Key Escrowing Today

The objective of the U.S. Government's Escrowed Encryption Standard and associated Key Escrow System is to provide strong security for communications while simultaneously allowing authorized government access to particular communications for law enforcement and national security purposes.

Dorothy E. Denning and Miles Smid

Sensitive communications transmitted through the phone system or computer networks are vulnerable to unauthorized interception. To protect against this threat, the communications can be encrypted (scrambled) before they are transmitted and decrypted upon receipt. Normally, the encryption and decryption processes are parameterized by a secret key that is shared by the sender and receiver for the duration of the communication. If the method of encryption is sufficiently strong, an eavesdropper will be unable to determine the secret key and break into the communications.

While protecting sensitive information against unauthorized interception, encryption also can be used to conceal criminal and terrorist activities. Court-authorized interception of communications has been essential for preventing and solving many serious and often violent crimes, including organized crime, drugs, government fraud and public corruption, and terrorism. By rendering communications immune from lawful interception, encryption threatens law enforcement and public safety. Similarly, by interfering with intelligence operations, encryption threatens national security.

On April 16, 1993, the U.S. Government announced a new encryption initiative aimed at providing a high level of communications security and privacy without jeopardizing effective law enforcement, public safety, and national security. The initiative is based on a special tamper-resistant hardware encryption device (Clipper Chip) and a Key Escrow System (KES), which gives the government access to a Device Unique Key that unlocks all communications encrypted by the chip. This key is generated and programmed onto the chip after the chip is manufactured, but before it is placed in a security product. At that time, the key is also split into two Key Components, which are encrypted and given to separate Key Escrow Agents for safekeeping. A government official pursuant to a lawful authorization must acquire the Key Components from both Escrow Agents in order to obtain the Device Unique Key. These components are combined inside a special Key Escrow Decrypt Processor, which is then able to decrypt the intercepted communications.

On February 4, 1994, the U.S. Government announced adoption of the technology as the Escrowed Encryption Standard (EES) [6]. The EES is a voluntary government standard for sensitive but unclassified phone communications, including voice, fax, and data transmitted on circuit-switched systems at rates of standard commercial modems or which use basic rate ISDN or a similar grade wireless service.

Several organizations and individuals have participated or will participate in the development, evaluation, and operation of the EES and supporting Key Escrow System (KES). These include the Department of Justice (DOJ) as sponsor of the system, the National Institute of Standards and Technology (NIST) as one of the two initial Escrow Agents, the Department of the Treasury Automated Systems Division as the other initial Escrow Agent, the National Security Agency (NSA) as system developer, the Federal Bureau of Investigation (FBI) as the initial law enforcement user, various organizations as outside contractors, and five independent experts as outside reviewers of the classified technology and KES. The program is managed by a National Program Manager for Key Escrowing (Key Escrow Program Manager) at NIST. Miles Smid serves as the Key Escrow Program Manager and Dorothy Denning as an outside reviewer.

The objective of this article is to describe the Escrowed Encryption Standard and Key Escrow System. Particular emphasis will be given to security, since potential users have been concerned that the hooks which provide authorized government access could be exploited or abused. We will describe many of the safeguards that have gone into the design of the KES in order to ensure that the risk of unauthorized access to EES-encrypted communications is negligible. We do not, however, give a risk assessment of the effectiveness of those safeguards.

The paper is based on procedures developed by the DOJ, FBI, NIST, NSA, Treasury, and Rapid Systems Solutions Incorporated of Columbia, Maryland.

DOROTHY E. DENNING is a professor of computer Science at Georgetown University.

MILES E. SMID is manager of the Security Technology Group Aat the National Institute of Standards and Technology.

0163-6804/94/$04.00 1994 © IEEE

The Escrowed Encryption Standard

EES specifies use of the SKIPJACK encryption algorithm, which uses 80-b keys, and a Law Enforcement Access Field (LEAF) creation method to be implemented in a tamper-resistant chip (Clipper) or another form of hardware device [6]. The standard also specifies that each device is to have a Device Unique Identifier (UID), an 80-b Device Unique Key (KU), and an 80-b common Family Key (KF), all of which are programmed onto the chip after it is manufactured, but before it is placed in a security product. Although KU is not used to encrypt communications, together with the LEAF and KF, it provides a means by which an authorized government official can obtain the secret encryption key and gain access to the communications. Both SKIPJACK and the LEAF creation method are classified.

The SKIPJACK Algorithm

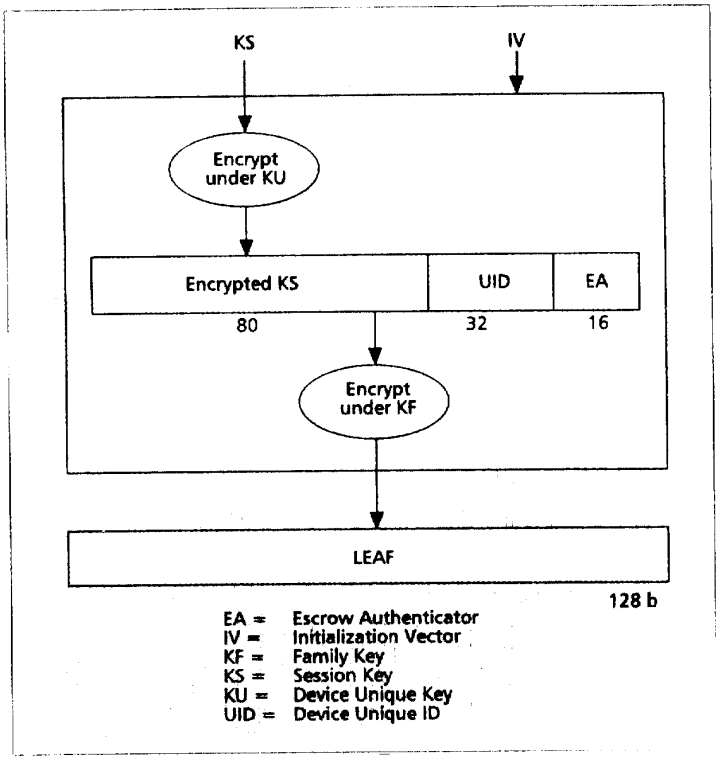
The SKIPJACK encryption algorithm transforms a 64-b input block into a 64-b output block using an 80-b secret key. Since the same key is used for decryption, that is, to restore the original data, the algorithm is characterized as "single key" in contrast to "public key," which uses separate encryption and decryption keys. SKIPJACK has the same block size as the Data Encryption Standard (DES), however, its key is 24 b longer than DES's 56 b. SKIPJACK can be used in one or more of the four operating modes defined in FIPS 81 for use with DES: Electronic Codebook (ECB), Cipher Block Chaining (CBC), 64-b Output Feedback (OFB), and 1, 8, 16, 32, or 64-b Cipher Feedback (CFB).

