change." He told *Science* that "population geneticists simply haven't addressed the question of stasis" and that "the genetics of developmental buffering is largely unknown."

J. S. Jones, a biologist from University College London, comments on Williamson's paper in the same issue of *Nature*, saying that to a geneticist, 50,000 years is a very long time. "It is equivalent of perhaps a thousand years in a *Drosophila* population cage, six thousand years in a mouse selection experiment, or 40,000 years when dealing with domestic animals such as dogs." Conventional selection can, he states, "accomplish dramatic genetic changes in morphology much more quickly than this."

Williamson suggests that Jones has missed two key points. First, that stasis is an important aspect of evolutionary patterns. As Hallam puts it, "you have to account for long periods of stasis; then suddenly it all changes." The second concerns the manner in which the rapid transition occurs. "It's not just that things change quickly," says Williamson, "no one is arguing about that. The important point is that the morphological variance rises sharply in the intermediate population." This, he suggests, is not seen as a necessary aspect of conventional selection.

Francisco Ayala of the University of California at Davis believes that the differences between paleontologists and population geneticists are, unlike the gaps in the fossil record, more apparent than real. "The disagreement between the two groups is unfortunate," he says.

Evolution is not a continuous process, says Ayala, and he cites Theodosius Dobzhansky and George Gaylord Simpson as two important voices in evolutionary biology who long ago said as much. "I have no problem with punctuated equilibrium," he says. "There's plenty of evidence for it. But you have to remember that large evolutionary steps can be accomplished by a series of small changes. People have emphasized gradual change because big steps rarely happen."

Ayala insists that geneticists have for a long time been aware of developmental homeostasis as an important influence on evolutionary change, and he cites C. H. Waddington's writings in the first half of this century as a prime source of insight into this issue. "In recent times," he admits, "it has been rather ignored, because we have no way to deal with it at the molecular level."—ROGER LEWIN

Cryptographers Gather to Discuss Research

Analyses of how to break codes and new ways to use codes were featured at the meeting

On 24 to 26 August, about 100 computer scientists, electrical engineers, mathematicians, and "cryppies," as National Security Agency cryptographers are called, gathered at the University of California at Santa Barbara, for Crypto 81, a workshop on current research in cryptography.

The discussions at Crypto 81 included old issues, such as NSA's concerns about public cryptography research, and new developments, such as innovative ways to use electronic mail. But, as might be expected, the focus of the meeting was on how to make and use codes rather than on how to break them. Code-breaking techniques are notoriously difficult to discover. Yet it is critically important to study code-breaking because the only way to learn if codes are secure is to have experienced people try to break them.

The codes used today are so good that the only obvious ways to break them are by brute force, by trying every possible cryptographic key to break the code. Among the few conference participants who focused on brute force attacks on codes were Martin Hellman and Hamid Amirazizi of Stanford University.

Hellman and Amirazizi began by considering the ways a brute force attack could be accomplished. At one extreme is what Hellman calls an exhaustive search—simply ask a computer to calculate every possible key to a code until the code is broken. But, for modern codes such as the DES, a code designed by IBM for protecting sensitive but nonclassified government information, an exhaustive search of all possible keys could easily take 30 years, even with the fastest computers. At the other extreme is "table lookup"—make up a table containing every possible key for a code. Then, given an encoded message, the computer would just look up the appropriate key and break the code. However, the table lookup approach can require an enormous amount of computer memory, as much as 10^{12} bits.

Hellman and Amirazizi decided to see what happens if they compromise. They analyzed the difficulty of breaking a code by brute force using computer calculations of some keys, computer memory of some keys, and processors so that calculations can be performed in parallel and so that the computer attempts to break several codes at once. They found a logarithmic relationship between the cost of an exhaustive search (which they call the cost of a solution) and the cost of a table lookup (which they call the cost of a machine). As a result, each time the cost of the machine is doubled, four times as many solutions can be obtained each day. Agencies, such as the NSA, that are in the business of breaking codes might then find it worthwhile to invest in expensive machines. Says Hellman, "You have an economy of scale in cryptanalysis. Snoopy people get their solutions cheap. The moral is that anyone building a cryptosystem should allow lots of safety margin."

As Hellman points out, this sort of analysis extends beyond the brute force breaking of codes. It can also be used in the design of very large-scale integrated circuits where the problem is to make the most-effective use of a large number of gates. And it can be used to determine when resources such as large special-purpose computers may become cost-effective for a network of users.

Many of the talks at Crypto 81 focused on electronic mail because it is of the utmost importance that it be protected by good codes. Otherwise, because eavesdropping is so easy, electronic letters would be more like postcards.

If electronic mail is to replace conventional mail, there must be equivalents of certified letters and contract signing. This is a problem that Manuel Blum of the University of California at Berkeley has worked on and, as he reported at the conference, finally solved.

Electronic certified mail and contract signing would have a number of immediate uses. For example, companies buy

0036-8075/81/1106-0646$01.00/0

oil on the spot market where prices change daily. If they could sign contracts electronically, it would not be necessary to have a representative physically present in foreign countries to conclude a deal.

