SYSTEM FOR AUTHENTICATION USING DIGITAL SIGNATURE TECHNIQUE

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENT FOR THE AWARD OF DEGREE
OF
MASTER OF ENGINEERING
IN
COMPUTER SCIENCE.
BY

JOGINDER SINGH

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY
(DEEMED UNIVERSITY) PATIALA (INDIA).
147004
AUGUST, 2001

DECLARATION

I hereby certify that the work presented in the thesis entitled "System of Authentication using Digital Signature Technique" for the fulfillment of requirement of the award of the degree of Master of Engineering in Computer Science is being submitted in the department of Computer Science and Engineering, TIET, Patiala.

It is further certified that the work carried out for the thesis is an authentic record done under the supervision of Dr. P.K. Bansal. The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other University.

Joginder Singh
(Joginder Singh)
13-08-2001

This is certified that the above statement made by the candidate is correct to the best of our knowledge.

(Dr. P.K. Bansal) 29.8.2001
Professor
Dept. of Computer
Science and Engineering.
TIET, Patiala.

Seema Bawa 21.08.01
Head,
Dept. of Computer
Science and Engineering
TIET, Patiala.

24.8.2001
Dean,
Academic Affairs.
TIET, Patiala.

The Viva Voice Examination was held on .....

(External Examiner)

ACKNOWLDGEMENT

I would like to thank Thapar Institute of Engineering and Technology, Patiala for providing me an opportunity to carry out the thesis on "System for Authentication using Digital Signature Technique" as a part of my M.E degree program.

I consider it a great privilege to place on record my deep sense of gratitude to Dr. P.K. Bansal, under whose inspiration, encouragement and expert guidance I have been doing the thesis. I express my heartfelt gratitude for his personal involvement in guiding me right from the start to the successful completion of the thesis.

I express my gratitude to Mr. Arun Khatri for sparing a lot of time for helping me from time to time during the course of my thesis work.

I would fail in my duty if I don't avail this opportunity to thank my family members especially wife and kids for their encouragement, moral support, inspiration, love and affection that provided the sustenance journey.

Finally, I express my gratitude to Sh. H.M.S. Rosha, Assistant Excise and Taxation Commissioner (Computer) for providing me the requisite environment to develop the System on the latest platform.

I am indebted to all the persons who supported me and assisted during my study and thesis.

.....Joginder Singh

ABSTRACT

Information Technology has changed the way of dealing with business activities in corporate, private and government organizations, which needs the sharing of data through net. The sharing of data causes the threats to the data at storage level or to the data in transit, causing the breach of Integrity, confidentiality and authentication. As authentication is the important aspect of security issues, techniques of authentication are required to be analyzed to suit the application. The shortcoming of traditional technology of ink and paper necessitates in devising the way to authenticate the identity of business partner. Cryptography and PENOP techniques are popular for authentication of electronic documents. PENOP technique needs the high-end infrastructure at both ends and is not applicable for the identified area. In this thesis, digital signature technique, which is an application of cryptography, has been applied to authenticate the documents of Excise and Taxation Department, Punjab.

One of the familiar technology for authentication of electronic documents is public key cryptography, which uses two keys. One is secret key (private key), which is known to the owner only, and the second is public key, which is known to all. The corresponding public key can only decrypt message encrypted with private key. The proposed work uses 64 bit long secret and public key and needs 2^{64} iteration to decode the key, which is very difficult for the intruder to decode. RSA and DSS are two algorithms of public key cryptography to create/verify the digital signature from the message. Therefore, both the algorithms have been analyzed and compared. The execution to generate the digital signature using RSA algorithm is an exponential function of private and public key. Therefore, execution time is very high to compute the digital signature and not suitable for real time applications. DSS algorithm is faster as it is straight

function of private and public keys but it needs to share six parameters among the partner, which is not feasible for the intended application. Therefore, a new model of digital signature has been formulated, which is very fast and needs only one key (public key) to share. This algorithm fulfills the requirement of the application under consideration i.e. authentication of documents at ICCs of the Excise and Taxation Department, Punjab. The proposed algorithm is applicable if the message is maintained in the form of tables of the DBMS system only. The environment used is Window-NT/Oracle.

The encryption technique is the way to codify the message in such a way that using the inverse function of encryption, encrypted message can be decrypted to the original form. The proposed system employs the technique wherein encryption function substitute the ASCII code depending upon the relative position of the character and ensures that the encrypted symbol of the same character will be different in the encrypted message. Therefore, encrypted symbol cannot be decoded from the statistical properties of the text.

A system for authentication using digital signature technique provides the three screens to facilitate the three types of users. First screen (form) is for the officer to allocate the secret key to the dealer. Second screen is for the dealer to make the entries for the inter-state consignment and generate the digital signature using his secret key. Third screen is for the official at ICC, who will prepare the form-III from the documents presented by the owner of the goods. After completing the data entry work, the official will verify the digital signature using the public key of the dealer. To secure the secret keys, a centralized database is maintained and secret keys are stored in the form of the ineligible form so that even DBA cannot read the private key. System shall read the key as and when required and give the appropriate message to the user. It is an

attempt to provide a high level of security to database in order to ensure that the dealer should not deny the transaction at a later stage and thus is bound to increase the revenue of the Excise and Taxation Department, Punjab.

CONTENTS

Chapter – 4 Model of Digital Signatures

Chapter – 5 System for Authentication

Chapter – 6 Conclusion

CHAPTER – 1

INTRODUCTION

1.1. Introduction

With the advent of computers in handling business applications within an organisation, information security is being managed by automated tools in addition to the physical methods that were being used earlier. As these computer systems in different organisations began to be networked with one another, information security acquired yet another aspect.[6]

Transmission of data has been steadily increasing in most parts of the world. The documents that are being exchanged electronically, include those related to commerce (e.g. Invoices, Purchase Orders & Requests for Quote), payment (e.g. Payment Orders, Remittance Advice & Credit/Debit Advice), transport (e.g. Booking Confirmation & Booking Status) and regulatory (e.g. Custom's Declarations). In the transition from traditional paper based methods to electronic methods for handling these business documents, it is extremely important to ensure that the same or higher level of security is achieved as has been the case in the paper system. Within this context, therefore, security of information needs to be addressed at three different levels:

- Application- this is internal to a company and defines different levels of information access rights to different categories of users.
- Network – to ensure that network facilities can be accessed only by authorised users/organisations.
- Message – to ensure that one & only one authorised copy of the message is sent and is received only by the intended recipient in its original condition.

The emergence of electronic commerce, electronic mail bulletin board services, telemarketing and on-line procurement systems have made

it critical to provide a trusted platform for transmitting and receiving business documents and other classified information. The new system, therefore, while providing major improvements in accuracy and speed in processing, should also take into account the following issues along with the potential threats and some possible countermeasures to these threats :

- Availability- To ensure that data is available at the right time and at the right place while protecting against unauthorised access.

  Threats – Network errors, power failures, operational errors, application errors, hardware errors, system software errors and viruses.

  Countermeasures – Alternative communication routes, uninterruptible power supply, software/hardware quality tests, access restrictions and data backup.

- Confidentiality – To protect against intruders eavesdropping on messages.

  Threats – Unauthorised access by insiders/hackers or through interception during transmission.

  Countermeasure – Message Encryption.

- Integrity – To prevent undesired creation, modification or deletion of messages. This also includes sequence integrity to guard against loss and reply of messages.

  Threats – Accidental or fraudulent errors at data entry, corruption of output.

  Countermeasures – End-to-end message authentication, message sequencing.

- Authenticity/Non-repudiability – To provide for reliable identification of sender and recipient along with proof of transmission and receipt of messages.

  Threat – Masquerading

  Countermeasures – Authentication by a combination of something user knows, something user possesses and/or user's physical characteristics. [6]

1.2. Authentication

Authentication is a method by which a process ensures that its communication partner is really the one that it says it is and not an impostor. This is a rather difficult problem to solve especially in the presence of malicious intruders trying to initiate the partner process.

It needs to be clarified that authorization is different from authentication. Authentication deals with the problem of verifying the identity of the remote partner process. Authorization deals with the tasks that the remote process can perform after its identity has been established beyond doubt.

All authentication mechanisms use the following fundamental process. The remote user process sends an initiation message to either the receiver or a key distribution centre which is always honest. A number of messages are exchanged between the initiator and the receiver. At the end of this exchange, there exists a secure connection between the initiator and the receiver for data transfer. There is also a secret or key session for data encryption during the data transfer.

Authentication schemes fall in two categories:

- Simple authentication where credentials are checked based on name & password, and sometimes on physical characteristics of the user.
- Strong Authentication where cryptographic techniques are used to protect the credential's information being validated. This scheme could also be implemented on smart cards, which can be interfaced with the users computer.

These cryptographic techniques are used in different ways to implement confidentiality, integrity, non-repudiation, and authentication.

When there are a large number of communicating partners, it is no longer practical to continue bilateral exchange of public keys. A central repository is needed to store all such public keys along with related information such as the algorithm used, expiry date, issuing authority etc. The credentials of users are stored in a directory as certificate, which are again digitally signed by a Certification Authority (CA). A Certification Authority should function as a trusted third party in providing such a service. The strong authentication methodologies used by the Certification Authority are again based on public key crypto systems. A public key Infrastructure is required to securely manage public keys for widely-distributed users or systems.[5]

1.3. Techniques of Authentication

Various techniques of authentication are described as under:

1.3.1 Traditional Ink and Paper Technique

Traditionally, paper based systems have achieved confidentiality by physically sealing envelopes and entrusting to a trusted carrier for communication for sending business messages. One could also be reasonably sure that a document is authentic by looking at the sender's signatures (in ink) imprinted on it. Any tampering with the context of the document is generally perceptible as well.

With the introduction of new technology, these concepts have acquired a new dimension. Signatures in ink on an electronic document are out of question. It is also impossible to know whether the information context or a part of it has been removed, changed or even been added to. These are some of the additional issues that need to be addressed so that security can be maintained in the electronic trading environment.

Technology based solutions have been developed to take care of all such requirements of security services. The implementation of which can be network based where message are protected independently on each communicating link. However, in the context of Electronic Commerce between two trading partners, security services are generally implemented 'end-to-end'.

Many risks afflict the traditional signing of a paper document. First, there is no standard method for signing in ink. User (A) is not taught or required to sign documents in a forensically reliable way. User(A) is free to sign in any way he chooses, and to change his signature from minute to minute. For any given signing, User(A) is free if he so desires to use as his signature any strange and indecipherable scribble. Whether any given document signed by User does or does not contain User(A) usual, verifiable signature is for all practical purposes a secret. Rarely is User(A) signature compared against specimens to confirm authenticity.

Ink signatures can be forged. There is no guarantee that any given ink signature can be verified by forensic science. Science can only offer an educated opinion as to whether the signature is authentic, and it can do so only under the right circumstances (including, for example, the availability of several good specimen signatures).

Other risks impede the linking of User(A) to a given paper document. If the document is multiple pages in length, one or two of the pages could be switched after the document was signed. There is even the risk that the document is organized in an ambiguous or confusing way, so that an observer cannot discern for certain which parts of the document User (A) agreed to and which part he did not.

These risks mean that in the event of a dispute, it is not always easy to tie User(A) to specific words in a paper document. When User(A) signs a document and gives it to User(B), User(B) is not guaranteed that he will later be able to prove that User(A) signed it. User(A) might raise any number of objections to repudiate the document. Conversely, User(A) is not guaranteed that he can repudiate a document that he in fact did not sign.

Under American law, the burden of proving that User(A) did sign is normally on User(B). This burden motivates User(B), at the outset of the transaction, to seed evidence of User(A)'s responsibility from things other than simply User(A)'s signature. This may mean that User(B) would ask User(A) to acknowledge his signature before a notary. More commonly, it means that User(B) establishes a relationship with User(A) in which they exchange feedback between each other - User(B) asks for partial advance payment, User(B) sends acknowledgements to User(A)'s independently verified address. The feedback reduces the risks to User(B).

The risks with a paper and ink signing are distributed across a number of features of the signing ritual - User(A)'s style of signing, User(A)'s secret choice whether to use his usual signature, the content of the signed document, the facts external to the document (such as any interaction between User(A) and User(B)) that place it in a historical context, the competence of the person whose opinion on the authenticity of the signature, and so on. In other words, the eggs are spread into many baskets. No single egg is highly reliable or highly important.

In a dispute over the authenticity of a document, the fact finder does not look at the signature in a vacuum. Rather it considers all the relevant facts and circumstances – the historical context of the document and all the

ambient clues (such as corroborating records or testimony) that might bear on the authenticity question.

Just as risks plague the authentication of paper document, so they will plague the authentication of electronic documents. To expect perfect binding of an individual like User(A) to words of an electronic document is not realistic.[5]

1.3.2 Cryptography

Cryptography protects sensitive information as it is transmitted from one location to another and Information is scrambled, which can then be safely transmitted. At the receiving end, the text is unscrambled (decrypted) using the same key, and the information can be read.

Cryptography is of two kinds: symmetric and asymmetric. Symmetric cryptography uses the same key to encrypt and decrypt the information and both the sender and receiver must know the key before the information is transmitted. In symmetric cryptography e.g. DES (Data Encryption Standard) secret key is shared between the sender and receiver. This is also called symmetric cryptography e.g. DES or the Data Encryption Standard algorithm.

Public–key or asymmetric cryptography uses two keys, one to encrypt the message and the other to decrypt it. Private key is used to encrypt the message and known to the owner only and public key is distributed to everyone whom to send messages. The receiver of the encrypted message uses the sender's public key to decrypt it. The two keys are mathematically related so that a message encrypted with one key can only be decrypted using the other key. This way, a receiver who successfully decrypts a message using the sender's public key, can be

assured that the massage has not been tampered with. This assurance is maintained only if the sender ensures that his private key is not disclosed to anyone else.

The messages to be encoded, called plaintext, are transformed by a mathematical function that is parameterized by a key. The output of the encryption process, called cipher text, is then transmitted. An intruder can read the transmitted message but to understand it, he has to decipher the key. The art of breaking keys (or ciphers) is called crypto-analysis. The art of devising ciphers and breaking them is collectively termed cryptology.

One of the fundamental rules of cryptography is that the method of encryption is reasonably well known and will not be changed often. The make it difficult to decrypt the encrypted message. The longer the key, it is secrecy comes in the key, which can be changed as often as required to more difficult to decrypt a message.

This method further states that the encryption and decryption algorithms should have the following properties.

- Applying the decryption algorithm on the encrypted message should give back the original plaintext.
- It should be extremely difficult to generate the decryption algorithm from the encryption algorithm.
- The encryption algorithm should not be broken by a chosen plaintext attach.

An algorithm that meets the above requirements is the RSA (Rivest, Shamir, Adleman) algorithm named after the initials of its inventors. **[1,5]**

1.3.3 PENOP Technique

PENOP employs a pen biometrics technology. It is a computer software component that augments the function of other computer

applications – such as applications that control electronic documents. PENOP has two primary features:

The Signature Capture Service **(SCS)** captures and permits the storage of certain data associated with the manual inscription of a signature (autograph) on a screen of a pen-based computer (or a digitizer pad on a PC). The SCS must work with a "Client Application," which is software that informs the pen computer user what he is doing and prompts him when and how to do it. A Client Application can be designed to manage an electronic document such as an expense voucher.

In coordination with the Client Application, the SCS receives information, such as a user ID or a name, showing who the user (User(A)) claims to be. It then prompts User(A) to inscribe his signature, using a stylus (or pen), to a window on the computer's screen. It supplies the wording of the prompt in the window, known as the "Gravity Prompt," which indicates the purpose for which the signature is being captured. The Gravity Prompt normally refers to an electronic document that is accessible to User(A) through the pen computer.

As User (A) moves the stylus across the screen, an image appears, that traces the movement of the stylus and he sees his autograph. At the same time, the SCS measures certain features of the inscription event, including the size, shape, and relative positioning of the curves, loops, lines, dots, crosses and other features of the signature being inscribed, as well as the relative speed at which each feature is imparted. The result of these measurements is known as "act-of-signing statistics." User(A) then has the option, by tapping indicated buttons on the screen, of approving the inscription event, retrying it or aborting it.

If User(A) taps the approval button, the SCS calculates a checksum, or a brief string of data, that represents the content of the electronic document referred to by the Gravity Prompt. The checksum is not a complete statement of the original document and the original document cannot be derived from the checksum. But the checksum bears a mathematical relationship to the document. If the document is changed, then it can no longer be mathematically matched with the checksum.