The algorithm was designed by the National Security Agency and is classified in order to prevent someone from implementing it in software or hardware without providing the key escrow feature. This would take advantage of the government's strong algorithm while rendering encrypted communications immune from lawful government surveillance. Moreover, if the algorithm, Family Key, and LEAF creation method were known, it would be possible to build such products so that they interoperated in real-time with those that correctly implemented the key escrow function.

Because the SKIPJACK algorithm is classified, it is not open to public scrutiny in the same way as DES. To help engender public trust in the strength of the algorithm, the government invited several outside cryptographers, including one of the authors of this paper, to review the algorithm and publicly report their findings. The review group concluded that there was no significant risk that the algorithm had "trapdoors" or could be broken by any known method of attack [2].

LEAF Creation Method

LEAF is transmitted with all encrypted communications and provides a mechanism for securely transmitting the encryption key for the communications, i.e., the Session Key (KS), so that an authorized government official, and only an authorized official, can obtain KS and decrypt the communications. Although KS is transmitted in the LEAF, the LEAF is used only for law enforcement access and not for the distribution of KS. A receiving chip is unable to extract KS from the LEAF.



■ **Figure 1.** *LEAF creation.*

The LEAF is computed as a function of the KS, an Initialization Vector (IV), the Device Unique Identifier (UID), and the KU. The resulting block includes KS encrypted under KU (80 b), UID (32 b), and an Escrow Authenticator (EA) (16 b), all encrypted under the Family Key (KF) as shown in Fig. 1. KS is protected under two layers of encryption so that it cannot be obtained without both KF and KU. The details of the algorithm are classified, including the SKIPJACK-based encryption modes and computation of the Escrow Authenticator.

The purpose of the EA is to protect the LEAF against tampering that could prevent an authorized government official from recovering KS. Of particular concern are "rogue" applications that would interoperate with legitimate ones by transmitting a bogus LEAF, which is accepted as valid by the receiving chip but proves useless to the government. A non-interoperable application is of less concern since a person intent on avoiding government access has the option of using an alternative means of encryption when interoperability is not needed.

Using a software interface to an early prototype of a PCMCIA Crypto Card (formerly called Tessera), which contains a Capstone Chip,[1] Matt Blaze showed that it might be possible to develop a non-real-time rogue application such as e-mail that would interoperate with a legitimate application at the other end but transmit a bogus LEAF [1]. His attack works by querying the PCMCIA card with possible LEAFs until one is found that is accepted as valid; that is, the Escrow Authenticator (EA) is a valid checksum of its input. Since the

[1] *A microcircuit chip containing SKIPJACK and other cryptographic functions, which comply with the Escrowed Encryption Standard (EES).*

Escrowed encryption products are exportable to most end users after initial review. In addition, such products will qualify for special licenses.

EA is 16 b, this requires 2^{16} trials on average, which is estimated to take about 42 minutes. The attack is not practical with real-time telephone applications and could not be done using the AT&T 3600 Telephone Security Device, since it has no external interface for testing LEAFs and, moreover, times out if a valid LEAF is not received within a short time interval. In addition, the Blaze attack will not pose a serious threat with the PCMCIA cards since production devices will implement techniques such as a faulty LEAF counter, which could pause or lock up the card if too many faulty LEAFs are detected.

Application

In order for two persons to use EES to encrypt their phone communications, each person must have a tamper-resistant security device, which contains an escrowed encryption chip. The security device is responsible for implementing the protocols needed to establish the secure channel, including negotiation or distribution of the 80-b secret KS that is used to encrypt the communications. KS could be negotiated, for example, using a public-key agreement method, which allows the two devices to compute a shared secret key by exchanging only public values. This is the approach used with the AT&T 3600 Telephone Security Device[2] (TSD). The TSD plugs into a phone between the handset and base set, and is activated by pushing a button.

Once KS is established for use with an escrowed encryption chip, it is passed to the chip and an operation is invoked to generate the LEAF from KS and an IV, which may be generated by the chip. The LEAF is then transmitted along with the IV to the receiving chip for synchronization and LEAF validation. After the two chips are synchronized, KS is used to encrypt and decrypt messages in both directions. The message stream for voice communications is first digitized.

In a two-way conversation such as a phone call, the security device of each party transmits an IV and a LEAF computed by the device's chip. However, both devices use the same KS to encrypt communications transmitted and to decrypt communications received.

The first set of escrowed encryption chips was manufactured by VLSI Technology, Inc. and programmed by Mykotronx. Mykotronx's MYK-78T chip, which is used in the AT&T 3600 Telephone Security Device, runs up to 21 Mb/s.

A more advanced chip, called Capstone, includes Clipper's components plus a public-key Key Exchange Algorithm (KEA), the Digital Signature Algorithm (DSA) [5], the Secure Hashing Algorithm (SHA) [8], a general-purpose high-speed exponentiation algorithm, and a random number generator that uses a pure noise source. Capstone provides the cryptographic functionality needed for secure electronic commerce and other applications on the National Information Infrastructure. It will have its first application in a PCMCIA Crypto Card, which will be used in the government's Mosaic system to implement secure e-mail for the Defense Messaging System.

Escrowed encryption products are exportable to most end users after initial review[4]. In addition, such products will qualify for special licenses.

[2]*Mention of product names does not imply endorsement or reccomendation by the authors or their organizations.*

Overview of Key Escrow System

The KES provides a means whereby a government official with legal authorization can decrypt the communications encrypted by a particular EES device, but whereby unauthorized access to communications is effectively prevented through an extensive set of safeguards. Fig. 2 shows the main elements of the KES and their relationship to each other and to the communications transmitted between two Telephone Security Devices (TSDs) that contain Clipper Chips.

The operation of the KES involves the Key Escrow Program Manager, two Key Escrow Agents, two Family Key Agents, a Programming Facility Representative, the Department of Justice, and law enforcement agencies. The responsibilities of these agencies and individuals is split so that their cooperation is required to operate the system.

Phased Implementation

The KES is being implemented in four phases. This paper focuses on the state of the system after implementation of Phase 2 in May 1994. The system up through Phase 2 is called the Interim System. The Interim System is characterized by a combination of manual and automated procedures to manage the key escrow data. Many of the manual procedures will be automated in the Final (Target) System in order to provide greater efficiency.

Phase 1 began in September 1993 and ran through April 1994. During Phase 1, chips were programmed in a prototype Programming Facility and Encrypted Key Components escrowed on floppy disks and stored in safes. There was no Key Escrow Decrypt Processor available to law enforcement and no procedures for releasing the escrowed Encrypted Key Components. Manual procedures were implemented for transmitting key escrow data between different sites and for generating audit records. Phase 2 added a single prototype Decrypt Processor, a simple Key Component Extraction Program for extracting an Encrypted Key Component from a floppy disk, and manual procedures for release of key components. Operational Key Components have not yet been released.

