Application of Encryption Techniques for Security Purposes in Financial Systems

by T.W.M. Jongmans

De Nederlandsche Bank N.V., Postbus 98, 1000 AB Amsterdam, the Netherlands

1. INTRODUCTION

Today's theme is 'how do I protect my data'. This theme is above all interesting for banks because, contrary to other enterprises, banks do not deal in goods whose amount and location are recorded in a stock accounting system. Sure, banks do operate an accounting system, but the data contained in it do not concern stored banknotes; rather, *the data themselves are money*. The balance on your bank account *is* money, which you can spend in a variety of ways or must repay, depending on whether you are in the black or in the red.

Allow me to give some statistics on different volumes of payments:

(a) Each year Dutch households pay some 90 billion guilders *in cash*. For enterprises the figure is 45 billion. However, *giro transfers* involve some 2,500 billion guilders a year.*

(b) Annually, the banks' clearing house (BGC) processes about *one billion* giro transfers.

(c) Annually, in the Financial Accounting System of De Nederlandsche Bank some 10,000 *billion guilders* is transferred between financial institutions.

It will be clear that for banks the quesiton 'how do I protect my data' is exceptionally important, since it is equivalent to the question 'how do I protect my money'.

In terms of substance, too, these questions are far from trivial. This is due primarily to the emergence of automated networks, so that money is handled

* These figures, established by the Scientific Research and Econometries department of De Nederlandsche Bank, are necessarily not more than indications. However, they do give an impression of the order of magnitude of real payments, excluding transfers between financial institutions.

by a widening variety of processes in ever-greater volume and at ever-higher speeds.

Hence, in a sense, the numbers that are money, the subject discussed by David Chaum (these Proceedings pp. ??-??), are already occurring in day-to-day practice, albeit in a more prosaic form than in his protocols. What I intend to do here is to give an impression of security practice with regard to financial systems (first the classical methods, followed by the modern ones). I shall do so from the perspective of the Nederlandsche Bank, and especially in the light of the Bank's main tasks, as they have been formulated in section 9 of the Bank Act:

- regulating the value of the guilder;
- facilitating transfers and external payments;
- supervising the solvency and liquidity of the banking system.

Each of these three principal tasks is in some way related to the reliability and security of the payments system and of the automated financial processes used in this system.

2. THE CLASSICAL BASIS OF SECURITY

The classical aim of security in automation is to ensure uninterrupted processing by safeguarding the proper operation of the automated systems and controlling the risks ensuing from the use of such systems.

Specific goals are:

- reliability (completeness and correctness) of the data produced and stored;
- controllability of processing;
- continuity of services.

It is generally known that measures are necessary in *classical* financial systems and are more or less (but not quite) sufficient in order to achieve these security aims. In brief:

(a) Structured systems development, focusing explicitly on processing checks, segregation of functions, audit trail, etc.

(b) Segregation between development, testing and operation in order to ensure software integrity and stability.

(c) Controlled access to software and data in order to permit only authorized actions by authorized persons in their proper interrelationship. This applies to the financial systems themselves, but also, more in general, to *all* the software and data present in the computer in order to ensure *total* system integrity.

(d) Operating procedures.
Financial systems must be operated in a controlled fashion in the same way as industrial processes. The systems must be stable, robust and easy to operate (when operators and systems managers have to run their systems

in a state of agitation, this means they are not fully in control of the situation. This must always be avoided, a computer room must be a dull place where no time-critical or otherwise critical decisions need to be taken unless they have been adequately tested and rehearsed).

(e) Backup, recovery, disaster recovery.
Procedures must have been prepared, tested and rehearsed for emergency situations, ranging from malfunctions to calamities, in order to permit data recovery and continuation of services, if necessary at a reduced functional level, until the problem has been resolved.

(f) Physical security.
All computer systems which permit physical manipulation of the hardware, software or variables are weak. As we have seen, a computer contains money and, hence, *also* requires a protected environment in a physical sense in the same way as banknotes are stored in vaults.