Next, the SCS compiles the following data and computes a second checksum from it:

- the first checksum
- the act-of-signing statistics
- the date and time of signing (as represented by the computer operating system under which the SCS is operating).
- the identity of the particular machine on which the signing occurred (based on identity information programmed earlier in the SCS).
- the claimed ID of the user (User(A)).
- The words that appeared in the Gravity Prompt.
- (optionally) data reflecting the graphic image of user's signature.

The SCS creates the second checksum in two steps. First, the SCS retrieves a secret key previously programmed into the Client Application and uses that key to encrypt the itemized data. (This is the "first level encryption.") Second, the SCS calculates from that encrypted data the second checksum. The second checksum establishes a link between the itemized data and the Client Application.

Finally the SCS encrypts the itemized data, plus the second checksum, using a different algorithm, one which does not use a secret key from the Client Application. This is the "second level of encryption". The

resulting encrypted string of data – called the "Biometric Token" is a tamper-resistant representation of the event in which User(A) inscribed his autograph.

The Signature Verification Service **(SVS)** reports the probability that a particular signature is authentic. First, in authorized enrollment sessions, the SCS captures and the SVS holds, in a database, act-of-signing statistics for a user like User(A) who has been identified to the SVS. Later, the SVS may be presented with a particular Biometrics Token and directed to evaluate whether it is a product of an authentic inscription of the signature belonging to the user identified in the token. The service decrypts the token and then compares the information therein with the signature statistics stored earlier in its database. Based on this comparison, it issues a " signature match percentage", e.g., 50 percent or 72 percent, and reports this percentage to a Client Application. The SVS applies scientific principles deemed relevant by PenOp's developers. **[5]**

1.4 Problem Definition

For this thesis work, Excise and Taxation Department of Punjab state has been chosen as a potential candidate for the introduction of the Digital Signature Technique in its existing information collection system. Department has setup Information Collection Centers (ICC) at Inter-state borders in order to monitor the movement of goods. The owner of the goods has to make the declaration regarding goods in transit by filling the form-III. These forms are available on computers at each ICC and are to be filled from bill through the software provided by the department. The

software has been developed in FoxPro under MS_DOS/Novell NetWare operating system. The department has engaged the services of private contractors to fill the form-III on computers. Copies of the filled forms are handed over to owners of the goods and simultaneously the data of the transaction is maintained on ICC server, which is consolidated at the head office fortnightly.. Since the data so prepared remains with the contractors for fifteen days, it becomes the cause of security threat to the database. To eliminate this problem, existing working environment needs to be changed from MS-DOS/Novell NetWare and FoxPro to Windows NT and Oracle based client/server environment, as it will provide the necessary security feature.

The declarations submitted by the owner of goods at ICCs are to be verified by the departmental field staff from account books of the dealer. From the report of verification, sent by the field staff, it has been observed that the dealer/evader some time gives the false declaration through the bogus documents at ICC. Since the entries collected at ICC and verified by the field staff do not match because of bogus billing, department is losing a substantial amount of sales tax. This loophole needs to be plugged in order to save the tax.

It is proposed to introduce the Digital Signature Technique for authenticating the documents at ICC so that the dealer should not be in a position to deny the transaction at the verification stage.

1.5 Organization of the thesis

The thesis entitled "System for Authentication using Digital Signature Technique" is aimed to design, develop and implement the system for authentication of documents transmitted through network. Organization of the work is described as under: -

Chapter-I : This chapter is aimed to describe the various aspects of security of documents transmitted on network along with the threats and its counter measures. Authentication is one of the components of security issue, which is also described in detail with various techniques along with the problem definition.

Chapter-II : This chapter describes the Digital Signature, need of Signatures, purpose of signature and Digital Signature Technology. The general technique of Digital Signature is described in detail, taking into consideration of various aspects of cryptography. As cryptography is the main tool of Digital Signature, it is described in detail including key generation, public key certificates and prospects of implementing the Digital Signature Technology.

Chapter-III : The model organization to implement the digital signature technique has been chosen and this chapter is aimed to describe the main function of department of Excise and Taxation, Punjab and areas have been identified where digital signature could be implemented.

Chapter-IV : This chapter is aimed to formulate the model of digital signature for the requirement identified in chapter–III. Various encryption techniques and algorithms have been analyses to form a model for the

application and model to implement the digital signature has been proposed.

Chapter-V : This chapter is aimed to design, and develop the software where the digital signatures can be implemented. It describes of overview of the proposed system, system processes, conceptual design, development phase, system security and testing.

Chapter-VI : This chapter concludes the thesis work. The objective of the work is to develop and test software to authenticate of documents transmitted through network.

1.6. Conclusion :

There are three basic techniques for authentication viz. Ink and paper, cryptography and PENOP technology. Ink and paper technique is primitive and out of context in the present scenario of increased electronic communication. PENOP technology needs the sophisticated setup at both the ends, which increases the cost of implementation. Cryptography technique is economical and better-suited solution of authentication of documents transmitted through network.

The chapter 2 focuses on the introductory notes on digital signature techniques and various aspects related with technology.

CHAPTER – 2

DIGITAL SIGNATURE

2.1. Introduction

The most important development on public key cryptography is in the area of digital signature. Digital signature provides a set of security capabilities that would be difficult to implement in any other way. Digital signature means the result of applying specific technical processes to specific information.[1] This chapter describes the technology of Digital Signature, the value of digital signature in legal applications, way to preserve the secret key and system to access the public key from the remote area. It also describes the role of trusted third party (Certification Authority) to generate, maintain and distribute the keys to the users.

2.2. Signatures and the Legalities

A signature is not part of the substance of a transaction, but rather a representation or form.[4] Signature writings serve the following general purposes:

(a) Evidence: A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.

(b) Ceremony: The act of signing a document calls to the legal significance of the signers act and thereby helps to prevent inconsiderate engagements.

(c) Approval: In certain contexts defined by law or custom, a signature expresses the signers approval or authorization of the writing, or the signers intention that it have legal effect.

(d) **Efficiency and Logistics**: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

The formal requirements for legal transactions, including the need for signatures, vary in different legal systems, and also vary with the passage of time. There is also variance in the legal consequences of failure to cast the transaction in a required form. The statute of frauds of the common law tradition, does not render a transaction invalid for lack of a written signature by the party to be charged, but rather makes it unenforceable in court, a distinction which has caused the practical application of the statute to be greatly limited in case of law.

During this century, most legal systems have reduced formal requirements, or at least have minimized the consequences of failure to satisfy formal requirements. Nevertheless, sound practice still calls for transactions to be formalized in a manner which assures the parties of their validity and enforceability. In current practice, formalization usually involves documenting the transaction on paper and signing or authenticating the paper. Traditional methods, however, are undergoing fundamental change. Documents continue to be written on paper, but sometimes merely to satisfy the need for a legally recognized form. In many instances, the information exchanged to effect a transaction never takes paper form and computer-based information can also be utilized differently than its paper counterpart. Computers can read digital information and transform the

information or take programmable actions based on the information. Information stored as bits rather than as atoms of ink and paper can travel near the speed of light, may be duplicated without limit and with insignificant cost.

Although the basic nature of transactions has not changed, the law has only started to adopt the advancement in technology. The legal and business communities must develop rules and practices which use new technology to achieve and surpass the effects historically expected from paper forms. [4]

To achieve the basic purposes of signatures outlined above, a signature must have the following attributes:

(a) **Signer authentication**: A signature should indicate who signed a document, message or record, and should be difficult for another person to produce it without authorization.

(b) **Document authentication**: A signature should identify what is signed, making it impracticable to falsify or alter the signed matter or the signature without detection.

Signer authentication and document authentication are tools used to exclude impersonators and forgers. It is called a non-repudiation service in the terminology of the information security profession. A non-repudiation service provides assurance of the origin or delivery of data in order to protect the sender against false denial by the recipient, or to protect the recipient against false denial by the sender. Thus, a non-repudiation service provides evidence to prevent a person from unilaterally modifying or terminating legal obligations arising out of a transaction effected by computer-based means.

(c) **Affirmative act**: The affixing of the signature should be an affirmative act which serves the ceremonial and approval functions of a signature and establishes the sense of having legally consummated a transaction.

(d) **Efficiency**: Optimally, a signature and its creation and verification processes should provide the greatest possible assurance of both signer authenticity and document authenticity, with the least possible expenditure of resources.[5]

2.3 Digital Signature Technique

Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures uses public key cryptography, which employs an algorithm using two different but mathematically related keys; one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed an asymmetric cryptosystem.[7]

The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed as private key, known only to the signer and used to create the digital signature. public key, which is ordinarily more widely known and is used by a relying party to verify the digital signature. If many people need to verify the signers digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible. Although the keys of the pair are mathematically related, if the asymmetric cryptosystem

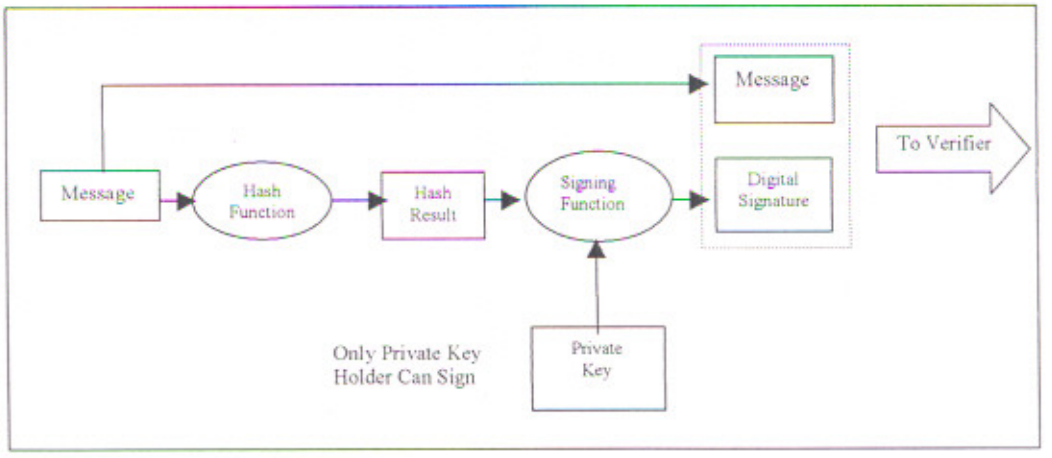
has been designed and implemented securely, it is computationally infeasible to derive the private key from knowledge of the public key. Thus, although many people may know the public key of a given signer and use it to verify the signer's signatures, they cannot discover that signer's private key to forge digital signatures. It is sometimes referred to as the principle of irreversibility.

A hash function is used in both creating and verifying a digital signature. It is an algorithm which creates a digital representation or fingerprint in the form of a hash value or hash result of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes termed a one-way hash function it is computationally infeasible to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

Digital signature verification is the process of checking the digital signature by reference to the original message. Given public key, thereby determine whether the digital signature was created for the same message using the private key that corresponding to the public key.[4]

Fig 2.1 below describes the process of digital signature creation. To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to

be signed is termed the message. Then a hash function in the signers software computes a hash result unique to the message. The signers software then transforms the hash result into a digital signature using the signers private key. The resulting digital signature is thus unique to both the message and the private key used to create it.



(Fig. 2.1)

Verification of a digital signature, as illustrated in Fig.2.2, is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks:

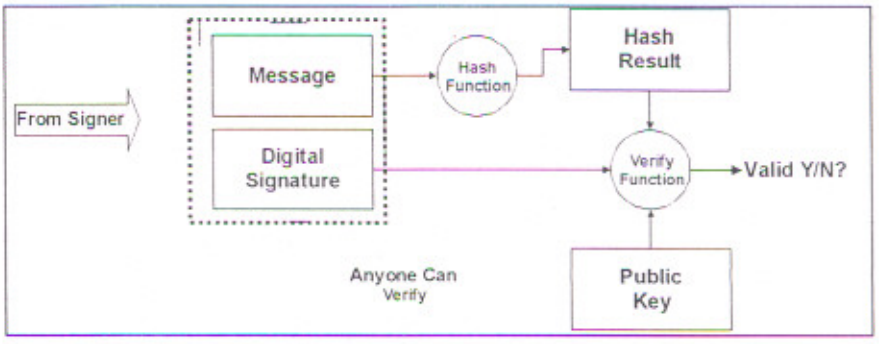
- Whether the digital signature was created using the corresponding private key; and
- Whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process.

The verification software will confirm the digital signature as verified if:

(a) The singers private key was used to digitally sign the message, which is known to be the case if the signers public key was used to

verify the signature because the signers public key will verify only a digital signature created with the signers private key

(b) The message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.



(Fig. 2.2)

Various asymmetric cryptosystem create and verify digital signatures using different algorithms and procedures, but share this overall operational pattern.

The processes of creating a digital signature and verifying it accomplish the essential effects desired of a signature for many legal purposes:

(a) **Signer authentication**: If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key, such as by divulging it or losing the media or device in which it is contained.

(b) **Message authentication**: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals tampering, since the comparison of the

hash results shows whether the message is the same as and when signed.

(c) Affirmative act: Creating a digital signature requires the signer to use the signers private key. This act can perform the ceremonial function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.

(d) Efficiency: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuine.

The processes used for digital signatures have undergone thorough technological peer review for over a decade. Digital signatures have been accepted in several national and international standards and being used by many corporations, banks, and government agencies. The likelihood of malfunction or a security problem in a digital signature cryptosystem designed and implemented as prescribed in the industry standards is extremely remote. [4]

2.4 Public Key Certificate

To verify a digital signature, the verifier must have access to the signers public key and have assurance that it corresponds to the signers private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. Some convincing strategy is necessary to reliably associate a particular person or entity to the key pair.

In a transaction involving only two parties, each party can simply communicate the public key of the key pair. Such an identification strategy is no small task, especially when the parties are geographically distant from each other and normally conduct communication over a convenient but insecure channel such as the Internet. As electronic commerce increasingly

moves from a bilateral setting to the many-to-many architecture of the World Wide Web on the Internet, where significant transactions will occur among strangers who have no prior contractual relationship and will never deal with each other again, the problem of authentication/non-repudiation becomes more considerable. An open system of communication such as the Internet needs a system of identity authentication to handle this scenario.

To that end, a prospective signer might issue a public statement, such as: Signatures verifiable by the following public key are mine. However, others doing business with the signer may for good reason be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of trusting a phantom or an imposter, or of attempting to disprove a false denial of a digital signature.

The solution to these problems is the use of one or more trusted third parties to associate an identified signer with a specific public key. To associate a key pair with a prospective signer, a Certification Authority issues a certificate, an electronic record which lists a public key as the subject of the certificate, and confirms that the prospective signer identified in the certificate holds the corresponding private key. A certificates principal function is to bind a key pair with a particular subscriber. A recipient of the certificate desiring to rely upon a digital signature created by the subscriber named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, this chain of reasoning provides assurance that the corresponding private key is held by the subscriber

named in the certificate, and that the digital signature was created by that particular subscriber.

To assure both message and identity authenticity of the certificate, the Certification Authority digitally signs it. The issuing Certification Authority digital signature on the certificate can be verified by using the public key of the Certification Authority listed in another certificate by another Certificate Authority and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. In each case, the issuing certification authority must digitally sign its own certificate during the operational period of the other certificate used to verify the Certification Authority digital signature.

A digital signature, whether created by a subscriber to authenticate a message or by a Certification Authority to authenticate its certificate should be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the operational period stated in the certificate, which is a condition upon verifiability of a digital signature.

To make a public key and its identification with a specific subscriber readily available for use in verification, the certificate may be published in a repository or made available by other means. Repositories are on-line databases of certificates and other information available for retrieval and use in verifying digital signatures. Retrieval can be accomplished automatically by having the verification program directly inquire of the repository to obtain certificates as needed.

Once issued, a certificate may prove to be unreliable, such as in situations where the subscriber misrepresents his identity to the Certification

Authority. In other situations, a certificate may be reliable enough when issued but come to be unreliable sometime thereafter. If the subscriber loses control of the private key, the certificate has become unreliable, and the Certification Authority may suspend or revoke the certificate. Immediately upon suspending or revoking a certificate, the Certification Authority must publish notice of the revocation or suspension or notify persons who inquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

The prospect of fully implementing digital signatures in general commerce presents both benefits and costs. The costs consist mainly of:

(a) **Institutional overhead**: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.

(b) **Subscriber and Relying Party Costs**: A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate. Hardware to secure the subscribers private key may also be advisable. Persons relying on digital signatures will incur expenses for verification software and perhaps for access to certificates and Certificate Revocation Lists (CRL) in a repository.

