PUBLIC VIDEOTEX: A DEMOCRATIC USE OF NEW TECHNOLOGY

I. Sebestyen
International Institute for Applied Systems Analysis, Laxenburg, Austria

M. Nimetz
Paul, Weiss, Rifkind, Wharton & Garrison, New York, USA

RR-83-32
December 1983

Reprinted from *Computerworld*, October (1983)

INTERNATIONAL INSTITUTE FOR APPLIED SYSTEMS ANALYSIS
Laxenburg, Austria

Research Reports, which record research conducted at IIASA, are independently reviewed before publication. However, the views and opinions they express are not necessarily those of the Institute or the National Member Organizations that support it.

Printed by Novographic, Vienna, Austria

FOREWORD

This Research Report focuses on selected potential impacts of new information and telecommunications technologies on the political life of society. Issues of this kind were addressed in the framework of the Information Technology Task of IIASA's former Management and Technology Area in 1981 through early 1983.

The article, published by *Computerworld* in October 1983, is actually the result of an experiment. One of the authors, Dr. Matthew Nimetz was, as Under-Secretary of State, one of the leading political figures involved in formulating the information policy in the United States.

The other author, Dr. Istvan Sebestyen, Research Scholar at IIASA and presently Visiting Professor at the Technical University of Graz, is primarily interested in the technological aspects of new information and telecommunications technologies.

In this report the authors address, in an interdisciplinary way, a special application of new generation videotex systems and how this new technology could be used for expressing public opinion. Their intention is to draw attention to an issue which might be one of the cornerpoints of a future "information society".

TIBOR VASKO
Leader
Clearinghouse Activities

Public Videotex

A Democratic Use Of New Technology

By Istvan Sebestyen
and Matthew Nimetz

For a democratic society to exercise the will of the people, it must be governed by the citizenry. It is essential that the flow of information between those who govern and those who are governed is secured. While it is assured that certain groups with a common interest (political bodies, churches, associations and so on) can make their voice heard through the mass media, it is still relatively difficult for the individual citizen to contribute on a regular basis to the flow of information between rulers and ruled, except for a "yes" or "no" every two, four or five years at election time.

Consideration should be given to introducing a system that gives due weight to the voice of the individual in a constant manner as policy is formulated and implemented by government. We believe that information and telecommunications technologies, such as the new generation of videotex systems, will soon provide valuable tools for expressing public opinion. At present, systems with such applications do not exist on any national level, except experimentally. But not much imagination is needed to foresee that within the next few years, such systems could be built and introduced on a wide basis.

It is because of this potential that engineers, media experts, industry representatives and other groups should join with politicians and legal experts to discuss and predict what this type of system could mean for society. With this article, we try to take the first step in that direction.

In order that we keep in touch with reality, the focus of our investigation will be special applications

—The Basic Forms of Videotex Systems—

One-way videotex broadcasts in a cyclical manner the data frames stored on a central computer. In the medium called teletext, either the vertical blanking intervals of traditional TV programs are used or dedicated separate channels, such as TV cable channels.

Different types of videotex decoders are used as teletext terminals. The decoder is usually built into the TV set, and a person uses a numerical key pad to select information frames (maximum 1,000 characters per frame) to be picked out from the information cycle by the decoder and displayed on an ordinary TV. Since the amount of information on teletext is limited to only a few hundred frames, not much local intelligence is built into the standard teletext decoders.

Such systems are already widely used. Teletext users in Austria already number approximately 130,000. In our view, the medium's strongest application is linked to normal TV programs, such as subtitling or information for the hearing impaired.

The amount of information cycled on full-channel teletext systems is considerably larger, up to about 50,000 frames, a considerable amount of data. Thus, in such cases, intelligent videotex decoders (basically dedicated personal computers) have to be used to utilize the data presented in the most appropriate way.

Interactive Versions

Two-way videotex systems — often called viewdata in Europe — are also built on computers storing data frames, similar to the one-way videotex systems, except that communication between the system and the user is based on interactive (individual) communication as opposed to teletext's broadcast communication.

The telecommunications medium used for interactive communications is the traditional telephone network, the emerging data networks and the upcoming two-way cable networks. Two-way videotex systems have advantages over one-way systems for certain applications, such as individual message sending, booking and transactions. In the future, one-way and two-way systems are likely to converge so that they supplement each other rather than compete.

At present, different types of two-way videotex systems are in use. The earliest type of videotex systems, such as the British Prestel, use modified TV sets with built-in videotex decoders as user terminals. They are equipped with numerical key pads allowing the user to search for any frame in the Prestel "information tree" by numbers.

The standard public-switched telephone network is used as the telecommunications medium between the videotex information center and the user through a serial interface in the TV set and a low-speed asynchronous modem.

of the new-generation videotex systems that support public opinion expression, such as an electronic "speakers corner," "notary public," "ombudsman" and electronic polling and voting. By "new-generation videotex systems," we mean a nationwide public system, such as will be introduced in the Federal Republic of Germany and Austria in 1984. These systems will be equipped with intelligent videotex decoders, such as the Austrian Mupid, which is already on trial in Austria, the Federal Republic of Germany, the UK and elsewhere. Mupid is rented from the Austrian postal, telephone and telegraph authority (PTT) for about $5 per month.

In our context, public videotex systems are really nothing more than an inexpensive — preferably packet-switched — computer network allowing mass computer networking applications for daily life. Uses include various information retrieval and transaction functions: flight schedules and reservations and, perhaps, payment, through a cheap home terminal. Such terminals may use the home TV set as an output device, combined with a cheap dedicated intelligent videotex decoder (basically a dedicated personal computer) and linked to suitable telecommunications channels — a telephone in most cases.

The intelligent videotex decoder allows for all the above components to be combined into an intelligent home terminal of a sophisticated but inexpensive computer network and, in addition, functions as a standalone personal computer.

Public-key cryptosystems and videotex. Videotex and public-key cryptosystems are relatively new concepts that emerged during the late 1970s (for a basic explanation, see In Depth/23).

New-generation videotex systems use alphanumeric keyboards and intelligent videotex decoders (basically dedicated personal computers, such as Mupid), which extend the original functions of videotex user terminals tremendously. Not only can information frames be retrieved and simple transactions (such as booking) be performed, but telesoftware frames (special information frames) can also be downloaded into the local processor of the intelligent decoder and executed. Through this philosophical change in the use of videotex, a whole new range of applications has been created.

One example of such a new application is the public-key cryptosystems, to be implemented on videotex by means of intelligent videotex decoders. Thus, from the technical point of view, videotex applications using public-key cryptosystems are made possible by the introduction of intelligent videotex terminals, the use of telesoftware, the standard videotex message-sending service and, in some applications, the use of a videotex gateway, which is really nothing more than a link between a specially programmed third-party computer, such as a bank computer, and the basic videotex computer network. Through this gateway, videotex users can access these third-party computers for special videotex applications, such as home banking.

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

propriate decryption key secret (Figure 1).

