Working Paper

PUBLIC-KEY CRYPTOSYSTEMS, TELESOFTWARE AND OTHER NOVEL APPLICATIONS OF VIDEOTEX

H.A. Maurer
I. Sebestyen

August 1982
WP-82-71

International Institute for Applied Systems Analysis
A-2361 Laxenburg, Austria

PUBLIC-KEY CRYPTOSYSTEMS, TELESOFTWARE AND OTHER NOVEL APPLICATIONS OF VIDEOTEX

H.A. Maurer
I. Sebestyen

August 1982
WP-82-71

INTERNATIONAL INSTITUTE FOR APPLIED SYSTEMS ANALYSIS
2361 Laxenburg, Austria

PREFACE

Telephone-based videotex systems are slowly changing from systems based on numeric, menu-type access methods that permit only information retrieval and limited message sending to more sophisticated, multiuser, interactive, transactional systems. This is partly due to the concept of adding external computers to the videotex network and partly due to the emergence of more intelligent terminals.

In this paper, some major application areas that have been made possible by these developments, but have not yet received the attention they merit, are discussed in some detail: teleplaying, telegambling, telesoftware, telecomputing, and public-key cryptosystems.

We maintain, and try to demonstrate, that these areas will significantly influence the market penetration and social impact of videotex. A number of the applications discussed will be available in Austria's videotex trial by September 82, making Austria the first country to offer such services on a nationwide videotex system.

CONTENTS

PUBLIC-KEY CRYPTOSYSTEMS, TELESOFTWARE AND OTHER NOVEL APPLICATIONS OF VIDEOTEX

H.A. Maurer
I. Sebestyen

1. INTRODUCTION

Telephone-based videotex systems, which we will simply call videotex systems, have only been in existence since the end of the seventies. (See Godfrey 1982, Woolfe 1980 and Maurer 1981 for general overviews.)

Originating with Prestel in the UK, videotex systems were conceived primarily as information retrieval systems capable of limited interactivity using very simple and cheap terminals. Now the character of videotex is changing due to several recent developments: the introduction of "external computers" available, for example, in Germany, providing whatever interactive options the information provider wishes to make; the arrival of more advanced terminals in Canada, the USA, and Austria; the introduction of alphabetic access techniques in French systems, etc.

Important for the success of videotex systems will be the scope of their application. The addition of external computers and intelligent terminals greatly broadens the range of applications. In fact, many potential and important applications have yet to be recognized.

In this paper we focus attention on some new applications that we feel will significantly influence the spread of videotex and its impact on society: teleplaying, telegambling, telesoftware, telecomputing, and--last but not least--public-key encryption systems which will be discussed in the last part of this paper.

Teleplaying refers to the fact that videotex allows the realization of complex multi-person games whose appeal may be comparable to that of TV shows. Telegambling refers to a special category of teleplaying. Telesoftware refers to the fact that a videotex system can be used to store programs that can be downloaded into the user's terminal and executed there, opening up the potential for a multitude of fascinating applications. Telecomputing refers to the fact that the gateway allows access to computational centers by videotex terminals. Public-key cryptosystems utilizing the "gateway" concept of linking external computers to videotex networks and the widespread use of intelligent videotex terminals--refer to the fact that videotex systems will be able to support secure and authorized communication, provide digital signatures, allow new potentials for novel forms of democracy and public voting, and provide innovative forms of network switching.

2. TELEPLAYING

In teleplaying, the external computer provides software for playing games with one, a few, or a very large number of participants. The significance of teleplaying lies in its social component and in the fact that it may help not only to strengthen existing personal ties but also to establish new contacts. As has been observed by Maurer (1981), the telephone network has not traditionally been an instrument for making acquaintances. The notion of multi-person telegames may change this. But before discussing such multi-person telegames, we will review briefly more traditional kinds of games made feasible by external computers in a videotex system.