The principal advantage to be gained is more reliable authentication of messages. Digital signatures, if properly implemented and utilized offer promising solutions to the problems of:

(a) **Imposters**, by minimizing the risk of dealing with imposters or persons who attempt to escape responsibility.

(b) **Message integrity**, by minimizing the risk of undetected message tampering and forgery, and of false claims that a message was altered

after it was sent;

(c) **Formal legal requirements**, by strengthening the view that legal requirements of form, such as writing, signature, and an original document, are satisfied. [4]

2.5 Conclusion :

In current scenario of Electronic Commerce over the internet, it become essential to authenticate the documents by using some secure techniques and Digital Signature technique provides the required security to transmit the secured message over the network. This chapter concludes that any department who have sufficient infrastructure of IT can adopt digital signature to authenticate the data of business partner. In the light of above discussion, the next chapter is intended to identify the area in Excise and Taxation Department, Punjab where Digital Signature technique can be implemented for authentication of documents submitted by business partner (dealer). [4]

CHAPTER – 3

REQUIREMENT FORMULATION & ANALYSIS

3.1 Introduction

In this chapter, the application of digital signature technique to the department of Excise and Taxation, Punjab, is being discussed, The need to change the existing system and the benefits of digital signature are enumerated. Various aspects of the total system are studied and analyzed to identify the area where digital signature technique can be introduced to plug the loopholes of tax evasion in the department.

3.2. Current Scenario

The Excise & Taxation Department, Punjab is the major revenue-earning source for the state contributing about 67% to the state exchequer. It collects the revenue by way of levying excise duty on liquor, sales tax on goods and entertainment and show tax. To facilitate the working of the department, the state has been divided into four divisions consisting of 21 districts and 173 wards. The department has also setup 32 Information Collection Centers (ICC) and 5 flying squads to monitor the movement of goods in the State. Computerization plays a vital role to maintain the huge amount of data related with various activities of the dealers. The following applications have been undertaken for implementation under the computer project.

3.2.1 Master Dealer File (MDF)

Department collects revenue from the dealer by levying Sale/Purchase tax on goods. The quantum of sales is measured in gross turn over (GTO). When the GTO of the dealer exceeds the limit of Rs 5

lakhs per year, it is mandatory for the dealer to get himself registered under the rules. He applies for registration through form –I. The officer in-charge of the area scrutinizes the application and business premises of the concerned dealer and the Registration Certificate Number (RC Number) is issued. Database of all the registered dealers maintained on computer is known as MDF. The data of approximately 2,00,000 registered dealers in the state have been collected through form-I and is fed into the departmental database. After data entry, regular reports are being generated out of which the most important is the dealer-wise directory. This report has been successfully used for the past many years by the field staff and detection of evasion of tax have been made with this help. The MDF data is also being used for other applications at the time of data processing to get the requisite information of the dealer.

3.2.2 Returns Analysis System.

Every registered dealer has to furnish the details of sales and purchases made by him on the prescribed form-II and which is known as filing of return. Periodicity of filing the return, is monthly, quarterly and yearly depending upon the discretion of the officer-in-charge of the area. Analysis of returns has been undertaken in Patiala and Fatehgarh Sahib at the ward level. Under this application, all the returns submitted by the dealer relating to the local wards are collected in the district computer centre and receipts of returns are being issued through computer. Returns so collected in computer centre are sent to concerned ward for complete data entry of Form-II.

After completing the data entry, data is appended in Master database which is used for further analysis. Following reports are being generated regularly.

(a) List of Returns Defaulters
(b) Dealer wise tax comparison.
(c) List of dealers whose tax is less than the previous year
(c) Trade wise tax analysis.
(d) Query reports as and when required.

3.2.3 Checklist of Assessing Authorities.

Assessing Authority is an officer in the department at the rank of Excise and Taxation Officer (ETO). He is responsible to make the assessments of the dealers and to ensure the timely tax collections of his area. A detailed statement of the work done by the Assessing Authorities in the state are prepared manually by the field officers themselves. This statement is called the checklist of Assessing Authorities. This checklist is redesigned to facilitate computerization by adding certain statements which were considered relevant to the work of Assessing Authorities and also deleting others which did not relate to the immediate sphere of work. This package is a very comprehensive one spanning almost the entire activity of the department under the Punjab General Sales Tax Act. It eliminates the need for preparation of manual statements by the field staff while at the same time making available to the controlling officers a flood of information relating to their daily work.

3.2.4 Analysis of documents from ICCs.

The registered dealers have the privilege to make the sales/purchases to the dealers of other states. These transactions are to be properly maintained on account books in order to evaluate the tax at the

time of assessment. Some dealers do not enter these transactions into their account books with the attention to evade the tax. To monitor the movement of goods from or into the state, 32 Information Collection Centres (ICCs) have been setup in the entire state at inter-state borders. Data flow diagram depicting the various processes at ICC in the existing system is presented at fig 3.1. Driver of every vehicle carrying goods is to appear before the officer on duty at ICC along with documents like declaration, bill and goods register (GR). The declaration forms are available on computer at each ICC and are to be filled through the software provided by the department. The software is developed in FoxPro under MS-DOS/Novell NetWare Operating system Declaration form (Form-III) contains the details of the transaction consisting of the name of consignor or consignee, description of goods, value, date, time, bill number and transporter. The volume of the transactions crossing the ICCs is very high i.e about 20,000 forms are to be generated per day on computers installed at all ICCs. It needs more than 100 computers and 400 employees to operate the system, which department could not manage due to procedural constraints. In order to streamline the functioning of computers at ICCs, department has engaged the services of the private contractors to prepare the declaration forms from the documents presented by the owner of goods. Copies of the forms are handed over to the owner of goods and the data of the transaction is saved on the server simultaneously. The contractor keeps on collecting the data on the server continuously at ICC on the server and send the same to the departmental server every fortnight. Since, the data so prepared remains with the contractor for 15 days, it becomes the cause of security threat.

Consolidated data in the head office of the department is processed and sent to the concerned officer for verification from the account books of the concerned dealer. From the report of verification sent by the officers, it has been observed that in some cases dealers had submitted the false declaration by submitting the bogus bill at ICC. A substantial amount of tax through such transactions have been evaded by using the bogus documents. To stop the modus operandi of the dealer / evader, it is intended that the identity of the dealer should be proved at the ICC itself when the vehicle carrying goods enters/leaves the state. In the light of this problem, it has been proposed to the department to introduce the system for authentication using digital signature technique. Software for the intended system providing the utility to generate / verify the signature is proposed to be developed. [14,15]

3.3 Data Flow Diagram of existing System

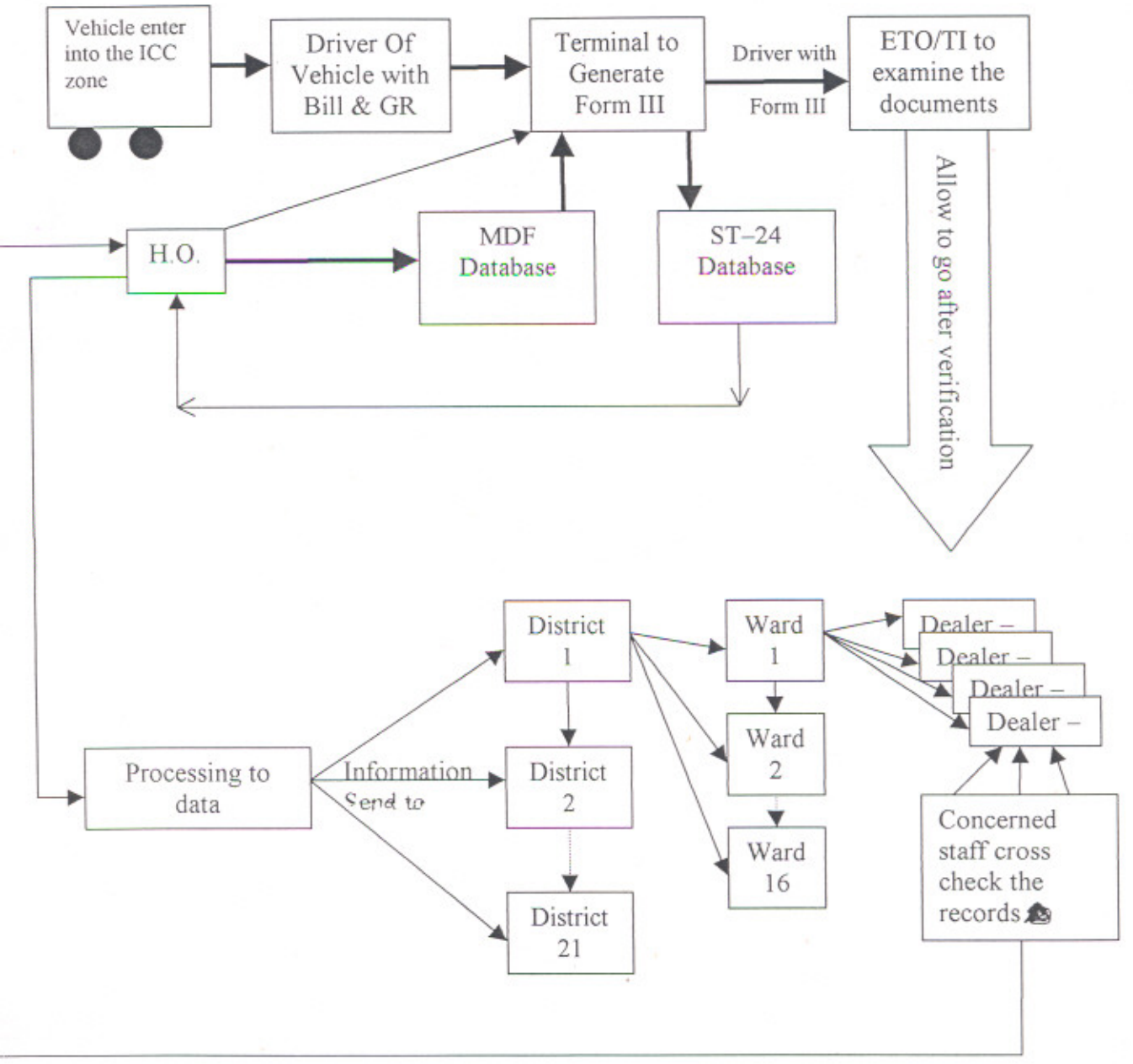


Fig. 3.1

3.4 Data Description of Existing Database

ST-XXIV-A

	Name	Character	Length	Description
1	Date	Date	10	Date of Entry
2	ICC	Numeric	2	ICC Code
3	Nature	Character	1	Import or Export
4	RC of Consignee	Character	10	License Number of Consignee
5	Name of Consignee	Character	40	Name of the Consignee
6	RC of Consignor	Character	10	License Number of Consignor
7	Name of Consignor	Character	40	Name of the Consignor
8	Description of Goods	Character	25	Description of Goods
9	Name & Address of Transport Co.	Character	40	Name & Address of the Transport Company
10	Driver Name	Character	20	Name of the Driver
11	Vehicle Number	Character	11	Vehicle Number
12	GR Number	Numeric	10	Goods Register Number
13	GR Date	Date	10	Date of Goods Registered
14	Bill Number	Character	12	Bill Number
15	Bill Date	Date	10	Date of Bill
16	Value	Numeric	12	Value of Goods
17	Destination	Character	20	Destination

3.5 System Analysis

In the light of current scenario, It has been observed that analysis of documents from ICCs is the most important application from revenue point of view. The remaining applications are being utilized for MIS reports. It is therefore, intended that necessary measure should be proposed to the department in order to plug the loopholes of tax evasion.

At each ICC, computers are installed proportional to the amount of work involved. Contractors have been directed to install one computer for 300 transactions per day. In case, there are more than one computer at ICC, it should be networked under Novell NetWare Operating system. Software has been prepared in FoxPro and supplied to the contractors by the department for filling the declaration forms. There are no security features in the existing environment. After analyzing the existing system, following drawbacks have been found:

3.5.1 Denial of Transactions

In the existing system, the dealer makes the interstate consignment from Punjab to other State or vice versa. The vehicle carrying goods have to cross the ICCs setup at Inter State borders and being the owner of goods at ICC, the driver has to make the declaration in the form-III which is being prepared from documents presented by him. Two copies of form-III are generated. The officer on duty retains one copy of the form-III for verification of goods. The second copy is returned to the driver for verification on the way if required.

Data so generated at ICC is integrated at Head Office to prepare the dealer-wise transactions for verification. The departmental staff visits the business premises or call the dealer randomly or periodically to show his account books for verification of transactions. Transactions not found in the account book are called the denied transactions. The dealer declare by submitting the affidavit that transactions are not made by the firm in question. If such eventually occurs, the, department fails to retrace the dealer. It causes the loss of tax of those particular transactions.

3.5.2. Security Issues

Data prepared at each ICC remain with the computer contractor for 15 days causing the security threats. During the period of 15 days computer contractor or his operator can temper the data with some ulterior motive to cause the breach to the confidentiality and integrity of data. Changing the working environment from MS-DOS, Novel NetWare and FoxPro to Windows NT/Oracle based client/server environment can eliminate this problem

3.6 Conclusion :

It has been observed after analysis that there are two major problems in the existing system of "*analysis of documents from ICCs*" vis-a-vis *problem of authentication* and *security issues*. First problem can be solved by adopting the system for authentication using digital signature technique and second can be solved by changing the working environment to Windows NT and Oracle based systems. Next chapter focuses on the formulation of model to generate/verify the digital signature.

CHAPTER-4
MODEL OF DIGITAL SIGNATURE

4.1 Introduction

The chapter is aimed to formulate the model of digital signature for the requirment identified in the previous chapter. Various encryption methods have been described to select the suitable technique for its application. Digital signature algorithms have been presented for comparative analysis. Algorithms have been analysed for the suitablity of the application and a model of digital signature has been proposed.

4.2 Encryption Techniques

Digital Signature is an application of asymetric cryptography which uses two keys: private and public keys. Private key is used for encrypting the message and public key is used to decrypt the encrypted message. The various techniques to encypt the message are described as under:

4.2.1 Substitution (Ceaser Cipher)

The simplest encryption technique involve substituting the plaintext alphabet with a new alphabet known as the ciphertext alphabet. For example, a ciphertext alphabet can be defined, which is the plaintext alphabet simply shifted by *n* places where *n* is the key. Hence, if the key is 3, the resulting alphabet is as follows :

Plaintext alphabet : a b c d e f g ....

Ciphertext alphabet : d e f g h i j .....

The ciphertext is obtained by substituting each character in the plaintext message by the equivalent letter in the cipher text alphabet. The

key is determined by the number of letters in the alphabet, for example, 26 in case of lower-case alphabets are to be transmitted or 128 if ASCII alphabets are being used.

Although this may seem to be a powerful technique, there are number of shortcomings that can be used to break such codes. The intruder is likely to know the context in which the message data is being used and hence the type of data involved. For example, if the messages involve textual information, then the statistical properties of text can be exploited : the frequency of occurrence of individual letters,(e,t,o,a,etc.), two-letter combinations (th,in,er,etc.) and three-letter combinations (the, ing, and, etc.) are all well documented. By performing statistical analysis on the letters in the cipher text such codes can be broken quickly.

4.2.2 Transposition

An alternative approach is to reorder (transpose) the characters in the plaintext. For example, if a key of 4 is used, the complete message can first be divided into a set of 4-character groups. The message is then transmitted starting with all the first characters in each group, then the second, and so on. As an example, assuming a plaintext message "this is a lovely day". The cipher text is derived as follows:

1	2	3	4	← key
t	h	i	s	
-	i	s	-	
a	-	l	o	
v	e	l	y	
-	d	a	y	

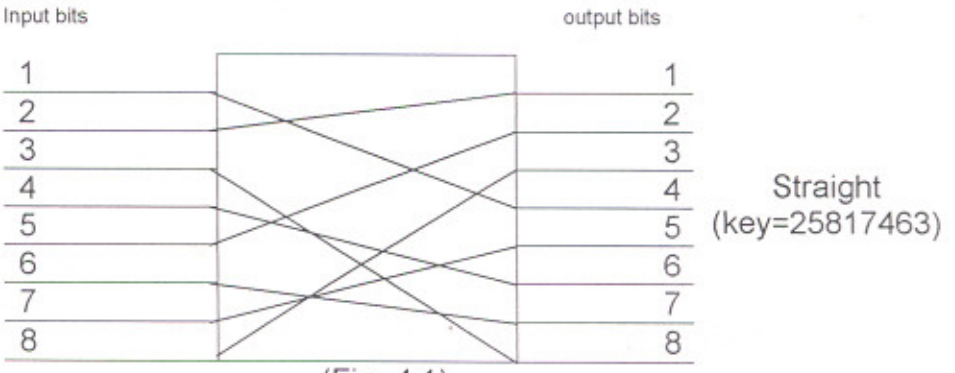
Cipher text = t-av-hi-edisllas-oyy

Clearly, more sophisticated transpositions can be performed but, in general, when used alone, transposition ciphers suffer from the same shortcomings as substitution ciphers.

