

Escrowed Encryption Systems

Çetin Kaya Koç

Oregon State University

US Cryptography Standards

- Digital Signature Standard: DSS
- Secure Hash Standard: SHS
- Escrowed Encryption Standard: EES

Skipjack encryption algorithm

Clipper and Capstone chips

Key escrowing procedure

Escrowed Encryption Standard

Proposed to reconcile conflicting interests:

- Industry wants secure communications
- Law enforcement wants wiretapping ability

Indiscriminate use of cryptography could make legal electronic surveillance more difficult

es•crow |es-,krō,es-| (MF *escoue* scroll)

a deed, a bond, or a piece of property held in trust by a third party to be turned over to the grantee only upon the fulfillment of a condition

Overview of EES

- Key is escrowed at time of manufacture
- Key is stored with two escrow agencies:
National Institute of Standards and
Technology (Department of Commerce)

Automated Systems Division
(Department of the Treasury)
- Escrow agencies give the key to the law enforcement agency which has the proper authorization
- Each escrow agency stores 80-bit strings, XOR to get the decryption key

Skipjack Algorithm

- Block cipher
- 64-bit input, 64-bit output
- 80-bit key
- 32 rounds of a nonlinear function
- Encryption rate: 15 Mb/s
- Same modes as DES:
64 bit ECB, 64 bit CBC, 64 bit OFB
1, 8, 16, 32, 64 bit CFB

Skipjack is Classified

- Not in software
- Only from authorized manufacturers
- Not open to public scrutiny
- One-month review by a team of five independent cryptographers: **Secure**

E F Brickell	Sandia Labs
D E Denning	Georgetown University
S T Kent	BBN Corporation
D P Maher	AT&T
W Tuchman	Amperif Corporation

Session Key K

- Encrypts the message
- Unique to each session

Unit Key U

- Encrypts the session key
- Embedded on chip, escrowed

Family Key F

- Encrypts “Law Enforcement Access Field”
- Common to all users

Unit Key Generation

- Certain details are not specified
- Programmed inside a vault at chip factory
- Two agents are involved
- Each agent generates random 80-bit string S_1 and S_2
- 32-bit serial number N padded to get three 64-bit strings N_1, N_3, N_3

- Triple encryption to get three 64-bit blocks:

$$R_1 = E(D(E(N_1, S_1), S_2), S_1)$$

$$R_2 = E(D(E(N_2, S_1), S_2), S_1)$$

$$R_3 = E(D(E(N_3, S_1), S_2), S_1)$$

- Concatenate: $R = R_1R_2R_3$
- 80-bit strings U_1 and U_2 are taken from R
- Unit key $U = U_1 \oplus U_2$
- Escrow agencies get U_1 and U_2

