Prying Open the Cryptographic Door

While conducting a court-authorized wiretap, an FBI agent encounters a completely unintelligible telephone conversation. Suspecting that this signal may actually represent encrypted speech, he sends it through an electronic device which establishes that a particular form of coding known as "escrowed" encryption is being used to scramble the conversation. The device also supplies the serial number of the integrated-circuit chip doing the scrambling at the suspect's telephone.

The agent submits this number and other documentation concerning the wiretap to two government agencies — the National Institute of Standards and Technology and the Automated Services Division of the Treasury Department — to obtain the "keys" required to decrypt this particular type of scrambled speech. When combined, the two keys enable the agent to decipher the conversation.

Last week, the Clinton administration announced several steps designed to make such a scenario possible. These actions, including the adoption of a voluntary federal standard for "key-escrow" encryption technology, represent an attempt to preserve the ability of law enforcement and national security agencies to intercept and decipher messages sent over computer and telephone lines.

First proposed last April, key-escrow encryption requires the use of a special chip (sometimes called Clipper) to encrypt digitized speech and data according to a classified mathematical formula developed by the National Security Agency (SN: 8/28/93, p.143). The scheme also provides a special master key, divided into two parts accessible only to authorized officials, to unlock an encrypted message.

If widely used, such a scheme would preserve the ability of government agencies to conduct authorized wiretaps. "We have long needed to rely on wiretaps to help protect society from some of its greatest dangers," insists Webster Hubbell, associate attorney general at the Justice Department. Officials say this capability is threatened by the rapidly increasing use of alternative, unbreakable encryption techniques.

Computer and communications companies, however, are concerned that customers will be reluctant to buy equipment to which the government holds a key. Groups such as Computer Professionals for Social Responsibility (CPSR) complain about potential threats to privacy and about the secrecy surrounding the federal government's internal review of cryptographic policy (SN: 6/19/93, p.394).

"We believe that if this proposal and the associated standards go forward, even on a voluntary basis, privacy protection will be diminished, innovation will be slowed, government accountability will be lessened, and the openness necessary to ensure the successful development of the nation's communications infrastructure will be threatened," CPSR's Marc Rotenberg and 42 others warned in a Jan. 24 letter to President Clinton.

Despite this opposition, the Clinton administration decided to go ahead with its original plan, making essentially no concessions to critics.

"They decided to completely ignore the public input that they had asked for," says Stephen T. Walker of Trusted Information Systems, Inc., in Glenwood, Md. Walker serves on the Computer System Security and Privacy Advisory Board, which last year held public hearings and solicited comments on the administration's proposal and made recommendations to the government.

Government officials hope that manufacturers will start incorporating this technology into telephones, modems, and other communications equipment sold to federal agencies. The Justice Department has already ordered about 8,000 encryption devices for its telephones.

"The government is going to spend a great deal of money buying equipment and setting up the key-escrow system, but it won't succeed," Walker predicts. Businesses will balk at buying such products for their own use, he says.

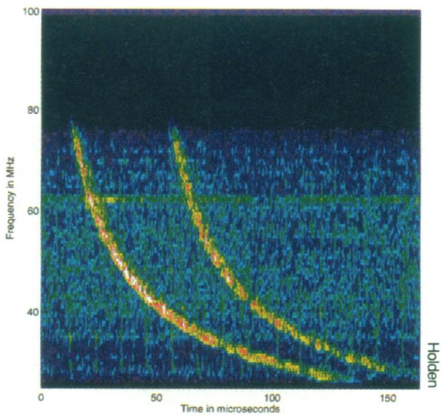
Meanwhile, the debate over cryptographic policy is sure to continue. "It's a complicated issue," says Lance J. Hoffman of George Washington University in Washington, D.C. "We're really trying to set in place our constitution for an electronic age." — *I. Peterson*

Puzzling atmospheric bursts spark interest

Weather aficionados have watched the skies for centuries, but that hasn't kept modern researchers from finding something new under the sun. Atmospheric physicists have recently detected a number of previously unrecognized or poorly studied phenomena, including pulses of radio emissions and odd flashes of light high above Earth's surface.

