Whose eyes on secret data?

A row in Britain over the Post Office's rights to inspect all data communications has died down, at least for the present. But recent attempts to stifle mathematical research into cryptography for data security suggest that data communicators, everywhere, are right to worry

Duncan Campbell
is a freelance technical writer

Systems for encrypting computer data, preventing unauthorised reception or interference with data in transit, are now coming into widespread use in Britain. New services like banks' cashpoints require that data on customer credit rating, and instructions to dispense money, stay secure. But it appears that there is no protection for users against Post Office demands to inspect what may be valuable commercial, or sensitive personal, data.

The Post Office Act 1969 granted the PO an "exclusive privilege" over all forms of telecommunications. In creating services for data transmission, the PO ruled that voice communications would not be allowed, and that third parties could not use the system. Otherwise its monopoly would be threatened. A specialist group of engineers now regularly monitors the 30-40 000 private data circuits in the UK, listening and checking messages to ensure that the rules are kept.

The problems became greater both with the arrival of computer networks which also passed messages between separate buildings but within a company, and with the availability of links to other computers on networks created by commercial agencies. The all-embracing powers of the Post Office Act left users in confusion.

Some of the confusion has now been removed. In May 1976 the PO published a General Licence which removed the aura of apparent illegality hanging over companies which used their private computer networks for sending messages from one terminal to another (*New Scientist*, vol 71, p 682).

In one sense, the licence merely recognised reality, and formally allowed the renters of private networks to do what they had been doing anyway. But it also spelled out forcefully, in paragraph 10, that the PO maintains rights to "monitor without further notice any message" and to "inspect any messages or records of messages". Clearly, this stated a right to inspect any secret computer data which were sent on a network. Users feared the licence empowered the Post Office—or "any person authorised in writing"—to demand the algorithms and keys to encryption systems designed to protect the data.

After a flurry of protest, the Post Office spelled out its interpretation. It wouldn't want to know details of encryption codes, provided it could inspect messages in an organisation's headquarters. So far, the Post Office has not apparently exercised these powers in any form, presumably because almost all data being transmitted are unencrypted and accessible to its normal monitoring checks on the lines. But users are unlikely to be happy while the PO still retains such dictatorial powers.

New data transmission services—in particular packet switched links now being introduced, in which blocks of data from different users are interleaved along main communication links—raise new problems of data security. These will presumably be monitored like the existing private data circuits. "The Post Office has made no assurances about the internal security of the data in all these services", according to data communications consultant David Hebditch, "I think that's disgraceful". He has had no answer to his questions about whether records of listings from monitoring are kept.

The Post Office rests on its legal powers, but told *New Scientist*, "Any inspection would be done by a PO servant. We would only ask for the log of messages switched. We've no interest in security codes." Unfortunately for users, the General Licence is still drafted in far wider terms.

Cash in electronic transit

Banks have been the first major UK users of data encryption systems. The international SWIFT transactions network uses encoders made by the Swiss cypher company, Gretag. Lloyds Bank is one of several to introduce cashpoint terminals, where a customer can order cash from a keyboard by presentation of a suitable magnetically encoded card

MESSAGE IN CLEAR UNENCODED FORMAT

YOU CAN'T BEAT SSIFATYPE SECURITY. FIRSTLY, TWO OPERATORS ARE THE MOST YOU NEED. SO ONLY THOSE TWO PEOPLE NEED TO HAVE ACCESS TO ANY GIVEN MESSAGE. SSIFATYPE DOES NOT NEED TO BE INSTALLED IN A SPECIAL COMMUNICATIONS ROOM. USE IT WHENEVER AND WHEREVER YOU LIKE - OFFICES, HOMES, HOTEL ROOMS, EVEN RADIO - LINKED CARS.

THERE'S NO NEED TO WORRY ABOUT TAPPED LINES EITHER - SSIFATYPES' INCREDIBLE 80 000 000 000 DIFFERENT CODES ARE VIRTUALLY UNBREAKABLE.

AT THE RECEIVING END, THERE'S NO NEED TO HAVE A DECODED HARD-COPY PRINT-OUT OF THE MESSAGEIF YOU DON'T REQUIRE IT - SO THERE'S NO WRITTEN RECORD OF A HIGH SECURITY MESSAGE. YET IF A HARD-COPY DECODED MESSAGE IS REQUIRED, SSIFATYPE CAN PROVIDE IT IN REAL TIME VERY EASILY.

SSIFATYPE MESSAGES ARE INSTANTLY READABLE DIRECT FROM THE SCREEN, IN PLAIN LANGUAGE.

MESSAGE IN ENCODED FORMAT

The SSiFATYPE, a commercially available, portable encrypting communications terminal marketed by Security Systems International. At the top is shown a message as the VDU screen reproduces it and, below, its encoded format

The revolution in cryptography

New developments in cryptography over the past two years may be a breakthrough to new kinds of secure systems. The new ideas, summarised by Diffie and Hellman in 1976 ('New Directions in Cryptography', *IEEE Transactions of Information Theory, IT-22, 6,* p 644, Nov 1976) rely on "one way" mathematical functions, and the possibility that both the enciphering system and the secret keys can be made totally public—so-called public-key cryptosystems, or cyphers.