An external computer can play the role of an opponent in most two-person card or board games, such as chess, go, superbrain, and so on. However, we do not feel that such applications will be very important as they are usually better handled by local microprocessors (in the user's home), either by loading them with suitable software from, say, a tape deck or (more to the point) from a videotex computer as telesoftware. (We will return to the latter point in section 4.) In passing we note that external computers cannot be used to play games of manual skill and reaction time as available in Penny Arcades (such as "Invaders," "Little-Brick-Out," etc.). The response times between the external computer and the communication network and the user are both too long and too unpredictable.

A kind of telegame for which we do feel external computers are useful is the one in which the computer does not act as player, but as administrator, referee, and provider of the tools necessary for the game. Suppose two persons in different locations want to play a game of chess. After having agreed on a starting time (using the videotex message service), they log into the same external computer via the videotex gateway and request the game chess. The computer displays a chess board with the initial configuration of pieces on both videotex terminals and proceeds to request moves in turn, checking them for legality and displaying the current situation on both screens at all times. A written conversation between game partners simultaneously with the game is possible. (As a matter of fact, such a version of tele-chess has been demonstrated successfully in Austria, where applicants of this nature are supported by

the fact that videotex is accessible Austria-wide for a charge of about US$ 1.80/hour, independent of the location of the participants.) Many other features will be available also: the computer will keep a record of how much time was required by each player; it could permit the game to be interrupted for as long as desired (for a dinner, or till next month); it could keep track of all moves, which would allow a re-play and analyses of the game after its termination.

Clearly, this kind of setup is not restricted to two-person games, but applies to all kinds of games, including card games. For example, in a game of bridge, the computer could deal the cards, keep score, even fill in for a missing fourth player, if necessary. Many features not available in ordinary bridge might be available in this version: the possibility of analyzing a hand after the game; the possibility to ask for an "extraordinary deal" (i.e., an unlikely distribution of cards); the possibility of dealing the same set of cards to various groups of people ("duplicate bridge" on a large scale, so to speak!), etc.

Certainly the variations will not be limited to currently available games. New games (some involving a very large number of participants) will emerge. There might be a simulated stock market game with an arbitrary number of participants who "buy" and "sell" stock, manipulate the "prices" of stock, perhaps even using real money; there may be "rallies" that start at a certain time, for which one has to pre-register and pay a registration fee, where one has to try to reach certain destinations (which can only be found by solving puzzles, answering questions, reacting in a certain way, and having a bit of luck) in order to obtain some prize, public recognition, or simply a particularly high score. The rally participant need not be one person, but could be a group of friends or a family unit, sitting around the same videotex terminal. This kind of joint, active participation contrasts favorably with the current passive and isolating TV-watching behavior that has greatly changed society over the last twenty years. The activities described may well help to dilute the activity- and communication-stifling influence of modern one-way media. We might see here one more instance of advanced technology helping to overcome negative side effects of some earlier technology.

Here we come to the point made earlier, that game and entertainment activities on external computers in videotex systems may help to establish contact and communication with persons with whom one would not have otherwise been involved, much in the same way as this happens over citizen band radio.

Let us consider some concrete examples of the type of situation we envisage. In a rally with many participants, the software may well provide players with knowledge about how other participants are doing and with possibilities for communicating with them, or even allowing them to join forces for part of the undertaking. On a simpler level, let us imagine a program that allows people to walk around in a maze, choosing a cover name, and meeting each other as they try to find an exit, a mystery place, treasure, etc. As they meet, they could exchange messages that, starting with greetings, information on the maze, and standard conversation, may lead to a

greeting on a rendezvous in the maze or might even lead to a get-together in real life. The possibilities are virtually limitless. A whole new entertainment and game industry based on videotex seems to us a possible prospect. The social impact of activities of the kind mentioned could be substantial. The success of shows allowing for broad public involvement seems to indicate that our vision of mass participation in an electronic mass game currently en vogue is not so very far-fetched.

3. TELEGAMBLING

Telegambling is a special class of telegambling. The appeal of gambling lies in the fact that the involvement of bets and money increases the excitement of gaming. Gambling is not new; it has existed throughout the history of mankind and will certainly continue to be with us.

Licensed "constitutionalized" forms of gambling can be found in practically all societies: "lotto", football-pool, state lottery, and racing are extremely popular in the UK, France, Germany, Austria, Hungary, Italy, Czechoslovakia, and many other countries.