Tens of thousands of pages have been written in the form of checklists, monographs and audit manuals about the purpose, design, implementation and cost of combinations of the above measures. On 20 September 1988 the Nederlandsche Bank added a modest 10 pages in the form of its memorandum on the reliability and continuity of EDP at banks.

The significance of the memorandum is mainly to be found in the fact that it requires the boards of the individual banks to pay attention to security issues. In this way the central bank, acting in its capacity as supervisor of the financial institutions, *stressed* that inadequate security of automated information systems may cause a bank's solvency and liquidity, and hence indirectly the function of the banking system in society, to be impaired.

The developments which have taken place in payments in the two years since the memorandum was published suggest that in the future the classical security techniques will no longer be adequate, so that more powerful procedures will be needed.

3. THE MODERN SECURITY TECHNIQUES

I shall now discuss the more advanced security techniques, which are notably applied within the framework of the new developments in payments.

First, an overview of some major forms of payments:

Card-oriented	- credit cards
	- cash dispensers
	- point of sale terminals
Paper-based	- personal sector giro payments (transfers, cheques, inpayment transfers)
Message-oriented	- business sector giro payments (magnetic tape, diskette, direct debits)
	- electronic payments (personal and business sectors) (home banking, telebanking)

- interbank payments (high-speed circuit of the banks' clearing house, SWIFT network, Financial Accounting system of the Nederlandsche Bank)
- settlement (Financial Accounting System)

The crucial questions in the case of card-oriented systems are: is the card *genuine*, is it used by the *rightful* owner, and is the transaction *within the applicable limit*?

Security has been known to be infringed in each of these three areas. Counterfeiting of cards is countered by using high-tech cards, with holograms, made with sophisticated printing techniques and employing esoteric physics. The card is combined with a PIN code in such a way that the only manner to gain access to financial services is through the combination of card and code. The PIN code is a cryptogram of the data contained in the magnetic stripe.

The most difficult problem is to enforce transaction limits. Strictly speaking, it is not necessary for cash dispensers and point of sale terminals to be connected on-line with a central computer, since it would be sufficient if the transaction data were transmitted once a day; however, in such off-line situations, it is difficult to prevent overdrafts. Hence, cash dispensers and point of sale terminals must have an on-line connection, leading to a considerable increase in the costs of data communication.

At present an experiment is being conducted at Woerden to solve the problem in an entirely new way, by using a smart card. Contrary to magnetic stripe cards, smart cards cannot really be counterfeited and are able to enforce transaction limits without any connection with a central computer. Although the experiment has not yet been completed, it is already evident that the smart cards technology is very demanding and that the cards still require some improvement. The consequent effect on costs is not yet clear.

Compared with the new method, paper-based payments (using cheques and transfer forms) are somewhat obsolete and uninteresting. Nonetheless, they give the banks serious cause for concern. Processing (sorting, data entry, filing) is expensive, and in the disastrous period round about 1986 the combined banks incurred losses of up to 100 million guilders per annum as a result of fraud with cheques. The profits of some banks suffered considerably as a result of these losses. Since that time, new procedures have been successful in reducing fraud. Through their structure of charges, the banks seek to influence consumer preferences towards more efficient and lower-cost payment methods.

By the way, I have already used a fair proportion of the time allotted to me and I have not even yet used the word encryption. Let us, therefore, turn to the message-oriented payment methods; I shall use the word message in a broad sense to denote magnetic tape and diskettes as well.

