

Topic (ii): software and computing developments

**CRYPTOGRAPHY AS A TOOL TO EXPAND COMMUNICATIONS AND EASE OF ACCESS  
AS WELL AS DATA SECURITY**

Submitted by Statistics Netherlands<sup>1</sup>

**Contributed paper**

**I. Introduction**

1. At present, the traditional ways of safeguarding data against unauthorised access and alteration, draw heavily on the physical presence in premises, on the use of passwords, on the assumption that a Local Area Network is hard to eavesdrop, and on the inherent security properties of operating systems. The use of cryptography can improve many of these security ingredients. Moreover it permits remote access to data at the same level of security as is achieved by local access, i.e. at the workplace. The main goal of this discussion paper is to investigate the possibilities of safe remote access to data in NSIs. In a modern society where teleworking will be more and more commonplace, and where data communications will become as common as making a phone call, NSIs can no longer delay exploring the possibilities and limitations of remote data access.

2. The current practice of data protection<sup>2</sup> in most NSIs can be compared with a mediaeval castle: moat, strong walls, defence is pointing outward, all communication is going over one drawbridge, which is heavily guarded and raised at night. A next step in the development might be comparable to an 18th century city: still walls (ramparts), but many gates, considerable traffic and during the day the traffic is only lightly guarded. In the more distant future, it is likely that a stage comparable to a modern city will be reached: many highways for an abundant 24-hour traffic in and out; the security forces are also patrolling the interior of the city; the important buildings in a city are separately guarded, though with lighter — but equally effective — means than the mediaeval castles, because the overall level of safety has increased from the middle ages to our days. Of course this metaphor has its limitations, and therefore has to be kept brief, but before leaving it, it has to be remarked that the purpose — safety against intruders and aggressors — has remained the same, but the means by which this purpose could best be realised has changed and will continue to change.

---

<sup>1</sup> Prepared by Leon Willenborg and Jan Kardaun. The views expressed in this paper are those of the authors and do not necessarily reflect the policies of Statistics Netherlands.

<sup>2</sup> Data protection is used throughout this paper short for protection against eavesdropping, burglary and unauthorised altering of data, and does not include the aspect of statistical disclosure control, i.e. (unintentionally) revealing information that can be related to individual respondents.

## II. The need for cryptology in data protection

3. A metaphor like the one above is nice for setting the atmosphere, but it is not convincing that cryptology<sup>3</sup> is an indispensable tool in the near future. There are 4 compelling reasons, however, that show clearly that cryptology will soon play an important role in daily operations of NSIs.

- The rapid penetration of mobile telephones will soon be followed by mobile computing, i.e. wireless access to a (wired) computer network. The radio-technique is the same, and becoming extremely cheap and economical with energy. Imagine a mobile phone with a larger screen and pen or voiced based I/O, and there it is: the mobile computing terminal. As radiocommunication is by nature easy to intercept, cryptology is mandatory.<sup>4</sup>
- The mobility of people (employees) will also increase, ... A special case in increasing mobility (when taking the NSI premises as origin!) is teleworking, where employees do not commute (every day) to the NSI office, but stay at home or go to a local 'hoffice' (hotel-office, i.e. office space to be let by the hour or the day). The communication involved encompasses for a considerable part confidential material, and the efficiency of the work can only be maintained if the communication is as safe as nowadays within the NSI premises.
- There will be a strong increase of telecommunications and data exchange between NSI branch sites, between NSIs and supranational SIs, and other parties, including information suppliers to NSIs. This Electronic Data Interchange (EDI) will only blossom if the communication is reliable.[2] Even at moments when it does *not* concern confidential data, some level of communication security is needed and expected.
- The traditional solution that the carrier (either the mail or telecom carrier) is responsible for correct delivery and preventing others to listen/read in, has met its limits. With the advent of deregulation, too many parties are involved in telecommunications, and though most of these companies are certainly no less reliable than the traditional "PTTs", it is too easy for a malignant person (or organisation) to find a position in this mêlée. And especially with telecommunications, it is easier to filter a huge stream of intercepted data for information, as compared with mail (which has to be opened, read and sealed again manually).

