Pharmaceuticals trio a popular choice for Nobel awards

London

If this year's Nobel prize in Physiology or Medicine was intended to cover the water-front of drug discovery, it could hardly have been better chosen. Sir James Black, the 62-year-old British winner, is credited with the discovery of drugs that block β -adrenergic receptors and histamine H₂ receptors, while the pair of US winners, 70-year old Gertrude Elion and 83-year old George Hitchings, discovered inhibitors of purine and pyrimidine metabolism, which have been of value in the treatment of leukaemia, malaria, gout, organ transplantation and bacterial infections.

Black spent 12 years in university posts before switching to the pharmaceutical industry, and has oscillated between the two ever since. In his first industrial post, as senior pharmacologist with Imperial Chemicals Industries, Black together with William Duncan developed propranolol, the first 'beta blocker'. Numerous drugs of this type are used in the treatment of angina and hypertension.

Propranolol was produced in 1964, the year Black and Duncan joined Smith Kline and French Laboratories to apply to histamine receptors the approach that had produced beta blockers. "About 700 compounds have been synthesized and tested", said their 1972 paper that announced the prototype histamine H₂ antagonist, burimamide (*Nature* **236**, 385; 1972). The most successful of the company's subsequent H₂ antagonists has been cimetidine (Tagamet), which is widely used in the treatment of peptic ulcers.

In 1973, Black left industry for the University of London, but by 1977 he was ready to return. Smith, Kline and French beckoned him to the United States, but a last minute bid kept Black in Britain. He was director of therapeutic research for Wellcome Research Laboratories until 1984, since when he has been back in London University at King's College Hospital Hospital Medical School.

Wellcome employed the other two prize winners from the mid-1940s until their semi-retirement. One result is their citation as co-inventors on 18 patents for purine and pyrimidine metabolites. In the words of a colleague, "they defined and delineated with unusual ingenuity the pathways of purine and pyrimidine metabolism".

Hitchings worked on both aspects, while Elion concentrated on the pyrimidines. Among the first drugs that emerged were 6-mercaptopurine and thioguanine, both active against leukaemia, and pyrimethamine (Daraprim) and trimethoprim, both inhibitors of dihydrofolate

reductase and used as antimalarials. Trimethoprim, usually in conjunction with a sulphonamide, is also a much-used antibiotic.

More recently, Hitchings and Elion developed azathioprine (Imuran), the immunosuppressive drug that has probably been used more than any others to decrease the rate of rejection of transplanted organs, and allopurinol, the xanthine oxidase inhibitor that is used in the treat-

ment of gout and kidney stones. While their citation also mentions acyclovir, it was more the anti-metabolite philosophy of Elion and Hitchings than their direct input that produced this recent anti-herpes drug.

While the rumour-mongers were firmly tipping oncogenes or retrovirus, perhaps including the human immunodeficiency virus, as the topics that would provide the winners of this year's prize, the Nobel Committee has opted for "important principles for drug treatment", and has chosen a trio whose recognition was, in the opinion of many pharmacologists, long overdue.

Peter Newmark

Numbers game is of prime importance to spies

Berkeley

By using electronic mail networks to link hundreds of computers an international team of computer scientists has succeeded in factoring a 100-digit number into two large prime factors. This task was until recently thought impossible because of the massive amount of expensive computer time needed — up to half a year on a Cray supercomputer.

The achievement has special signifi-

cance for some professions, because it could make it easier for spies to break code systems. A common form of encryption relies for its security on the difficulty of factoring very large numbers. "People designing keys should be careful", said project co-organizer Arjen Lenstra, of the University of Chicago, "because there is much more computer power around than they realize". The technological advance that put the problem within reach was made in 1985 when Robert Silverman of Mitre Corporation in Bedford, Massachusetts, found a means of breaking up the factorization algorithm so it could be run in parallel, on a network of computers. Though the calculation used no new mathematical approaches, the organizers say it shows the ease of parallel computing through electronic mail.

Mark Manasse, of the Digital Equipment Corporation's Systems Research

Center in Palo Alto, California, said he and Lenstra began the project to explore the power of loosely-coupled distributed processing between machines that "barely know each other". The factorization algorithm was broken down to parts and sent to each of 400 participating computers in Holland, the United States and Australia, which then reported back to Manasse daily, and supplied enough data for him to solve the problem in less than four weeks.

Any computer that uses C language could participate, and the network included micro-VAXs, Suns, and a Cray. The network "didn't spend one single penny for computer time", said Lenstra, because the computers were devoted to the problem only during time when they would otherwise have been idle. While only 30 per cent of the computers working on the 100-digit number were from outside Digital's Palo Alto facility, the outside arm of the project is growing, and Manasse expects to amass 5,000 to 20,000 computers, enabling the network to factor larger numbers.

Lenstra said the experiment may have increased the safe threshold for the popular RSA code system, in which codes based on large numbers of 100 or more digits can be broken by anyone able to factor the number. Loosely coupled computer networks may bring factorization within the reach of would-be code breakers.

Silverman doubts that the DEC experiment has given cryptographers anything to worry about, however. RSA system users have been advised for some time to base their codes on numbers of at least 150 digits, he said, a size that Lenstra and Manasse agree remains unfactorable with currently-known algorithms. Since each addition of three digits doubles the computing power necessary to factor the number, a 150-digit number would require over 100,000 times the computing power for a 100-digit number. Marcia Barinaga