4.2.3 Product Cipher

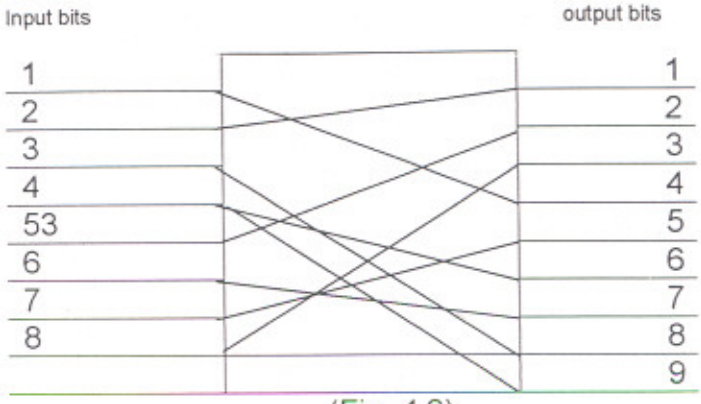
Most practical encryption algorithms tend to use a combination of the two techniques and are known as product ciphers. It uses a combination of substitutions and transpositions. Also, instead of substituting/transposing the characters in a message, the order of individual bits in each character are transposed. The three alternative transposition operations are shown in the following table. Each is normally referred to as a P-box.

The first involves transposing each 8-bit input into an 8-bit output by cross-coupling each input line to a different output line as defined by the key, and is known as a straight permutation (Fig.4.1).



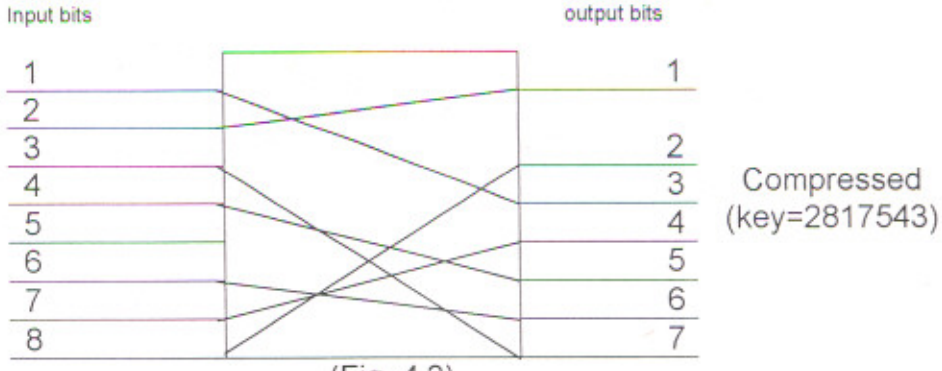
(Fig. 4.1)

The second has large number of output bits than input bits. reordering the input bits and passing selected input bits to more than one output . This is known as an expanded permutation (Fig.4.2).



(Fig. 4.2)

The third has fewer output bits than inputs: it is formed by transposing only selected input bits. This is known as a compressed or choice permutation (Fig.4.3).



(Fig. 4.3)

4.2.4 Monoalphabetic Substitution

Monoalphabetic substitution are more difficult to break than their caeserean counterparts. Here each character can stand for another, and there is no reason why one replaces another e.g. :

A=P
B=R
C=O
Etc...

This code is much more difficult to break, as each character now has 26 posibilities.

4.2.5 Vigenere Techneque

With standard mono-alphabetic encryption, the key to breaking the code is figuring out what each character stands for. Once, this is done, the code is solved, for each character maintains the same meaning throughout the duration of the encryption. Vigenere encryption adds one more level of difficulty, in that the value of each character is different each time it is used.

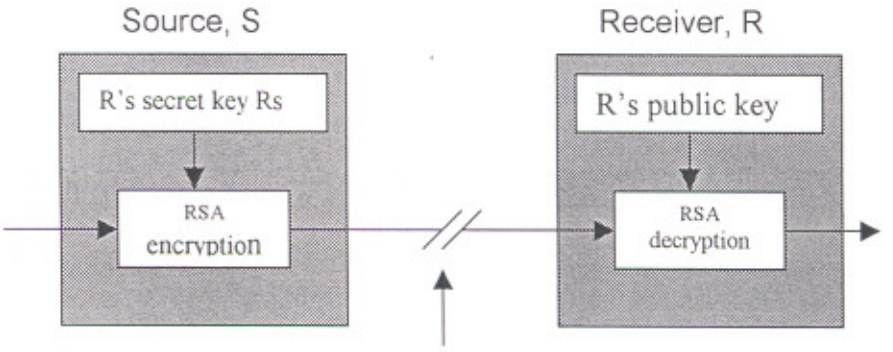
The key is computed by adding something to the equation which was formed from mono-alphabetic technique.

4.3 Algorithms of Digital Signature

Algorithms to generate and verify the digtal signature are described as under:

4.3.1 RSA Algorithm

RSA (Rivest, Shamir, Adleman) algorithm uses number theory to develop a method of generating a pair of numbers in such a way that a message encrypted, using the first number of the pair, can be decrypted only by the second number.



(Fig. 4.4)

Further, the first number cannot be derived from the second. This property means that the second number of the pair can be made available to anyone who wishes to send an encrypted message to the holder of the

first number as only that person can decrypt the resulting cipher text message. The first number of the pair is known as the private key and the second as the public key. The principle of the method is shown in Fig. 4.4.

The basic algorithm used to compute the two keys is simple and is summarized here together with a much-simplified example.

To create the public key Kp:

	Example:
• Select two large positive prime numbers P and Q	P = 7, Q = 17
• Compute X = (P-1)*(Q-1)	X = 96
• Choose an integer E which is prime relative to X, i.e., not a prime factor of X or a multiple of it, and which satisfies the condition indicated below for the computation of Ks	E = 5
• Compute N = P * Q	N = 119
• Kp is then N concatenated with E	Kp = 119,5

To create the secret key Ks:

• Compute D such that MOD (D*E,X) = 1	D*5 mod 96 = 1 D = 77
• Ks is then N concatenated with D	Ks = 119, 77

To compute the ciphertext C of plaintext P :

• Treat P as numerical value	P=19
• C = MOD (P^{E}, N)	C = MOD(19^{5}, 119)
	C=66

To compute the plaintext P of ciphertext C:

• P = MOD (C^{D},N)	P = MOD(66^{77},119)

The choice of E and D in this example is best seen by considering the factors of 96. These are 1,2,3,4,,6,8,12,16,24,32,48. The list of numbers which are prime relative to 96 are thus 5, 7,9,10,11, etc. If we try the first of

these, E = 5, then there is also a number D = 77 which satisfies the condition MOD(D*E,X) =1

From this example, it is deduced that the crucial numbers associated with the algorithm are the two prime numbers P and Q, which must always be kept secret. The aim is to choose a sufficiently large N so that it is impossible to factorize it in a realistic time.

The RSA algorithm requires considerable computation time to compute the exponentiation for both the encryption operations. However, there is simple way of avoiding the exponentiation operation by performing the following algorithm which uses only repeated multiplication and division operations :

```
C : = 1

Begin for I = 1 to E do
        C: = MOD (C*P,N)
End
```

Decryption is performed in the same way by replacing E with D and P with C in the above expression; this yields the plaintext P. For example, to compute C= MOD (19^5, 119):

Step 1: C = MOD(1 * 19, 119) = 19
2: C = MOD(19 * 19, 119) = 4
3: C = MOD(4 * 19, 119) = 76
4: C = MOD(76 * 19, 119) = 16
5: C = MOD(16 * 19, 119) = 66

Note also that the value of N determines the maximum message that can be enclosed. In the example this is 119 and is numerically equivalent to a single ASCII- encoded character. Therefore, a message comprising a string of ASCII characters would have to be encoded one character at a time. [2]

Disadvantages of RSA

(1) The RSA Algorithm is very slow when there are large number of business partners e.g. if there are 2 lakhs partners, it needs 4 lakhs prime numbers. As the number increases, execution time increases many fold. Thus it is not applicable for large number of partners for real time applications.

(2) Each key consists of two parts: first one is Modulus and the second one is exponential. In RSA algorithm, modulus of both the keys are equal. If someone succeeds to workout the product of two prime numbers which comes out equal to the few digits of public key, then one can workout the exponential of secret key by using RSA algorithm and can form the private key.

4.3.2 Digital Signature Standard (DSS) Algorithm

The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS PUB 186, known as the Digital Signature Standard (DSS). The DSS makes use of the Secure Hash Algorithm (SHA) and presents a new digital signature technique, called the Digital Signature Algorithm (DSA). The DSS was originally proposed in 1991 and revised in 1993 in response to public feedback concerning the security of the scheme.

In this algorithm there are three parameters that are public and can be common to a group of users. A 160 bit prime number q is chosen. Next, a prime number p is selected with a length between 512 and 1024 bits such that q divides (p-1). Finally, g is chosen to be of the form $h^{(p-1)/q}$ mod p,

where h is an integer having value between 1 and (p-1) with the restriction that g must be greater than one (1).

To create a signature, a user calculates two quantities, r and s, that are functions of the public key components (p,q,g), the user's private key (x), the hash code of the message, H(M), and an additional integer k that should be generated randomly or pseudorandomly and be unique for each signing. The following formulas are being used for signing and verification purpose:

Signing

$$r = (g^k \bmod p) \bmod q$$

$$s = [(k(H(M))^{-1} + xr)] \bmod q$$

$$\text{Signature} = (r,s)$$

Verifying

$$w = (s')^{-1} \bmod q$$

$$u1 = [H(M')w] \bmod q$$

$$u2 = (r')w \bmod q$$

$$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$$

$$\text{TEST: } v = r'$$

M=Message to be signed

x= Private key

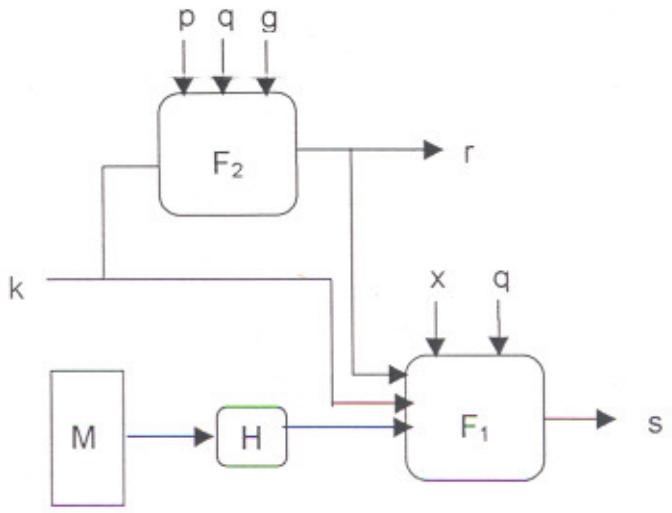
p,q are prime numbers

H(M)= Message digest

$y = g^x \bmod p$

$g = h^{(p-1)/q} \bmod p$

At the receiving end, verification is performed using the above formulas. The receiver generates a quantity v that is a function of the public key components, the senders public key, and the hash code of the incoming message. If this quantity matches r component of the signature, then the signature is validated.[1] Fig 4.1 depicts the functions of signing and verifying.



a) Signing

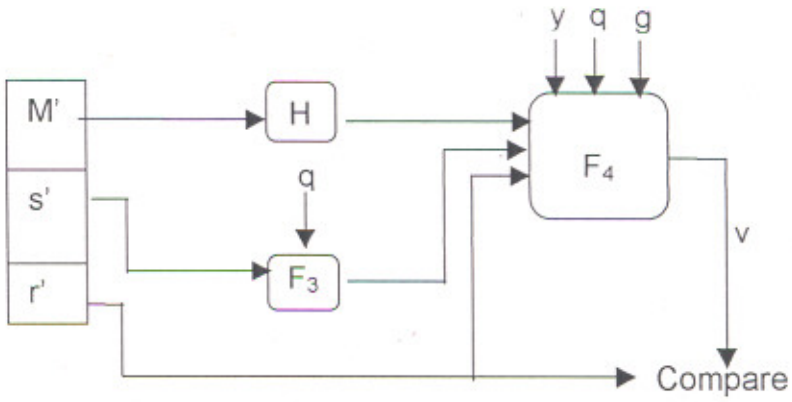


Fig 4.1 (b) Verifying

4.4 Analysis of Algorithms

Algorithms explained in the previous section contradicts the approaches for generating the digital signature. In the RSA approach, the messsage to be signed is input to a hash function that produce the secure hash code of fixed length. This hash code is then encrypted using private key to form the signature. Both the message and the signature are then transmitted. The recipient takes the message and produce a hash code. The recipient also decrypts the signature using the public key of the sender. If the calculated hash code matches the decrypted signature, the signature

is accepted as valid. Because the sender knows the private key, therefore, only the sender could have produced the valid signature.

The DSS approach also make uses of hash function. The hash code is produced as input to the signature function along with a random number k generated for the particular signature. The signature function also depends on the sender's private key and set of parameters known to the group of communicating partners. We can consider a set of parameters as global public key. The result of signature consisting of two componets, labeled as s and r.

At the receiving end, hash code of of the incoming message is generated. This plus the signature is the input to the verification function. The verification function also depends upon the global public key as well as sender's public key which is paired with the sender's private key. The output of the verification function is the value that is equal to the signature component r if the signature is valid.

From the analysis of both the algorithms, it has been observed that RSA algorithm is slow due to computation and could not be applied for real time applications. The DSS algorithm is efficient as compared with RSA, but it needs to communicate the global key (six parameters) for every transaction, alongwith the private and public key. This algorithm is applicable for direct digital signature scheme where partners can exchange keys on secure channel. Requirment of the application is to communicate between many to many partners and it needs the key distibution centre (KDC) for the management of keys. In view of these dificulties, a algorithm to generate/verified the digital signature has been proposed for the intended application by combining RSA and DSS approaches.

4.5 Model for the proposed system

In view of the shortcoming of the above algorithms to generate the digital signature, a algorithm is proposed which generate the digital signature efficiently for real time applications. In the algorithm, two large unique numbers are chosen instead of prime numbers. These two large numbers are the private and public keys. The relationship between two unique numbers is defined by the hash function. Hash parameters are to be stored along with keys in the centralized database. Third key is generated from the hash parameters, which acts as the pointer key. This key is used to encrypt/decrypt the Digital Signature. Vigenere technique of encryption has been used to generate the digital signature. Fig 4.2 depicts the functionality of the algorithm. Following parameters are generated for the proposed algorithm.

Secrete key = Concatenate (STR((N+C)) /D + Mod((N+C) /D))

Where N = Public Key
D = Val(Substr(Str(N,8),4,8)
C = Val(Substr(Str(N,8),1,3)

MD=Str(Rc,8)+Name+Address+Value+Bill_Date+Bill_no

Public Key = Licensee Identification Number popularly known as RC Number of the dealer.

Encryption Hash Function = ASCII(Enc_Chr) – Mod(C,26) + CNT
Where CNT = relative position of the Encrypted character.