In many countries gambling has become a huge industry. For example, in 1979, gambling casinos in the UK had a revenue of US$ 280 million. And this amount shows an annual growth of 10.2% (Predicast World Cast P-1 1981). Similarly, the gambling industries in Las Vegas and Monte Carlo cannot complain about low earnings.

According to the Encyclopaedia Brittanica, it has been estimated that during the 1960s the total amount bet in gambling games in the United States alone approximated US$ 50 billion (!) each year; that in England 48% of the adult population risked some money by gambling; and that throughout the world the amounts risked annually approached 6.66% of personal income.

By comparison, only about 5% of personal income is spent on information (newspapers, TV and radio license fees, books, etc.). In fact, it is this portion of income that is expected to be redistributed through videotex services.

This introduction to gambling was needed in order to point out that whenever new opportunities for nationwide or local gambling arise, there are strong financial interests on the parts of most governments and some enterprises to enter this business and make as much money as possible. New information technologies such as videotex offer not only excellent opportunities in information retrieval, electronic fund transfer, electronic mail, teleplaying, etc. They can be "used" or "misused" for telegambling as well.

Let us examine as one theoretical example football-pool. Football-pool is a traditional nationwide gambling game. For example, the Austrian newspaper Kurier reported in its issue of November 14, 1981 about a "Toto" boom in Austria (population 7.5 million) whereby Austrian pool players placed bets amounting to AS 20 million (US$ 1,3 million) for a single weekend. Another example: in Hungary, several hundred thousand football pool coupons are sold every week. The weekly pool guide "Turf" containing competitors' hints and a broad variety of football statistics is one of the country's best selling weekly papers.

In a likely videotex version of football-pool, players would place their bets into the videotex system by filling in an appropriate response frame. The access fee for the response frame would be equal to the price of one football-pool coupon. Should the player require background information in order to determine the wisest selections, the "electronic" (videotex) version of the pool's guide could be accessed to retrieve the necessary information, such as statistics or time series of previous games. Bets could be placed until the first football match contained in the pools begins. If a player wins, his prize could be transferred to his bank account by the electronic fund transfer service of videotex.

The list of gambling games that could be played on videotex is practically endless. Many questions remain open, however, such as whether or not telegambling is desirable from a societal viewpoint.

Let us assume that it is. In this case, what kind of data security measures would have to be taken in order to assure that, for example, children do not get access to the system even if they should get hold of their parent's user name and password? Or what should happen if an adult is addicted to gambling and does not care whether he loses his monthly salary within a few hours...?

And last but not least, there is another important aspect of telegaming and telegambling. The social role of gaming and gambling is not and should not be primarily to win or make money. The more important role of these activities is to bring people together while entertaining them and thereby to provide the precondition for establishing human contacts; for creating opportunities for serious and less serious chats, talks, and discussions; for making new friendships and maintaining old ones, or for simply getting away from the daily rut. Whether or not the interactive capability of videotex is adequate for these purposes has yet to be proved.

4. TELESOFTWARE

External computers are extensions of basic videotex at the information providers' end. It is also possible (the first implementation was Austria's MUPID-system, cf. Maurer 1982a and 1982b) to extend videotex at the users' end by providing intelligent terminals, i.e., terminals that can execute stored programs. The programs to be executed may have been created by the users, may have been loaded from a local external storage medium (like a tape deck) or may have been loaded from the videotex system. Such software, stored in the videotex system and "downloaded" similar to ordinary data but executed in the videotex terminal, is called telesoftware.

It is our contention that telesoftware is a viable alternative to program storage and distribution and that it will have a major influence on the spread of videotex penetration. Before we discuss the typical telesoftware that might be made available in the future, a number of technical and economical facts should be brought to mind.

Intelligent videotex decoders capable of handling telesoftware are now entering the market (Maurer 1982a) for about US$ 500. Compared with the price of other electronic and media equipment competing for the same segment of households' budgets, this should be sufficiently

low to allow significant market penetration. In addition to the cost factor, two other obstacles have been responsible for the lack of decisive progress in the area of telesoftware. One is the question of programming language: since there is no universally accepted programming language for microprocessors, severe compatibility problems arise. (Note that even the use of a more or less standard language such as Mini Basic does not really solve the problem, since the non-standard input/output and graphics commands block cross-micro compatibility.)

