Digital signature

repudiation are provided to the communicating parties. Objective This project has been developed keeping in view the security features that need to be implemented in the networks following the fulfillment of these objectives: To develop an application that deals with the security threats that arise in the network. To enable the end-users as well as the organizations come out with a safe messaging communication without any threats from intruders or unauthorized people. To deal with the four inter-related areas of network security namely Secrecy, Authentication, Non-repudiation and Integrity. Project Overview

This application makes use of Digital Signature Algorithm (DSA) along with a hash function. The hash code is provided as input to a signature function along with a random number generated for this particular signature. The signature function also depends on the sender's private key and a set of parameters known to a group of communicating principals. This set constitutes a global public key. The result is a signature consisting of two components. At the receiving end, verification is performed. The receiver generates a quantity that is a function of the public-key components, the sender's public key, and the hash ode of the incoming message.

If this quantity matches with one of the components of the signature, then the signature is validated. This application makes sure that the security services Authentication, Secrecy, Integrity, and Non-repudiation are provided to the user. This application allows to keep the information out of the hands of unauthorized persons. This is called Secrecy. It also deals with determining whom a person is communicating with before revealing sensitive information or entering a business deal. This is called

Authentication. Non-repudiation deals with proving that a particular message was sent by a articular person in case he denies it later. Integrity makes sure whether a particular message has been modified or something has been added to it. The project mainly deals with maintenance of the above mentioned security services thereby allowing the users as well as the network organizations to keep track of intrusions and thus enhancing the security services. [pic] Existing system These days almost all organizations around the globe use a messaging system to transfer data among their employees through their exclusive intranet.

But the security provided is not of high standards. More and aining access to confidential data. Disadvantages: The validity of sender is not known. more unauthorized people are The sender may deny sending a message that he/she has actually sent and similarly the receiver may deny the receipt that he/she has actually received. Unauthorized people can gain access to classified data. Intruders can modify the messages or the receiver himself may modify the message and claim that the sender has sent it.

Proposed system The system will provide the following security services: Confidentiality: Confidentiality is the protection of transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit.

Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Authentication: The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such s the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic (i. e. that each is the entity that it claims to be).

Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception. Integrity: Integrity basically means ensuring that the data messages are not modified. An integrity service that deals with a stream of messages assures that messages are eceived as sent, with no duplication, insertion, modification, reordering or replays. The destruction of data is also covered under this service.

Thus the integrity service addresses both message modification and denial of service. Non-repudiation: Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver