CAPSTONE CHIP TECHNOLOGY

CAPSTONE is an NSA developed, hardware oriented, cryptographic device that implements the same cryptographic algorithm as the CLIPPER chip. In addition, the CAPSTONE chip includes the following functions:

1. The Digital Signature Algorithm (DSA) proposed by NIST as a Federal Information Processing Standard (FIPS);
2. The Secure Hashing Algorithm (SHA) recently approved as

FIPS 180;

3. A Key Exchange Algorithm based on a public key exchange;
4. A general purpose exponentiation algorithm;
5. A general purpose, random number generator which uses a pure noise source.

The Key exchange Algorithm is programmable on the chip and uses functions 1-2 and 4-5 above.

Prototypes of the CAPSTONE chip are due the last week in April.

The chips are expected to sell for $85.00 each (programmed).

The first CAPSTONE chips are to be installed in PCMCIA electronic boards and used for the PMSP program for the security of the Defense Messaging System.

The CAPSTONE chip is big, complex and powerful. Over 850 megabytes are required by the automated design system to define the functions of the chip. VLSI Technology is fabricating the chip, and MYKOTRONX is designing and testing the chip.

1. What are the power requirements of the CAPSTONE chip? Will they fit the power requirements of battery-operated, hand held devices?

   The CAPSTONE chip requires a 5 volt DC voltage source. Power ratings are currently estimated at 3.5 milliamps per MHz, i.e. at 10 Mhz and 5 volt DC, power consumed is 175 milliwatts. These estimates will be refined as data are taken into the actual chips. In comparison, the CLIPPER chip consumes approximately 150 milliwatts at 5 volts DC and 10 MHz. As you can see, both chips fall within the power requirements of hand held, battery-operated devices.

2. Will the CAPSTONE chip incorporate the key escrow features of the CLIPPER chip?

   Yes, it will.

3. When will CAPSTONE be announced and available?

   Prototypes of the CAPSTONE chip are due the end of this month. We ask that you contact the manufacturer, Mykotronx Inc., for further information concerning the timetable for availability of CAPSTONE.

4. Is the Department of Defense working now to incorporate CAPSTONE in the Pre-message Security Protocol?

   Yes

5. Will CAPSTONE meet the design requirements of a PCMCIA card that combines voice and/or data communications with encryption capabilities?

   Yes

6. Will CAPSTONE use the Digital Signature Standard? What kind of key management scheme will be employed in the CAPSTONE chip? Will CAPSTONE allow the use of RSA public-key encryption in conjunction with, or as an alternative to, the DSS? If RSA is implemented on the CAPSTONE chip, will the key escrow feature function?

CAPSTONE implements the Digital Signature Algorithm (DSA), proposed by NIST as a Federal Information Processing Standard (FIPS), to perform the digital signature functions. Key management is handled by an algorithm based on a public-key exchange technique. The CAPSTONE chip does not implement RSA.

4/30/93