Investigators believe these unusual features relate somehow to thunderstorms, although scientists remain unsure what causes such events and have yet to resolve whether a connection exists between the light flashes and radio bursts.

Dan Holden and his colleagues at Los Alamos (N.M.) National Laboratory discovered the radio phenomenon while studying measurements made by the ALEXIS satellite. The craft was launched last year as part of an effort to develop technology for identifying nuclear blasts. Since November, ALEXIS' radio receiver has recorded some 100 pulses of radio energy 10,000 times stronger than the radio noise generated by lightning. Each pulse consists of a pair of emissions separated by 40 millionths of a second.



Curved lines represent paired bursts of radio energy detected by satellite. Passage through the ionosphere causes the dispersion of frequencies seen in curve.

Researchers have ruled out the possibility that the radio bursts come from another planet or star, because the emissions show a characteristic distortion, caused by passage through Earth's ionosphere — the layer 200 to 400 kilometers above the planet's surface. Generated below the ionosphere, the radio discharges disperse as they travel toward the ALEXIS satellite orbiting 800 km above the Earth, says Holden.

The satellite thus far has detected most of the events over Africa and the South Pacific, places lacking the background electromagnetic noise generated by radio and television signals common in the United States and Europe. Holden suspects the bursts occur over many parts of the globe, but "the radio noise is so loud over the United States we have a hard time seeing [the pulses] here."

While researchers have not previously recognized such pulses, Holden says he has found some hints that classified military satellites have detected the emissions, which resemble the radio noise from nuclear blasts.

Holden and his colleagues think the pulses have some connection with thunderstorms because ALEXIS most often detects them in the afternoon and early

morning, typical times for convective storms. Yet the bursts do not come from lightning because they carry much more energy and are much shorter than the radio releases associated with lightning.

Atmospheric physicists wonder whether the enigmatic bursts relate at all to odd flashes of light recently documented high above thunderstorms. Although researchers have long heard anecdotal reports of such features, mainly from pilots, they have obtained confirming evidence only within the last five years. Last year, scientists reported the first detailed measurements of the flashes, made by investigators on the ground as well as by detectors carried by a NASA airplane.

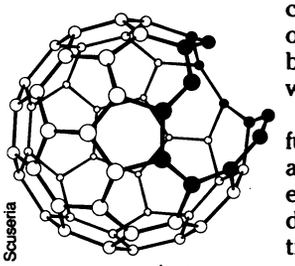
The observations showed that the above-cloud flashes reached roughly 60 km in altitude and covered a vast horizontal distance 10 to 50 km wide, making them distinct from the narrow channels of regular lightning. The flashes resemble glowing auroras more than bright lightning bolts.

Research teams will spend this summer studying the new phenomena. And this week, Holden worked with NASA to obtain simultaneous observations by the ALEXIS radio receiver and video cameras on the space shuttle mission. Such dual observations should resolve whether the radio bursts occur at the same time as optical flashes within or above thunderstorms. *— R. Monastersky*

Laser may loosen the buckeyball's bonds

The intriguing soccer-ball-shaped molecule called a buckyball continues to tantalize chemists, who wrestle almost obsessively with the question of how to fill the molecule's empty interior.

The problem with this molecule, made of 60 carbon atoms, derives from its stable bonds, which keep the spherical cage dutifully closed. Yet a window does appear to be opening into this otherwise sealed surface. Robert L. Murry and Gustavo E. Scuseria, both chemists at Rice University in Houston, Texas, describe in the Feb. 11 SCIENCE a theoretical mechanism to literally "open a window" into the C_{60} molecules, as well as related molecules in the fullerene family.


Scuseria

Tinkering with the tiny carbon cages, the two noticed that certain atomic bonds lend themselves better than others to temporary adjustments. Indeed, the molecule's unique shape comes from an alternating pattern of carbon rings bonded together as hexagons and pentagons — the pattern found on a soccer ball.