In this way, secure one-way communications could be established. Anyone could create and send a secret message to the owner of the decryption key (secret key) without having to fear that his message could be decrypted by anyone else but the

Corresponding encryption/decryption key pairs should have the following properties:

1. Ds(Ep(M))=M — Encrypting (E) of message 'M' with public key 'p,' then transmitting and decrypting (D) with secret key 's' should result in the original message. This is essential for secure messaging.

2. Dp(Es(M))=M — Encrypting the message with secret key 's,' then transmitting and decrypting with the public key 'p' should result also in the original message. This is essential for authentication.

3. Publicly revealing encryption and decryption procedures and the so-called public keys does not allow individuals to find out easily the secret key of a particular user of the system. This is needed for secure messaging and authentication.

4. Public and secret key pairs should be easy to generate.

Figure 1

owner of the secret key. In order to have two-way (person-to-person) communications, everyone participating in the public-key system must possess and keep his individual, secret decryption key while announcing publicly his encryption key. That encryption key is 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 points of view, should already be obvious:

1. The encryption keys (public keys) of users for public access can ideally be 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 telecommunications software 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 and keeping track of transactions, can also be solved with relative ease by videotex networks.

The reason 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 basic services

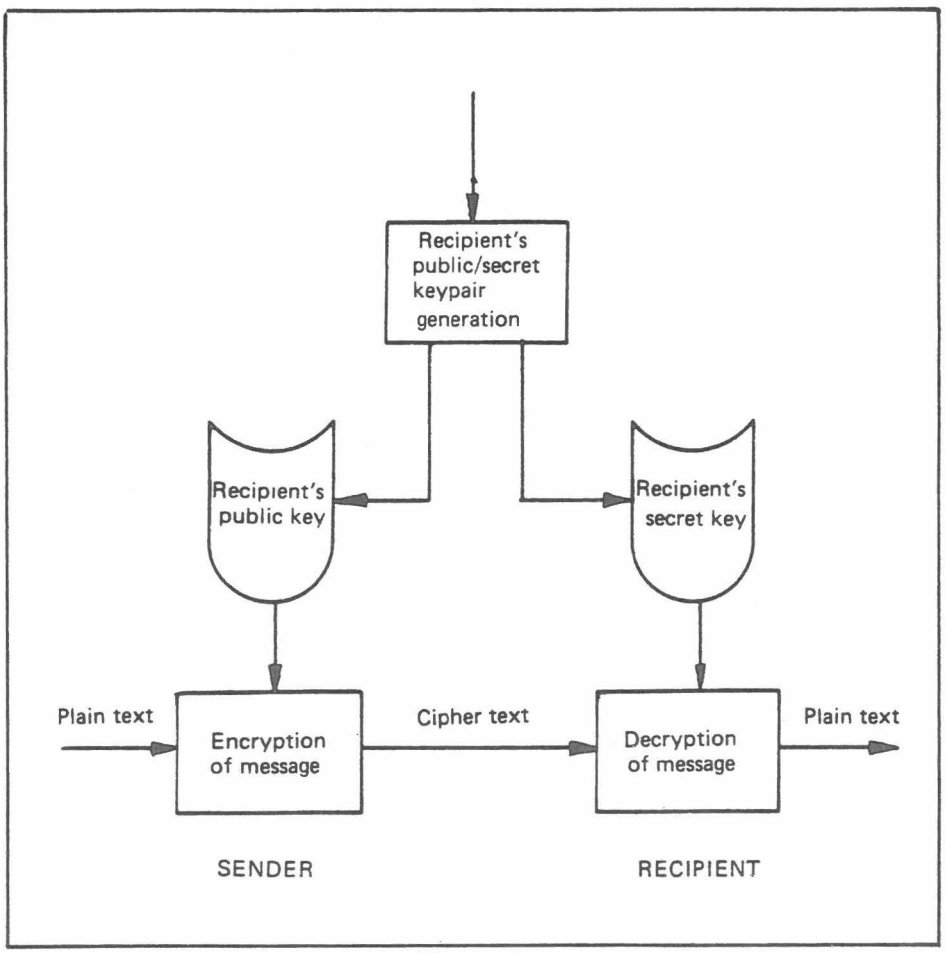

Figure 2a

that will be needed in a future information society.

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, which should be spelled out separately:

1. Couriers or other secure means are not needed to transmit keys, since a message can be encrypted using an encryption key that was publicly revealed earlier by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key (see Figure 2a on In Depth/ 24).

Thus, for the distribution of encryption keys, an "insecure" channel, such as a

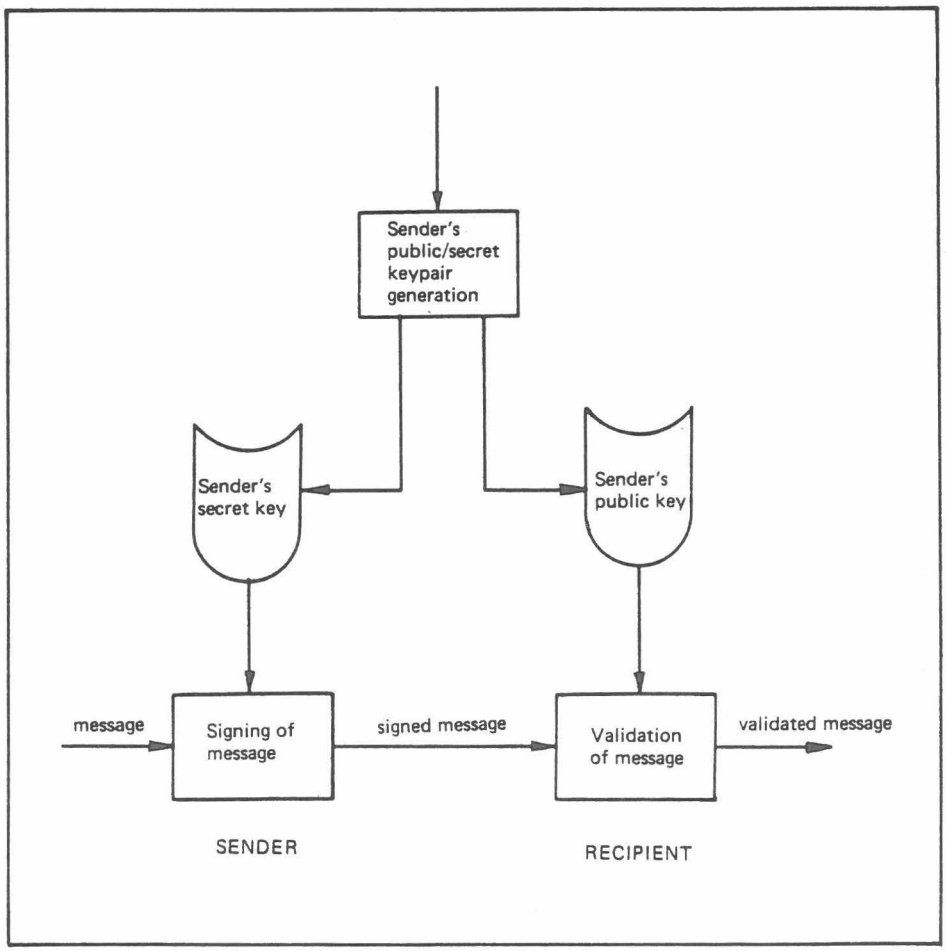

Figure 2b

videotex data base (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 only sees "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 secret key. Anyone can verify this signature using the corresponding publicly revealed key in the "public-key directory" of videotex. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This feature has obvious applications in electronic mail, electronic funds transfer, electronic voting or "electronic contracts" (Figure 2b). If electronic message sending and transaction systems based on videotex are partly to replace the existing paper mail and other transaction systems, "signing" an 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 secret key (known only to him) to "compute" his "signature." This coded message can be decrypted by the recipient by using as a decryption key the public key of the sender found in the "public-key directory," which is, 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.

3. "Signed" messages can obviously also be sent "secretly" from sender to recipient, if the sender encodes his "signed" message (through his own secret key) according to the public key of the recipient looked up in the videotex public-key directory (Figure 2c). 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.

We believe that public-key cryptosystems can be widely used in videotex networks for a number of novel applications. In what follows, we only mention a few possibilities, some of which are linked with the expression of individuals in public opinion.

Public opinion expression. An "electronic speakers corner" can easily be implemented, even on most of the present, first-generation videotex systems. A prerequisite is to appoint or accept a special information provider who is willing to function as an electronic speakers corner. Anyone who then wants his voice to be heard can send his message to the information provider through the message-sending (note: only with full alphabetical keyboard) service of videotex or through the response frame capability of the videotex textframes.

It is then the function of the speakers corner to put the received message on his information frames. The question of what or what not to put up — thus to exercise a kind of

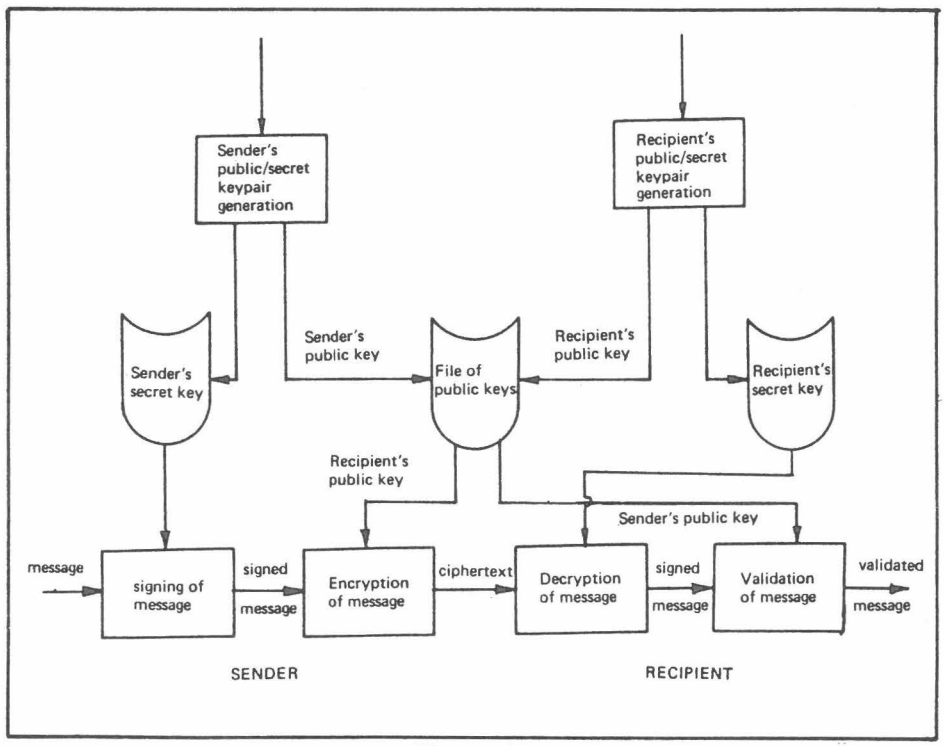

Figure 2c

censorship function — is a key issue on how the electronic speakers corner would function. (At this point, it should be mentioned that by accepted convention at Speakers Corner in Hyde Park in London, the Queen and the Royal family, for example, may not be abused.)

Information frames on public opinion could be kept on the system for a designated time period. Some information frames could also be supplemented by response frames to ask for public reaction to a specific issue. For example, a citizen claiming there is a need to build a road that bypasses his village could seek support for his appeal from fellow villagers through the response frames.

The speakers corner would, of course, cost money to operate. To cover expenses, the operator of the videotex services — for example, the PTT — might be required by law to provide the electronic speakers corner service. In a similar situation, cable TV operators in the U.S. are often required as a condition of their franchise to offer the public citizen channel free of charge. The amount, frequency and type of information for which citizens might use this free videotex information channel would need to be clearly established by law or regulation.

Electronic voting. A simple type of electronic voting and public opinion polling is also possible on existing first-generation videotex systems with or without a full alphabetic keyboard. The information provider performing the public opinion polling or voting could put up question-

naire-type response frames on the system. Subscribers looking up the frames of this special information provider could then fill in and send back the appropriate response frames.

If the information provider had an intelligent videotex terminal, such as Mupid, he could then process the collected response frames, for example, to produce integrated final statistics to show polling and voting results. This technique may not, however, be sufficient under all conditions. Polling and voting through response frames is linked to a specific user identification and password, but not to individual people. For example, the International Institute for Applied Systems Analysis is listed as one subscriber on the Austrian videotex system. It would be a similar case with a family, where in Europe the head of the family is usually by law the subscriber.

The videotex system therefore can only distinguish a particular subscriber and not the individual users working under that subscriber identification. For this reason, no guarantee is provided by the system, for example, to identify whether a new car that was ordered through videotex was ordered by the father who really wants a new car or by his children who just thought it would be nice to own.

The same is true, of course, for public polling or voting, when individual family members may have different opinions and certainly have separate votes. In order to gain further identification, then, usually one of the questions asked on a response frame is the name of the person filling it in. There is, however, no way for the system to check whether this type of identification is authentic, and in many applications, especially voting, authentication is essential. As already mentioned, one way to solve the authentication problem is by public-key cryptosystems.

Secret message sending is also often a required need for certain transactions — for example, the message between a customer and his bank. For this reason, even though any traditional computer transaction system or videotex provides a certain degree of data security, additional measures to increase the level of security — for example, through cryptography — are always welcome. To introduce cryptography on videotex systems through public-key cryptosystems is one potential way, especially if intelligent videotex decoders, such as Mupid, are used.

In many cases, both authentication and secrecy are required. In the case of voting, the vote has to be authentic. There must be assurance that the vote has come from the person to whom it was ascribed and that it is a valid vote (that is, that the vote has been placed only once and not later or earlier than it should have been).

The content of the vote, however, should remain hidden from the authentication-checking process. Nobody else should know or be able to find out, for example, whether Franz Joseph Strauss voted for the SPD (it is purely his private affair). Also, at the second stage, when the content of all votes are revealed and the valid votes are added up, again no one should be able to recognize that a given "yes" for the SPD actually came from Franz Joseph Strauss.

