as mentioned under Rule 6 of the CA Rules. These encryption algorithms are very strong and secure as compared to a 40 bit encryption key standard.

[1] Clause 2.2 (vii) of the ISP License

[2] Schneier, Bruce (1996). Applied Cryptography (Second ed.). John Wiley & Sons

[3] Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations, 2011

[4] Report on Internet Based Trading by the SEBI Committee on Internet based Trading and Services, 2000; It is useful to note that subsequently SEBI had acknowledged that the level of encryption would be governed by DoT policy in a SEBI circular no CIR/MRD/DP/25/2010 dated August 27, 2010 on Securities Trading using Wireless Technology

- The ISP License also contains a clause which provides that use of any hardware or software that may render the network security vulnerable would be considered a violation of the license conditions.[5]{style="text-align:justify"} Network security may be compromised by using a weak security measure such as the 40 bit encryption or its equivalent prescribed by the DoT but the liability will be imputed to the ISP. As a result, an ISP which is merely complying with the license conditions by employing not more than a 40 bit encryption may be liable for what appears to be contradictory license conditions.
- It is noteworthy that the restriction on the key size under the ISP License has not been imported to the Unified Service License Agreement (UL Agreement) that has been formulated by the DoT. The UL Agreement does not prescribe a specific level of encryption to be used for provision of services. Clause 37.5 of the UL Agreement however makes it clear that use of encryption will be governed by the provisions of the IT Act. As noted earlier, the Government has not specified any limit to level and type of encryption under the IT Act however it had released a draft encryption policy that has been suspended due to widespread criticism of its mandate.

The Telecom Licenses (ISP License, UL Agreement, and Unified Access Service License) prohibit the use of bulk encryption by the service providers but they continue to remain responsible for maintaining privacy of communication and preventing unauthorized interception.

**Gaining access to means of decryption or decrypted information**

Besides restrictions on the level of encryption, the ISP License and the UL Agreement make it mandatory for the service providers including ISPs to provide to the DoT all details of the technology that is employed for operations and furnish all documentary details like concerned literature, drawings, installation materials and tools and testing instruments relating to the system intended to be used for operations as and when required by the DoT.[6] While these license conditions do not expressly lay down that access to means of decryption must be given to the government the language is sufficiently broad to include gaining such access as well. Further, ISPs are required to take prior approval of the DoT for installation of any equipment or execution of any project in areas which are sensitive from security point of view. The ISPs are in fact subject to and further required to facilitate continuous monitoring by the DoT. These obligations ensure that the Government has complete access to and control over the infrastructure for providing internet services which includes any installation or equipment required for the purpose of encryption and decryption.

The Government has also been granted the power to gain access to means of decryption or simply, decrypted information under Section 69 of the IT Act

[5]Clause 34.25 of the ISP License

[6]Clauses 22 and 23 of Part IV of the ISP License

and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

1. A decryption order usually entails a direction to a decryption key holder to disclose a decryption key, allow access to or facilitate conversion of encrypted information and must contain reasons for such direction. In fact, Rule 8 of the Decryption Rules makes it mandatory for the authority to consider other alternatives to acquire the necessary information before issuing a decryption order.
2. The Secretary in the Ministry of Home Affairs or the Secretary in charge of the Home Department in a state or union territory is authorised to issue an order of decryption in the*interest of sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence*. It is useful to note that this provision was amended in 2009 to expand the grounds on which a direction for decryption can be passed. Post 2009, the Government can issue a decryption order for investigation of any offence. In the absence of any specific process laid down for collection of digital evidence do we follow the procedure under the criminal law or is it necessary that we draw a distinction between the investigation process in the digital and the physical environment and see if adequate safeguards exist to check the abuse of investigatory powers of the police herein.
3. The orders for decryption must be examined by a review committee constituted under Rule 419A of the Indian Telegraph Rules, 1951 to ensure compliance with the provisions under the IT Act. The review committee is required to convene atleast once in two months for this purpose. However, we have been informed in a response by the Department of Electronics and Information Technology to an RTI dated April 21, 2015 filed by our organisation that since the constitution of the review committee has met only once in January 2013.

**Conclusion**

While studying a regulatory framework for encryption it is necessary that we identify the lens through which encryption is looked at i.e. whether encryption is considered as a means of information security or a threat to national security. As noted earlier, the encryption mandates for banking systems and certifying authorities in India are contradictory to those under the telecom licenses and the Decryption Rules. Would it help to analyse whether the prevailing scepticism of the Government is well founded against the need to have strong encryption? It would be useful to survey the statistics of cyber incidents where strong encryption was employed as well as look at instances that reflect on whether strong encryption has made it difficult for law enforcement agencies to prevent or resolve crimes. It would also help to record cyber incidents that have resulted from vulnerabilities such as backdoors or key escrows deliberately introduced by

law. These statistics would certainly clear the air about the role of encryption in securing cyberspace and facilitate appropriate regulation.