Decryption Hash Function = ASCII(Dec_Chr) + Mod(C,26) - CNT

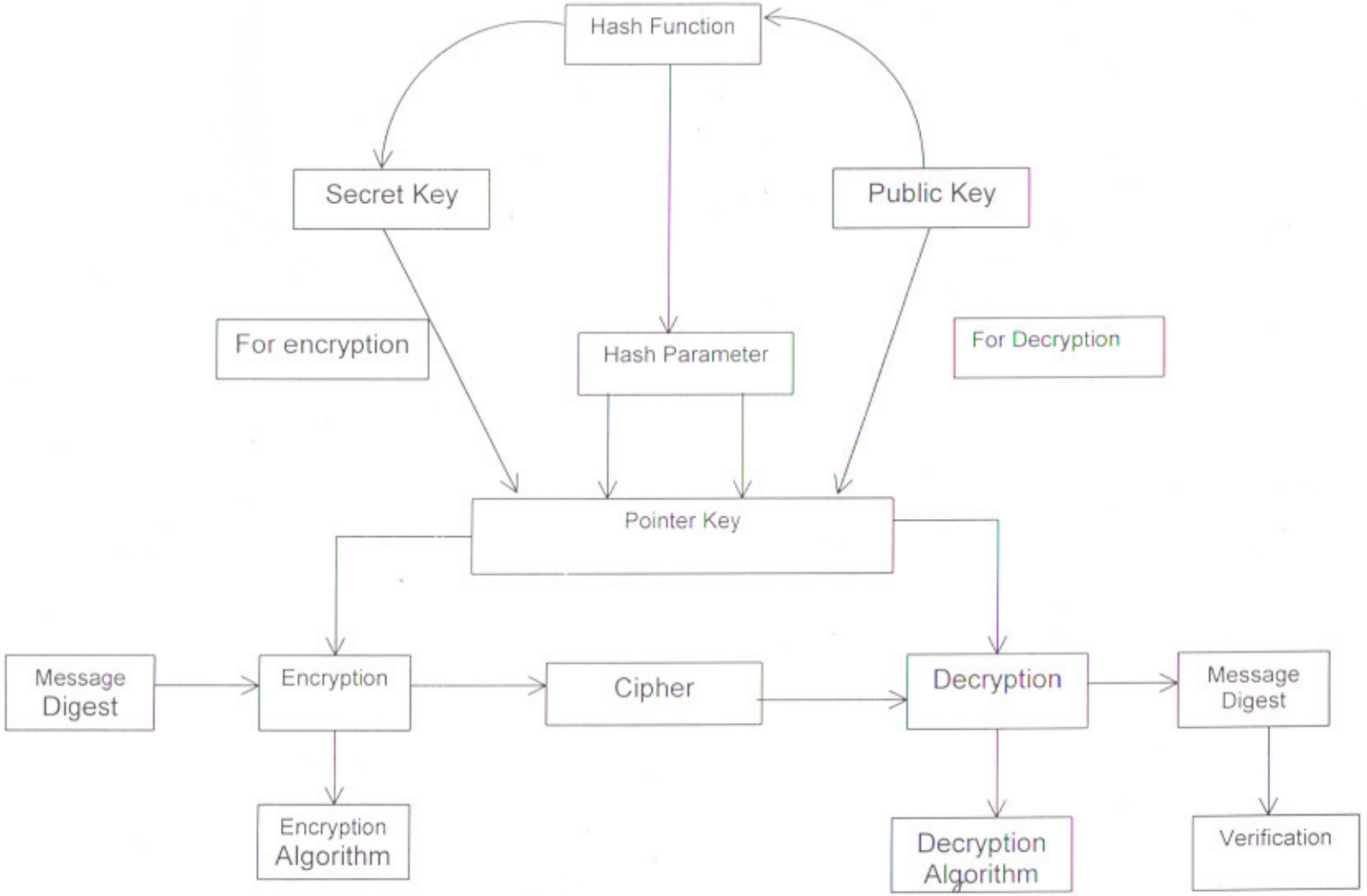


Fig. 4.2 Proposed Model

Advantages :

1 Encryption key not known to the owner or business partner.

2 Keys are independent of each other, Relation between private and public key is defined by the hash function in the system itself.

3 Speed of encryption is very fast as compared with RSA Algorithm

4 Only private key and public keys are to be distributed.

Disadvantage :

The main disadvantage of this model is that it is applicable only for the message digest stored in tabular form (database). Digital signature of documentary files could not be generated.

4.6 Conclusion

In this chapter, model of digital signature has been formulated after analyzing the encryption techniques and digital signature algorithms. Drawbacks of the algorithms are highlighted and solution to the problem has been proposed to meet the requirement of the applications. Next chapter focuses on the system of authentication for the requirement formulated in chapter III by using the proposed model of digital signature.

CHAPTER –5

SYSTEM FOR AUTHENTICATION

5.1 Introduction

This chapter aims to describe the various components of **system for authentication**, in order to meet the requirement formulated by the Excise and Taxation Department, Punjab. The proposed environment for the system is Windows-NT/Oracle to provide security to the database by granting permission at various levels. Digital Signature has also been generated/verified by using the proposed model. It describes the system processes, network model, data flow diagram conceptual design, ER diagram, tables and screen layouts. System security and testing of the software are also described.

5.2 Objectives of the System

Main objectives of the proposed system are mentioned as under:

1. To generate private keys for the dealer from unique RC-No. (Public key).
2. To maintain database of private keys, hash parameters, dealer's detail.
3. To provide utility to the dealer to make request for making transactions and generate the digital signature.
4. To generate the form-III proposed from bill and GR and verify the digital signature generated by the dealer.
5. To provide security to the database

5.3 Overview of the proposed system

In the proposed system for authentication, it is intended that head office, district office, sub offices and ICCs are networked through VSAT/Leased Line connectivity. Each ward will have the node connected with the district server and each district server is connected with head office. In each office, one guest terminal shall be provided for the use of dealer to make queries and requests. Fig 5.1 depicts the network arrangment of Excise and Taxation Department, Punjab.

It is intended in the system that the dealer shall make the request to the department to get a private key. For this purpose, he should apply to the concerned office for grant of secret key. His application shall be forwarded to Head Office for grant of secret key. The system shall provide the screen on every node to make the request for grant of secret key or dealer can apply on plain paper for grant of secret key. The information regarding the dealer like RC Number of the dealer, name and address, and trade are to be furnished by the dealer. This information shall be uploaded into the master data at H.O. At the H.O., all the applications seeking secret key shall be processed to generate the secret key against the Rc.No. This secret key shall be conveyed to the dealer through a registered post in order to avoid the leakage. After supplying the secret key to the dealer, it is desirable that whenever the dealer transact interstate consignement, the dealer should make a request to the

department by using the secret key provided to him by the department, at any office of Excise and Taxation Department, Punjab.

He will furnish the information like RC No., Name, Address, Date of Consignment, bill no., ICC, bill date, vehicle, Commodity etc.. This information will be uploaded in the master data base in the H.O. H.O. will send information to the concerned ICC after a fixed interval. When the vehicle carrying consignment arrives at ICC, it will submit the bill & GR in order to prepare the Form-III. Computer itself will seek the digital signature of the dealer from the request database and decrypt the digital signature furnished in the request. Computer shall prepare the message digest from data entered and compare it with the message digest transmitted by the dealer through NET. If these two message digest found to be matching then the vehicle shall be allowed to go otherwise computer shall print on Form-III that the dealer have the invalid secret key. The officer incharge on duty can verify the vehicle before clearing the transaction. [14,15]

Operational Enviornment :

(i)	Backend RDBMS	–	Oracle 8 or above
(ii)	Front End Tool	–	Developer 6
(iii)	Operating system Back end.	–	Windows NT
(iv)	Operating system Front End	–	Windows 95 or 98.

Hardware

Head Office : RISC based application Server under Unix Operating System.

District Office: Windows NT-Server with client nodes.

ICC : Window NT Server with client nodes.

Total No. of Locations	:	81 all over the state.
Head Office Server	:	One RISC Based Server
Total No. of Servers	:	60 (App.) [for districts and ICCs]
Thin Client Nodes	:	300 (App.)

Network

(1) LAN
(2) WAN through VSAT / Leased Line

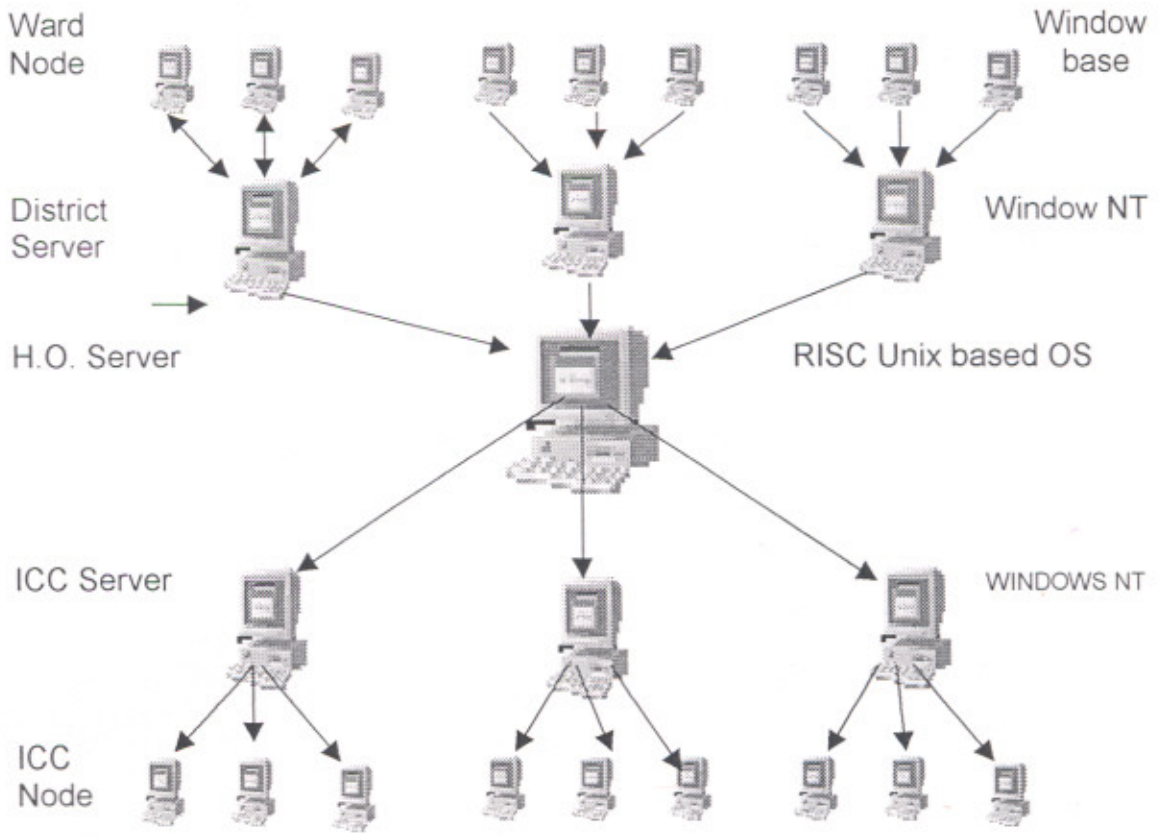


Fig-5.1

5.4 System Processes

(1) Dealer shall make the request to grant the private key at the local office of ETD, which will be forwarded to H.O.

(2) H.O. Shall issue the secret key against the RC Number. The RC Number of the dealer shall be treated as public key.

(3) Once the private key is issued to the dealer, he will make the request to the ETD for making inter state consignment, this request shall be made at the local office of ETD.

(4) In the request, dealer shall make the relevant entries for message digest in the computer of local office and digital signature shall be generated.

(5) The Digital Signature of the dealer generated from message digest shall be transferred to the server at the Head Office.

(6) H.O. server shall transfer the Digital Signature to the concerned ICC.

(7) When the vehicle will reach at the ICC for preparation of form-III, details of bill/GR shall be entered into the computer.

(8) Computer will verify from the database whether the dealer has the digital signature.

(9) If the dealer does not have the digital signature, it will skip the verification process.

(10) If the dealer has the message, it shall execute the verification process.

(11) Computer will decrypt the encrypted message.

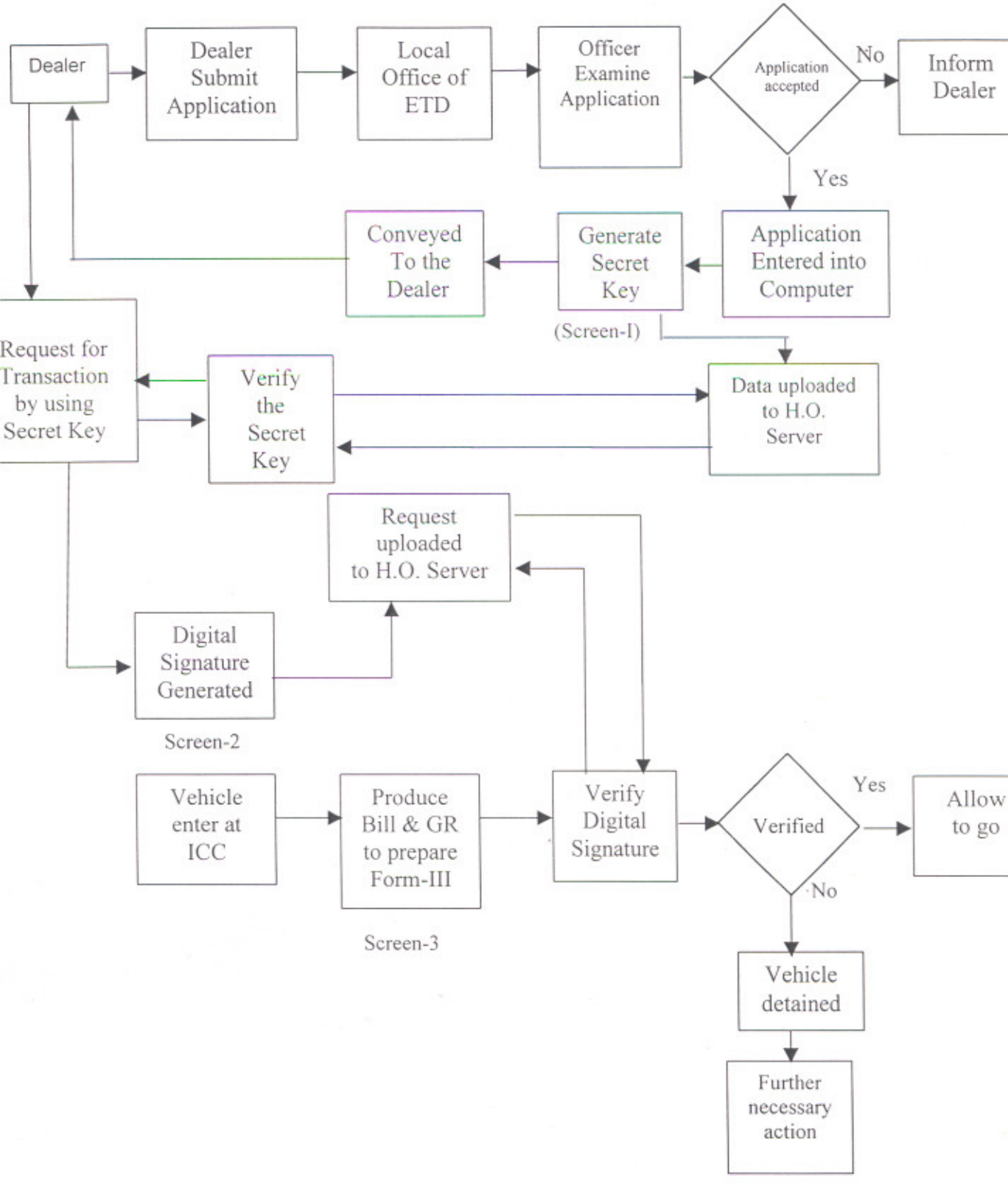
(12) Message digest as decrypted from digital signature and message digest generated from the data entered currently, will be compared.

(13) If both the messages match, vehicle shall be allowed to go.

(14) If it does not match, vehicle shall be detained assuming that the evader has made the consignment.

(15) Computer shall issue the detection notice to the dealer to prove the identity of transaction.

5.4.1 System Flow Diagram



5.5 Conceptual Design

The major step in conceptual design is to identify the entities and relationship that reflect the organization 's data. The objective of this step is to specify the conceptual structure of the data and is often reffered to as data modelling. Data modelling consist of E-R diagram and tables formed after normalization process.