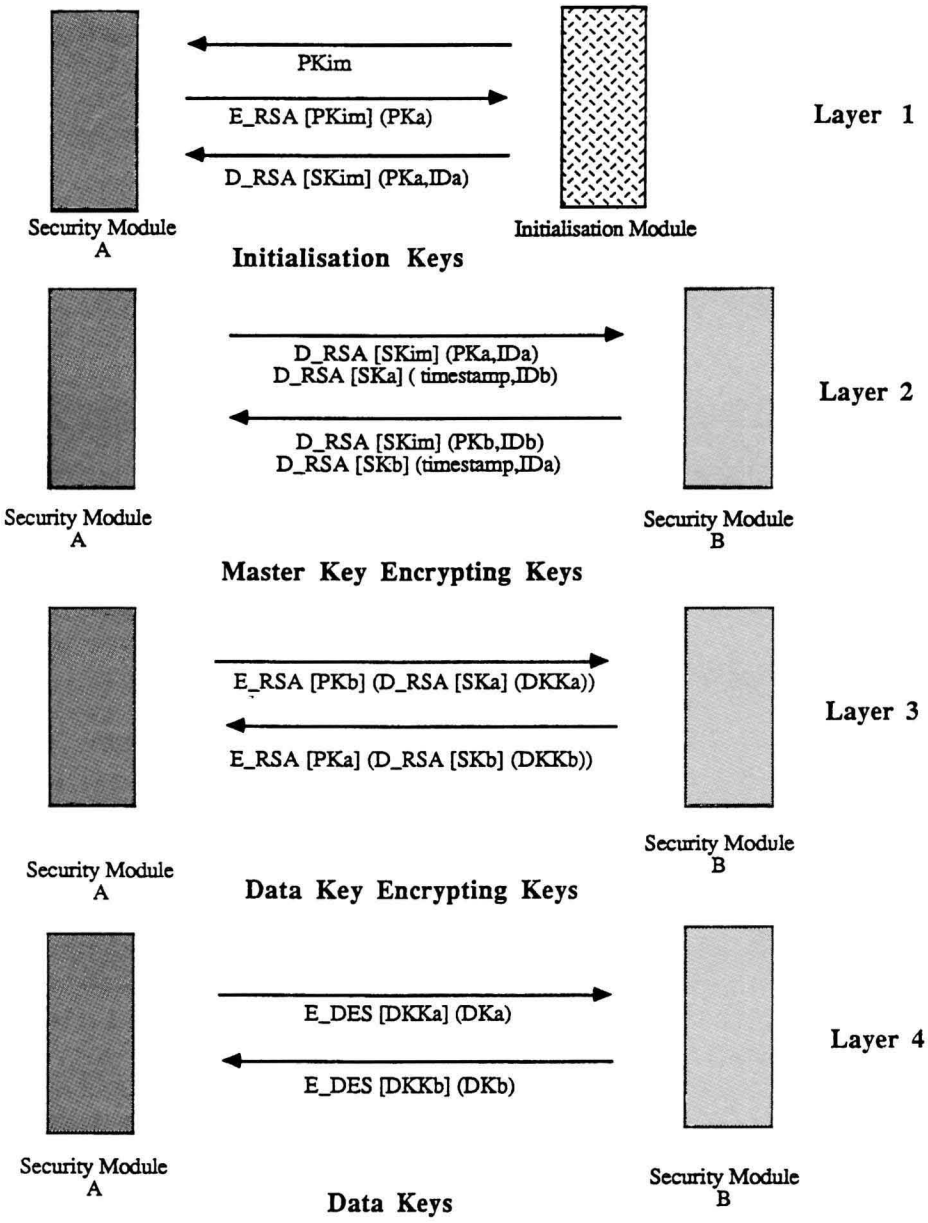
In message-oriented payments, the crucial security questions are: has the integrity of the messsage been preserved (is the message unchanged or unmutilated), is it authentic (has it actually been sent by the person indicated as the sender) and has it been authorized (is it a valid instruction)?

The integrity of the message, which concerns what security experts in banking usually call layer 1 security, is checked by means of a hash count relating to the contents of the message. A hash count contains information *about* a message which very probably changes when the contents of the message are changed. A constant is not a hash count. The sum total of amounts or the number of items in a message are poor hash counts; cryptographic one-way functions are excellent hash counts. One of these has been developed by IBM, termed MDC (modification detection code). Another has been developed by an interbank working party under the auspices of the banks' clearing house (BGC); it is known as the BGC hash. In the Dutch banking system the BGC hash is the standard. It has also been proposed for standardization within the ISO. Writing the hash count on a piece of paper, signing it and adding it to the message ensures not only the integrity but also the authenticity of the message. Adding the signature of an authorized signatory furthermore proves the authorization or validity of the transfer order. Unfortunately, this is possible only for magnetic tapes, diskettes and similar media but not for data transmitted by means of data communication.