In principle, all these requirements can be implemented using public-key cryptosystems. How these basic functions can be implemented on videotex is shown in Figures 3, 4 and 5. Text editing, encryption and description of messages are performed locally by intelligent videotex decoders. The programs and en-

cryption keys needed are downloaded from the videotex system.

In the figures, we show the videotex public-key directory and the videotex telesoftware file separately for better understanding, but these are stored on standard information frames. Messages are sent to the receivers' mailboxes in a store-and-forward manner through the standard message-sending function of videotex. Actually, the following applications are built on the basic functions shown in Figures 3 through 5.

In this whole process, there are a few critical technical points that have yet to be solved properly. One problem is the distribution of the secret private keys. First, appropriate key pairs have to be generated, preferably by the key administrator. This function could best be accomplished on a dedicated third-party computer linked to the videotex network. The public keys can be put on the videotex system in a public file by the key administrator. The secret key then has to be forwarded to the subscriber who wants to receive crypted messages or send authenticated messages.

The problem here is that if sent through the "insecure" videotex message channels, this information, in principle, could be wiretapped by a third party. One possibility would be to pick up the private key in person from the key administrator. This option is certainly secure, but then one particular beauty of the public-key system, the flexible change of crypto-keys, is lost. Another possibility would be to pick up in person a crypto-key that is only used for the distribution of keys between admin-

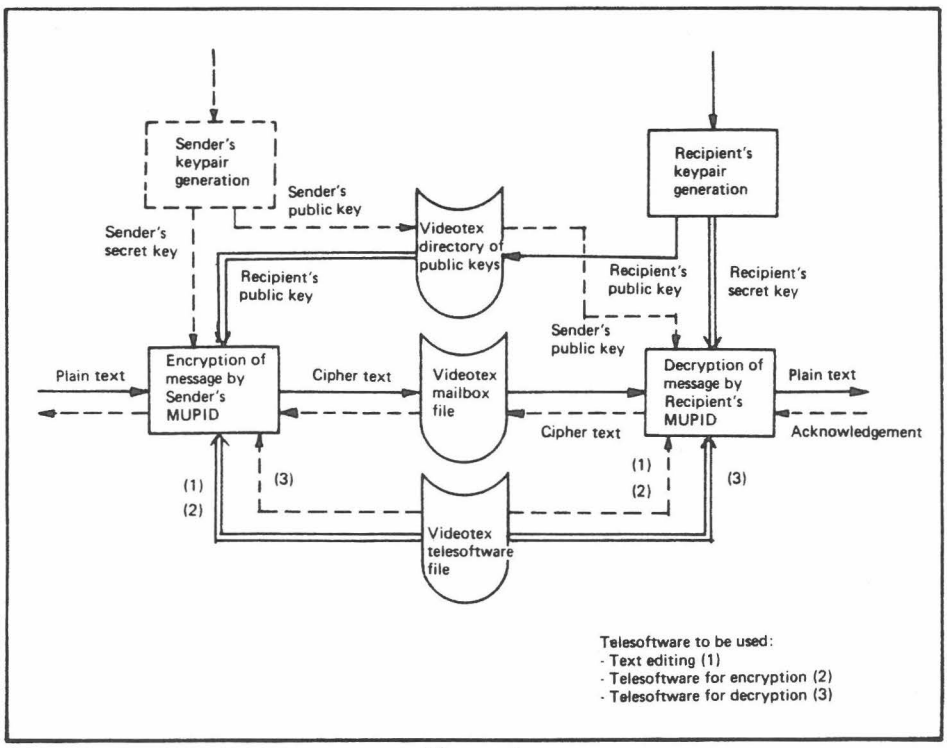

Figure 3

istrator and user. In this way, the request for new keys would have been authorized both by this special key and the old private key — the new key would be sent through the special key. The likelihood of both keys being stolen is far less than for just tapping the private key.

A third possibility might be for the key administrator to send out in a random way special pages containing various unused private-key options; each key would get an identification number. If a user wants to change his private key, he simply selects one of the upcoming private keys, which he stores locally, and informs the key administrator through the public key which key he has selected as the private key.

A fourth possibility could be that this selected key is used only temporarily between user and key administrator to establish a secure temporary channel through which the user would finally receive his private key.

A completely different method of key distribution would result if the generation of public-key pairs could be performed locally by every user. In this case, the user would simply retain his secret private key and only submit his newly generated public key to the key administrator. In this fashion, the "dangerous" distribution of private keys from the key administrator could be avoided. The key administrator would first check that the submitted public key does not already belong to another subscriber, in which case it would be necessary for an alternative key pair to be generated and submitted.

This checking procedure could be done by a third-party computer. Even if the list of subscribers stored