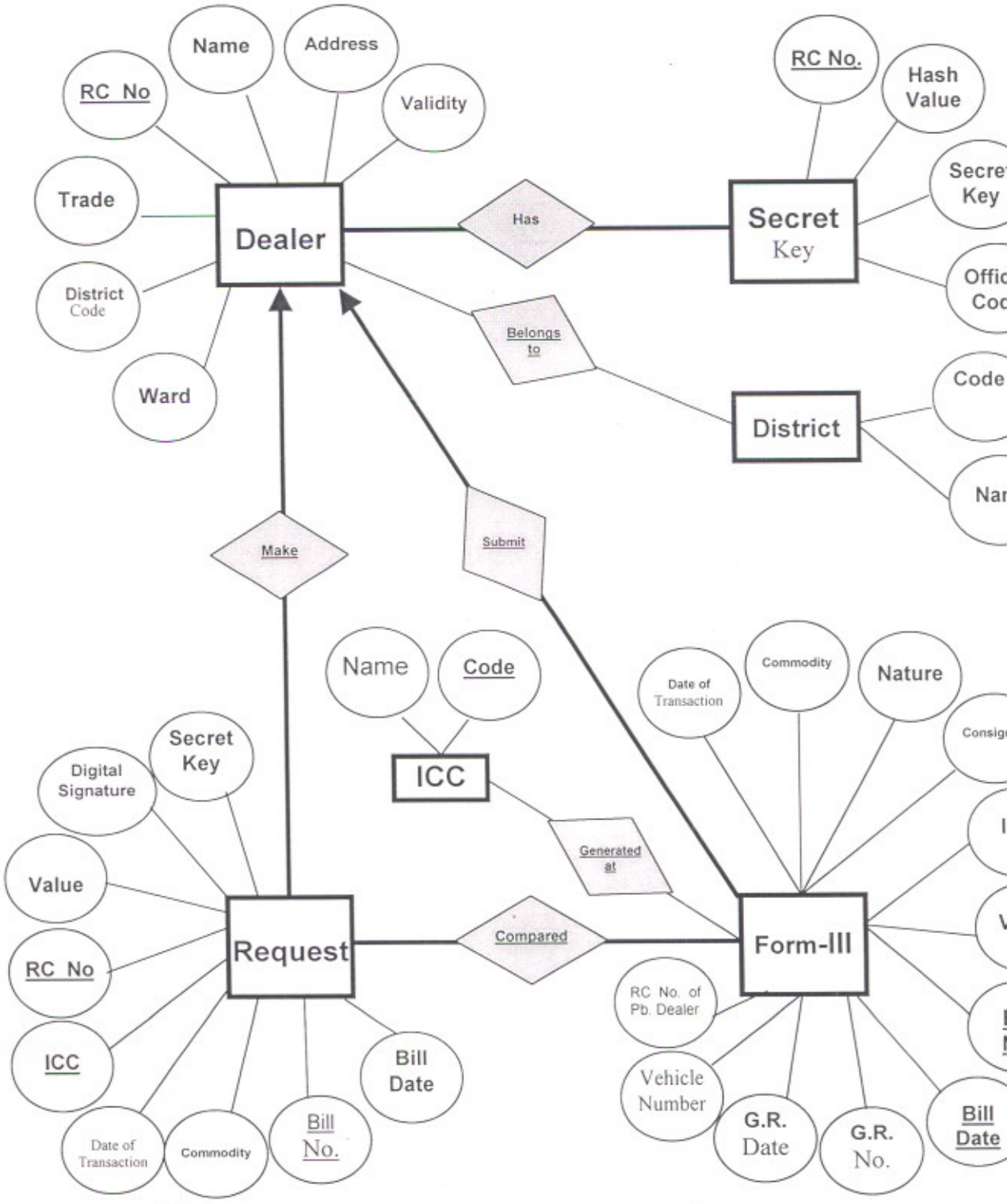
E-R diagram depicting the identified entities and attributes are shown in fig 5.3. Four entities namely dealer, application,request and transaction have been identified for the requirment. Relationship of entities is also depicted which are summarized as under.

Dealer to application	one to one
Dealer to request	one to many
Request to transaction	one to one

Normalization is the process of refining the data model built by the E-R diagram. The normalization techniques , logically groups the data over a number of tables, with the minimum redundancy on the data. Normalization process also removes any undesirable errors, resulting from database activities like inserting,deleting and updating value in the table. Storage space may also be conserved, thus resulting in a more efficient database. On the basis of E-R diagram and relationship between entities, tables have been designed and presented in the next section along with description after performing normalization process. Primary keys and foreign keys have also been identified to access the database items.

5.5.1 ER Diagram

It describes the entities, its attributes and their relationships.



Relations
Dealer – Secrete key – One to One
Dealer – Request - One to Many
Dealer – ST-XXIV-A – One to Many
Request – ST-XXIV-A – One to One

keys
Dealer – Primary Key – RC No.
Request – Primary Key – RC No. + Bill No.
ST-XXIV-A – Foreign Key – RC No.+Bill
Secret Key – Foreign Key – RC No.

5.5.2 Table Formulations

Following tables have been created to store the data after normalization.

Secret-key-Master

Sr. No.	Field Name	Attributes	Length	Description
1.	Rcnum	Number	8	RC Number of the Dealer
2.	Dist	Number	2	District Code
3.	Ward	Number	2	Ward Number
4.	Name/Address	Character	100	Address of the dealer
5.	Dt_validity	Date	10	Validity date of the dealer
6.	Trade	Number	2	Trade Code
7.	C	Number	3	Hash function parameter
8.	D	Number	4	Hash function parameter
9.	Q	Number	5	Hash function parameter
10.	R	Number	4	Hash function parameter
11.	Secret Key	Character	8	Secret Key of the Dealer

ICCs

Sr. No.	Field Name	Attributes	Length	Description
1.	ICC Code	Number	2	ICC Code
2.	ICC Name	Character	15	ICC Name

Districts

Sr. No.	Field Name	Attributes	Length	Description
1.	District Code	Number	2	District code
t.	District name	Character	15	District Name

Request For Transaction

Sr. No.	Field Name	Attributes	Length	Description
1.	Rcnum	Number	8	Rc Number of the Dealer
2.	Bill No.	Character	10	Bill No. of the Dealer's Transaction
3.	Bill Date	Date	10	Bill date of the Dealer's Transaction
4.	Value	Number	10	Bill amount. of the Dealer's Transaction
5.	Date of Transaction	Date	10	Transaction Date
6.	ICC code	Number	2	ICC Code
7.	Secret key	Character	8	Secret Key of the Dealer ineligible form
8.	Nature Code	Character	1	Import/Export/Transit/Intra-State
9.	Digital Signature	Character	256	Encrypted Message

Application for issue of private key

Sr. No.	Field Name	Attributes	Length	Description
1.	Rc_no	Number	8	Rc Number of the dealer
2.	Name	Character	40	Name of the Dealer
2.	Date of Application	Date	10	Application Date
3.	Application accepted	Character	1	Whether Yes or No
4.	Application status	Character	1	Whether Secret Key allotted or not.
5.	Officer Code	Number	3	Officer Incharge of the Ward or ICC
6.	User ID	Character	3	Identification number of the User

Form III (Declaration Form)

Sr. No.	Field Name	Attributes	Length	Description
1	ICC Code	Numeric	2	ICC Code
2	Date	Date	10	Date of Transaction
3	Time	Character	8	Time of Transaction
4	Nature	Character	1	Import/Export/Transit/Intra-State
5	RC of Consignee	Character	10	Rc Numbe of Consignee
6	Name of Consignee	Character	40	Name of the Consignee
7	RC of Consignor	Character	10	RC Number of Consignor
8	Name of Consignor	Character	40	Name of Consignor
9	Description of Goods	Character	25	Commodity Name
10	Name & Address of Transport Co.	Character	40	Transport Company's Name and Address
11	Driver Name	Character	20	Name of the Driver
12	Vehicle Number	Character	11	Vehicle Number
13	GR Number	Numeric	10	Goods Receipt Number
14	GR Date	Date	10	Goods Receipt Date
15	Bill Number	Character	12	Bill Number
16	Bill Date	Date	10	Bill date
17	Value	Numeric	12	Value of Goods
18	Destination	Character	20	Place of destination
19.	Authenticated	Character	1	Whether authenticated or not (Yes or No)

5.6 System Development

The main objective of the system development is to convert the conceptual design in the form of user view, which is also known as external view. This view of the system is the interface between the user and the computer system. The user need not know the processes occurring at internal level. This is achieved by developing the source programs for each process. The programming depends upon the platform being used. The platform for the intended system is mentioned in section 5.2. i.e. System is to be developed in Oracle as RDBMS and Window NT as backend operating system. Developer 2000 version 6 has been chosen for front-end development. Brief description of the RDBMS concepts are presented as under:

A database is a collection of interrelated data from which some information can be extracted. A database is designed and built for specific purpose, keeping in mind the needs of the applications. It is managed by software packages known as Database Management System(DBMS). A DBMS is a general purpose software which enable user to manipulate the database. It create an environment wherein, data can be stored and retrieved from database easily and most efficiently. A Relational Database Management System (RDBMS) is an information system that presents information in the form of rows contained in a collection of tables, each table possessing a set of one or more columns. Today, the RDBMS system is at the core of information system for the

organization. Oracle is one of the powerful RDBMS product which provides efficient and effective solutions for the organization. Oracle 8i is the latest version which provides the high transaction processing capability, security features and client/server environment.

Developer 2000 version 6 is the latest oracle product that can be integrated to build comprehensive applications. Development of application is performed by three parts of the oracle forms:

1. Oracle Form Builder
2. Oracle Form Compilers
3. Oracle Form Runtime.

Development of intended application i.e. *System for Authentication* can be initiated by creating the tables. Four tables have been designed after normalization to store the data in the relevant tables using SQL prompt. For making the utility of these tables, following screens (forms) have been designed using the data block wizards.

(a) Creation of secret key;

The main objective of this screen is to create the private key for the dealers. The input for this screen will be the attributes of the application, submitted by the dealer for the issuance of the private key. The screen layout is shown in the next section along with description of every column. All the columns have been validated and the properties have been set for each column. Following buttons are provided for navigation of screens.

- NEXT to select next screen
- BACK to select previous screen
- EXIT to quit from the system
- CREAT SECRET KEY :

When **CREATE SECRET KEY** is pressed, computer shall generate the secret key by using hash function described in the proposed model of digital signature. This is a ***when button pressed*** trigger event. Secret key generated from the hash function taking RC-No. as input is stored in the respective column.

(b) Request for transaction

The main objective of this screen is to provide the utility for the dealers to make online request for making the transaction. The input for this screen will be the values from the bill on which one is to make the interstate transaction. The screen layout is shown in the next section along with description of every column. All the columns have been validated and the properties have been set for each column. Following button is provided in addition to the screen navigation buttons:

- CREAT DIGITAL SIGNATURE :

When **CREATE DIGITAL SIGNATURE** is pressed, computer will generate the digital signature by using algorithm stored in the program unit. This program unit is activated through the trigger, which is attached with this button. Source code of the creation of digital signature is appended as appendix. This is a ***when button pressed*** trigger event.

Digital signature generated is stored in the respective column along with other parameter as mentioned in screen description.

(c) Declaration Form-III

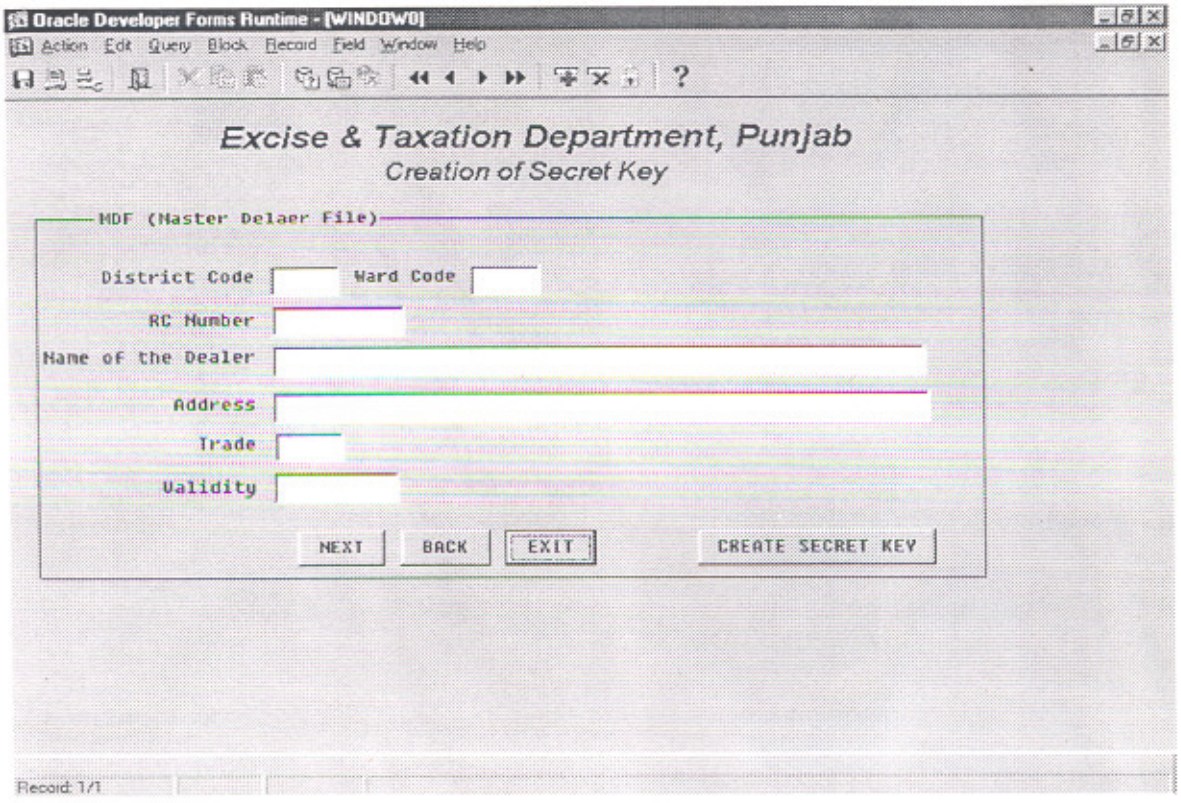
The main objective of this screen is to fill up form III from the details of bill and GR submitted at computer counter at ICCs. Operator on duty will fill up the relevant column from the document. At the end of completing the data entry, The Operator will verify the authentication of the transaction by pressing the button. All the columns have been validated and the properties have set for each column. A button is provided for verification of digital signature.

- VERIFY SIGNATURE:

When **VERIFY SIGNATURE** is pressed, computer will search the digital signature created by the dealer. If the signature is found in the database, it shall execute the program unit for verification. Source code for verification of digital signature is appended in the appendix.. This program unit is activated through the trigger which is attached with this button.

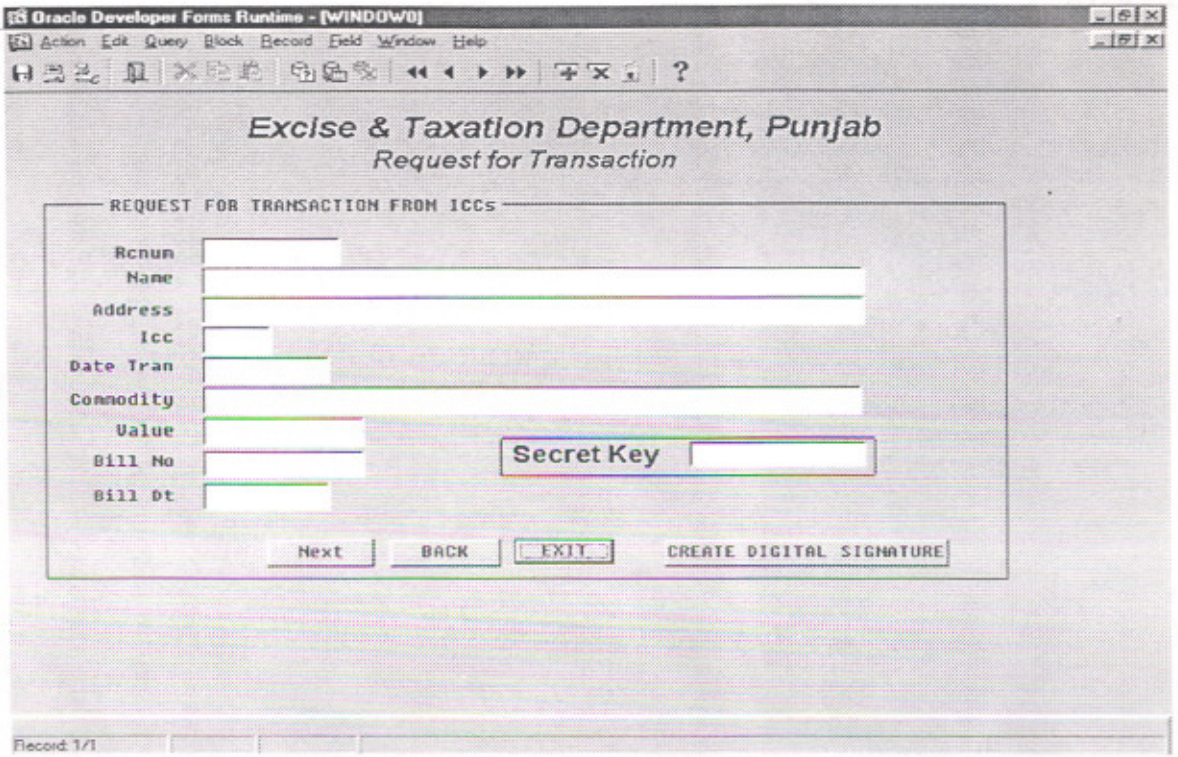
Buttons which have been provided by Developer by default are create new record, next record, previous record, save records , next block, previous block. These button can be used for every screens to navigate the tables