All these developments mean that cryptology is (soon) needed as an additional measure, where in the recent past, the means of controlling physical access and of exercising social control were sufficient.

## III. Compartments

4. For a rational, efficient and practical system of data protection it is necessary to think in terms of compartments of data, each with different protection requirements. Instead of dividing the world into two groups, the 'ins' and 'outs' (i.e. all NSI employees vs. the rest of the world), and building an imaginary 'wall and moat' around the offices of a NSI, the data of an NSI are split into several (3 to 5) categories, with a varying level of security needs and measures.<sup>5</sup> The highest security level is, of course, for individual data with identifiers; one step less secure could be e.g. individual but not

---

<sup>3</sup> Cryptology is a combined term that covers cryptography (encrypting, keeping messages secure) and cryptanalysis (breaking cryptography).

<sup>4</sup> Most of the GSM mobile phone providers – who have their own security needs – offer encrypted transmission for the wireless part.

<sup>5</sup> This statement should not be read as that the insiders of NSIs are allowed any access, and outsiders none. Within the NSI there are in use several protection mechanisms and compartmentalisations (users, user groups, projects, departments, job function, etc.). The point is that these different access privileges within NSIs are usually for a large part *not* based on the security level of the data.

identifying data; other security categories might be: aggregated statistical data; ‘general office’ correspondence, and public data and reports. There needs to be some way of communication between the different security levels. One of the main issues is how to control and safeguard these communication ‘bridges’, because they would be among the vulnerable spots.

5. More than 3–5 security levels would not be practical, but there may be more than one compartment of the same security level. The latter is also current practice, as in most NSI departments, or even smaller units, they usually cannot read and certainly cannot alter each other’s data. In fact, it pays to dwell for a moment at the normal situation that there are already compartments within NSIs, e.g. several equally ranked departments,<sup>6</sup> a computing service where a selection of people have access to all data (for specific purposes), and a “guest room”, e.g. for registered visiting researchers who have severely restricted access, and a fourth, perhaps a fifth compartment for the financial and the personnel departments. There is nothing to lose, and a good deal to gain, if this approach is extended outside of the NSI’s premises, but only if the security mechanisms in the software can be relied upon.<sup>7</sup>

6. The solution if these mechanisms are NOT trusted is not, however, to forsake the benefits of a multicompartmental, localisation independent approach. At least NSIs should complain about this lack of security mechanisms<sup>8,9</sup> to the software suppliers – which will only be possible successfully if there is a data security plan for the NSI.

7. If we have a few security levels, there is a choice to consider these as rings of decreasing security needs and measures, each surrounding the inner (more secure) levels, or to consider “parallel lanes” of each security level, where no surrounding takes place. The first, circular approach is most attractive conceptually, but the price we have to pay is that outside workers (interviewers, e.g.) cannot access the inner core – where their data belong – in one hop. They must cross compartment boundaries several times.

#### **IV. What should be protected against what?**

8. It seems ideal to protect every piece of information against anything unintended – but it is the wrong ideal. This would give too many security measures and not enough functionality and ease of use. More realistic goals are those that specify that a certain class of security breach should be rare or hard to perform. Consider the consequences of the following security breaches, which are more or less in increasing order of severity (which is a matter of debate, of course):

- The Website of an NSI was hacked and a clearly false home page appears;
- The Website was hacked and some of the statistical data were realistically altered;
- Some office memos were stolen and made public;

---

<sup>6</sup> In contrast to the security levels, of which there should be only a few, there may be tens or hundreds equally-ranked compartments within each security class.

<sup>7</sup> Most of the operating systems have several of the mentioned features, rings (classes) of security levels, access control lists with propagation rules, encryption, etc., but we need something that transcends particular operating systems.

<sup>8</sup> Not meant here is bugs in the software that lead to security holes in an otherwise soundly designed security approach. These exist, and should lead to complaints also, but the goal is set higher here. The software should support the organisation’s needs for security and not the manufacturer’s.

<sup>9</sup> The basic problem for trusting the current inherent security mechanisms in most operating systems, is that there is built-in a class of ‘system tasks’ and ‘super-users’ who can by-pass all security mechanisms. This built-in escape mechanism is the target for malevolent intruders. Another major problem is that security mechanisms in computer software (both operating system and application software) usually only work well if they are designed into the software from the start. Experience has taught that features that are added afterwards, are usually inadequate.

- Some office memos were secretly altered in meaning (and this was not made public);
- A (word processor macro) virus was entered which randomly introduces negations in sentences;
- The full e-mail correspondence of a high-level manager was stolen and published;
- The same full email correspondence was stolen and used for blackmail;
- An arbitrary record with individual data was “stolen” and made public;
- A particular, specified, record with individual data was stolen and made public;
- A full dataset of individual records was stolen and made public;
- Several related datasets with individual data were stolen, and secretly abused;
- The same related datasets were stolen, abused and this afterwards published;
- Hackers erased the computer disks after having corrupted the back-up program for some weeks.

Even though the *exact* order in severity of damage is hard to ascertain, it is clear that there is a wide range in seriousness. Consequently, the effort for and burden of security measures need to have the same range.

9. All the above examples are about outsiders gaining illicit access to data. This is only one category of security breach, but likely the most serious one for NSI's.<sup>10</sup> We postulate that the important goals should be *to keep outsiders (burglars, hackers) out and keep confidential data in*. Other goals like keeping (unwelcome) programs (viruses, Trojan horses)<sup>11</sup> or illegally copied software out and keeping copyrighted software in are less important: though legitimate goals in itself, NSI's are not special in this respect, and “the usual protection mechanisms” should do.

10. A completely different goal, that is not to be intermixed with that of data security, is the control over how NSI employees can or should perform their tasks and the (ease of) management of computer services. Here, completely different balancing of cost benefit aspects of different solutions are to be made.

## V. Storage or communication?

11. There is a difference in encrypting information for storage and for communication. For (long-term) storage, the keys necessary to decrypt should not be lost in the meantime. This means that the keys should not be changed too often, and that the keys should be securely kept somewhere. In order to decrease the risk of stolen keys or lost keys, some systems have been designed that work with “any n out of m keys” (say 2 or 3 keys out of 6 keys-bearers).[4] Encrypted storage for long-term storage concerns mostly data, while short-term storage includes also documents. Most of these sensitive short-term documents are work-documents only, with a limited time of use. Documents that are of interest to have available electronically after more than a decade are mostly published reports, which do not have to be encrypted.

12. While the emphasis in this paper is on cryptography for communication, two important benefits of cryptography for storage need to be mentioned. One is that encryption can be very well done for part of the variables in a data set.<sup>12</sup> This allows that the remainder of the data set can be used by a wider audience. This is more convenient than the alternative, that these variables are split off and kept in a separate data set. Data set proliferation is already a nuisance, and the necessary record linkage is hard

<sup>10</sup> Protection against insiders (employees) taking confidential data out can only partly be reached by encryption: the relevant confidential data is usually small in size and can be printed on one sheet of paper. Short of body-searching employees before leaving a building, there is no other defence against this besides a good and shared work ethic.

<sup>11</sup> The need to keep Trojan horses out is derived from the first goal: keeping burglars out.

<sup>12</sup> For example Social Security Numbers, postal code + house number + date of birth. The encryption of these fields should *not* be performed symmetrically or in the same way throughout the whole organisation.

to guarantee over time. The other major benefit is that if the sensitive part of data sets are encrypted, the necessary access privileges for the “system-, operator-, backup-, supervisor- and support- tasks” are less prone to abuse.<sup>13</sup> These tasks require access to all (data) files, but rarely that the contents of the files can be understood. Some complication of encryption for storage is that provisions are needed if more than one person (or cryptologic entity) needs to access the data, or even access the data simultaneously.