Hence, there is a need for suitable layer 2 security, that is, the authentication of the message. MAC (ISO 8730, ANSI) is a standard for a message authentication code. Other methods have been developed as well, such as the BGC layer 2 authentication, the French system Etabacc5 and the German Deutsche Bank system. The principal theoretical issue concerns the use of symmetrical or asymmetrical algorithms (in practice the choice is between DES and RSA). (For RSA, see Massey's contribution to these Proceedings, p. 27.) The principal advantage of DES is the fact that high-speed hardware and software are available; a few megabytes per second are easy to achieve. The disadvantage is that, because of its symmetrical nature, DES is sensitive to insider attacks: secret keys must be managed and transported. In the case of RSA, this drawback carries less weight: only the user's own key is secret but it need never be transported. The major drawback of RSA is that implementations are very slow: a few kilobytes per second is considered a very high speed in this context. If operations are conducted at that rate, how can the banks' clearing house ever process its three million transactions a day? This problem has led to the development of hybrid systems, which employ DES for bulk transactions and RSA for the upper layers of key management. By the way, development may be too big a word: hybrid systems have been conceived, but I for one have never seen one implemented in either hardware or software.

I would like to discuss with you the design of a hybrid system in which I myself was closely involved: the security concept for the National Payments circuit, known as the NBC. The NBC is a project to achieve uniform direct interbank payments. After many years of preparation, the project was started in 1985 and it is being realized in stages and on a limited scale. In the period 1987–1989 an interbank working party designed a security system for the future data communication within the NBC. The chart shows the key management protocol developed by the working party. The bottom layer of key management

is the exchange of data keys, for instance daily (layer 4 in the Chart); it is implemented in conformity with the ISO 8732 point to point protocol. The exchange of the symmetrical encryption keys (layer 3) is effected weekly or monthly and takes place under an asymmetrical algorithm with authentication. The public keys are exchanged in the forms of a certificate in layer 2. This certificate is prepared by a central institution in layer 1.



Exchange of keys between Security Modules and Initialisation Module

It took only a few months to prepare the concept and to have it approved by the banks. However, the search for suitable implementations in hardware and software is still in progress. Even at this moment I cannot say that the search has been completed in the sense that the concept has been successfully implemented. NBC is at present secured by other means. Indirectly, a success has been scored in that, within the ISO context, a closely parallel concept is now a candidate for standardization. At present, it has the status of a committee draft (ISO/TC68/SC2 Committee Draft 11166).

I would like to use the last part of this address to discuss the practical aspects of encryption.

4. PRACTICAL ASPECTS OF CRYPTOGRAPHY IN FINANCIAL SYSTEMS

Cryptography is one of the most powerful security methods and has very specific areas of application. For some security requirements it is the only feasible solution. On the other hand, it is a complex and difficult subject, with which just a few experts are conversant.

I should like to discuss what I think are the two key problems of applied cryptography in banking.

First: Finding a cryptographic solution to a security problem is virtually always possible; the difficulty is to define precisely the security problem itself. Yet this is essential in order to know exactly

- what is secured, and, at least as important,
- what is not secured.

Anyway, from the viewpoints of both sound banking and competent investment, it is necessary to know exactly the security performance of measures taken and whether the measures do *indeed* satisfy the relevant requirements. The Vernam Cipher (cf. the first paper of these Proceedings, p. 5) is a case in point. Suppose that a transfer message has the following layout: account number of the ultimate payee 64 bits and the amount 64 bits. Someone who changes bit number 66 of such an encrypted message can be pretty sure that he substantially raises the amount. The security *performance* of the Vernam Cipher is confidentiality, which is not the same thing as authenticity and integrity. The lesson is that even a very powerful security tool may not be appropriate to your application.

