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