13. Encryption for communications — where the information is decrypted almost instantaneously at the other end — needs frequently altered keys, even to the extent that for each session a ‘disposable key’ is generated. There needs to be some mechanism for key-exchange and the verification of the identity of the other party, but with the advent of public key cryptosystems (see below), this has been reduced to a manageable task. Unless a cryptologic algorithm has been broken — which in case of public, well researched algorithms is a rare event —, there is only limited damage if one session key is stolen — which is also a rare event, because it is not written down or kept. Still there are some risks that a person’s (secret) key is stolen, or that a person’s laptop is stolen. In the case of laptops, encryption for communication has to be combined with encryption for storage.<sup>14</sup> All in all, it can be said that the encryption of communication has matured to an extent, that it is not necessary to use private lines or even shielded lines, if the cryptologic techniques are properly applied.<sup>15</sup> This implies that also the (open) Internet and wireless communications can be used for transmitting sensitive information and for ‘remote login’.

## VI. Encrypted communication and gateways

14. The possibility of a ‘remote login’ session is such an important application, which is now usually lacking, that a special paragraph will be devoted to it. In an extreme, liberal variant, we suppose that we will allow a NSI employee to work from a mobile laptop on the central office LAN as if he was sitting at his desk. The connection may be initially by GSM (or regular phone) to an Internet Service Provider, and then to a special communications server ( $S_{EM}$ ) outside the LAN (*extra muros*) of the NSI. There is plenty of opportunity for eavesdropping (interception), and we will refrain from the possibility of ‘dial back’ or other identification based on telephone numbers.

15. If this  $S_{EM}$  and the laptop communicate using a protocol that is from begin (prompt) to end (after logout) protected by a cryptologic protocol, and from the  $S_{EM}$  all normal ‘login’ and terminal-programs and most internet programs are removed, this  $S_{EM}$  is hardened against internet attacks. First of all, the usual entries for Internet attacks are not present, second a normal crack would not come very far. Only an encrypted session can continue, so even ‘taking over’ an interrupted telephone call does not work. Even in order to specify a destination within a LAN, a session has to be encrypted. This  $S_{EM}$  communicates *only* with a special server within the LAN (*intra muros*:  $S_{IM}$ )<sup>16</sup>, likely with an additional protocol that ensure that no data in this stream can be added or altered. The  $S_{IM}$ , finally makes connections within the LAN.

---

<sup>13</sup> The people that perform system maintenance and back-up tasks, etc., are usually (selected to be) of a very reliable kind, but they carry privileges that are the target of less reliable people.

<sup>14</sup> For laptops with confidential information, not only storage encryption should be used, but also an easy to remove hardware piece – to be removed always when the laptop is not used – and some key memorised by the legitimate user.

<sup>15</sup> There exists a number of reliable and well-tested cryptographic algorithms. The weakest point is often the people that have to apply them properly.

<sup>16</sup> This construction of a special pair of servers is much like elaborate forms of firewalls. In both cases the forwarding (‘routing’) of traffic is not left to the operating system, but is performed entirely at a more stringent application level. A firewall is less secure, because it relies only on this mechanism., while the cryptologic protection described above means that no interception or trial and error attacks are effective.

16. The Internet community, which has been aware for a long time of the insufficient security aspects of Internet, has planned cryptographic security enhancement in Internet Protocol V 6,[6] which is upcoming, and in the SSH – secure shell – program.[5] that is available for Unix, Windows and some other systems.

17. The added security can easily outweigh the added risk of interception of the session and intruder attacks on this  $S_{EM}/S_{IM}$  combination. It is sufficient that we make the successful attack on a remote login session (much) less likely than that an outsider gains access to a NSI building and finds a logged-in, unguarded, terminal, or than the possibility that — how awful — an outsider talks, threatens, blackmails, bribes or otherwise coerces a NSI employee of supplying the information, or that — how absurd — an outsider thinks that the easiest way to gain access is to apply for certain jobs at NSIs.