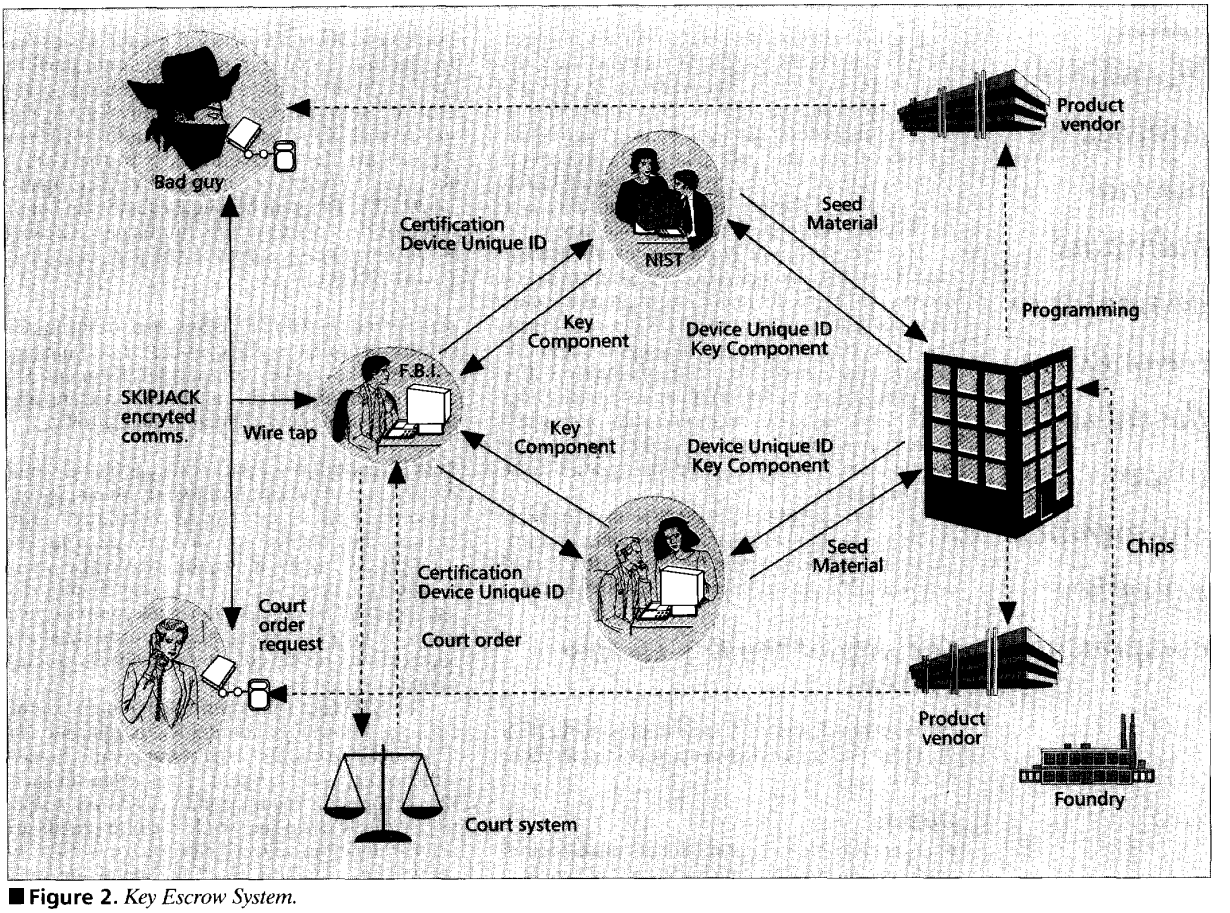
Interim System

This section summarizes the operation of the Interim System. A more detailed description is given in the section on operation of key escrow system.

Clipper and Capstone Chips are programmed in batches inside a secure facility. During a programming session, Escrow Officers representing both Escrow Agents must be present along with a Programming Facility representative who operates the Chip Programming Device.

Before each programming session, the Escrow Agents each generate a Key Number and Random Seed for use in that session. These values are generated on PCs using NIST's Advanced Smart Card Access System. Similarly, before the first session, the Family Key Agents each generate a longer-term Family Key Component.

The random values generated by the Escrow Agents and Family Key Agents are loaded into a workstation at the beginning of a programming session. The Family Key Components are combined to form the Family Key, and the Key Numbers



■ **Figure 2.** *Key Escrow System.*

are combined to form a Key Component Enciphering Key (KCK).

The Random Seeds are combined with additional random input to generate a stream of random Device Unique Keys (KU) for the chips. Each KU is programmed onto a chip along with a Device Unique Identifier (UID) and the Family Key (KF).

When KU is generated, two Key Components (KC1 and KC2) are generate such that KU is their exclusive-or (XOR). The components KC1 and KC2 are encrypted with KCK and written to floppy disks. One set of components is given to each of the two Escrow Agents for safekeeping. The escrowed Encrypted Key Components (EKC1 and EKC2) are released to an authorized government official, normally a law enforcement agent, only when the government has been authorized to intercept the communications of individual(s) using a device with the chip containing KU.

When a law enforcement agent detects encrypted communications on a lawfully installed intercept, the communications are passed through a Key Escrow Decrypt Processor, which decrypts the LEAF and extracts the chip's UID. The UID is then presented to the two Escrow Agents along with certification of the legal authority to conduct the intercept. In all cases, a government attorney involved in the investigation must confirm that an authorized wiretap is being conducted.

Escrow Officers at each Escrow Agent extract the chip's Encrypted Key Components (EKC1 and EKC2) from the storage disks, and bring disks with the extracted key components and their corresponding Key Numbers to the law enforcement agency. The values are loaded into the Decrypt Processor, where the Key Numbers are combined to form the KCK, and the EKC1 and EKC2 are decrypted under KCK and combined to form the chip's KU. The KU is then used to decrypt the Session Key for each communication, which in turn is used to decrypt the communication.

A law enforcement agent erases KU from the Decrypt Processor no later than the end of the period of authorized surveillance. At that time, an authenticated confirmation of the key destruction is sent to each Escrow Agent.

Extensive audit records are maintained throughout the entire KES to make sure that keys are used only as authorized and not retained.

Target System

The Target System will be automated to reduce human involvement. In addition, it will be built utilizing evaluated products and trusted software design principles to provide high assurance that the system provides strong security.

The Target System will include a more advanced Programming Facility, Key Escrow Decrypt Processor, and Escrow Agent Workstation, plus a new Key Escrow System INFOSEC Device (KID). Encrypted Key Components will be stored on the Escrow Agent Workstations, and key escrow

The KES is designed so that no individual ever needs to see or know the value of any cryptographic key or key component.

data will be transmitted electronically between the Escrow Agent Workstations and the Chip Programming Device, and between the Escrow Agent Workstations and the Decrypt Processor. Transmitted information will be protected by the KID located at each site. The KID will provide cryptographic services including SKIPJACK encryption, the Digital Signature Algorithm, and a public-key-based method of key exchange.

The Escrow Agent Workstations will include automated logging facilities, access controls, and other security mechanisms to ensure the secure and reliable long-term storage of Key Components. The Programming Device will support automatic logging and high-volume chip production. The Decrypt Processor will support automatic deletion of the Unique Key at the end of the authorized surveillance period and automated logging and transmission of the key deletion confirmation to the Escrow Agents.

A design goal of the Target System is for a law enforcement agent to be able to decipher encrypted communications within two hours after a valid certification is presented to each Escrow Agent.

Security of the Key Escrow System

This section describes the major threats to the KES and the safeguards that are used to counter those threats.

Threats

There are two major classes of threats: unauthorized disclosure of sensitive data and denial of service.

The KES is designed to prevent unauthorized access to sensitive data. Some of the data used by the KES, including the SKIPJACK algorithm and LEAF creation method, are classified SECRET while other data, including the Unique Keys, the Key Components, the Family Key, the Key Numbers, and the Random Seeds are considered sensitive unclassified. The KES protects all sensitive data, whether classified or not.

The KES is also designed to resist attempts at rendering the system inoperable. This includes attacks aimed at destroying key escrow data. While it is impossible to prevent every conceivable denial of service attack, measures have been taken to prevent likely attacks.

The KES protects against both insider and outsider attacks. An insider is anyone who is authorized to use any part of the system. Since insiders have greater access to the system than outsiders, many of the safeguards explicitly counter the insider threat.

Safeguards

The following is a partial list of safeguards employed by the KES as operated today.

Separation of Duties — The principle of separation of duties is used throughout the KES. The Escrow Officers representing the Escrow Agents witness chip programming, but are not allowed to program the chips. Similarly, they insert disks with Encrypted Key Components into a Decrypt Processor, but are not allowed to use a Decrypt Processor to decrypt communications and do not have a Decrypt Processor in their possession. Individuals who program chips cannot perform the functions of either Escrow Agents or of law enforcement officers. The Family Key Agents never hold Key Components, and the Escrow Agents are never given access to the Family Key since they have no need to decipher a LEAF. The Program Manager oversees the operation of the entire system, but has no access to Key Components unless in the presence of an Escrow Officer.

Key Secrecy — The KES is designed so that no individual ever needs to see or know the value of any cryptographic key or key component. Keys and key components are generated in computers and are never displayed or output in human readable form.

Split Knowledge — Split knowledge has been used by the financial industry and military for many years. It is employed by splitting knowledge of some critical value between two or more persons. For example, a bank might require two combinations to open the bank vault, one known by one vice president and the other known by a second vice president. A missile system might require that two codes be entered by different individuals in order to launch a missile.

The KES uses split knowledge to protect critical keys. Knowledge about a KU is split into two Key Components, and each component is held by a different Escrow Agent. Thus, even if one of the components is compromised, KU will still be secure. Only when the two Key Components are combined within a Decrypt Processor will KU be recoverable. Similarly, the Key Component Enciphering Keys are split between the two Escrow Agents, and the Family Key is split between two Family Key Agents.

Split knowledge is also used when physically controlling access to sensitive data. Unique Key Components and Family Key Components are stored in safes which require two combinations in order to gain access.

Two Person Control — Two person control requires that at least two individuals be present when a critical function is performed or when sensitive data might be exposed. At the Escrow Agent sites, all sensitive key escrow data, including audit logs, are stored in double locked safes so that two persons are always required to gain access to the data. Similarly, two persons (one from each Escrow Agent) are required to supervise chip programming, and two persons are required to transport sensitive data. When Key Components are transported on floppy disks, they are wrapped in numbered, tamper-detecting packages. The number and condition of a package is checked by two Escrow Officers both before transportation and upon arrival.

Redundancy — Redundancy is used throughout the KES to protect against accidental and intentional denial of service. Each Escrow Agent operates a backup storage facility which can be used if the Key Components in the prime facility are ever destroyed. When Key Components are generated at the Programming Facility, four copies of that Escrow Agent's encrypted Key

Components are produced. Each of the two Escrow Officers representing the Escrow Agent carry two copies back to their facility. When they arrive, two copies are placed in the primary storage facility and two copies are placed in the backup facility.

Clearances — All system designers, implementors, and Escrow Officers are cleared to at least the Secret level, although the same might not be true of all law enforcement officers who eventually could have access to a Decrypt Processor. Thus, the target Decrypt Processor is being designed under the assumption that the users may be uncleared.

Although clearances help protect against threats to the KES, the KES does not rely solely on them. All components use additional safeguards to protect against attacks that could be made by cleared personnel.

Physical Security — Physical security is used extensively throughout the KES to protect the Escrow Agent facilities, the Programming Facility, the Decrypt Processor, the floppy disks used to transport key escrow data, and the chips. Programming is performed in a Sensitive Compartmented Information Facility (SCIF), which provides the strongest form of physical security used in the U.S. Government. The Decrypt Processor is stored in a secured room and requires a physical key to operate. Key Components are always stored in an area approved for classified information and requiring two persons to gain access. When key escrow data are transported on floppy disks, the disks are wrapped in tamper-detecting packages. Finally, the chips are designed to be highly resistant to reverse engineering.

Cryptography — The KES uses cryptography to prevent the unauthorized disclosure of sensitive data and to control access to the system by authenticating users. Key Components generated at the Programming Facility are encrypted using the SKIPJACK algorithm before they leave the computer, and are not decrypted until used in a Decrypt Processor. The Key Component Enciphering Key used to encrypt the Key Components is derived from Key Numbers supplied by each Escrow Agent, so that neither agent alone can decrypt the components.

Sensitive information stored on the Decrypt Processor is encrypted. A physical cryptographic key must be inserted into the Decrypt Processor in order to operate the machine.

In the target system, cryptography will be used more extensively so that key escrow data can be electronically transmitted rather than manually carried. Digital signatures will be used to provide authentication.

Computer Security — Computer security practices are employed to protect against unauthorized access and against malicious software. The workstations used by the KES are dedicated to key escrow functions and kept in secured facilities. Before a workstation is used initially, its hard disk is wiped and shrink-wrapped software is installed. This process is repeated if control over the workstation is ever lost. When the target system is fully operational, trusted operating systems will be used to maintain access control and need-to-know protection.

Summary of Notation

EES	Escrowed Encryption Standard
KES	Key Escrow System
LEAF	Law Enforcement Access Field
SCIF	Sensitive Compartmented Information Facility
KFC1	Family Key Component of Law Enforcement Agent 1
KFC2	Family Key Component of Law Enforcement Agent 2
KF	Family Key = KFC1 XOR KFC2
KN1	Key Number of Escrow Agent 1
KN2	Key Number of Escrow Agent 2
KCK	Key Component Enciphering Key = KN1 XOR KN2
RS1	Random Seed of Escrow Agent 1
RS2	Random Seed of Escrow Agent 2
AI1	Arbitrary Input entered by Escrow Agent 1 on keyboard at Programming Facility
AI2	Arbitrary Input entered by Escrow Agent 2 on keyboard at Programming Facility
UID	Device Unique Identifier
KC1	Key Component for Escrow Agent 1 = f(RS1, RS2, AI1, AI2, UID)
KC2	Key Component for Escrow Agent 2 = g(RS1, RS2, AI1, AI2, UID)
KU	Device Unique Key = KC1 XOR KC2
EKC1	Encrypted Key Component held by Escrow Agent 1 = EKCK(KC1)
EKC2	Encrypted Key Component held by Escrow Agent 2= EKCK(KC2)
f,g	classified functions
XOR	exclusive or (shown as in figures)
EK(x)	encryption of x under key k

Auditing — The KES makes extensive use of logging and auditing. Each occurrence of the following events is logged:

- Generation of keying material.
- Storage of and access to keying material.
- Request for Key Components.
- Confirmation of a key release certification.
- Notification that a Unique Key was deleted in the Decrypt Processor.

Originals of logs are stored in safes to protect them from loss, destruction, and tampering. At the Escrow Agents, the logs are under two-person control whenever they are accessed and updated.

Each site's security administrator is responsible for assuring that the proper journals are kept. The Department of Justice will audit the system periodically to assure that all Key Component releases conform to Attorney General prescribed procedures. Even though logging and auditing serve only to detect unauthorized actions after the fact, they are a strong deterrent.

Configuration Management — Configuration management is important componenet in the establishment and maintainence of a secure operation. The KES will use configuration management to protect against unauthorized modifications of software. Changes to software will require approval by a Configuration Management Board.

Operational key components will not be released until the software has been placed under configuration control. In addition, the KES must be given interim accreditation by the Department of Justice.

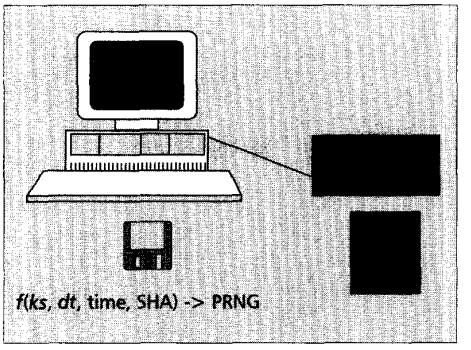


Figure 3. *Generation of random values.*

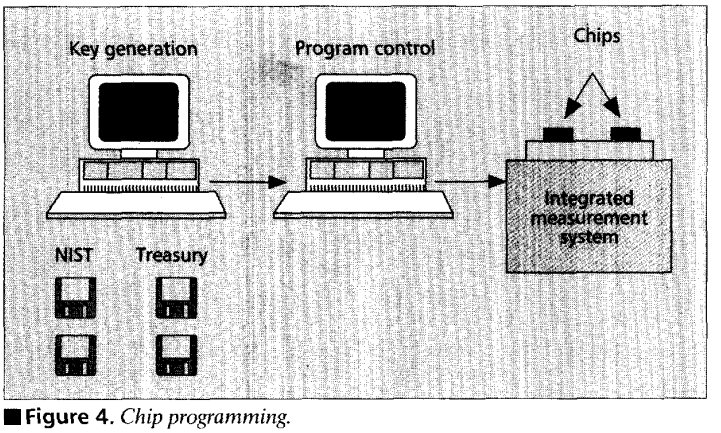


Figure 4. *Chip programming.*

Operation of Key Escrow System

This section describes in greater detail the operation of the Interim system.

Key Number, Random Seed, and Family Key Component Generation

Before Unique Keys and their respective Key Components can be generated at the Programming Facility, certain keys and Random Seeds must be generated. The current KES uses a NIST-developed smart card connected to a personal computer by means of a smart card reader employing an RS232 connection (Fig. 3). The smart card implements the X9.17 pseudorandom number generator (PRNG), which was approved for government use for cryptographic key generation (FIPS 171) [7]. Input from the computer keyboard (*ks*) is used together with keystroke timing (*dt*) and the current time as input to the Secure Hash Algorithm (FIPS 180) [8]. After hashing, the result is fed to the PRNG.

This process is used by the Escrow Agents to generate the Key Numbers and Random Seeds needed for a programming session and by the Family Key Agents to generate the Family Key Components.

Family Key Components — Each Family Key Agent generates its Family Key Component at its respective site. Four copies of the component are written to floppy disks and the disks are sealed in numbered tamper-detecting containers. Two copies are placed in each of two separate safes. Logs of the generation and storage are maintained.

Key Numbers and Random Seeds — Before each programming session, each Escrow Agent generates four copies (disks) of a Key Number. Each disk is sealed in a numbered tamper-detecting container and two disks are placed in each of the two safes at the Escrow Agent site.

Each Escrow Agent also generates one disk with a Random Seed. This disk is also sealed and placed in the safe.

When the Escrow Officers are ready to travel to the Programming Facility for a programming session, they remove two of the disks containing the Key Number and the disk containing the Random Seed. Each Escrow Officer carries one copy of the Key Number, and one of the officers carries the Random Seed.

Chip Programming

The Programming Facility — Chips are programmed inside a Sensitive Compartmented Information Facility (SCIF). Operation of this facility requires the authorization of the Key Escrow Program Manager and participation of Escrow Officers from each Escrow Agent, two Family Key Officers or their designated Programming Facility Representative, and a Programming Facility Representative. The facility contains a UNIX™ workstation, which is used to generate the Unique Keys and Key Components, a PC, which controls the programming of the chips, and a Chip Programming Device, also called an Integrated Measurement System (IMS), which is currently capable of programming about 120 Clipper Chips an hour (Fig. 4).

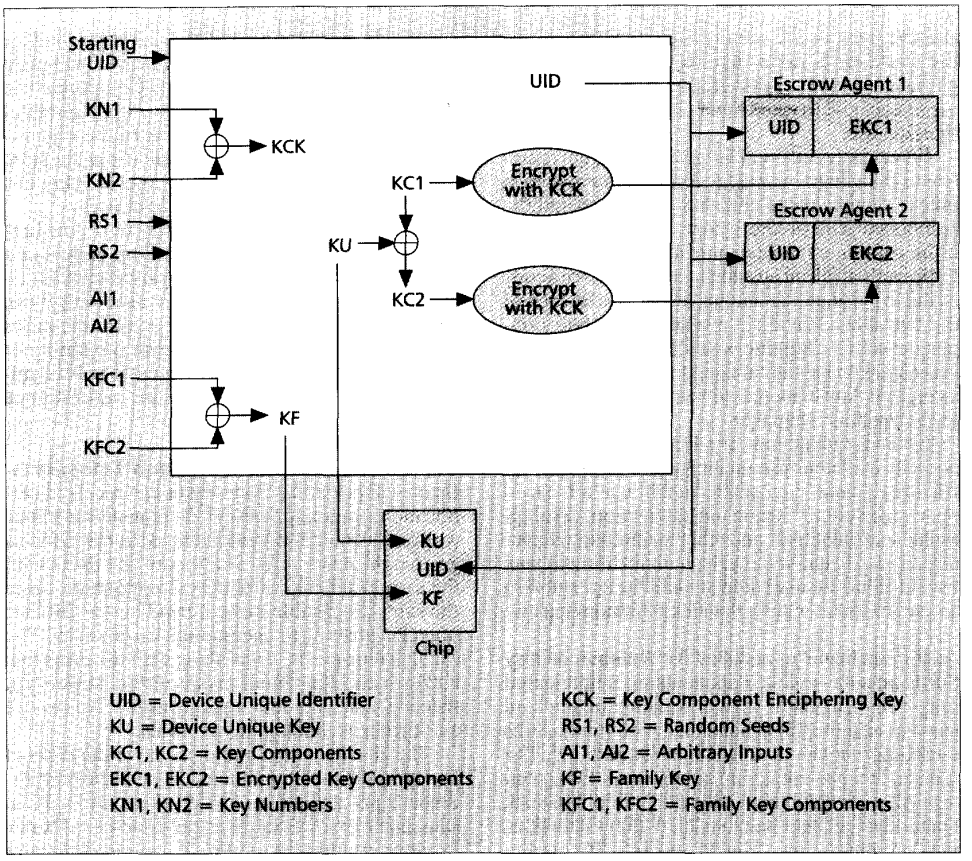
The facility also contains a double-locked safe for storage of key escrow data. An Escrow Officer from each Escrow Agent is needed to unlock the safe, which also contains a locked box for storing the Family Key Components. The lock on this box was originally controlled by the Family Key Agents and subsequently turned over to a Programming Facility Representative.

At least one Escrow Officer from each Escrow Agent must be present inside the SCIF during key generation and chip programming. If one needs to leave the room temporarily, then all personnel must exit from the SCIF. The SCIF is then double-locked and both Escrow Officers are needed to reopen it.

Initialization — When the Programming Facility went into production mode, one copy of each Family Key Component was sent via overnight mail to the Programming Facility, and the other transported to the site by a Family Key Officer. The disks were placed in the locked box inside the double-locked safe for storage, the lock was turned over to a Programming Facility Representative, and the Family Key Officers returned to their sites.

For each programming session, the Escrow Officers bring their sealed disks of Key Numbers and Random Seeds. The officers unlock the double-locked safe, and a Programming Facility Representative, operating on behalf of the Family Key Agents, removes the disks of Family Key Components from the locked box inside the double-locked safe.

Following a sequence of prompts, the disks of Family Key Components (KFC1 and KFC2) are inserted into the Unix workstation, and the components are combined (XORed) to form the Fam-



■ **Figure 5.** *Key generation and chip programming.*

ily Key (KF). Then the Escrow Officers load the disks of Key Numbers (KN1 and KN2) and Random Seeds (RS1 and RS2) into the workstation and enter Arbitrary Input (AI1 and AI2) from the keyboard. The Key Numbers are combined to form the KCK, which is later used to encrypt the Key Components before they are written to floppy disks. The Escrow Officers also enter a starting serial number for generating a sequence of UIDs for the chips. Fig. 5 shows the initial inputs and values generated during key generation.

Generation of Keys — The Random Seeds are combined with the Arbitrary Inputs from the keyboard to generate a stream of pairs of values. One of these values forms a KU and the other a Key Component (KC1). These two values are XORed together to form a second Key Component (KC2); thus KU is the XOR of KC1 and KC2. KC1 and KC2 are encrypted with KCK to form the Encrypted Key Components (EKC1 and EKC2). All three values are separated, and each is paired with the next UID in the sequence.

The stream of KU/UID pairs is passed to the Programming Device, where each pair is programmed onto a chip along with the KF. The first set of encrypted Key Components (EKC1) is written along with corresponding UIDs onto four identical floppies. Similarly, the EKC2s are written onto four additional floppies. These floppies are packaged in tamper-detecting containers and stored in the double-locked safe until the programming session is complete.

Removal and Transportation of Keys — When the programming session is complete, each of the two Escrow Officers from the first Escrow Agent takes two of the four disks with the EKC1 Key Components back to their offices, while each of the two Escrow Officers from the second Escrow Agent takes two of the four disks with the EKC2 Key Components. Before leaving the SCIF, the Escrow Officers write audit records that log their activities, including the range of UIDs generated. They also execute a program that erases key-related data from memory and disk files, and they store the hard disks and copies of the audit logs in the double-locked safe. The originals of the audit logs are carried back to the Escrow Agents.

In the Target System, key escrow data will be transmitted electronically between the Escrow Agent Workstations and the Programming Device using Key Escrow INFOSEC Devices. Cryptography, including confidentiality protection and digital signatures, will be used to protect those communications. The Programming Device will also support automatic logging and high volume chip production.

Key Component Storage and Release

Key Component Storage — Each Escrow Agent stores its disks of key escrow data in two sets of double locked safes. Each safe contains two complete sets of Encrypted Key Components, so there are four sets total. The safes are double locked,

The KES will use configuration management to protect against unauthorized modifications of software. Changes to software will require approval by a Configuration Management Board.

The Attorney General has specified separate procedures for releasing Key Components for wiretaps conducted under Title III, FISA, and state statutes.

and two persons are required to open each. Thus, the storage facilities use two person control, physical security, cryptography, and redundancy to protect the Encrypted Key Component from unauthorized use.

When the two officers for an Escrow Agent return from a chip programming session, they examine each other's tamper-protective disk containers and the numbers placed on those containers to determine if the containers were compromised. The Escrow Officers then fill out an audit record and store a copy of the log along with one set of floppies in each of the two safes. The disks are stored in their tamper-detecting containers and remain untouched in the safes unless they are needed for an authorized intercept. Any evidence of tampering is reported to the Program Manager.

In the target system, the Encrypted Key Components will be stored on an Escrow Agent Workstation. These workstations will use a trusted operating system, strong authentication, cryptography, access controls, and other mechanisms to protect the key escrow data from unauthorized use. In addition, the workstations will be operated in an environment which provides physical security.

Authorization Procedures for Release of Key Components — Key components are to be released only in conjunction with a lawfully authorized wiretap and only in accordance with procedures established by the U.S. Attorney General [9]. The federal law governing interceptions of the content of communications is codified in Title 18, United States Code, Sections 2510-2521 (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by, among other things, the Electronic Communications Privacy Act of 1986) and in Title 50, United States Code, Sections 1801-1811 (the Foreign Intelligence Surveillance Act (FISA) of 1978). In addition, 37 states, as well as the District of Columbia, Puerto Rico, and the Virgin Islands, have statutes permitting interceptions by state and local law enforcement agencies. For a description of the laws and procedures for government wiretaps, see [3].