5.6.1 Screens & Descriptions

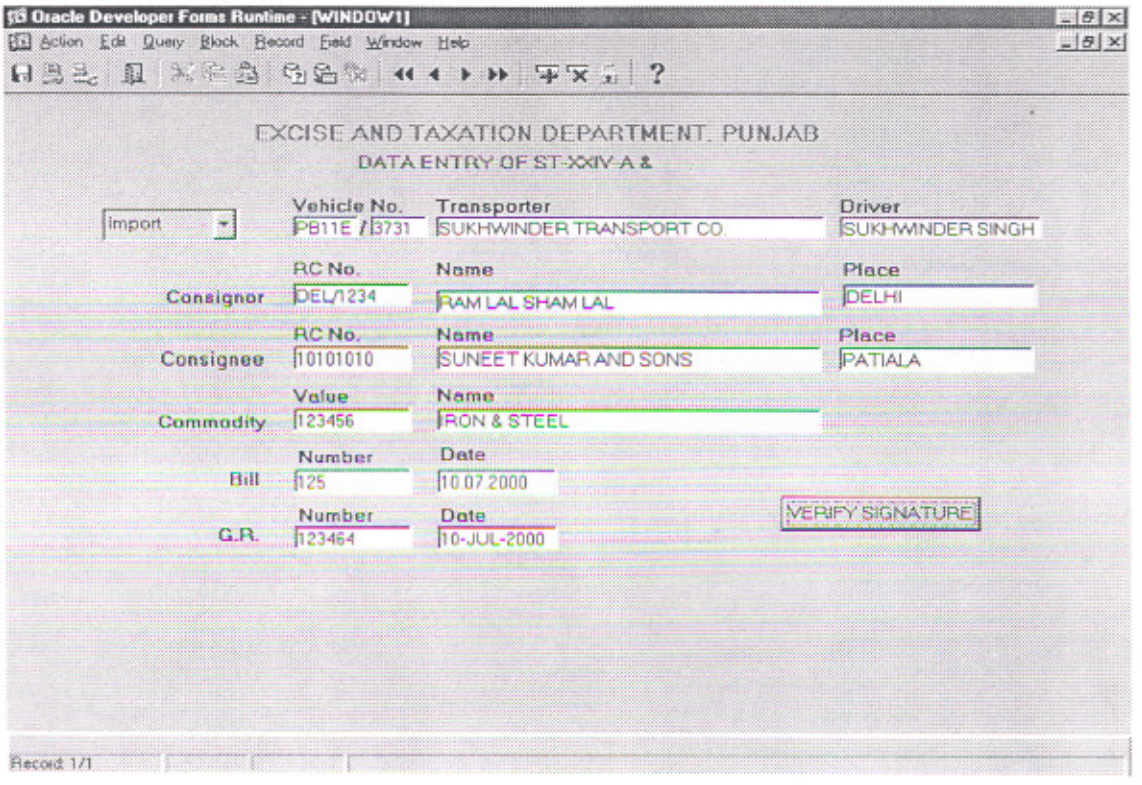


Description

Sr. No.	Column Name	Description
	District code	Screen shall provide the facility to enter the district to which the dealer belongs. District code shall be validated from LOV.
2.	Ward code	It will accept the ward code under which the liability of the dealer falls.
3.	Officer Code	It will accept the valid officer code from LOV.
4.	RC Number	It will accept the correct RC number of the dealer, incorrect RC number shall not be accepted, the number also work as a public key of the dealer.
5.	Name of the dealer	This is a display item which will be derived from the master data.
6.	Address of the dealer.	This is a display item which will be derived from the master data.
7.	Validity	It would accept the validity date of the dealer.
8.	Create the secret key	When this button shall be pressed it shall create the secret key of the dealer from the public key (RC Number) by using Hash function stored in the procedure.



Sr. No.	Column Name	Description
1.	Rcnum	It will acept the correct RC number of the dealer, incorrect RC number shall not be accepted, the number also work as a public key of the dealer.
2.	Name	This is a display item which will be derived from the master data.
3.	Address	This is a display item which will be derived from the master data.
4.	ICC	It will accept the ICC code.
5.	Date Tran	It will accept the date of transaction.
6.	Commodity	It will accept the name of the commodity.
7.	Value	It will accept the value of goods.
8.	Bill No.	It will accept the bill no.
9.	Bill date	It will accept the bill date
10.	Secret Key	It will accept the valid secret key of the dealer.
11.	Create Digital Signature	When this button shall be pressed, it shall create the secret key of the dealer from the public key (RC Number) by using Hash function stored in the procedure.



Sr. No.	Column Name	Description
1.`	Vehicle No.	It will accept the vehicle number .
2.	Transporter	It will accept the name of the transport co.
3.	Driver	It will accept the name of the driver
4.	Consignor's RC No.	It will accept the RC No. of the consignor.
5.	Consignor's Name	It will accept the name of the consignor.
6.	Consignor's place	It will accept the place/address of the consignor
7.	Consignee RC No.	It will accept the RC number of the consignee
8.	Consignee Name	It will accept the name of the consignee
9.	Consignee place	It will accept the place/address of the consignee
11.	Commodity Value	It will accept the value of goods
12.	Commodity date	It will accept the name of the commodity
13.	Bill Number	It will accept the number of the bill
14.	Bill Date	It will accept the date of the bill
15.	GR number	It will accept the number of the GR.
16.	GR date	It will accept the GR date
17.	Verify signature	When this button will be pressed it will be verified the values by comparing with the digital signature created by the dealer.

5.7 System Security

The system has been developed in Window NT Operating System, which provide the password security to the user. Unauthorized users are not allowed to login the system. The database is maintained in Oracle 8i. It provide the password security to the user and database. Using oracle 8i, the user can be strongly authenticated , even remotely, and the data is protected in transit using network encryption. Oracle 8i, ensure that the same strong security is enforced whether the data is accessed directly by the user, or through the middle tier, such as transaction processing monitors or application server. Columns of the database can be protected by granting access permissions to the users.

5.8 Testing

A system has been developed for Excise and Taxation Department, Punjab for authenticating the documents at ICC as per the reqiurment formulated in chapter 3. In the light of software engineering, the existing system should not be discarded immediately but should run in paralell with the new system in order to find out the shortcoming. Therefore, the test data was collected and input is fed into the tables through the screens provided by the system. The results of the system are satisfoctory yet further improvements can also be incorporated as deem fit at the time of implementation. Sample output is appened in appendix.

5.9 Conclusion :

This chapter is aimed to develop the software for creation of secret key from the application of the dealer, create digital signature from Inter-state consignment and authenticate transactions by using digital signature. The officer in charge of the ward can generate secret key in order to authenticate the dealer's identity and secret key shall be conveyed to the dealer. After obtaining the secret key, the dealer can make request to make inter-state transaction, which can be authenticated at ICC. Three screens have been provided for use by three different kind of users at different levels. One is for officer in charge, second for the dealer and third for the operator at ICC. All users have to use the centralized database through network. The software for the authentication of transaction have been tested and found working satisfactory.

CHAPTER -6

Conclusion

Change is being forced upon business for global growth and the communication ties within the firm for which information technology is playing the major role. The impact of Information technology on all those involved in trade has been very significant, Information technology has not only created new problem for administration but also opened up new possibilities for re-orienting the business activities. The security mechanism that will enable the wide spread use and acceptance over network should uphold the principle of authentication confidently and integrity of Information. To ensure the basic principles of security, there are various level of security like user level, file level, resource level, application level and network level security. The thesis is aimed to the explore the possibility of user level security for which cryptography and PENOP technology are familiar. Digital Signature technology, an application of cryptography is chosen keeping in view the existing problem of authentication. The required software has been developed to generate the digital signature from the database (message) and verification of transaction by taking Excise and Taxation Department, Punjab as a model organization.

5.1 Conclusion

The main objective of this work is to evolve a system for verification of transactions transmitted through electronic means. In the intended application, there are three type of users. One (dealer), who send the information along with his digital signature, second one (DBA), who maintain the databases for users and third one(at ICC), who verify the transactions transacted by the dealer. In order to provide the facility to each user, three input screens (forms) have been designed in the software along with buttons. Dealer can make transactions only by using his private key. Since only dealer knows his private key and only dealer can generate digital signature with his private key, therefore, it has the effect of identifying the person or entity. Department know dealer's public key and can decrypt something encrypted with dealers private key by using dealer's public key.

In this system an attempt has been made to explore the benefit of Digital Signature technique for authentication. It shall wipe out many modus operand ices being used by the tax evader as described in chapter-III. The technique gives the advantage that the system ensures the flow of genuine transactions and the revenue is bound to increase in the state. The same system could be extended for other applications where dealer's identity is required to be proved. The technique of authentication secures the tax liabilities of the department and avoid the

unnecessary harassment of the dealer for verification if the documents are suspicious. The development and use of authentication technology is a dynamic process. It is not an end as it is an endless journey in which the good people hurry to stay a step or two ahead of the bad people.

5.2 Scope for further Investigation

Once this comprehensive system is streamlined, it can be investigated to extend this application on Internet. Implementation of this application will enable the registered dealer to furnish the information like form-III, sales tax returns and RD sales & purchases on the WEB. The shortcomings of the proposed system are needed to be analyzed and necessary alteration/modification for its implementation for any other organization are required to be in corporate.

References

1. William Stalling, Cryptography and Network Security, Prentice Hall, second edition, 2000.

2. Fred – Halsall, Addission, Data Communication, Computer Networks and Open System (Computer Science Series), Tata McGraw-Hill,1994.

3. Gerd E. Kieser. Local Area Networks, Tata McGraw-Hill, 1989.

4. Digital signature tutorial and guidelines, http://www.commerce.state.ut.us/digsig/tutorial.htm,2000.

5. Benjamin Wright, "Eggs in Basket : Distributing the Risks of Electronics Signature", workshop on Electronic Commerce and Trade Procedure held at NIC, Delhi,1996, Page No.213.

6. A. Lekhtakia, level of internet security, workshop on Electronic Commerce and Trade Procedure held at NIC, Delhi,1996, Page No. 203.

7. Debjani Nag, Security aspects of Electronic Commerce and EDI, workshop on Electronic Commerce and Trade Procedure held at NIC, Delhi,1996, Page No. 196.

8. Networld Computer Education, Jalandhar, Course material on internet security,2000.

9. Abraham Silberschatz, Henry. F.Korth and S. Sadarshan; DataBase System Concepts, Third edition,Tata McGraw-Hill,1997.

10. Ivan Bayross, Commercial Application Development using Oracle Developer 2000, BPB Publication, 2000.

11. Micheal Abbey, Michal J. Corej IAN Abranson; Oracle 8i, Beginners Guide, First Edition,Tata McGraw-Hill, 1997.

12. Course material on Programming with Developer 2000 form and tools, STG Publication, 2000.

13. Course material on Oracle for Database Management Administrator Oracle 8i, STG Publication,2000

14. PC Garg, Sales Tax Manual, Punjab, Mahavir Law Publication, Malerkotla House, Civil Line, Ludhiana, Fourth edition,1995.

APPENDIX

APPENDIX - I

SOURCE CODE OF ENRYPTION

```
----------------------------------------
-- THIS MODULE IS DEVELOPED  TO
-- ENCRYPT THE STRING STORED IN THE
-- TABLES USING SUBSITUTION TECHNIQUE
----------------------------------------
 DECLARE
   RC CRYPT.RCNUM%TYPE;
  -- PUBLIC KEY AND UNIQUE REGISTAATION NO.
   DC CRYPT.DEC%TYPE;
-- STRING TO BE ENCRYPTED
   EN CRYPT.ENC%TYPE;
-- ENCRYPTED STRING
   LN NUMBER;
-- TEMP VAR TO COUNT THE LENGTH OF THE STRING
   CNT NUMBER;
--  TEMP VAR COUNTER
   ENC_CHR CHAR(1);
-- TEMP VAR TO STORE ENCRYPTED STRING
   ASCII_VAL  NUMBER;
-- TEMP VAR WHICH RETURNS THE NUMERICAL VAL OF THE
-- ENCRYPTED STRING
   COMP_VAL NUMBER;
-- COMPUTED VALUE USING HASH FUNCTION
   ENC_STR VARCHAR(1);
    ENCRYPTED_STRING VARCHAR(256);
    CN NUMBER(3);
--  TEMP VAR
  BEGIN
   rc:=&rc_num;
  SELECT CRYPT.DEC INTO DC FROM CRYPT WHERE CRYPT.RCNUM=RC;
  LN:=LENGTH(DC);
   FOR CNT IN 1..LN
   LOOP
     ENC_CHR:=SUBSTR(DC,CNT,1);
   cn:=TRUNC(CNT/100);
   ASCII_VAL:=ASCII(ENC_CHR);
   COMP_VAL:=ASCII_VAL-12+cnt-CN*100;
   ENC_STR:=CHR(COMP_VAL);
   ENCRYPTED_STRING:=CONCAT(ENCRYPTED_STRING,ENC_STR);
--    DBMS_OUTPUT.PUT_LINE(AB||'  '||CHR(QQ));
    END LOOP;
UPDATE CRYPT SET ENC=ENCRYPTED_STRING
where rcnum=rc;
--    DBMS_OUTPUT.PUT_LINE(SS);
  END;
/
```

SOURCE CODE OF DECRYPTION

```
-------------------------------------------------
  -- THIS MODULE IS DEVELOPED  TO
  -- DECRYPT  THE ENCRYPTED STRING STORED IN THE
  -- TABLES USING SUBSITUTION TECHNIQUE
  -------------------------------------------------
   DECLARE
     RC CRYPT.RCNUM%TYPE;
   -- PUBLIC KEY AND UNIQUE REGISTATION NO.
     EN CRYPT.ENC%TYPE;
  -- STRING TO BE DECRYPTED
     LN NUMBER;
  -- TEMP VAR TO COUNT THE LENGTH OF THE STRING
     CNT NUMBER;
  --  TEMP VAR COUNTER
     ENC_CHR CHAR(1);
  -- TEMP VAR TO STORE DECRYPTED STRING
     ASCII_VAL  NUMBER;
  -- TEMP VAR WHICH RETURNS THE NUMERICAL VAL OF THE
  -- ENCRYPTED STRING
     COMP_VAL NUMBER;
  -- COMPUTED VALUE USING HASH FUNCTION
     DEC_STR VARCHAR(1);
      DECRYPTED_STRING VARCHAR(256);
      CN NUMBER(3);
  --  TEMP VAR
    BEGIN
     rc:=&rc_num;
    SELECT CRYPT.ENC INTO EN FROM CRYPT WHERE
CRYPT.RCNUM=RC;
    LN:=LENGTH(EN);
     FOR CNT IN 1..LN
     LOOP
       ENC_CHR:=SUBSTR(EN,CNT,1);
     cn:=TRUNC(CNT/100);
     ASCII_VAL:=ASCII(ENC_CHR);
     COMP_VAL:=ASCII_VAL+12-cnt+CN*100;
     DEC_STR:=CHR(COMP_VAL);
     DECRYPTED_STRING:=CONCAT(DECRYPTED_STRING,DEC_STR);
  --    DBMS_OUTPUT.PUT_LINE(AB||'   '||CHR(QQ));
      END LOOP;
  UPDATE CRYPT SET DECR=DECRYPTED_STRING
  where rcnum=rc;
  --   DBMS_OUTPUT.PUT_LINE(SS)
END;
/
```

APPENDIX - II

Sample Outputs

Plain Text –1

63156786 SATAYAM KARYANA STORE, LAHORI GATE
PATIALA. VALUE- 456577 BILL-5446567 DATE_TRAS-10-JAN-2000 ICC-12

Encrypted Message (Digital Signature)

+)(-/132□Q@TB[DQ%QHZbKYM-
ac_cW?4aW_gkc;c^rd*qcwmfrhVI€lx,s\PegiilmWz,†‡irrsvvxzd‰‡›□¨ž□□{€€~œ"
¢,ˆ‡$
%□@;<·.

