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.

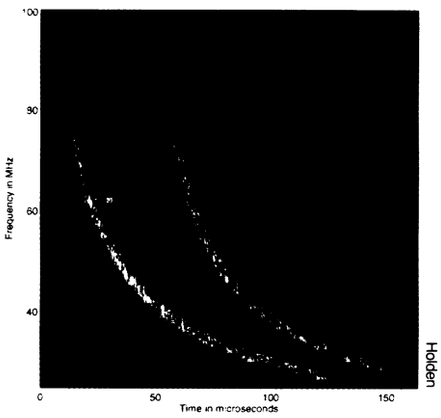
Meanwhile, the debate over cryptographic policy is sure to continue. "It's a complicated issue," says Lance J. Hoffman of George Washington University in Washington, D.C. "We're really trying to set in place our constitution for an electronic age." — *I. Peterson*

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