The Attorney General has specified separate procedures for releasing Key Components for wiretaps conducted under Title III, FISA, and state statutes. In all three cases, a request in the form of a certification must be submitted to the Escrow Agents. This certification must identify the agency responsible for the investigation and individuals involved, certify that the agency is involved in a lawfully authorized wiretap, specify the wiretap's source of authorization and its duration, specify the Device Unique Identifier (UID) whose Key Components are sought, and specify the serial number of the Key Escrow Decryption Processor being used. In addition, a government attorney must be involved in the process. For a federal wiretap, confirmation of the fact of authorized electronic surveillance is provide by an attorney in the U.S. Attorney's Office supervising the investigation (for Title III wiretaps), or the Department of Justice, Office of Intelligence Policy and Review (for FISA wiretaps). For a state wiretap, the principal prosecuting attorney of the state or political subdivision thereof responsible for the investigation will submit the certification.

The procedures specify that upon receiving such certification from an agency requesting the Key Components for a particular UID, the Escrow Agents shall release their Encrypted Key Components to the requesting agency. Prior to or upon completion of the surveillance, the ability of the requesting agency to decrypt communications must be disabled, and the requesting agency may not retain the Key Components for later use.

The Department of Justice will conduct inquiries to verify that the Key Components for a chip are released only in conjunction with an authorized wiretap, that they are used only by an agency authorized to intercept communications encrypted with that chip, and that the ability of the agency to decrypt communications is terminated at the end of the electronic surveillance phase of the investigation.

Key Component Extraction and Transportation — Once an Escrow Agent has received certification requesting the Key Components associated with one or more UIDs, designated Escrow Officers go to one of the safes and locate the disks with the associated Encrypted Key Components. Since the safes are double locked, two Escrow Officers must be present to access the stored disks. The officers remove the disks along with the disks that contain the Key Numbers needed to decrypt those particular Key Components, and write audit records that log the removals.

The Escrow Officers then remove the disks of Encrypted Key Components from their tamper-detecting containers and insert them into a PC in response to instructions (prompts) from a Key Extract Program running on the PC. The program locates the Encrypted Key Components for the given UIDs and writes them, along with their UIDs, onto a separate Key Extract disk. The officers put the Key Extract and Encrypted Key Component disks in tamper-proof containers and return the Encrypted Key Component disks to the safe.

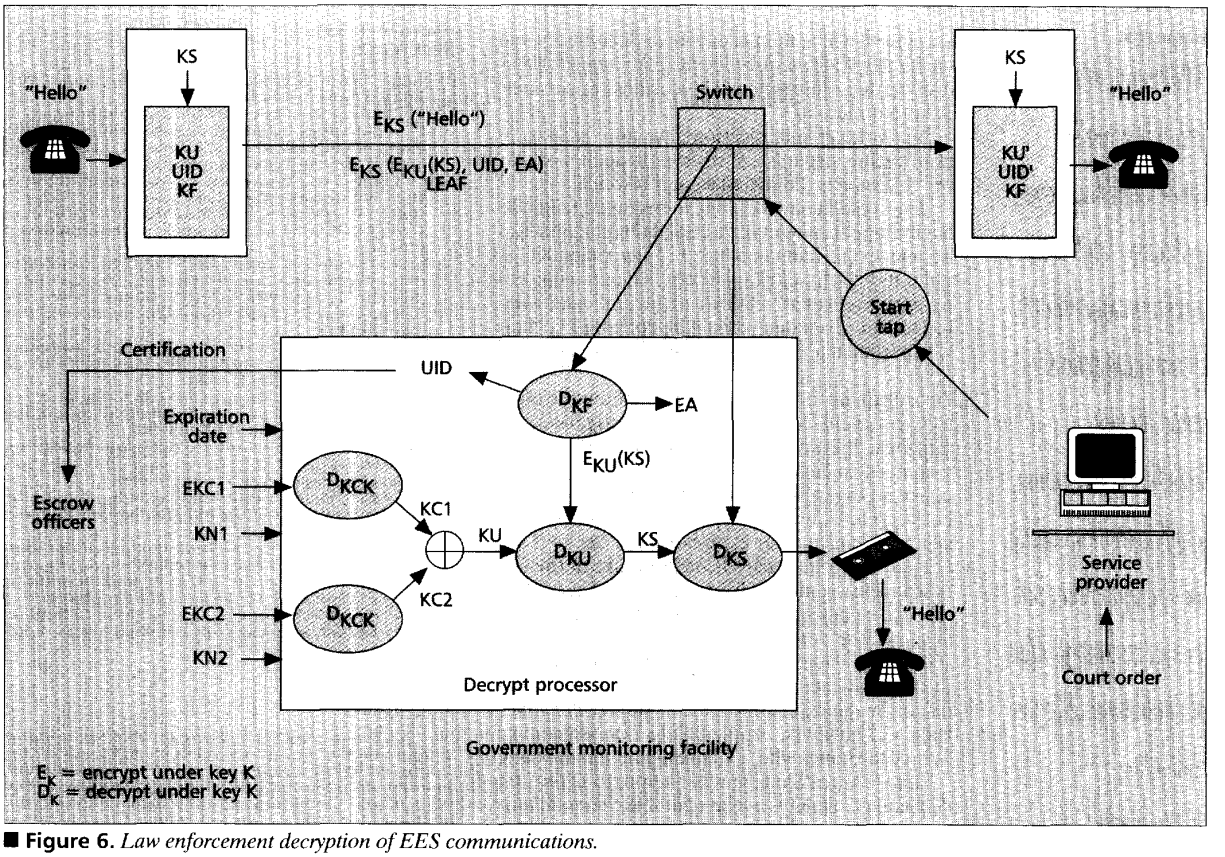
Finally, two Escrow Officers from each Escrow Agent hand carry the Key Extract and Key Number disks to the law enforcement monitoring site. Upon arrival, the Escrow Officers present credentials showing they are authorized to enter the facility.

In the Target System, the entire process will be automated. The Key Components will be extracted from electronic storage by the Escrow Agent Workstation and transmitted electronically to the Key Escrow Decrypt Processor at the law enforcement monitoring site. Cryptography will be used to protect all transmissions. The Escrow Agent Workstation will generate the audit records automatically.

Key Escrow Decryption

After a law enforcement agency has obtained a court order to intercept a particular phone line, the order is taken to the telecommunications service provider in order to gain access to the associated communications. Normally, the agency leases a line from the service provider, who transmits the intercepted communications to a government designated monitoring facility over that line.

If the law enforcement agent monitoring the communications suspects they are encrypted, the line will be set up to pass the communications streams to the Key Escrow Decrypt Processor, which is a PC with a specially designed board. For voice com-



■ **Figure 6.** *Law enforcement decryption of EES communications.*

munications, additional equipment is needed to convert the decrypted digital streams to voice. The complete decryption process and set of equipment involved are non-trivial.

