the major drawback in practice is that encryption of data is extremely slow- with public key algorithms. Many block and stream ciphers can encrypt about one hundred to one thousand times faster than public key algorithms. Thus somewhat ironically, public key cryptography is rarely used for actual encryption of data. On the other hand, symmetric algorithms are poor at providing non-repudiation and key establishment functionality. In order to use the best of both worlds, most practical protocols are hybrid protocols which incorporate both symmetric and public key algorithms. example include the SSL/TLS protocols that is commonly used for secure web connection, or IPsec, the security part of the Internet communication protocol.

5. References

[1] William Stalling, "Cryptography and Network Security Principal and Practice", Third Edition, Pearson 2006.

[2] Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Education Private Limited, Seventh Edition 2009.

[3] Himanshu Gupta, Dr Vinod Kumar Sharma, " Multiphase Encryption: A New Concept in Modern Cryptography", International Conference on Intelligent Network and Computing(ICINC 2010), pp V2-475-V2-478.

[4] Vivak Kapoor, Vivak Sonny Abraham, Ramesh Singh, "Elliptic Curve Cryptography", ACM Ubiquity Volume 9, Issuse 20, May 2008 .

[5] P. K. Shau, Dr. R. K. Chhotray, Dr. Gunamani Jena, Dr. S Pattnaik, "An Implementation of Elliptic Curve Cryptography", International Journal of Engineering Research and Technology(IJERT) ISNN: 2278-0181, Vol 2 Issue 1, January 2013.

[6] Swadeep Singh, Anupriya Garg, Anshul Sachdeva, "Comparision of Cryptograpic Algorithms ECC and RSA", International Journal of Computer Science and Communication Engineering (IJCSC), Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013, ISSN 2319-7080.

[7] S Nithya, Dr E. George, Pankaj Raj, "Survey on Asymmetric key Cryptography Algorithms", Journal of Advanced Computing Technologies (ISSN: 2347-2804) Volume NO. 2 Issue No. 1, Febuary 2014.

[8] Christof Paar, Jan Pelzl, Understanding Cryptography, Sprigner, ISBN 978-3-642-04100-6, 2010, page no. 170-172.

Algorithm Family	Crypto system	Security Level(in bit)				Advantage	Disadvantage
		80	128	192	256		
Integer factorization	RSA	1024	3072	7680	15360	Only intended user can read the message using their private key.	Many secret key encryption methods that is significantly faster than any current available public-key encryption.
Discrete logarithm	DH	1024	3072	7680	15360	The shared key (i.e the secret) is never itself transmitted over the channel.	Lack of authentication.
Discrete logarithm	DSA	1024	3072	7680	15360	It is used for authentication and integrity.	The security of private key depends entirely on the security of the computer.
Discrete logarithm	ElGamal	1024	3072	7680	15360	The same planetext gives a different ciphertext(with near certainly) each time it is encrypted.	The need for randomness and slower speed and has long ciphertext.
Elliptic Curves	ECC	160	256	384	512	Short key is faster and requires less computing power.	It is more expensive and it shortens the life time of batteries.

Table 1