It is quite possible that the existence of various "dialects" of a programming language will impose an additional burden on intelligent terminals. In that sense, countries where videotex developments are controlled centrally (such as France and Austria) are most likely to be able to overcome compatibility problems.

The second obstacle is transmission speed. Due to the essential need to check for transmission errors when loading executable programs, the down-loading of a substantial program may require up to three minutes. A number of techniques for reducing the required transmission time are emerging, the most noteworthy of which are ideas for initiating program execution before the program is fully loaded and for separating text (such as in explanations and error messages) from the program itself, retrieving it from the videotex system only when needed. Thus despite the obstacles presented by terminal price, the need to standardize programming languages, and the need to shorten loading times, it is foreseeable that telesoftware will become a workable option.

The appeal of telesoftware and its underlying concept lies in the fact that a user, without requiring any external storage device at home (likely to develop occasional mechanical problems), nevertheless has access to virtually unlimited random access storage within the videotex system: user programs, user data, and programs and data from other sources are all available within the system. Indeed, videotex may offer an optimal means of distributing software to the residential and small business market. New software releases could replace obsolete ones without the user even noticing.

Many of the game applications mentioned in Section 2 under teleplaying (on an external computer) could also apply to the local computer, i.e., the intelligent terminal, if it is down-loaded with the appropriate software.

Indeed, the intelligent terminal is a better solution in a number of instances. This is true first of all of the Penny Arcade variety of games of skill, which cannot be realized with external computers as explained earlier. We believe that even multi-person games of skill requiring half a dozen or so game controls can be implemented using telesoftware and have substantial relaxation and entertainment value, something that has been overlooked so far. Secondly, it is true for those games in which one person plays against the computer. The down-loading of a chess program with its subsequent execution, independent of the videotex network is more reasonable than tying up the computing power of an external computer and requiring an open telephone line and port all the time.

Even games involving a number of people at different locations can often be accomplished using intelligent terminals rather than an external computer, even if no messaging is supported.

Thus, much of what has been described under teleplaying on external computers applies to intelligent videotex terminals, also.

Telesoftware will also include programs for "home economics" such as mortgage and installment payments, and income tax calculations; a package to evaluate a portfolio of stock; or a program simulating a very sophisticated desk-top calculator; software for creative tasks like composing music, which can be played using an attachment to the intelligent terminal, etc.

A number of applications will use the videotex system "in the background" in an essential way: after a picture has been composed as mentioned above it might be stored in vidoetex and a request could be sent to a company to produce a slide, print, or poster from the frame deposited; or after having edited an address-file it might be sent off to some firm to prepare address labels; or after having edited a letter it might be sent off to an appropriate institution to print it and mail it to the designated address(es). (This possibility will be provided in Austria's videotex by December 82.)

Assuming that the intelligent terminal is sufficiently well equipped, just about any software now available for commercial purposes may be made available via videotex as telesoftware. Even if terminals end up with a disc drive attached to them, the most elegant way to rewrite a floppy disc with a piece of systems software may be to load it from videotex rather than copy it from a master diskette (which would no longer be needed).

Among the telesoftware available on an intelligent videotex terminal will be some that will make the use of the videotex system more convenient. Typical possibilities include software for marking frames for convenient later recall, for performing alphabetic searches based on a numeric menu-type index, for automatic polling of certain frames (e.g., to collect statistical data or to evaluate response frames), and, of course, for editing videotex pages. Although intelligent terminals will not allow all of the complex possibilities found in dedicated information provider systems a reasonable amount of frame preparation and editing will be possible as demonstrated, for example, by MUPID (Maurer 1982a and 1982b).

Intelligent terminals may also be programmable by the user. In this case telesoftware could include language systems, compilers, and supervisory systems to allow the user to work with a wide choice of languages and software systems. Again, MUPID is an example of this concept.