The PC will not start up and operate without a physical encryption key, which is used to decrypt software stored on the PC. The Decrypt Processor has limited functionality so that it can be used only through a menu of key escrow commands.

Initialization of Key Escrow Decrypt Processor — Before the Decrypt Processor can be used to decrypt Clipper communications, it must be initialized with the KF. To do this, representatives of the two Family Key Agents each insert a disk containing their Family Key Component, which they have brought with them in tamper detecting packages. These components are XORed inside the Decrypt Processor to form KF.

Extraction of LEAF and UID — The Decrypt Processor recognizes communications encrypted with an escrowed encryption chip, extracts the LEAF transmitted in each direction, and decrypts the two LEAFs using the KF in order to obtain the UIDs. Once the UIDs have been extracted, they are displayed on the screen. Fig. 6 shows decryption of the LEAF transmitted in one direction.

Although the Decrypt Processor extracts the UID for both the caller and called, the Unique Key of one suffices to decrypt both ends of the conversation. This is because the same Session Key is used for communications sent in both directions. Thus, the UID(s) associated with the subject(s) of the electronic surveillance will be given to the Escrow Agents with the request for Key Components.

Loading of Key Components and Key Numbers — After the Escrow Officers arrive with their disks of Key Numbers (KN1 and KN2) and Key Extract disks of Encrypted Key Components (EKC1 and EKC2), they check that the serial number of the Decrypt Processor is identical to the one specified in the certification request (see the section on authorization procedures for release of key components). If it is, they remove the disks from their tamper-detecting packages and load them into the Decrypt Processor as instructed by prompts. In addition, they type in the expiration date for the electronic surveillance. The Decrypt Processor combines each pair of KN1 and KN2 values and uses the resulting KCK to decrypt the EKC1 and EKC2 values that were encrypted with that key. The Key Components (KC1 and KC2) are then XORed to form the Unique Keys. The Key Extract disks are destroyed and the Key Number disks carried back with the Escrow Officers in new tamper-detecting containers.

Decryption — Once the Decrypt Processor has the KU for a given chip, it is ready to decrypt communications encrypted or decrypted with that chip. To do this, the Decrypt Processor intercepts each LEAF transmitted by the chip at the beginning of a conversation. Using the Family Key, it decrypts the LEAF and extracts the UID and

When the electronic surveillance phase of an investigation terminates, the law enforcement officer issues a command to destroy the Unique Keys in the Decrypt Processor.

encrypted KS. It then uses KU to decrypt KS and verify the EA. Assuming the EA is valid, KS is used to decrypt the communications transmitted in both directions.

For voice communications, the decrypted communication streams are routed through a device which converts the digital signals to voice.

Encrypted conversations intercepted from the beginning of the wiretap up until KU is obtained can be decrypted from recorded tapes. Once KU is obtained, the law enforcement officer can monitor the current conversations in near real-time. Minimization procedures must be followed so that non-pertinent activity is not listened to or recorded.

Termination of Decryption — When the electronic surveillance phase of an investigation terminates, the law enforcement officer issues a command to destroy the KUs in the Decrypt Processor so that subsequent communications cannot be decrypted. This is to be done on or before the date when the court order expires. When the keys are erased, an authenticated confirmation of the key destruction is sent to each Escrow Agent. Thus, retention of keys beyond the period of authorized surveillance will be detected through the audit records. If the Escrow Agents do not receive notification that the KUs have been destroyed within a specified period following expiration of the court order, then they will notify the appropriate Department of Justice authority who will investigate the incident.

The Target System will support automatic deletion of the KUs at the end of the surveillance authorization period. Confirmation of the deletion will be automatically generated and transmitted to the Escrow Agents by the Decrypt Processor.

Summary

We have described the operation of the Interim Key Escrow System as of June 1994. This system is characterized by a combination of manual and automated procedures to manage the key escrow data, and includes extensive safeguards to ensure that escrowed keys are used only in conjunction with lawfully authorized electronic surveillance. In the Target System, many of the manual procedures will be automated, particularly those for transporting keys and generating audit logs.

References

[1] M. Blaze, "Protocol Failure in the Escrowed Encryption Standard," AT&T Bell Laboratories, draft of May 20, 1994.

[2] E. F. Brickell, *et al.*, "The SKIPJACK Review, Interim Report: The SKIPJACK Algorithm," July 29, 1993; available from Georgetown University, Office of Public Affairs, Washington DC, from cpsr.org, or by e-mail from denning@cs.georgetown.edu.

[3] D. P. Delaney, *et al.*, "Wiretap Laws and Procedures: What Happens When the Government Taps a Line," September 23, 1993; available from Georgetown University, Department of Computer Science, Washington DC, from cpsr.org, or by e-mail from denning@cs.georgetown.edu.

[4] M. Harris, "Encryption—Export Control Reform," Statement of Deputy Assistant Secretary of State for Political-Military Affairs, Feb. 4, 1994. (For further information, contact Office of Defense Trade Controls, Bureau of Political-Military Affairs, Department of State, 703- 875-6644.)

[5] National Institute for Standards and Technology, "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication (FIPS PUB) 186, May 19, 1994.

[6] National Institute for Standards and Technology, "Escrowed Encryption Standard (EES)," Federal Information Processing Standards Publication (FIPS PUB) 185, Feb. 9, 1994.

[7] National Institute for Standards and Technology, "Key Management Using ANSI X9.17," Federal Information Processing Standards Publication (FIPS PUB) 171, April 27, 1992.

[8]. National Institute for Standards and Technology, "Secure Hash Standard," Federal Information Processing Standards Publication (FIPS PUB) 180, May 11, 1993.

[9] U.S. Department of Justice, "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III," "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA," and "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to State Statutes," Feb. 4, 1994.

Biographies

DOROTHY E. DENNING is a professor of computer Science at Georgetown University, Washington, D.C. She is author of *Cryptography and Data Security* and numerous papers in the area of information security, and has served as president of the International Association for Cryptologic research. Her current research is focused on policy and technical issues relating to cryptography and wiretapping, and she has been a reviewer of the government's new escrowed encryption technology.

MILES E. SMID is employed by the National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, as manager of the Security Technology Group. His special interest is the integration of cryptography into computer networks for user authentication and secure communications. He has served as a member of both retail and wholesale financial institution data security working groups of the American National Standards Institute (ANSI) and is now the NIST representative to Accredited Standards committee, X9, for Financial Services. He designed the key management system used by the Department of the Treasury in its Electronic Certification System, which is currently in use by more than 60 agencies and represents the first Treasury use of cryptographic methods in place of written signatures for protection of Federal payments. He managed the development of the NIST Cryptographic Smart Card, which provides digital signature and user authentication capabilities, and he was responsible for the development of Federal Information Processing Standard (FIPS) 140-1, "Security Requirements for Cryptographic Modules." Recently, he has been appointed National Program Manager for Key Escrowing. He holds B.S. and M.A. degrees in mathematics and a patent on Cryptographic Key Notarization.