## VII. Two families of cryptological systems

18. This paper does not describe cryptological techniques, but tries to delineate applications. A good overview of the ingredients and the state of the art in the *public* literature can be found in [2,4]. One technicality has so much influence, that it must be mentioned here: the distinction between *symmetric* (DES [4]) and *asymmetric* (RSA [4], PGP [8]) cryptosystems, more commonly but less precisely called *secret key* and *public key* cryptosystems,<sup>17</sup> resp. The asymmetric systems make the encryption and decryption a separate (but matched) process, each with its own key. Correspondents do not share a common (secret) key. This approach overcomes the cumbersome and vulnerable exchange of (secret) keys between correspondents, and is suitable if one has many correspondents. Even if there are thousands of information suppliers.[1–4,8] If a key is lost or stolen, the two correspondents cannot blame each other, because they each have their own secret key. This makes this asymmetric systems also attractive for communication between an employer (NSI) and employees [3]: they are each responsible for their own secret key.

## VIII. Several PC's on one desk top?

19. The use of several rings of security levels only works if the data are processed fully within their proper security compartment. This has important implications for how computing services within a NSI are organised. One method is that a desktop PC belongs to a fixed security level, the level that it is used for most of the time. To gain access to another security level, a user must have several PC's on his desk top, or at least have access to several PC's within walking distance. Another approach is to view the desktop as a keyboard, mouse and monitor only, from which the user logs in onto servers in a certain security ring, similar as we have described above with a SEM/SIM approach. Now the data are *not* processed on the user's PC, but on the server; we are almost back to the good old days of mainframes with terminals. Care must be taken that data cannot leak, on purpose or by negligence, to another security level, which makes that local storage should be prohibited.

20. A mixture of this approach is possible, with at the extreme end to consider all desk top PC's in the NSI's building in the same way as external laptops in the example above: all communication and sessions are encrypted (using strong authentication), local storage is encrypted appropriate to the current security class. A user can only work on a local machine if his 'dongle' or similar hardware key (smartcard) is inserted (and after he gives his personal password). From the same PC we can now access the servers with individual data and Internet, but not at the same time.

21. Paradoxically, we have gained now much flexibility by applying cryptological techniques in stead of physical techniques. In the terms of the introduction, we have matured from mediaeval castle to modern city.

---

<sup>17</sup> The asymmetric cryptosystems involve both a secret and a public part of a key.

## IX. Conclusions

22. We made a case for the following:

- The advent of cryptography is unavoidable, among other things because of mobile and wireless computing, teleworking, and EDI;
- Physical and social control can be augmented or partially replaced by cryptological = mathematical control. Cryptological control gives more flexibility in many respects;
- The range of security measures should be wide, and always ‘just appropriate’ for the protection goal;
- Each NSI should have a data security plan, involving some levels of confidentiality and security and further compartments within levels, with a controlled way of exchange between the levels. It should be specified what data classes belong at each level;
- Encryption of communication is relatively straightforward, and its security is sufficient to compare with current levels of security against unauthorised access;
- Asymmetric cryptosystems are preferred over symmetric;
- If we have solved the access problem for a roaming laptop, we can apply it to the office desktops, and gained much flexibility.

### *Literature*

- [1] D. Denning, 1982. *Cryptography and Data Security*. Addison-Wesley, Reading, MA.
- [2] J.W.P.F. Kardaun and L.C.R.J. Willenborg: *Cryptography for secure EDI. Netherlands Official Statistics*, 1997; **12**:16–24.
- [3] J.W.P.F. Kardaun and L.C.R.J. Willenborg, 1995, *Cryptological applications in Official Statistics*. Seminar on New Techniques and Technologies for Statistics, Bonn, Nov 20–22, p. 203–215.
- [4] B. Schneier, 1994, *Applied cryptography*, Wiley, New York.
- [5] SSH (Secure Shell) remote login program. <http://www.ssh.fi> and <http://www.ietf.org>
- [6] R. Stainov, 1997. *IpnG – Das Internet de nächsten Generation*. Bonn, International Thomson Publishing.
- [7] Voorschrift Informatiebeveiliging Rijksdienst 1994. (*Regulations about Information security for the national government 1994*)
- [8] P. Zimmerman, 1995. *The Official PGP’User’s Guide*. Cambridge, MIT Press.