Asymmetric or symmetric encryption

ASSIGN BUSTER

Asymmetric or Symmetric Encryption In today's scenario it is vital to secure and maintain the confidentiality of information or data. It becomes all the more imperative when it is related to the research studies encompassing set of trials, studies, endurance, intellect and rigorous efforts taken to generate a meaningful research. The methods available to encrypt data involves asymmetric and symmetric means. The present article emphasizes upon the benefits of these methods for data protection. Introduction Encryption of data is necessary in transmitting information through electronic means, to safeguard- data or information, sensitive documents and private communications made through internet, else the information could be distorted, filched, or misrepresented. Unprotected data could be accessed unscrupulously to fetch devastating consequences for any organization. Protection of data is mediated by various algorithms meant to encrypt the information (Symmetric and asymmetric cryptography overview). Asymmetric encryption or public key encryption involves two set of keys one is public key for encryption and another key for decryption, a private key. On the other hand symmetric encryption encompass a secret key that is applicable to encrypt plus to decrypt the information. It is a private single key common to both the receiver and the sender to decipher the information. It is essential that the key is kept covertly and sturdily and should be shared between two parties only. It gains convenience over asymmetric encryption process because of its ease and rapidity in operation but becomes cumbersome if the key is to be shared between more than two parties. Public key can be utilized by individuals as well as for business, where the trader seizes the private key and all the clients have access to the public key, as exploited by Lotus and Microsoft (Conventional versus Key

Exchange Encryption). Keys can be wrecked by means of: (1) Simple guess work for the password or key. (2) By means of interception where access to communication could be made or access to computer could be accomplished. (3) By means of Brute force where computer knowledge is exploited to decipher the key (Conventional versus Key Exchange Encryption). Symmetric encryption method is more vulnerable to all three above mentioned methods but asymmetric method is vulnerable to third one only. Symmetric method sounds weak method but it possess ease in its operation whereas asymmetric is complicated process and requires decrypting software in many cases. However, if smallest amount of care and protection is taken then symmetric method is more handy and protected (Conventional versus Key Exchange Encryption). Conclusion In the present case only two organizations namely ABC and XYZ are involved to share same set of information and therefore symmetric encryption method is best to encrypt genetic research findings and records. Symmetric encryption is summarized as: Correspondent> Encryption with key > Receiver > Decryption with key Asymmetric encryption is summarized as: Correspondent> Encryption with Receiver's Public key > Receiver > Decryption with receiver's private key (Conventional versus Key Exchange Encryption). Since the encryption requires lot of programming in asymmetric encryption process, it is a time consuming process moreover it requires expertise to decrypt the information. A researcher working in the field of genetics need to be more focused on the research rather than the tiresome procedures of encrypting the data, one must adopt symmetric means of data encryption process. Reference Conventional versus Key Exchange Encryption. Available at http://www. centurionsoft.

com/centurionmail/wpencryption. html. [Accessed on 28th January 2011].

Symmetric and asymmetric cryptography overview. Available at http://www. netlab. tkk. fi/opetus/s38153/k2003/Lectures/g33symm_asymm_crypto. pdf. [Accessed on 29th January 2011]