The possibilities for electronic certified mail and electronic contract signing are based on a discovery by Michael Rabin of the Hebrew University of Jerusalem of what he calls the "oblivious transfer." With this system, a person can transfer a prime number to a recipient in such a way that there is a 50–50 chance that the transfer is successful, but the sender does not know whether he succeeds. [The way it works is that person A sends person B a number n that is the product of two large primes. Person B picks a number x from the set 1, 2, . . . n-1 and sends x^2 (mod n) to A. A knows the factors of n and can use them to find a square root of x^2 (mod n). There are four square roots, two of which give away the factors of n. A sends B one of the square roots and so there is a 50–50 chance that B will get the information he needs to factor n. If the square root is one B wants, he adds it to x and takes the greatest common divisor of the sum and n. The result is a prime factor of n.]

To send certified mail, according to Blum, the sender makes up ten numbers, each of which is a product of two large primes. He then imbeds the mail in the ten numbers in such a way that the recipient can read his mail only if he can factor each of the ten numbers. Then comes a sequence of "oblivious transfers." The recipient requests each of the ten numbers in order and the sender obliviously transfers them one at a time. Since, in each case, there is a 50 percent chance that the number is transferred, the recipient will end up with, on the average, five of the ten numbers he needs. He then repeats his request for each of the ten numbers and the sender transfers them again. After this the recipient will probably have seven or eight of the ten numbers.

The recipient keeps requesting the ten numbers and the sender keeps transferring them until the recipient has them all. It will probably take three or four of these sequences of "oblivious transfers," according to Blum. The sender's receipt is his requests for the numbers, and this receipt is, in fact, a description of the mail that was sent.

Contract signing, Blum explains, is equivalent, in this scheme, to sending certified mail. Person A would send a contract to a cosigner B, along with a clause saying that the contract is good only if B has the contract and a receipt for sending the identical contract to A. Both A and B, then, would have the contract and a receipt that they sent the contract to each other. The contract and the receipt would constitute a signature.

One of the problems cryptographers are having, according to the meeting participants, is that the market is sluggish for cryptographic equipment. Despite the extreme vulnerability of electronic communications systems, many users are reluctant to invest in cryptographic protection. Michael Nye of Market Consultants International in Hagerstown, Maryland, said, "Most of the domestic vendors [of cryptographic equipment] are quite literally starving to death and even some of the big boys in the business have gotten out."

A number of the meeting participants said that although the ideas and technology for cryptographic protection are ahead of market demands, this situation should change. At the very least, with the current explosion of research in cryptography, there should be plenty of product ideas for future users.

—GINA BARI KOLATA

Buying Time for "Blue Babies"

A new drug that offers fresh hope for "blue babies" and other infants with rare congenital heart defects was approved by the U.S. Food and Drug Administration on 21 October. The drug provides an alternative pathway for oxygenating the blood of such infants and buys time to recover strength before surgery to correct the heart defect.

The drug, developed by The Upjohn Company of Kalamazoo, Michigan, is Prostin VR, also known as prostaglandin E_1 (PGE_1). It is most useful for infants who have a defect or blockage in their hearts that prevents normal flow of blood from the heart to the lungs. The blood is thus not oxygenated adequately, the infant has trouble breathing, and its skin takes on a blueish cast. Without treatment, nearly all these babies die during the first month after birth, many in the first week. Before the advent of the new drug, physicians had little choice but to operate as soon as possible after the defect was detected to prevent further deterioration. Many of the infants were so weak and sick, however, that fully 70 percent of them did not survive the operation. Today, with use of a prostaglandin and refinements in surgical technique, that figure is down to about 35 percent.

Newborn babies have a special blood vessel near the heart known as the ductus arteriosis; it connects the aortic arch to the pulmonary artery. In the fetus, this vessel serves to bypass the nonfunctioning lungs. Normally, the ductus arteriosis begins to close just after birth, but if it can be kept open, it provides a "shortcut" by which blood can be pumped from the heart through the aorta to the lungs. PGE_1 provides a means to keep it open.

In 1967, Flavio Cocceani and Peter M. Olley of the Hospital for Sick Children in Montreal observed that PGE_1 is present in umbilical cord blood vessels. They subsequently observed that it could be used to keep the ductus arteriosis open in newborn lambs, an observation confirmed in calves by Michael B. Starling of the University of Aukland in New Zealand. Starling first used PGE_1 successfully to treat a blue baby, followed shortly thereafter by Cocceani and Olley. Since 1976 Upjohn has been sponsoring tests of the substance in a number of children's hospitals around the United States.

"The drug buys us some very critical time," says Alan B. Lewis of the Children's Hospital Medical Center in Los Angeles. Treatment is generally begun as soon as the defect is discovered, allowing the operation to be scheduled 24 to 36 hours later. "Their color improves," notes Lewis. "Their oxygenation improves. We can stabilize the baby, provide time for the baby's body to correct the many metabolic and circulatory abnormalities that have developed over the time that the ductus has been closing."

That first operation is usually a palliative procedure to provide a more stable alternative route for blood to reach the lungs, and the heart defect itself is generally corrected in later operations. Scientists at Upjohn estimate that only four out of every 10,000 newborn babies might benefit from the drug. Even so, that is about 1500 of the 3.6 million babies born in the United States each year.—THOMAS H. MAUGH II

0036-8075/81/1106-0647$01.00/0