5. TELECOMPUTING

Looking from the broader viewpoint of information technology, telesoftware is merely the transfer of data files containing "source" or "machine" computer programs from a videotex computer to the personal computers of end users. If, however, one regards videotex

technology as the "cheap computer network for the man on the street," one should also consider other videotex application classes supporting computation in general. An external computer with a high computational capability linked by the "gateway" concept to the videotex network could perform time sharing or batch computations for users with simple modified TV sets using an extended alphanumerical keypad/board or for users whose own personal computers are connected to the videotex network. In the latter case, only those computations that cannot be performed locally would be carried out by the external computer by utilizing its bigger core and secondary storage capacity. Also in applications requiring some sort of special hardware or output device, based on the resource-sharing principle, external computers with appropriate peripherals would also be accessed. For example, a special high quality laser printer could be used to print text demanding high quality printing.

External computers could also be used for storing and maintaining "telesoftware". Thus, if one type of personal computer connected to the videotex network cannot understand the programming language "dialect" of a particular type of telesoftware stored on the system, an appropriate "precompiler" run on an external computer could modify the telesoftware into the programming language "dialect" required.

The key to the success of telecomputing is user-friendliness. In order to reach the mass market in supporting computing and calculation the software of the dedicated external computers has to be extremely user-friendly. An important step towards improving the user-friendliness of computing has been made with the introduction of personal computers into the mass market. Many of the programs available on "Apples," "Oranges," and "Grapes" perfectly satisfy the above requirement. Before introducing a large computational center attached to a videotex network, the lessons learned in the field of personal computer applications should be closely looked at and considered.

6. PUBLIC-KEY CRYPTOSYSTEMS

From the technical point of view videotex applications using public-key cryptosystems were made possible by the introduction of intelligent videotex terminals, the use of telesoftware, the videotex message sending service, and in some applications the videotex gateway.

The reason why we are interested in cryptography, and especially public-key cryptosystems, is that this technique--if linked to a public videotex system equipped with gateway and intelligent videotex decoders--could provide many services that will be needed in a future information society.

The basic--revolutionary--principle and mathematics of public-key cryptosystems have described in an extensive way throughout the literature (see references at the end of this paper).

Public-key cryptography is based on Whifield Deffie and Martin Hellmann's (both from Stanford University) suggestion to break with traditional schemes of using the same encryption/decryption key for

coding and decoding of secret messages. They suggested using different keys for the encoding and decoding processes, so that it would be possible to reveal the encryption key publicly while still keeping the appropriate decryption key secret. In this way, secure one-way communication could be established, anyone could create and send a secret message to the owner of the decryption key without having to fear that his message could be decrypted by anybody else than the owner of the decryption key. In order to have two-way (person to person) communication each person participating in the public-key system must possess and keep his own individual, secret decryption key while announcing publicly his encryption key--which is to be used by the rest of the community when secret messages are to be addressed and sent to him. The usefulness of linking public-key cryptography to videotex, from the technical point of view, should already be obvious: (1) the encryption keys of users for public access can ideally put on public videotex information frames as a "public-key directory", whereas decryption keys have to be kept secretly at the videotex user's location. (2) The message sending capability of videotex can be ideally used for sending the coded messages. (3) The telesoftware programs needed for encryption and decryption of messages are to be stored as information frames on the videotex system as well and are to be downloaded into the intelligent videotex terminal for execution when messages are to be encoded or decoded. (4) Certain administrative types of functions, such as administration of keys, keeping track of transactions, etc., can also be solved with relative ease by videotex networks.

The fact that public-key cryptosystems with the novel property of publicly revealing an encryption key--in our case on videotex--do not thereby reveal the corresponding decryption key has some important consequences:

(1) Couriers or other secure means are not needed to transmit keys, since a message can be encrypted using an encryption key--earlier publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

Because of this, for the distribution of encryption keys an "insecure" channel, such as a videotex database (the "public-key directory"), is ideal. Nonetheless, privacy of messages can still be guaranteed since a potential "wiretapper" who gets hold of the transmitted encrypted message sees only "garbage" (the ciphertext) which makes no sense to him since he does not know how to decrypt it.

