disrupted many lives. In Times Beach 800 families ponder their future finances and health. Judy Piatt sold her horse arena and now rents a few mobile homes, generating income that barely keeps up the medical bills that she says stem from her family's exposure to dioxin. Six families from the Minker-Stout site are waiting to return to their homes. Russell Bliss is the target of several lawsuits for his involvement with the oil spraying.

Lafser wrote in a recent lengthy report to Governor Bond, detailing the history of dioxin in the state. "Overall," he said, "the history shows the clear need for statutes which were developed in the later part of the 1970's and early 1980's. . . . Unfortunately, these statutes were not enacted in time to prevent these problems."—**MARJORIE SUN**

Flaws Found in Popular Code

The Data Encryption Standard has "weak" keys which may make the code easier to crack

A coding system that government agencies are required to use to protect documents classified "confidential" may be relatively easy to break, according to several cryptography experts. The system, known as the Data Encryption Standard (DES), is the only coding system certified secure by the National Security Agency (NSA) and it is widely used in the U.S. banking industry.

The system, which was designed in the early 1970's by IBM, has always been controversial. Critics charged several years ago that it could be broken with the aid of sophisticated computer technology, but the new findings suggest that it may be even more vulnerable than previously realized.

The original objection to the DES—and one that still stands—is that the key size simply is not big enough. A key is a string of 0's and 1's used to inform a computer how to encode data with the DES and how to decode it as well. The DES key is 56 bits long and each user has a unique key, chosen from the 2^{56} possibilities. A number of computer scientists, notably Martin Hellman of Stanford University and Whitfield Diffie of BNR in Palo Alto, argued in 1976 that a machine could be built that could determine any user's key in half a day by the brute force method of trying all possibilities (*Science*, 29 July 1977, p. 438).

This would require an expensive code-breaking machine, however, and only the NSA—or its counterpart in other technologically advanced countries—would be likely to spend the money.

Recently a number of investigators have found "weak" keys for the DES—keys that, if used, may make the code substantially easier and cheaper to break. The catch is, most users have no way of knowing whether the key they select is one of the weak ones. Cipher Deavours of Kean College in New Jersey, who is a former NSA employee and is editor of *Cryptologia*, says, "These weak keys are surfacing right and left. The question is, How many weak keys are there?"

Another question is, Why are there weak keys at all? Robert Morris of Bell Laboratories in Whippany, New Jersey, remarks, "You would normally expect that good systems won't have weak keys." One possible reason is that the NSA wanted weak keys to make the code easier to break. But some experts think they arose accidentally, perhaps because the IBM people who designed the code did not have enough experience to avoid them.

The first group of four weak keys are nothing new and are so blatantly insecure that IBM cautions users to avoid them. With these keys, the function for enciphering and deciphering is the same. Donald Davies of England's National Physical Laboratory says these keys are "not a serious problem" because they are so well known.

Davies discovered 12 other keys that he calls semi-weak. These keys come in pairs—one will decipher the messages that the other enciphers. IBM also cautions against using these keys.

In addition, Davies found 240 "semi-semi weak" keys. "The semi-semi weak keys look good but some of the operations [during the encoding procedure] take on special values." Any such special values may make the code easier to break.

The DES takes a computer message, which is a string of 0's and 1's, and scrambles it 16 times. With the semi-semi weak DES keys, however, some of the 16 scrambling functions, which are supposed to be different from each other, are the same or are inverses of each other.

It would be "awkward," Davies says, to reject all semi-semi weak keys. "But none of these properties need to have been present. When I looked inside the DES, I began to wonder if it was not as secure as it is thought to be."

Richard Polis of the Geneva Management Group in Switzerland has been collecting data on weak keys for some time. (Polis classifies as "weak" what Davies calls weak, semi-weak, and semi-semi weak.) So far, Polis knows of 25 categories of weak keys which, he says, result in "a substantially less complex transformation of plain text [unencoded message] to cipher text." No one is sure how many keys are in each category. "Every few months there seems to be another category or two added to the list. The list keeps getting bigger," Polis says.

Polis, like earlier critics, notes that it would be easy to break the DES anyway if anyone were willing to develop the necessary computer programs. In the worst case, using keys not known to be weak, he estimates the code could be broken in 8 hours. Weak keys would speed up this process substantially. With the strongest of the weak keys, it might take 4 hours to break the DES.

Deavours agrees that the DES can easily be broken. He himself worked out "lots of ways of attacking it." When he began carefully analyzing the code, he began to notice peculiarities. For example, there is a permutation in the code that lines up all the 0's and 1's—"just the sort of thing you'd want for cryptanalysis," Deavours says. He found "dozens of little things like that. At first I thought I was just seeing patterns where there aren't any but eventually I realized there's something wrong here."

Carl M. Meyer of IBM in Kingston, New York, takes issue with these charges that the DES is easily broken. He knows of weak keys, he says, and he

recently published 200 semi-weak and semi-semi weak keys of the sort Davies discovered. "But it's debateable how weak is weak. How you are going to attack the system is not clear. I would not hesitate to use a semi-semi weak key. I personally don't think you can do anything with them."