One-way mathematical operations are not difficult to understand. To multiply together two numbers A and B is simple, resulting in a product C. To calculate A and B given C is far less simple. When A and B are prime numbers of the order of 10^{40}, factorisation would take millions of years. Even for large fast codebreaking computer systems, it is thought impossible, and even though it is known that C is the product of two large prime numbers, A and B are impossible to find. The mathematical operation is one-way.

The public key cipher uses the one-way properties of the encrypting procedure to gain security. Anyone wishing messages to be sent securely to them can publish their algorithm for encryption, together with the keys they are using. They also know, having selected the keys, a short cut to decrypting the message in reasonable time. But an eavesdropper, even though he knows the full details of the encryption process, is computationally unable to invert the one-way function to decrypt the ciphertext.

Examples of such systems have now been published, although they are inhibited by NSA pressure and patent applications. The best known so far, from a group at MIT led by Ronald Rivest, uses the problem of factorising large primes. A message for transmission is converted into numerical form as M. The encrypted message is calculated by the expression M^S (modulo R). R is the product of two large prime numbers, each greater than at least 10^{40}, and S may be around 10^4. (Modulo R means that the expression is divided by R and the remainder taken). This produces a coded numerical message, C.

The authorised recipient of these messages has publicised his "public key", the numbers R and S. But only he knows the prime factors of R. With this knowledge, the encrypted message can be quickly rendered into plain text by a similar function C^T (modulo R). But calculation of the vital decrypting factor, T, is only possible if you know the prime factors of R. And only the person who published the key will thus be able to understand such messages. (Readers can test this technique; take $S=3$, $R=55$, and $T=7$, for trial messages.)

With one exception, it is not possible to prove that a cipher is totally secure. So its security value is certified by employing every possible technique to break it, and if you fail, certifying it as secure.

This could take some time, according to Hellman, because the whole concept is very new. He hopes, but doubts, that agencies like NSA might expose any flaws before a system came into general use. So far, however, no flaws have been found in Rivest's prime-number system.

A related development of public key ciphers allows the automatic verification of the source of a message. The one-way function allows the sender to send a "decrypted" message using the inverse of the one-way function which only he knows. His public key can then be used to "encrypt" the message, to give cleartext which could only have come from him. In this way, public key ciphers could enable highly secure digital "signatures" to be sent to, say, authorise electronic transfer of funds. *D.C.*

and the entry of a secret validation number. He can then automatically withdraw money from his account—the terminal interrogates a central computer which then sends an instruction authorising payment. Encryption of the signals is clearly necessary—otherwise anyone intercepting the line with a standard data modem could send instructions to the terminal to dispense a stream of £5 notes to a waiting accomplice.

Lloyds uses an IBM 3614 cashpoint which encodes data using the recently adopted US Data Encryption Standard (DES). All US agencies wanting to encrypt non-classified data are now obliged by law to use the DES, and a wide range of commercial products is becoming available incorporating the standard for commercial use.

A mathematical controversy

But the actual security of the DES, originally developed by IBM but available for use free by others, is at the centre of a mathematical controversy in the United States. It seems certain that the US intelligence community—and in particular the National Security Agency (NSA) which intercepts overseas and foreign communications—has forced the adoption of a standard for commercial, etc, use which is just below the limit of "crackability". When the standard comes into general use, US intelligence could decipher secret data, using a computer which might require a parallel array of up to a million special-purpose processors and cost over $20 million. Although no commercial rival would be likely to afford such a development to steal data, foreign governments such as the USSR and the UK could. Some US corporations have decided not to use the standard, although it is generally reckoned to be better than other commercially available techniques.

The DES enciphering technique recommended by the US National Bureau of Standards (NBS) is based on enciphering a 64-bit (binary digit) block of data using a *key*, also of 64 bits (although 8 are only error safeguards, leaving 56 effective bits). The concept of a key is fundamental in cryptography; a standard cipher uses a mathematical algorithm to encode the "plaintext" (input message) into "ciphertext" (which, one hopes, is an incomprehensible output). At the receiving end, the ciphertext is converted back to plaintext by an inverse algorithm using the same key.

Designers of ciphers always have to assume that the secrets of their algorithm may be discovered by an eavesdropper—in military use, an enemy may capture a coding machine. So security lies in making it impossible for deciphering to take place unless a secret key is also known. A fundamental problem in cryptography is still the distribution of the secret keys, which are frequently changed. Now, new kinds of cipher may revolutionise this aspect (see box).

The Data Encryption Standard performs a complex 16-cycle series of permutations and substitutions on the input 64-bit block to generate the enciphered output. One of the key features of the system is a series of so-called "S-Boxes", which should make it much more secure at least than existing commercial systems.