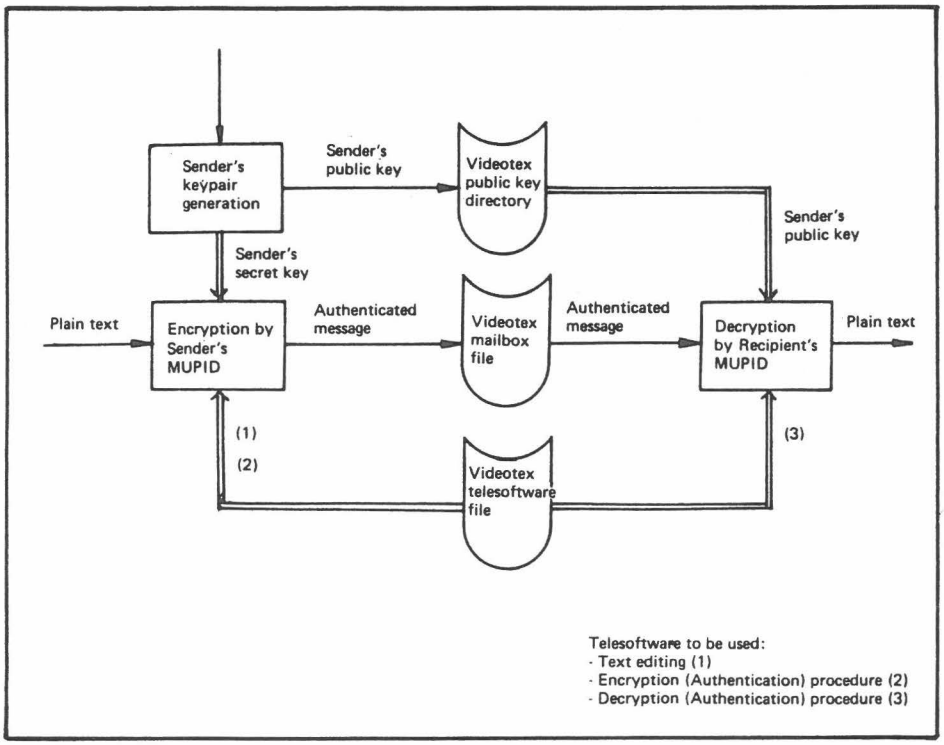

Figure 4

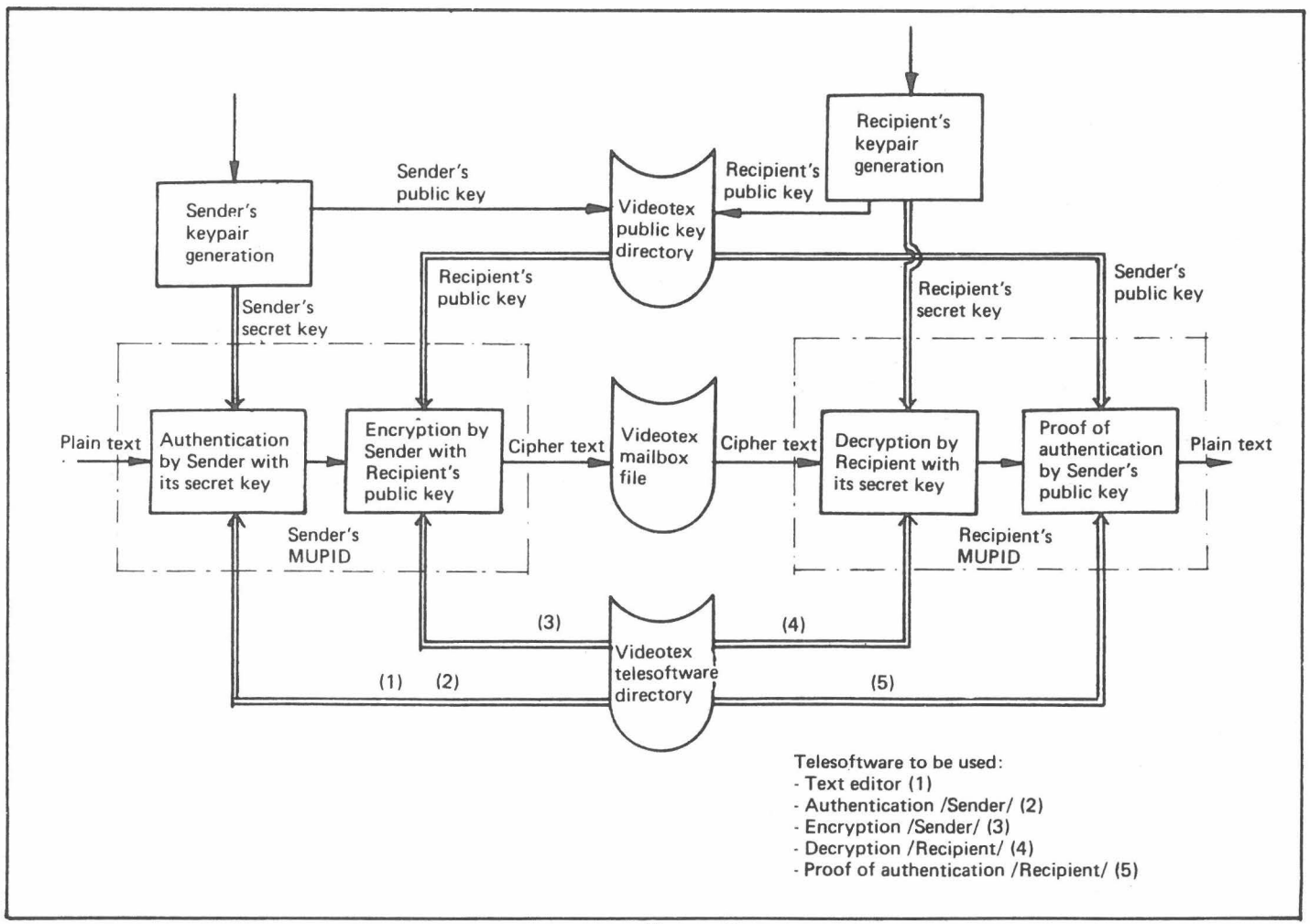
Recipient's keypair generation
Sender's public key
Videotex public key directory
Recipient's public key
Sender's keypair generation
Sender's secret key
Recipient's public key
Recipient's secret key
Sender's public key
Plain text
Authentication by Sender with its secret key
Encryption by Sender with Recipient's public key
Cipher text
Videotex mailbox file
Cipher text
Decryption by Recipient with its secret key
Proof of authentication by Sender's public key
Plain text
Sender's MUPID
Recipient's MUPID
(3)
(4)
Videotex telesoftware directory
(1) (2)
(5)
Telesoftware to be used:
- Text editor (1)
- Authentication /Sender/ (2)
- Encryption /Sender/ (3)
- Decryption /Recipient/ (4)
- Proof of authentication /Recipient/ (5)

Figure 5

in the system is large (say, millions of subscribers), special programming techniques can easily be arranged so that the checking procedure is fast. One known technique, for instance, could be to list the public keys in increasing order; then, by using a binary searching technique, it would be simple to find out quickly if the same key already exists or not.

There are certainly many technical problems associated with this technique; for example, the key length would need to be as long as possible, not only to provide increased security but also to make the creation of new, unoccupied key pairs by the subscriber easier. Another problem to solve is key generation itself, which is a rather long, complicated, number-crunching process.

The number of key distribution options is rather broad. The question is how far it is worth going in this process. Another problem is the processing capability of the intelligent video-decoder. Let us assume that the problem of key distribution is solved. According to the Rivest, Shamir and Adleman article, "A Method Obtaining Digital Signatures and Public-Key Cryptosystems" (in *Communications of the ACM*), the length of the keys used determines whether an "enemy cryptanalyst" would be able to break the method in a reasonable time period. The authors' estimates have shown that a 50-digit key could be broken by the fastest algorithms and machines of today in approximately 3.9 hours; 75-digit keys would take 104 days; 100 digits, 74 years; and 200-digit keys, 3.8 times 10^9 years (3.8 billion years).

Common sense suggests that even for the most sensitive daily applications, 75- to 100-digit keys would be sufficient. At present, however, it would be a cumbersome and time-consuming problem for microcomputers to process 75- to 100-digit keys. Mupid, for example, even with its floating-point-Basic version, can only handle 12-digit keys in the simplest programming form.

There is, however, hope on the horizon. Reportedly, microcomputer encryption/decryption software based on the public-key principle is already on the market using a 77-digit key. The software operates on Zilog Z80 microcomputers under Digital Research, Inc.'s CP/M system. The time needed to generate the encryption and decryption keys ranges from 15 minutes to four hours. The message encryption and decryption take about one minute plus the necessary disk access time. Ron Rivest, one of the fathers of the RSA public-key cryptosystem, and his colleagues are reportedly working on a single-chip implementation of the system that can be used on a microprocessor bus, which should be able to process about 150 characters per second. It seems, therefore, possible.

Electronic voting. A possible electronic voting system built on new-generation videotex is shown in Figure 6 (on In Depth/31), although only the basic functions and links are represented. In order not to overcomplicate the chart, we have left out the videotex information files containing the appropriate piece of telesoftware needed for encryption/decryption procedures, the file of public keys and the videotex mailboxes.