Secure Communication

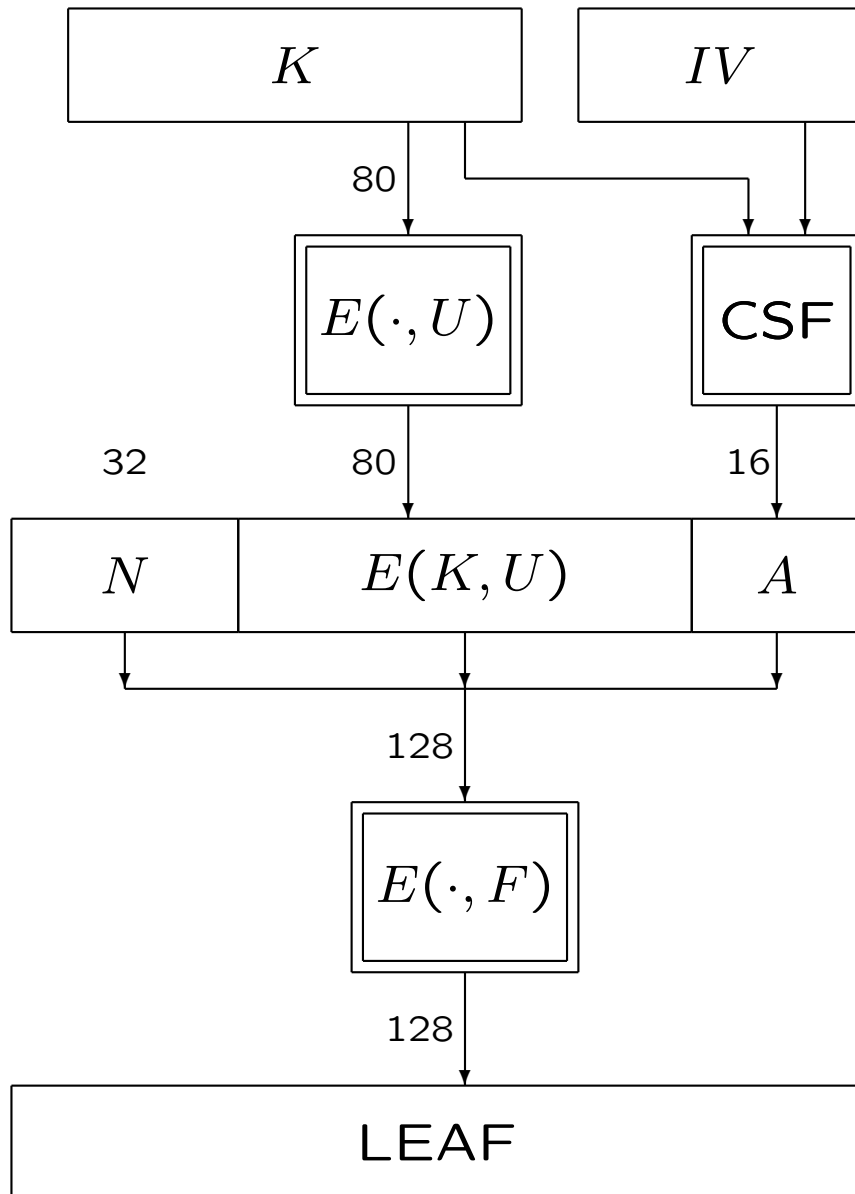
- Agree on a session key K (80 bits)
 - Protocol is not specified
 - A public-key method, e.g., Diffie-Hellman key exchange algorithm can be used
- Message M is encrypted with K
 - Plaintext block: M
 - Ciphertext block: $E(M, K)$
 - E : Skipjack encryption algorithm
 - K is not escrowed

- Law enforcement access field: LEAF
 - Serial number of sender: N (32 bits)
 - Session key is encrypted with unit key: $E(K, U)$
 - Checksum string: A (16 bits)
Computed from session key K and synchronization variable IV
 - Encrypt the 128-bit block $N, E(K, U), A$ with family key: F

$$\text{LEAF} = E(\{N, E(K, U), A\}, F)$$

- LEAF is sent at the beginning of session

LEAF Generation



Receiver

- Decrypts LEAF to get checksum string A
- Examines checksum string A
- If LEAF is valid, then
 decrypts message using session key K

The 16-bit checksum string A is placed to prevent users chopping off LEAF

However, 16-bit may not be enough for secure LEAF generation

Court-authorized Wiretapping

- Uses family key F to decrypt LEAF
- Now has serial number N and encrypted session key $E(K, U)$
- Obtains wiretap authorization from court
- Presents authorization to escrow agencies
- Obtains unit key U to decrypt session key K
- Uses session key K to decrypt the message

Clipper Chip (MYK-78)

- Contains Skipjack and LEAF generation
- 1 micron CMOS technology
- 28 pin, 0.35 watts power, TTL interface
- Unit & family key are installed at the factory
- Design and programming by Mykotronx Inc
- Chip fabrication by VLSI Technology Inc

Capstone Chip (MYK-80)