(2) As a special use of public-key systems, a message can be "signed" using the privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key in the "public-key directory" of videotex. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications such as in "electronic mail", "electronic funds transfer", "electronic voting", or "electronic contracts".

If electronic message sending and transaction systems based on videotex are partly to replace the existing paper mail and other transaction systems, "signing" and electronic message is fundamental and must be possible.

An electronic signature must be message-dependent, as well as signer-dependent. Otherwise the recipient could modify the message before showing the message-signature pair to a judge. Or he could attach the signature to any message whatsoever, since it is impossible to detect electronic "cutting and pasting".

These conditions can be fulfilled by a public key cryptosystem. When sending a signed message the sender uses his own decryption key (only known to him) to "compute" his "signature". This is nothing more than using his decryption key now as an encryption key for the message to be signed. This coded message can be "decrypted" by the recipient by using as decryption key the public-key of the sender found in the "public-key directory" of the videotex system, which is moreover--as we have seen above--also used when encoded messages are sent to him. If the decoded message is meaningful, then the recipient of the message has the proof that it originated from the sender.

"Signed" messages can obviously also be sent "secretly" from sender to recipient, if the sender encodes his "signed" message (through his own decryption key) according to the public key of the recipient looked up in the videotex "public-key directory". Such a message transmitted by the message sending service of videotex can as we have seen above only be decoded by the addressee.

To enable public-key systems to be used for signature, it has to be ensured that the encryption/decryption key pairs used allow subsequent coding and encoding (or vice versa) of each message without changing the original context of the message. According to the literature referred to at the end of this paper, such key pairs exist in principle and can be created by using various techniques.

We believe public-key cryptosystems can be widely used in videotex networks for a number of novel applications; in what follows we only mention a few of them.

(1) "Value added" message service and transaction service

As an example, to bill a customer for goods he ordered--in a way that would be acceptable to a court--could not be done by a videotex system equipped with standard message sending capability, because (to list a few, but not all arguments):

- -- there would be no guarantee that the message (the bill in the above case) had been transmitted through the videotex network without distortion
- -- there would be no real proof of the originator of the message (bill)
- -- there would be no real guarantee that the message was not changed (deleted, added, etc.) by a third party
- -- there is no proof that the message was really received by recipient (customer) who was addressed (acknowledgment)
- -- there would be no "track" (record) in the system that the message, in our case bill, was sent from the department store to the customer
- -- it would be possible to store copies of the bill both at the department store's computer and the user's site in a "low court ready" format and manner, which would be adequate for documentation storage and retrieval

-- there would be no guarantee that the bill would not be read by someone who was not supposed to see it.

With a public-key cryptosystem applied to the nationwide videotex network, that we are proposing, all these conditions could be easily fulfilled, and through this much of the role of paper in the present society could be transferred to an electronic videotex based medium.

(2) Teledemocracy, electronic voting

Teledemocracy and political power exercised through computers and computer networks are the fears most often heard, expressed, and read in the literature. Technically it is easily feasible to build, for example, a nationwide "political forum" through videotex where everybody could express publicly his own views without the fear of being found out in a reasonable time. Furthermore it would also be technically feasible to design and implement a system where citizens could denounce each other to a special authority without the fear that any other citizen may "wiretap" or detect it. (We leave the judgment of the necessity for such systems to readers....) Or in another application members of groups or parties could provide statement forums for themselves with the security that non-members of the community could not "wiretap" the communication.

Direct voting by citizens--another much discussed and controversial topic--could also be easily implemented through an appropriate public-key cryptosystem based on videotex. By this manner citizens with voting rights--and only those--could vote almost instantaneously on any matter that arose, could send their votes safely to a central voting register without having to fear that their votes could be "seen" by those who are not supposed to. On the other side, the "voting authorities" could be sure, that all voters only vote once, the authority of the voters is perfectly secured, and a guarantee could be provided that the vote was not altered by a third party. Furthermore--after closing the voting--final results could be produced almost instantaneously and put on display to the public, e.g., to be followed soon by a full analysis of the results (e.g., voting distribution by age, sex, occupation, geographical location).