As mentioned earlier, in electronic voting we have three major "actors": the voter community, a kind of "notary public" (or election board) and a so-called "vote collector." The functions of the notary public include maintaining the list of voters, checking the validity of voters and making entries in the voter's list that

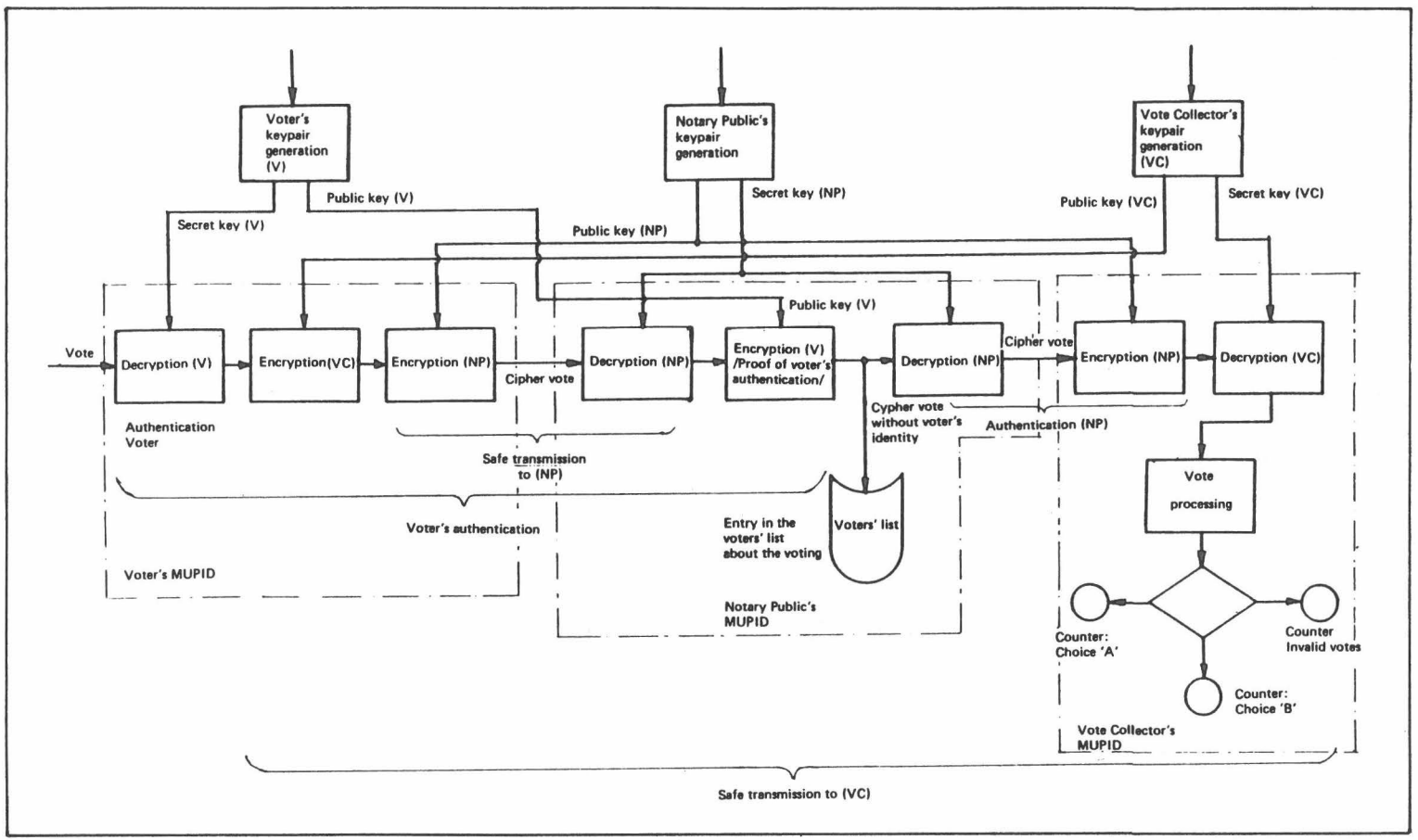
Voter's keypair generation (V)
Notary Public's keypair generation
Vote Collector's keypair generation (VC)
Public key (V)
Secret key (V)
Public key (NP)
Secret key (NP)
Public key (VC)
Secret key (VC)
Public key (V)
Vote
Decryption (V)
Encryption(VC)
Encryption (NP)
Cipher vote
Decryption (NP)
Encryption (V) /Proof of voter's authentication/
Decryption (NP)
Cipher vote
Encryption (NP)
Decryption (VC)
Authentication Voter
Safe transmission to (NP)
Cypher vote without voter's identity
Authentication (NP)
Vote processing
Voter's authentication
Entry in the voters' list about the voting
Voters' list
Voter's MUPID
Notary Public's MUPID
Counter: Choice 'A'
Counter Invalid votes
Counter: Choice 'B'
Vote Collector's MUPID
Safe transmission to (VC)

Figure 6

a vote was made by a certain voter and so forth. The notary public must also make sure that the votes are authentic and are received in time. He should not, however, be aware of the content ("yes" or "no") of the vote.

Aggregation of the votes should be done independently by a vote collector. The vote collector should basically be a third-party computer that counts the results and prepares various statistics instantaneously. The vote collector must, of course, know the content of each individual vote, but should not know who voted what. All these basic functions can be fulfilled by public-key cryptosystems as shown in Figure 6.

In our voting system, the voter's intelligent videotex decoder provides for the authentication of the voter by use of his private key, then allows the user to vote in an interactive way. It encrypts the actual vote ("yes" or "no") with the public key of the vote collector and then makes sure that the whole message, that is, his authentication (name and digital signature) and the encrypted vote, is received by the notary public safely. To achieve this, the whole voting package is encrypted with the public key of the notary public that only he can decrypt. The actual transfer of the vote is done through the message-sending service of videotex.

To process the votes, the notary public either has to use intelligent videotex decoders or, perhaps, videotex decoders combined with a third-party computer. His first function is to decrypt the votes with his private key and then to check the authentication of the voter by using the public key. If proof of user authentication is gained and the vote is formally correct, an entry then has to be made onto the voter's list to ensure that the voter does not vote again on the same issue.

At this point, the content of the vote and the identity of the voter have to be separated so that only the encrypted vote content is sent over with the videotex message service to the vote collector. In order to prove that this vote was correctly administrated by the notary public, the notary public must use his own private key to authenticate the message and perhaps even put a time stamp on it. Also, at this point, an additional encryption would assure that the transmission from the notary public to the vote collector is done secretly. This action, however, seems to be unnecessary because the actual content of the vote is still encrypted.

The vote collector is also based on an intelligent videotex decoder, and an external computer would perform the following functions: First, it checks whether the messages received were authorized by the notary public; second, it encodes the actual content of the vote with its private key and performs the vote counting and preparation of the various voting statistics. With this step, the voting chain is closed.

Since the entire process is fully computerized, any type of voting can be performed without major preparation once the whole system is set up. A national system can be installed with the technology available today.

Electronic feedback. In addition, electronic voting technically could offer other aspects on a completely new horizon, namely, voting with feedback. What do we understand this new concept to mean?