Decrypted Message from Digital Signature

63156786 SATAYAM KARYANA STORE, LAHORI GATE
PATIALA. VALUE- 456577 BILL-5446567 DATE_TRAS-10-JAN-2000 ICC-12

Plain Text –2

10101010
JOGINDER SINGH MALHI, 3151-PHASE-II, URBAN ESTATE PATIALA. HE IS DOING ME COMPUTER SCIENCE) FROM THAPAR INSTITUTE OF ENGG. AND TEECNOLOGY
(DEEMED UNIVERSITY) PATIALA.

Encrypted Message (Digital Signature)

?E>AG>@N□QHNHJ#QFROQ5*>=B?<`YSfYB_`D9om^^I?etvdxjFwi}slxn\OxvR|‡?z†□‡
□[‰,^,□Ž'˜˜Š˜g›Œ"□š□"xp—¤¢¡u ª Ÿ5
E7I□BHNPFRTTF"RJ%KUOP8+M[R/dVWVbdbf_r$C<acdmffCyso}m{}t€†WO€r†|u□we

Decrypted Message from Digital Signature

JOGINDER SINGH MALHI, 3151-PHASE-II, URBAN ESTATE PATIALA. HE IS DOING ME COMPUTER SCIENCE) FROM THAPAR INSTITUTE OF ENGG. AND TEECNOLOGY
(DEEMED UNIVERSITY) PATIALA.

Source Code of RSA Algorithm

```
set talk off
set stat off
set inte off

set alter to aa
set alter on

sele 1
use prime

sele 2
use prime2
store space(10) to tm1,tm2

sele 2
do while .not. eof()
   q=b->p
   tm1=val(substr(time(),7,2))
   sele 1
   go top
   do while .not. eof()
      p=a->p
      *q=7
      qq=p*q
      R=(P-1)*(Q-1)
      i=2
      do while i<r/2
         s=mod(r,i)
         if s>0
            e=i
            exit
         endif
         i=i+1
      enddo
      if e<10
         aa='0'+str(e,1)
      else
         aa=str(e,2)
      endif
      *?"secret Key :"+str(qq)+aa
      i=2
      do while i<r
         jj=mod((i*e),r)
         if jj=1
            d=i
            exit
         endif
         i=i+1
      enddo
      *?"Public Key :" +str(qq)+str(d)
      pp=67
      c=pp
      i=1
      do while i<e
         c=mod((pp*c),qq)
         i=i+1
      enddo
      *?'Plaintext '+str(pp)
      *?'Chiper ' +str(c)
```

```
        cc=c
        a=1
        do while a<d
           cc=mod((c*cc),qq)
           a=a+1
        enddo
        *?"Plaintext "+str(cc)
        ?p,q,pp,c,cc,(val(substr(time(),7,2))-tm1)
        skip
   Enddo
   sele 2
   skip
enddo
```

Sample Output of RSA Algorithm

First Prime Numbe	Second Prime Number	Cipher text	Exponential Value (d)	Plaintext	Execution Time in Seconds Per Character
197	5	67	338	67	1
199	5	67	652	67	1
211	5	67	997	67	1
223	5	67	597	67	1
227	5	67	1123	67	1
229	5	67	647	67	1
233	5	67	193	67	1
239	5	67	818	67	1
241	5	67	1193	67	1
251	5	67	818	67	1
257	5	67	73	67	1
263	5	67	943	67	1
269	5	67	828	67	1
271	5	67	308	67	1
277	5	67	792	67	1
281	5	67	93	67	1
283	5	67	27	67	2
293	5	67	438	67	2
307	5	67	507	67	2
311	5	67	648	67	2
313	5	67	1172	67	2
317	5	67	1198	67	2
331	5	67	1563	67	6
337	5	67	322	67	6
347	5	67	608	67	7
349	5	67	1157	67	7
353	5	67	713	67	7
359	5	67	998	67	7
367	5	67	2	67	7
373	5	67	1252	67	7
379	5	67	142	67	7
383	5	67	108	67	7
389	5	67	1233	67	7
397	5	67	1552	67	7
401	5	67	13	67	7
409	5	67	1792	67	7
419	5	67	1178	67	7
431	5	67	1218	67	8
433	5	67	797	67	8
439	5	67	362	67	8
443	5	67	1738	67	8
449	5	67	2178	67	8
457	5	67	867	67	8
461	5	67	1113	67	8
463	5	67	902	67	8
467	5	67	1883	67	8
479	5	67	1388	67	8
487	5	67	397	67	8
491	5	67	1253	67	9
499	5	67	767	67	9
503	5	67	1478	67	9
509	5	67	453	67	9
521	5	67	1188	67	9

First Prime Numbe	Second Prime Number	Cipher text	Exponential Value (d)	Plaintext	Execution Time in Seconds Per Character
523	5	67	607	67	9
541	5	67	2633	67	9
547	5	67	562	67	9
557	5	67	2768	67	9
563	5	67	2373	67	9
569	5	67	2038	67	10
571	5	67	2163	67	10
577	5	67	2807	67	10
587	5	67	1393	67	10
593	5	67	1298	67	10
599	5	67	1263	67	10
601	5	67	613	67	10
607	5	67	2322	67	10
613	5	67	1802	67	10
617	5	67	1518	67	10
619	5	67	2542	67	11
631	5	67	673	67	11
641	5	67	2698	67	11
643	5	67	1932	67	11
647	5	67	3143	67	11
653	5	67	383	67	11
659	5	67	918	67	11
661	5	67	983	67	12
673	5	67	2982	67	12
677	5	67	2883	67	12
683	5	67	243	67	12
691	5	67	1458	67	12
701	5	67	2838	67	12
709	5	67	1222	67	12
719	5	67	2378	67	13
727	5	67	2502	67	13
733	5	67	1412	67	13
739	5	67	1667	67	13
743	5	67	3563	67	13
751	5	67	518	67	13
757	5	67	467	67	13
761	5	67	168	67	13
769	5	67	3342	67	13
773	5	67	3158	67	14
787	5	67	2997	67	14
797	5	67	1888	67	14
809	5	67	1433	67	14
811	5	67	258	67	14
821	5	67	1098	67	14
823	5	67	1837	67	14
827	5	67	3043	67	15
829	5	67	3272	67	15
839	5	67	2918	67	15
853	5	67	972	67	15
857	5	67	813	67	15
859	5	67	447	67	15
863	5	67	3028	67	16
877	5	67	1147	67	16
881	5	67	1223	67	16
883	5	67	447	67	16
887	5	67	3618	67	16

First Prime Numbe	Second Prime Number	Cipher text	Exponential Value (d)	Plaintext	Execution Time in Seconds Per Character
907	5	67	1187	67	16
911	5	67	133	67	16
919	5	67	3827	67	16
929	5	67	3483	67	17
937	5	67	1807	67	17
941	5	67	4348	67	17
947	5	67	2458	67	17
953	5	67	568	67	17
967	5	67	4542	67	17
971	5	67	4608	67	18
977	5	67	2778	67	18
983	5	67	948	67	18
991	5	67	788	67	18
997	5	67	2662	67	18
503	7	67	1178	67	7
509	7	67	1080	67	7
521	7	67	2195	67	7
523	7	67	3222	67	7
541	7	67	1551	67	7
547	7	67	562	67	8
557	7	67	2781	67	8
563	7	67	1563	67	8
569	7	67	3614	67	8
571	7	67	2734	67	8
577	7	67	499	67	9
587	7	67	2214	67	9
593	7	67	4055	67	9
599	7	67	72	67	9
601	7	67	613	67	9
607	7	67	1108	67	9
613	7	67	576	67	10
617	7	67	1388	67	10
619	7	67	1304	67	10
641	7	67	536	67	10
643	7	67	646	67	10
647	7	67	3033	67	11
653	7	67	2550	67	11
659	7	67	1493	67	11
661	7	67	4288	67	11
673	7	67	4328	67	11
677	7	67	2963	67	11
683	7	67	4174	67	11
691	7	67	767	67	11
709	7	67	513	67	12
719	7	67	2725	67	13
727	7	67	3229	67	13
733	7	67	5077	67	13
739	7	67	3145	67	13
743	7	67	2718	67	13
751	7	67	2020	67	13
757	7	67	3495	67	14
761	7	67	3728	67	14
769	7	67	4111	67	14
773	7	67	4853	67	14
787	7	67	1423	67	15
797	7	67	1528	67	15

FORM S.T.I [FORM-I]

[*See* Rule 3]

1. Application for Compvlsory/Voluntary Registretion under section 7 and 8 of the Punjab General Sales Tax Act, 1948.

The Assessing Authority

Ward ——————

District

Passport size
of the photograph
Proprietor, Managin
Partner (s)
Managing Director or
General Attorney

I..... Proprietoyr Managing Partner (s)/Managing Director/General Attorney/Head of Department (or an other Joint Officer/Officers duly authorised by him in writing) of the business known as..... whose head office in Punjab is situated at.....hereby apply on behalf of the said business, for a certificate of registration under the Punjab Gerera l Sales Tax Act, 1948, and attach herewith a treasury/bank receipt for rupees.....being registration fee.

2. Nature of busines.....

3. The concern manufactures the following classes of goods for traders..... .....

4. The concern does/does not import goods direct from other countries/ states .....

5. Particulars of the proprietor/partner (s) all other persons having any interest in the business' :—

Sr. No.	Name in full	Father's/Husband's Name	Age	Extent of interest in the business
1	2	3	4	5
1				
2				
3				
4				
5				
7				

Present address	Permanent address	Phone No.	Signature	Signature and address of withness attesting signature in column No. 9
6	7	8	9	10

6. The proprietor or any partner or any other person having an interest in the business has interest in no other business anywhere in India/has interest in the followiug other business in India :—

Serial No.	Name of the proprietor/ Partner or other person	Name and particulars of the business	Address of places of business
1			
2			
3			
4			

Notes :—(i) In the case of Government Dapartment, the name of the Department and in the case of institution or concern, officer incharge of the institution or concern only be given;

(ii) Column No. 5 to be filled in if the appliticant is not a company incorporated under the Indian Companies Act, 1956, or unper any other law.

7. The business in respect of which this applicatiih is made, has been registered with the Registrar of Firms and Societies, Punjab if registered in any other State/Union Territory, name of such State/Union Territory.....) R.C.No.....

8. Location of the place of business	Additional place of business
(i) Shop No....	
(ii) Mohalla Road, Market.....	—
(iii) Town	
(iv) Post Office	
(v)	

(vi) Name of the adacent dealers..... .....

(a) Right Hand Side .. ..

(b) Left Haud Side .....

(vii) Previous occupant of the premises.....

(viii) His Registration Certificate Number.

(ix) Whether any other dealers is functioning from the same

prmises. If so, his name and registration certficate ....

9. Name of the Head office ....

Complete addree..... ....

10. State whether the applcant is the owner of the business premises of tenant (if, a tenent, copy of rent deed to be enclosed.)

....

11. Constitution of the concern. Whether partnership deed executed (copy

of deed to be enclosed, if executed)..... ....

12. The following classes of goods are ordinarily purchased by the business : —

(a) for purpose of manufacture..... ... .

(b) for resale..... ....

(c) for containers or other packing materials..... ....

13. Details of the first purchase Details of first sale

(i) Bill No.....Bill No..... ....

(ii) Date.... .....Date ....

(iii) Amount..... .... .Amount ....

(iv) Seller's name and address Purchaser's name and address

....

....

14. Total purchase and sale since the start of business———————— Rupees————————

15. Average Sale/Purchase per day Rs.————————

16. Gross turnouer during the year Rs.————————

17. The annual taxable turneover is estimated at———————— percent of annual gross turnover.

18. Details of first import, if any:

(i) Bill No._____

(ii) Date _____

(iii) Amount _____

(iv) Goods Receipt No._____

(v) Octroi Receipt No. _____

(vi) Seller's name and address _____

19. Particulars of Bank account :—

(a) Name of the Bank _____

(b) Account No. _____

20. Total working capital of the concern _____

21. Details of account books maintained/to be maintained :—

1. _____

2. _____

3. _____

4. _____

22. The account are kept in the _____ script.

23. Accounting period _____

24. State whether the Registration certificate was ever refused to dealer/Firm partner (s) if so, give details :—

_____

_____

25. State whether the registration certificate of the dealer/firm/partner (s) was over cancelled. If so, give details :—

_____

_____

DECLARATION

I hereby declare that the above statments are true and complete to the best of my knowledge and belief.

Place _____ _____

Signature of applicant

Date _____ Status _____

7. In the said rules. for Form ST-IV, the following form shall be substituted, namely : —

FORM-II

912—7-4-99—10,50,000—Pb. Govt. Press, Pat

FORM S. T VIII

RETURN OF SALES/PURCHASE TAX PAYABLE

(See Rule 20, 24, 25, 27, 29, 30, 40, 48 and 53)

For Office use or

Control Number

Dealer's Name.....

Address.....

Distt.	Ward	R.C. No.	Dealer Category	Return Field	M M Y
				M—Monthly Q—Quarterly Y—Yearly	

Under I.T. Act GIR/PN A/c. No.....Place and Circle of I.T. Assessment.....

SALES TAX

	Tax Free Goods	Goods Taxable at General	Schedule A Goods	Declared goods other Wheat than Wheat	Goods Taxable at 1st stage	Goods T Taxable at Special Rate
A. Sale Price received and receivable for goods sold or supplied during the return period.						2
B. Cash discount and trade discount allowed according to ordinary trade practice and included in the Sales prices but separately shown as such.						
C. Gross Turnover (A—B)						
D. (i) Turnover of Tax-Free goods, Section 3 (2) (a)(i)						
(ii) Turnover of goods sold to Registered dealer Section 5 (2) (a) (ii)						
(iii) Turnover of other exempted sales, Section 5 (2) (a) (iv), (v) and (vi)						
(iv) Turnover of goods exempted under section 5 (1—A)						
(v) Total of D (i), D (iii) and D (iv)						
E Balance [C—D (iv)]						
F. Deduction under section (5) (2) (b)						
G. Taxable Turnover (E—F)						
H. Amount of Tax payable on the Taxable turnover						

PURCHASE TAX

		Rupees
I.	Purchase price paid and payable for goods specified in Schedule C or for goods for purchase whereof Tax is payable under any provision of the Act.	.....
J.	(i) Cost of freight and delivery, if any, separately included in the purchase price.	.....
	(ii) Cash discount and trade discount according to ordinary trade practice and included in the purchase price.	.....
	(iii) Purchase price of goods purchased outside the State of Punjab or in the course of Inter-State trade or commerce or inpot out of territory of India.	.....
	(iv) (a) Purchase price of goods sold to Registered dealers	.....
	(b) Purchase price of goods sold in the course of Inter-State trade or commerce.	.....
	(c) Purchase price of goods sold in the course of export out of territory of India.	.....
	Total J (i) to J (iv)	.....
K.	Taxable turnover (I—J)	.....
L.	Amount of Tax payable on the Taxable turnover (K) at the prescribed tax rate (Calculated) to the nearest paisa.	.....

Total Tax payable Sales.....

Purchase..... Total AMOUNT.....

Refund Adjustment Order Book No. Voucher No. D D M M Y Y

	DDMMYY	AMOUNT.....

M. Tax paid under the Punjab General Sales Tax Act.

Treasury/Bank Name.....Dated.....Receipt No..... AMOUNT.....

M M Y Y

Tax paid under the Central Sales Tax Act AMOUNT.....

Bank Name.....Cheque/D.D. No.....Dated..... AMOUNT.....

DECLARATION

I hereby declare that the above statements are true and complete to the best of my knowledge and belief.

Name.....

Dated..... (Signature of Dealer)

"EXCISE AND TAXATION DEPARTMENT, PUNJAB

FORM ST-XXIV-A

(See Section 14-B)

Name of ICC _____ Code No. _____ Serial No. _____

Date _____ Time _____ Import/Export _____

DECLARATION

1. RC No. of the Consignor : _____
2. Name & complete Address of the Consignor : _____
3. RC No. of the Consignee : _____
4. Name & complete Address of the Consignee : _____
5. Description of goods : _____
6. Name & Address of the Transport Company : _____
7. GR/TR/Log Book/Trip Sheet No. _____ Date _____
8. Vehicle No. : _____
9. Name & Address of the owner or the person incharge of goods : _____
10. Bill/Delivery Note No _____ Date _____ Value of goods _____
11. Destination of goods _____

Signature of the Officer-incharge alongwith Signature Code No. & Stamp appended after the check

Signature or thumb impression of the person transporting the goods

"