lute alcohol in an hour) have fetal wastage and offspring with decreased body weights, growth retardation, and behavioral aberrations resembling hyperactivity and learning disorders. However, says Abel, with animals there are definite threshold effects. When pregnant animals are intoxicated each day to a level less than 100 milligrams of alcohol per kilogram of body weight, there is no apparent effect on their offspring. When they are intoxicated to a level of 100 to 150 milligrams of alcohol per kilogram, their offspring weigh less at birth but later catch up in weight.

Why, then, in light of the equivocal evidence that anything other than heavy drinking during pregnancy is harmful, did the NIAAA decide to recommend no drinking at all? "The key science behind the decision is based on the fact that at the moment we don't know a safe level of drinking," says NIAAA director DeLuca. Yet, a number of scientists ask who the NIAAA's message is going to help. Says Sokol, "The 95 percent of women who probably will not experience any effect from their drinking have been warned. The 5 percent whom we know may have adversely affected infants are not helped by the advice. That is the group that really needs study and treatment." Says Kline, "Neither the birth weight finding nor the spontaneous abortion finding is so secure that women should feel guilty if they take a drink. As scientists, I don't think any of us believe that a little bit of alcohol causes these effects."—GINA BARI KOLATA

No Gap Here in the Fossil Record

Fluctuations in the history of an African lake have trapped the detailed steps in species evolution

Peter Williamson, a paleontologist at the Museum of Comparative Zoology, Harvard University, has just reported the first detailed documented evolution of one species into another, as revealed by the fossil record.* This new evidence, which comes from a series of fossil mollusk species near Lake Turkana in northern Kenya, has important bearings on the current discussion of the mechanisms that shape the pattern of evolutionary change.

The floodplain and delta deposits near the lake are extensive and clearly stratified. They therefore offer a rare opportunity to follow the periodic morphological changes in fossil species over relatively short periods. Added to this, the lake basin is virtually a closed system so that ecological and evolutionary events are to some degree self-contained. Anthony Hallam, a paleontologist at the University of Birmingham, England, describes the material available there as "the nearest thing you could get to an evolutionary experiment."

Williamson examined 3300 fossils from 13 different species of the lake snails, through a depth of 400 meters of sediment. Using selected morphological criteria, he traced the changes in these species over several million years. "The most immediate impression is the tremendous morphological stasis," says Williamson. "Some species still live in the lake today looking exactly as they did several million years ago," he observed in an interview with *Science*.

The most interesting observation comes at two points in geological history when the lake level dropped sharply. When this happened, all the species that Williamson studied underwent a brief period of change, at the end of which time clearly identifiable progeny species were established. By brief here is meant something between 5,000 and 50,000 years. "Compared with the millions of years during which we see complete morphological stasis for these organisms, 50,000 years is a brief period in which a new species arises," says Williamson. In his *Nature* paper Williamson writes that the pattern he sees "conforms to the punctuated equilibrium model" of evolutionary change.

The significance of the coincidence of the rise of new species with major regressions in the lake is, says Williamson, that the organisms "in the basin are likely to have been both isolated and under [environmental] stress." This is consistent with Ernst Mayr's classic 1954 paper on speciation, which Williamson paraphrases in the following way: "Mayr's model considers that homeostatic mechanisms and gene flow prohibit significant evolutionary change in large panmictic species populations, but in small, stressed, geographically isolated populations, homeostatic mechanisms break down during 'genetic revolution' and rapid evolution may ensue."

Paleontologists have known for a long time that new species appear to come into the fossil record abruptly, with no intermediates between the parental and progeny forms being apparent. There are two explanations for this. First, as Mayr suggests, new species arise in small peripheral populations and their apparently sudden occurrence in the fossil record coincides with their reinvasion of the ancestral range. Second, the transition period is very short compared with the time resolution that obtains in much of the fossil record, and the "instant" of speciation may therefore be missed.

In the case that Williamson describes the instant is not missed: it is documented with intermediates along the path from the old species to the new ones. "Williamson finds what we all find, but his data are so much better," comments Hallam.

At least as important as a record of intermediate forms, says Williamson, is a demonstration that, during the transition, the morphological variation of the species increases markedly. "For most of a species' lifetime, the genetic variation in individuals is to some extent buffered in embryological development so that the adult phenotype is relatively constant," he says. "When the population is isolated and under stress, buffering breaks down, and the phenotypic variance rises dramatically. It settles down again later, as a new species is established."

When the lake rose again it was no longer cut off from other lake systems in the continent, and the ancestral species returned to Turkana from elsewhere. This transgression of the lake coincides with an abrupt disappearance of the new species from the fossil record. "Mayr considers this pattern of events to be the common fate of new species in geographical isolates," says Williamson.

Williamson concludes his paper by suggesting that "speciation is a qualitatively different phenomenon from gradual, intraspecific microevolutionary

Nature (London) 293, 437 (1981).

0036-8075/81/1106-0645$01.00/0

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. Codebreaking 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