Let us take another example. One might well wonder what the *legal* status is of certain measures, such as non-repudiation. Non-repudiation is the situation where the sender of a message cannot deny having sent the message. It can be achieved by means of an authentic signature on a piece of paper. However, will the Courts also accept digital signatures in the case of data transmission? I do not know. Within the NBC, we did consider whether complicated legal non-repudiation procedures were actually necessary. We decided that this was not the case, because that is not the way banks go about things with their fellow banks; most disputes never reach the courtroom. This is perhaps best illustrated

by the manner in which foreign exchange dealers work. They transact their business by telephone, somewhat like this: 'Do you have 10 million dollars for me?' 'Sure, at 1.6720.' 'Okay, it's a deal!' This two-second dialogue between dealers entails the same obligations as a duly signed legal document. (By the way, the dialogue is taped; if one of the parties has made a mistake, the tape is used to clear the matter; however, the verbal agreement will always stand!)

Identifying and solving a security problem in respect of a system must be based on an analysis of the system made by the owner of that system. This must not be done by an encryption expert who has no authentic affinity with the system. The typical automation situation, in which the one who *experiences* the problem (the security problem owner), is not the same as the one who *solves* it, is very evident in the area of security, and even more so when cryptography is used.

Second: practically no-one (including in any case many cryptographers) is really aware of the immense difficulty of operating encryption techniques *in practice*. This is due not so much to encryption itself as to the limited availability and flexibility of encryption hardware and software; another problem is the lack of common ground between encryption experts and systems designers.

To conclude this address, I shall give an overview, based on my own personal experience, of the numerous vexing practical problems and constraints, which cannot be avoided:

- The cost problem (good encryption hardware and software can cost up to 5,000 guilders per work station and that may be more than the cost of the station itself; this is acceptable in special cases only).
- The labour-intensity of key management (initializing a smart card requires that the card is inserted in a card reader, packed and sent, something that will easily take a minute or so. Doing this for 100,000 smart cards takes a lot of time).
- Global secrets, which are present at various locations, must be avoided. Such secrets require tamper-resistant hardware, which is expensive; moreover, if the secret leaks out, the system must be stopped. Also, situations must be avoided where institutions must know each other's secrets.
- Details of security measures must be kept secret, whereas a knowledge of the system must be present within a stable group of operational staff. These are conflicting requirements.
- Dependence on a single supplier must be avoided. However, this is practically impossible in the case of hardware and difficult in the case of software (due to imcompatible implementations).
- Strict security measures are hard to reconcile with sound backup, recovery and disaster recovery procedures. Furthermore, they complicate operation (remember, operators in a state of agitation are a sure sign of serious problems), repairs, and especially maintenance and change-over to new releases.
- Security always detracts from the user-friendliness of a system, because of:

- more management effort, such as the issue, monitoring and withdrawal of access rights and authorizations (a typical problem is that, once issued, an encryption key certificate cannot be withdrawn);
- stricter procedures (segregation of functions, limitation of functions, frequent log-on);
- psychological and ergonomic factors; care must be taken to ensure that the end user, who experiences the burden (never the fruits) of security, is intuitively able to grasp and accept the significance of the measures taken and to appreciate that he has an *inherent* interest in adequate security. If that is not achieved, all security efforts are in vain;
- lack of uniformity: users are sometimes confronted with a multitude of devices, diskettes, bank cards, PIN codes, log-on/log-off procedures, etc., if more than one bank is involved; this may degrade the commercial viability of automated banking services.

CONCLUSION

I hope that, through this overview of the potential applications of cryptography in the financial area, I have succeeded in showing that cryptography is not just interesting from a theoretical viewpoint, but that it also holds out fascinating prospects in practice.

REFERENCES

Boeschoten W.C. and M.M.G. Fase - The way we pay with money, Journal of Business & Economic Statistics, July 1989, Vol. 7, No. 3, 319-326.

Boeschoten W.C. and M.M.G. Fase - Het bankbiljet van *f* 1.000,-, Economisch Statistische Berichten **73**, no 3658 (June 1, 1988), 523-527.

Boeschoten W.C. and M.M.G. Fase - Betalingsverkeer en Officieuze Economie in Nederland, 1965-1982, Kluwer, Deventer 1984.

The Memorandum on reliability and continuity of electronic data processing in financial institutions was published in the fourth quarterly report of 1988 of De Nederlandsche Bank.