Murry and Scuseria realized that the juncture between the pentagons and hexagons, called a "5-6 bond," yields relatively easily to the prying forces of a laser's energy. When properly irradiated, an opening would temporarily appear in the fullerene.

This method permits the bond to open widely without disturbing the ball's overall structure, thus permitting one or more atoms — perhaps even small molecules — to enter the carbon cage. Furthermore, by opening more than one bond in this way, "multiple windows" are possible.

Efforts to "custom-fill the fullerenes' void" continue apace, the researchers say, eyeing potential uses in drug delivery, molecular transport, medical imaging — even superconducting devices.

When "doped," or mixed, with an alkali metal, fullerenes do have the potential to become useful as superconductors.

"We'd like to try to make a fullerene superconductor by putting a lanthanum or scandium atom inside the C_{60} cage," says Scuseria. "This is a very exciting idea, but still theoretical."

"Whether it will work," he adds, "remains to be seen." *— R. Lipkin*

Mother's smoking linked to child's IQ drop

Preschool children whose mothers smoked heavily during pregnancy scored significantly lower on standardized IQ tests than kids whose mothers did not smoke, according to a new study.

This isn't the first time that researchers have suggested that a pregnant woman's smoking habits might have an impact on her offspring. Last year, a Canadian researcher reported that children born to women who smoked during pregnancy may have subtle auditory difficulties (SN: 7/10/93, p.23).

David L. Olds of the University of Colorado Health Science Center in Denver and his colleagues wanted to find out whether a maternal tobacco habit had an adverse effect on a child's intellectual ability later in life. From 1978 through 1980, the team enrolled 400 women pregnant with their first child.

The researchers asked each woman about her diet, smoking habits, and alcohol or drug use. To verify self-reported smoking behavior, the team measured a nicotine metabolite in urine samples collected from a subset of smokers enrolled in the study.

After delivery, the team continued to check on mothers and their offspring. When the children in the study reached preschool age, Olds and his co-workers began measuring intellectual ability with the Stanford-Binet IQ test.

They report in the February PEDIATRICS that IQ scores of 3- and 4-year-old children whose mothers smoked 10 or more cigarettes daily during pregnancy averaged 9 points lower than those of kids whose mothers did not smoke. When the team controlled for factors known to influence a child's test scores, such as maternal IQ and alcohol use, they found that they could explain some, but not all, of the difference. The children of mothers who had smoked still scored about 4 points lower than the offspring of nonsmoking mothers.

Four points doesn't seem like much, but it is equivalent to the deficit seen in children exposed to moderate amounts of lead, says coauthor Charles R. Henderson Jr. of Cornell University. That doesn't necessarily mean an individual child will have trouble in school, Henderson adds. At the same time, smoke-exposed children may not reach their full intellectual potential, he says.

In a second study, which also appears in the February PEDIATRICS, the same research group tried to reduce the risk of childhood cognitive deficits by modifying the behavior of mothers who smoked.

Many of these women were visited frequently during and after their pregnancy by nurses, who counseled them about smoking and diet. The researchers discovered that such women cut back on their cigarette use and improved their diet. Moreover, their 3- and 4-year-old children had about the same average IQ scores as children whose mothers didn't smoke.

Reductions in maternal smoking explain part of the improvement in test scores; however, better nutrition may also play a role. "It would be nice to have a complete biological explanation, but we don't have that," Henderson says.

Further research must confirm the theory that mothers who smoke during pregnancy will impair their children's cognitive abilities. The reported link between maternal smoking and a child's performance on an IQ test years later may simply be a statistical fluke, the researchers note. The team plans to continue to look at IQ differences in the smokers' offspring, who are now in their teens.

On the other hand, something in tobacco smoke may harm the developing fetal brain. Cigarette smoke contains an estimated 2,000 to 4,000 chemicals, some of which could damage fragile fetal cells, Henderson notes. It may be that subtle smoke-induced damage doesn't show up until a child reaches age 3 or 4, when higher-order cognitive skills kick in, he adds. *— K.A. Fackelmann*