Permutation of the key and plaintext bits is in effect a juggling operation, and is mathematically *linear* as are the other operations in the DES cipher not involving the S-Boxes. (S is for substitution.) If a cipher uses linear techniques, security is drastically reduced. But the S-Boxes eliminate any linearity in DES so that the only known way to crack it is the "brute force" technique. This requires the decrypter to get hold of the plaintext corresponding to a given ciphertext, in the hope of discovering the key, and hence the contents of other messages sent with the same key. This may happen if, for example, parts of a secret message are subsequently declassified or "leaked".

There are 2^{56} possible keys in DES, which is roughly 7×10^{16}. Even if a million keys were tested every second, the "brute force" method would still take an impractical 3000 years to find the right key. But if there were any linearities throughout the algorithm, the problem would be reduced to solving 64 simultaneous equations—a matter of a few seconds.

The non-linear substitutions in the S-Boxes are the real

strength of DES. But a group of computer scientists and mathematicians has claimed that DES is crackable ultimately. And, they claim, the S-Boxes contain "suspicious" mathematical structures "close to linearity". One of the specialists, Professor Martin Hellman of Stanford University told *New Scientist* that he had performed tests to see if other S-Boxes, which he had derived experimentally, also possessed such structures. These had indicated that the structures in the DES S-Boxes had been "built in". He and his colleagues had asked IBM to publish the work done in designing the S-Boxes. But the NSA then told IBM to classify the papers, successfully. Hellman admits that no one has yet shown how to use the "nearly linear" structures to get results quicker than by brute force. But it is vital to users of DES to know the strength of the encryption standard. Instead, important material and studies have been withheld or classified.

Brute force control

More significantly still, NSA has apparently ensured that the brute force approach is just within its, if no one else's reach. IBM obliquely admits that the key length of 56 bits was selected at NSA's request—a longer key length and it would not have been possible to export the equipment, curtailing substantial international sales. NSA controls the granting of licences to export crytographic equipment—as well as deciphering foreign communications around the world.

Hellman and a colleague, Whitfield Diffie, believe that a DES-cracking computer could be built, using a million special-purpose chips each capable of trying one million keys every second. On average, a solution would be found within 12 hours, and would cost $5000. To build such a machine, they estimate, would cost $20 million. Yet to resist such an attack on DES would have been simple—doubling the key length would make brute force quite impossible now or in the future, as the number of keys to be searched would be multiplied by a further 2^{56}. NBS and others claim, however, that Diffie and Hellman have seriously underestimated the costs of such a code-breaking supercomputer.

More recent controversy has centred on the NSA's apparent attempts to stifle further open development of new ciphers, such as the "public key" arrangement devised by Diffie and Hellman. A cryptology symposium was arranged by the US Institute of Electrical and Electronic Engineers (IEEE) in New York last October. But some months before the symposium, the IEEE received a mysterious letter from a J. A. Meyer of Bethesda, Maryland, which alleged that publication and export of papers on cryptology would violate the Munitions Control Act, unless clearances were first obtained from the government. This would give NSA effective control over the publication of discoveries of any scientist in the Information Theory Group of the IEEE. The Meyer letter singled out some overseas seminars and publications by Hellman.

Research by the US journal *Science* revealed the unsurprising fact that Meyer was employed by the NSA. NSA denied prompting Meyer, but would comment no further. Nevertheless, the seminar proceeded, although Hellman and others undertook to protect students from possible legal action by presenting their papers for them. Earlier in February, Hellman told *New Scientist* that NSA "harassment" had apparently abated, and that a Stanford University cryptography course would be run in April.

In Britain, there are few specialists in cryptography other than NSA's partner agency, Government Communications Headquarters (GCHQ), a department of the Foreign Office. The National Physical Laboratory recently commenced a programme of research in civil cryptography, which is now likely to be broken up unless strong industrial or other support is apparent. The government's National Computing Centre (NCC) organised a first seminar on data encryption last autumn, by Don Bell and Donald Davies of NPL. (NPL Report COM-98, January 1978.)

Last summer, the British Computer Society circulated draft proposals on encryption data standards for Britain. They suggest four levels of security, two much lower than DES, but at least one being more secure. The chairman of the Society's Standards Committee, Frank Taylor of NCC, is unhappy about the safety of adopting the US standard under commercial pressure. "Europe should go its own way on this," he said. Taylor is hoping that the EEC may fund the development of a suitable European standard. Other British specialists are worried about the varying BCS proposals, however, claiming that once a good secure standard is developed, and microcircuits to implement it are in quantity production, there would be no worthwhile saving in adopting a lower level of security.

There are many similarities between the interests of British and US codebreaking agencies which may in future bring conflicts between them and scientists in Britain. NSA admits to monitoring all US overseas telephone, telex and other communications, and the same has been reported to happen in Britain, at least to private cables. An Export Control Order parallels the US act cited in Meyer's letter to IEEE scientists which, in partnership with the Official Secrets Act, could censor civil cryptographic research. British manufacturers of cryptographic equipment acknowledge, too, that equipment for export is subject to GCHQ approval—which, like NSA, is unlikely to approve for export equipment whose codes it cannot break. If this attitude continues, and development of a new British or European standard mirrors the row in the US, data communicators may well complain about perfidious Albion. □