Robert Juneman of Satellite Business Systems agrees with Meyer. These keys, he says, "have certain structural properties that make you lift your eyebrows a little bit." But he knows of no way to use the weak keys to break the DES code. Still, he remarks, "The more I learn the less certain I get about anything. I'm just saying I haven't found a way of putting these keys to any particular use."

One reason that Deavours and Polis find the weak keys so disturbing is that the DES is *the* cryptographic standard in the United States. If anything is wrong with it, there is no well-known or reliable alternative. "It makes no sense to have just one cryptographic standard," says Deavours. "The NSA doesn't use just one code. Why should we?" George Davida of the University of Wisconsin in Milwaukee agrees. "The need for encryption is immense and the absurdity of having just one encryption standard is becoming clearer."

Davida attributes the situation to the government's "attempts to meddle in this area" by, for example, encouraging cryptography researchers to submit their papers to the NSA prior to publication and by restricting the export of cryptological devices. As a result, few investigators in this country publicly do cryptography research. But private corporations, Davida says, are quietly developing their own codes. He consults for some companies that have doubled the DES key length and have altered the internal functions to make the code more secure for their own private use. "What's sad is that the corporations with money will design their own codes anyway. They will have the protection they need but private persons will not."

An intriguing question is whether NSA already has the ability to break the DES code. Since the DES is sold abroad as well as in the United States, the NSA would want to be able to break the code and it is widely believed that it can do so. Deavours points out that the NSA cannot think the DES is particularly hard to break since it only certifies it for "confidential" information. Says Deavours, "That's practically the stuff you read in newspapers." And a former director of research at the NSA told an NSA employee that the agency has always been able to break the code.—**GINA KOLATA**

Large Volkswagens in the Western Sky

A dozen antinuclear groups have filed a lawsuit against the Pentagon in an attempt to get a formal assessment of the world environment in the aftermath of a limited or full-scale nuclear war. The suit, filed on 12 January, specifically seeks a statement on the environmental impact of deploying the MX nuclear missile in Wyoming. But the plaintiffs say that a primary goal is to force the government to predict what happens to the environment when a weapon such as the MX is either used or attacked.

No previous federal environmental impact statement related to the deployment of strategic weapons has included such a statement. The plaintiffs say that this is because no private group ever requested it before. The law mandating such assessments prior to the start of large federal construction projects requires only that they address "adverse environmental effects which cannot be avoided." Thus, a key argument of the lawsuit is that MX deployment sharply increases the likelihood of a nuclear war.

The novel request was prepared by Nicholas Yost, who is a recognized legal expert in this area. Yost served as the attorney for the White House Council on Environmental Quality during the Carter Administration. "We want to be sure they produce an environmental impact statement on the basing mode, whether it be Dense Pack or something else," he said. "We want to be sure there is an opportunity for public comment. And we also want them to look at the effect of the missiles if used as designed." Plaintiffs in the suit include Friends of the Earth, the Council for a Livable World, the United Church of Christ, Environmental Action, Greenpeace, the Sierra Club, the Wyoming Church Coalition, and the Tri-State MX Coalition.

The Reagan Administration has not yet stated whether it plans to do an impact statement of any kind on its final missile-basing proposal. But Senator John Tower (R–Tex.), a major Administration supporter who chairs the Armed Services Committee, said in December that "once a site is selected, the provisions of the National Environmental Policy Act will be fully complied with." Grant Reynolds, an assistant general counsel to the Air Force, which is responsible for MX deployment, would say only that the lawsuit "doesn't have any merit, and will be vigorously defended."

Any formal Administration statement about the aftermath of an attack on Dense Pack could be extremely interesting. In congressional testimony late last year, the Air Force mentioned casually that an attack would send enormous boulders into the sky, "some of them larger than a Volkswagen." Other, more harrowing phenomena would doubtless ensue.

—**R. JEFFREY SMITH**

Britain to Study Health Effects of Nuclear Tests

London. The British Ministry of Defense announced last week that it is planning to carry out a survey of 12,000 servicemen and civilians who were involved in nuclear weapons tests in the South Pacific in the 1950's, to investigate the validity of claims that they face an abnormally high risk of cancer and other related diseases.

The survey is being carried out in response to growing public concern in Britain that the long-term effects of exposure to fallout from the tests are only now becoming apparent. On a program broadcast on 12 January by the British Broadcasting Corporation, for example, it was alleged that at least 130 individuals involved in the tests had died from cancer and other diseases which might have been the result of their participation.

Whether there is a link between an individual's exposure to low levels of radiation during the South Pacific tests, which took place between 1952 and 1958, and their subsequent medical history is currently a major point of controversy among the British government's health experts.

The Department of Health and Social Security, for example, recently agreed to award a war widow's pension to the wife of one serviceman who had suffered from skin sores after helping to hose down an aircraft which had just flown through the center of