causes that might help to advance science, too inhibited (by their constitution) even from having views on many important matters and yet, paradoxically, whimish — too much inclined to react unpredictably to changing circumstances and changing needs.

This complaint, harsh though it may seem to the devoted people who work hard at making the unprofessional societies function, is, nevertheless, quite fair. For what, in the past few years, have these societies done to help resolve some of the important problems in their declared fields of interest? Issues such as the hazards (if any) of genetic manipulation, public policy on nuclear power and even public policy towards the universities, may have been mentioned at the annual meetings of the British and American societies, but neither organization have used the diversity of its membership hammer out possible solutions. Providing a forum for opposing views on such issues is much easier, but also much less valuable, than attempting to resolve conflicts of opinion in ways that will carry conviction in and outside the scientific profession. Providing opportunities at the annual meetings for well known people to put their well known views on grand subjects such as "Energy", "Population" or "Food" is similarly a largely unproductive enterprise. So how should the unprofessional societies put their houses in order? The most urgent need is that they find a way of tackling problems that at present impede the advancement of science — for one example see below. Organizations that cannot constitutionally have a view on issues such as the organization of research or the safety of nuclear power (and which may not even have studied them) can no longer claim to assist the advancement of science. The unprofessional societies have also been known to make links with their unprofessional constituencies — school teachers, industrial scientists and the like; this, however, is a task that could and should be tackled. (Both the Americans and the British societies will protest that many of their members are teachers, but that is not the same thing.) To accomplish these and other goals will undoubtedly require that the organizations themselves should change, perhaps substantially, but there is no reason to suppose that the change need be so drastic that the valuable aspects of what they do at present would be jeopardized.

Public-key cryptography muddle

The National Science Foundation and the National Security Agency in the United States are making a frightful muddle for themselves by their new policies on academic research in cryptography, made public last week. This is not the first time that there has been trouble between academic cryptographers and the United States Intelligence Agencies. Four years ago there was a minor storm when it turned out that an official of the security agency had written to the (American) Institute of Electrical and Electronic Engineers suggesting that articles on the design of new codes should not be published in the interests of security. Eventually, the row died down only when the official concerned was said to have written in a personal capacity. The latest development is more serious. The National Science Foundation and the National Security Agency have apparently reached an understanding on the processing of future research grant applications in cryptography. The National Security Agency will, it seems, now see all applications in the field that may be sent to the National Science Foundation and will, if it thinks fit, back good projects with its own funds. One consequence may be that more funds are available for research cryptography, which might lift the spirits of the academics in this field. Another is that the National Security Agency may attach to research grants the condition that the results should not be published without prior agreement from the intelligence people, a prospect that will dismay academics.

Is all this, then, a sinister plot to muzzle scientific research in the absence of legal instruments or 'classified' data as in the years immediately after the war? This is one reading of the new arrangement. Whatever the objectives of the National Security Agency the most likely consequence of the Washington agreement will be to make a monkey of the two partners, the National Science Foundation and the National Security Agency. The pace of academic research in this novel field is unlikely to be impeded. Publication, it is hoped, will continue without hindrance. And nobody's national security will be endangered.

What offends the intelligence people is the whole concept of public-key cryptography. They earnestly wish that it had never been invented. The notion is simply that of an unsymmetrical coding system, one in which it is not possible to infer the key for decoding a message in cypher from a knowledge of the rule by which coded messages are themselves produced from ordinary text. Consequently, with these novel codes, instructions for turning messages into codes could be published in the newspapers and it would, nevertheless, be impossible for somebody intercepting a coded message to decipher its meaning. For most people, the difficulty is that of understanding how there can be codes whose writing and reading keys cannot instantly be inferred one from the other. The demonstration theorem required to dispell this scepticism has now been amply proved, most conspicuously by Professor L. J. Adelman of the Massachusetts Institute of Technology. The feasibility of the new coding system depends on the power of their computers now in service, which can use exceedingly complicated rules to turn ordinary text into coded messages. The basis of public-key cryptography is that the unpublished reading key cannot be inferred from the publishable writing key except with such a gigantic commitment of computer power that nobody in his senses would attempt the job.

Plainly, the National Security Agency is unconvinced. How can it be, these men in dark glasses whisper to each other, that a person can write in a code but be unable to decipher his own coded message? Somebody, they suspect, is pulling their legs. And they also appear to have forgotten that unsymmetrical coding systems, like those now being developed, are precisely the instruments needed to make commercial as well as military computer systems private and immune to espionage. Hitherto, there has been no means by which, for example, banks using public telex systems to transmit confidential information can have done so except by the old-fashioned methods of classical cryptography in which the intended recipient of a message is first provided with a secret code book. With the new codes, in principle at least, the writing key can be made freely available and the recipient of coded messages, the only one with access to the reading key, will be the only one able to decipher. The same techniques can and no doubt will be used to safeguard the privacy of personal data stored in central computing systems. The commercial importance of developments such as these is so self evident and so great that now that the potential value of public-key cryptography is appreciated, nothing will prevent the commercial computer companies from working hard towards the development of practical systems. Even if funds for research are not forthcoming from the National Science Foundation, there will no doubt be eager sponsors for academic research in the field of cryptography among the potential commercial users. For many academics however, the commercial sponsorship of research may be as irksome as the possibility that publication could be restricted — as the National Security Agency may choose to do. In practice, however, the sums of money needed in these fields are not large. The importance of free publication is self evident; quite apart from the intrinsic value of the new coded system, this is also a time when interest in the new field of cryptography needs to be stimulated. Is this not eminently a field in which private foundations should step in?