(3) Network switching

According to Gordon B. Thompson, one of the most important applications of public-key systems is communication switching. In this sense, information is put in a "shared information space"--such as a cable, or in the case of videotex on information frames accessible for all users.

Using a public-key system, however, it can be controlled--i.e., "switched"--to decide who should be able to receive the information and who not. Using these techniques the concept of Closed User Groups can be implemented in a novel way--e.g., all "dog lovers" would get the very same encryption--decryption keys. Obviously individual communication is also possible using this technique: in this case everybody must receive his own decryption key and all encryption keys must be publicly announced.

We must point out that there is basic difference between this concept and the standard videotex message sending mechanism, which is

based on the mailbox principle where all users have their own mailboxes, where messages designated to them are sent to, and where the messages have to be taken from by the recipient. Here, instead of using mailboxes all messages are put on a common "message board". However, since the messages are encoded by the public-key systems, although all encoded messages are accessible to every one in principle, they can only be decrypted and understood by the owner of the decryption key. The advantage of this technique is obvious for all "multiaddressee" messages (group messages), which have to be stored only once. If "mailboxes" are used any group message has to be put in each of the group member's mailboxes.

As can be seen from the above examples, we believe that public-key cryptosystems would enable many of the present "ground rules" of our society on how to create, handle, transmit and store documents, messages, contracts, etc. to be transferred from the "medium" paper to an appropriate, new electronic medium based on videotex. In addition, it would most likely provide a new basis for the creation and addition of new "ground rules" never exercised before.

7. CONCLUSION

In this paper we have argued that future videotex systems will differ significantly from the original numeric menu-driven information retrieval and response-page-only systems. They will include much local processing due to the use of intelligent terminals such as MUPID.

Those additional facilities will not only provide some of the standard services often mentioned in the literature (like direct booking, money transfer and enhanced graphics) but will also provide a spectrum of other possibilities which has not received much attention. Particular areas we have focused on are the areas of teleplaying, telesoftware, telecomputing, and use of public-key cryptosystems, all of which we believe will have a substantial impact both concerning penetration and societal impact of videotex.

We have not considered in depth the legal problems that may arise in connection with some of the more unorthodox applications: some of the multi-person telegames involving the possibility of winning prizes may conflict with games-of-luck laws in some countries and there might be numerous legal problems around telegambling; the message sending aspect emerging in many situations may violate some postal-laws, etc. Concerning such potential legal restrictions we consider it natural that, videotex being a new and unforeseen development, a number of laws may have to be modified to permit reasonable and useful applications of videotex.

REFERENCES

Godfrey, D., E. Chang, 1982. The Telidon Book. Porcepic Press, Toronot.

Maurer, H.A., 1981. Bildschirmtextaehnliche Systeme. Study prepared for the Austrian Federal Ministry for Science and Research.

Maurer, H.A., W. Rauch, I. Sebestyen, 1981. Videotex Message Service Systems. Electronic Publishing Review, Vol. I, No. 4, 267-295.

Maurer, H.A., 1982a. Will MUPID Revolutionize Austria's Videotex? Videotex 82: Proceedings of Conference, New York, June 28-30, 82.

Maurer, H.A., R. Posch, 1982b. MUPID - An Austrian Contribution to Videotex. Report F 87, Institute for Information Processing (IIG) Graz, Austria.

Predicast World Cast P-1, 1981. Issue 62. Reference Made to Financial E. 5/8/80. Ohio, USA: Predicast Inc., May 29.

Rivest, R.L., A. Shamir, L. Adleman, 1978. A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communication of the ACM, Vol. 21, No. 2, 120-126, February 1978, USA.

Ryska, N., S. Herda, 1980. Kryptographische Verfahren in der Datenverarbeitung, Informatik - Fachberichte, Vol. 24. Springer - Verlag, Berlin, Heidelberg, New York.

Thompson, G.B., 1982. Personal Communication, Ottawa, Canada.

Willet, M., 1982. A Tutorial on Public-key Cryptography, Computers & Security, Vol. 1, 72-79. North Holland Publishing Company, Amsterdam, Holland.

Woolfe, R., 1980. Videotex - The New Television/Telephone Information Services. Heyden & Sons Ltd., London, UK.