In control theory, there are two classes: control with and without feedback. In both systems, certain control actions are taken on one side in order to change the behavior of the system. The basic difference is that in a system with feedback, cer-

tain measured characteristics of the behavior of the controlled system are fed back to the controller in order to allow for adjustment in the controlling process. In a system without feedback, the controller takes controlling action on the assumption that the system will obey his controlling measures. This assumption, however, does not always come true.

A typical example taken from daily life which covers both systems is one's own daily bath. In a control system without feedback, one regulates the temperature and volume of the water in advance through the water tap with the aim, say, that after five minutes the bath is filled with sufficient water at the right temperature. All of us have certainly experienced occasions when this assumption did not work; either the water was far too hot or too cold or the quantity of water was insufficient or excessive. For this reason, a control with feedback provides much better results. One can check from time to time whether the temperature and level of the water in the bath are right.

In terms of elections, of course, the system is much more complex

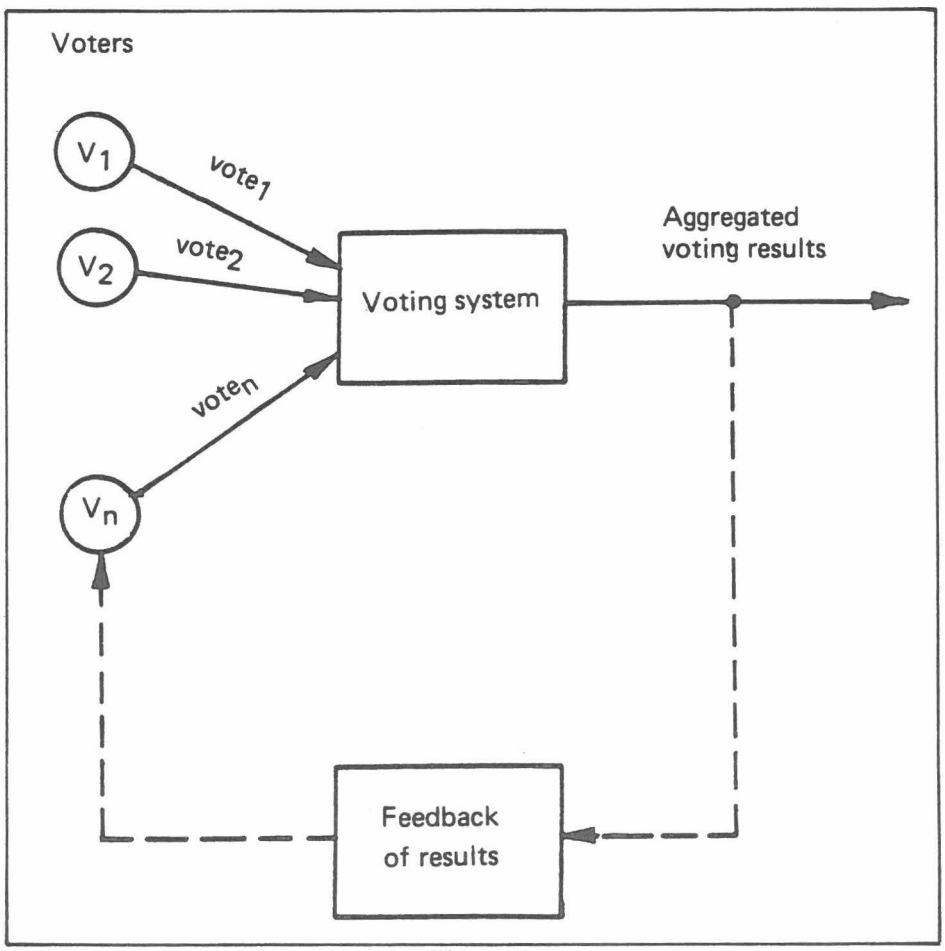

Figure 7

(Figure 7). The system to be controlled is the voting process. The controllers of the system are the individual voters, whose controlling functions are summed up in the system. The output is the aggregated results of the voting. No such voting system yet exists in which the results are fed back directly into the voting process. One of the reasons is certainly the technical difficulties encountered in doing so efficiently.

Rudimentary voting systems that do try to take feedback of a first election step into account are implemented in a number of countries. For example, in France, presidential elections are divided into two steps.

There is, however, no known system where the actual results are available to the voters during the election process where voters could modify their votes as long as the voting deadline is not past. In an electronic system as described above, this feedback would be technically possible. This set-up could mean that in a given election in which the expected results are not a simple "yes" or "no," voters would have better control over the voting process than they do today.

> Here we take the election system of West Germany as an example. Every voter has two votes.
>
> With his first vote, he can elect a person to represent the local community in the Bundestag for the next four years. The election process is simple. The candidate who receives the most votes wins. He is, in most cases, a member of a given political party, whose policies he will likely follow during the next term.
>
> The second vote in this system counts in the general elections. A voter places his vote for a given party, thus basically controlling the "strength of representation" of that party in the new Bundestag. These two votes are at present the only rudimentary means available to any voter. As long as the answer is just a simple "yes" or "no," this system is fine. However, the nature of the real questions asked is much more complex and their number far more than two. In a parliament with several political parties, each with different but slightly overlapping programs, the actual questions might better be put as follows:
>
> 1. Which of the parties should be represented in the parliament and should most likely form the government? (In the Bundestag, those parties with less than 5% of the vote may not even be represented.)
>
> 2. How strongly should those parties that are elected be represented in the parliament?

For a great number of voters in the 1983 election, for example, the question was not a matter of whether they wanted to vote for party A or B, but rather, whether parties A, B, C, D and so on should even be represented and, if so, how strongly. In an interactive voting system, these questions could indirectly be asked and answered by the voters. One of the present-day fears in elections is that even after time-, resource- and energy-consuming campaigns, no real decision is reached because according to

the voting results, no one government with a ruling majority can be formed.

This situation is usually deemed to be undesirable both for the party concerned and for the voter. But because of the lack of feedback in the election process, it could easily happen and does happen.

A second concern during the recent West German election campaign was those "lost" votes, which because of the 5% limit clause, could have unforeseen effects on the election process. If, for example, the smallest party now represented, the so-called "Greens," had received 6% fewer votes than they did, then the conservative party (CDU-CSU) would have obtained a majority and there would have been no necessity for creating a coalition with the Liberals. The representation share of the "left" would also have actually been severely influenced.

In an interactive system, the voters could have influenced whether the "Greens" should be "in" or "out" and if "out," who should have gotten the votes instead.

How could such a system really work? Let us take the following very simple scenario: An election starts at 6 a.m. on a particular day, but using the electronic voting system of videotex, some votes could have been sent to the notary public a few days earlier. Voting, as described above, could be done at home. Now let us assume that there is no feedback on the election progress before noon in order to "set the stage," but that after noon, voters could get information on the voting results through the national videotex system or some other media. Thus, every voter would have the chance to modify his vote before the close of the election.

In the U.S., some interaction occurs because voting concludes and is tabulated in the Eastern states while voting is still taking place in the West's later time zones. In the 1980 election, President Jimmy Carter conceded defeat before the polls closed in the West. Political analysts believe this action influenced Democratic voters to stay home, which led to the defeat of some Democratic candidates in those states.

By this point, careful readers will have many serious questions. Yes, an interactive voting system is a complex system with dynamic behavior. In order to design a stable system with functioning feedback, the rules of control science have to be applied, and the dynamic system behavior and feedback mechanism have to be fully understood and entirely under control. This task is very complex and goes beyond the scope of this article. But there is good reason to assume that such a stable interactive voting system could, in principle, be designed and implemented if there were a political consensus supporting this approach.

Such a system could be fully implemented in the next 20 to 30 years for full penetration, provided we start to think now about how these issues and problems could be investigated and resolved and consider all the technical problems. It would seem worthwhile to carry out pilot projects on a local rather than national basis.

Thought need also be given to the political implications of such systems — whether voting will be encour-

aged or discouraged; whether certain classes of voters will benefit disproportionately by an interactive system; whether an interactive system will cause distortions or otherwise negatively affect the sense of equal participation; or whether a combinated system of traditional ballot plus electronic ballots for those choosing the new system will be feasible for a transitional period.

Electronic opinion polling. Technically, electronic public opinion polling is not much different from secure message sending, with or without authentication or the mechanism presented for electronic voting. Its main advantage over the presently used techniques would be that it could allow for public opinion polling results to be more quickly and frequently collected and on a larger scale than practiced today.

At present, there are still many problems associated with public opinion polling. Very often there are insufficient resources available to obtain truly representative public opinion, and usually the time span is too short to obtain decent results. It is almost technically impossible to obtain solid public opinion polling results on any current issue in two or three days at acceptable costs.

Today, 1,000 citizens interviewed on a certain topic is considered to be a representative result. With electronic public opinion polling, a much better job could be done in a shorter time at less cost. With full market penetration of videotex, the citizens who could be involved easily in public opinion polling could be much larger than today. Similar to electronic voting, processing of the data can be done instantaneously, almost automatically and practically without any cumbersome data preparation.

If this instrument is applied correctly, it may provide a most valuable and powerful tool for those who are (or should be) really interested in the public's opinion.

Electronic ombudsman. The "electronic ombudsman" concept obviously does not mean that complaints could be received and investigated automatically by new information and telecommunications technologies, only that these new tools could considerably help.

The technical solution for an electronic ombudsman is rather obvious. Through the ombudsman's public key, everyone could send secret messages to him, which could either be signed through private keys or be kept anonymous. It is not possible to send an anonymous message in the present videotex systems. But should such a function be required, another independent body — let's call it the "public's representative" — could be established to put messages in an anonymous form.

The messages could be encrypted as well. The sender encodes his message according to the ombudsman's public key and sends it to the public's representative for "anonymization."

The public representative would then remove the sender's name when transmitting the message to the ombudsman. The public's representative would, of course, not necessarily be able to read the content of the message.

Problems and prospects. There are many problems to be solved before one could actually start with the above applications. From the technical point of view, an electronic speaker's corner could be started any time; only the *modus operandi*, the legal status and the costs need to be clarified.

As far as electronic voting is concerned, we are not ready at this point, even from a technical point of view, to start, but there can be little doubt that all the hardware and software problems could be solved in the near future.

We estimate that a fully operational system could be set up in about two or three years' time.

The actual problems lie in a different area. First, the user penetration of such systems takes time. Market penetration to 80% of all households in the U.S. for new media were:

- Radio in 19 years.
- Black-and-white television set, nine years.
- Color television set, 25 years.
- Telephone, 72 years.
- Cable television, projected at 73 years. The penetration of videotex, the cheap computer network for daily life, on the market will certainly not take place any more quickly than the fastest of the above media.

For this reason, our guess would be that at least one generation (25 years) would be required to achieve an acceptable level of videotex coverage so that instant voting could be possible from virtually every household.

If full user penetration is not achieved, then a possible political concept of "more direct democracy by the citizens through new information and telecommunications technologies" could also not be achieved.

Those people who for some reason do not have easy access to videotex terminals (because they cannot afford it, because they live in remote areas with an insufficient telecommunications infrastructure, or because they do not want it) would not have an equal ability to participate with those people who do own them. We estimate that the shortest time horizon possible for full penetration and introduction of such systems would be one generation — and then, only for the most developed parts of the world. Until then, electronic voting could become one of the election alternatives, such as voting by mail or at polling booths. But its full impact would, of course, not be felt or really gained in respect to a more direct democracy.

In the moderately developed and less-developed countries, the penetration period is, of course, even longer. Thus, unforeseen conflicts may arise. Let us assume that more public participation and direct democracy is desired in two given countries in a future information society and that one is well-developed and the other not. Is this not yet another source of difference between rich and poor?

Another possible conflict situation could be the following. Imagine a well-developed country in which more public participation in government and more direct democracy were technically possible, but the present establishment wishes to retain the status quo in governing and restricts the introduction of technologies that would allow more citizen participation.

This situation may lead to political conflicts and changes in dynamics between government and governed.

In general, in any information-rich society with the appropriate technical infrastructure for direct democracy and public participation in governing, it will be important to consider:

1. The domain of those issues in which decisions should be made jointly with the public through increased direct democracy.

2. The domain of those issues where the opinion of the individual is requested and the results of the

public polling are publicly announced but the final decisions are taken by the appropriate governmental bodies.

3. Finally, the domain where decisions are taken solely by the government without asking for public opinion (for example, in some national security questions).

Determination of the above domains could prove to be a major issue in an election campaign, depending on how each party would handle these questions if it won power.

In public-key cryptosystem applications (such as secure message sending, authentication, public opinion polling, electronic voting and so on), the administration of the public keys will also be of major importance.

In the case where the encryption/decryption key pairs are generated by the key administrator, then the administrator — and, in principle, only he — will be in a position to control all information and transactions flowing through the system.

In some countries, this control might simply not be acceptable. For these countries, the system whereby the keys are generated by the user and only the encryption key is forwarded to the key administrator might prove to be more acceptable.

However, even then the administration of the encryption keys is so important that some countries may decide in public systems that the administration of public keys should be a government monopoly, say, the PTT or some central governmental agency. In other countries, a commission somewhat independent of the government might inspire greater confidence.

Vulnerability is also a problem issue. If banking transactions, electronic voting and so forth are performed by means of public-key systems, then the vulnerability of the system and especially of the key administration is of utmost importance. A terrorist attack on a single key administration center could seriously affect the daily life of society in a way similar to the effect that a poison attempt on a city's water supply by terrorists or lunatics would have.

All in all, there are plenty of problems to be solved.

About the Authors

Istvan Sebestyen is a research scholar at the International Institute for Applied Systems Analysis in Laxenburg, Austria. He is also a guest professor at the Technical University of Graz, Austria. He concentrates in the field of new-generation videotex systems, especially intelligent videotex terminals.

Matthew Nimetz is a partner in the law firm of Paul, Weiss, Rifkind, Wharton & Garrison in New York City, where he specializes in corporate and international law. He served as Under Secretary of State for Security Assistance, Science and Technology in the Carter administration from February through December 1980.