Clipper plus

- Public-key exchange
- digital signatures
- modular arithmetic functions
- random number generation

Analysis of EES

- Points of attack (external or internal)
 - Escrow agencies
 - Chip factory
 - Courts
- Other Abuses
 - Wiretap beyond authorization period
 - Intentional trapdoor

- Advantages of EES
 - Police can wiretap suspected criminals
 - Citizens obtain secure communication

- Disadvantages of EES
 - Government invasion of privacy
 - Criminals will use unescrowed cryptography or super-encryption
 - Hinders economic competitiveness in security and communications

EES Protocol Failure

In June 1994, Bell Labs researcher Matt Blaze showed that two 'rogue' applications can interoperate without transmitting a valid LEAF

- Generate random LEAFs until the correct checksum string A is obtained

Also a 'rogue' application can interoperate with legal EES users without valid LEAF

Thus, it is possible to have encrypted communication among EES processors without valid LEAF transmission

EES Politics

- Large opposition
- Distrust of government
- Industry sees restrictions
- Effective against criminals?

Fair Public-Key Cryptography (FPKC)

Public-key cryptosystems with escrowed keys

(Proposed by Silvio Micali of MIT)

- Software implementation
- Users generate their own keys
- Users choose their cryptosystem
- No need for tamper-proof hardware
- No need for secret algorithm

Overview of FPKC

- Choose public-key cryptosystem
- Distribute pieces of private key to escrow agencies
- Escrow agencies can verify that they have pieces of private key corresponding to user's public key without disclosing pieces of key

Diffie-Hellman

- Prime p and element g common to all users
- Alice:
private key x , public key $A = g^x \pmod{p}$
- Bob:
private key y , public key $B = g^y \pmod{p}$
- Alice and Bob both calculate the shared key:

$$K = g^{xy} \pmod{p}$$

Fair Diffie-Hellman

- Assume 5 trustees (esrow agencies)

- Alice chooses 5 secret numbers

$$x_1, x_2, x_3, x_4, x_5 \in [1, p - 1]$$

- Let $x = \sum x_i \pmod{p - 1}$

- Private key: x , Public key: $A = g^x \pmod{p}$

- x_i s are private pieces of key

- Public pieces of key: $t_i = g^{x_i} \pmod{p}$

- Trustee i gets x_i and t_i
- Trustees together verify that $\prod t_i = A$
$$\prod t_i = \prod g^{x_i} = g^{x_1+x_2+x_3+x_4+x_5} = g^x = A$$
- This ensures that $\sum x_i$ is Alice's private key
- Four of the trustees cannot find Alice's private key
- Alice and Bob communicate as usual

RSA Cryptosystem

- Pick two primes: p and q
- The modulus is the product: $n = pq$
- Euler's function $\phi(n) = (p - 1)(q - 1)$
- Select $e \in (1, \phi(n))$ with $\gcd(e, \phi(n)) = 1$
- Compute $d = e^{-1} \bmod \phi(n)$
- Public key: e , Private key: d
- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$

Making RSA Fair

- Let p be a prime and $t = x^2 \pmod p$
- The equation $x^2 = t \pmod p$ has two solutions: $\pm x$
- If $p = 3 \pmod 4$, then x can be found easily
$$x = t^{(p+1)/4} \pmod p$$
- If $n = pq$, then the equation $x^2 = t \pmod n$ has four solutions: $\pm x$ and $\pm y$
- Solving $x^2 = t \pmod n$ is hard; If you can find both roots x and y , then you can factor n

- Since $x^2 = t$ and $y^2 = t$ modulo n , we have

$$\begin{aligned}x^2 - y^2 &= 0 \pmod{n} \\(x - y)(x + y) &= 0 \pmod{n}\end{aligned}$$

Thus, either $\gcd(n, x - y)$ or $\gcd(n, x + y)$ is one of the prime factors p or q

- Jacobi symbol: $J(a, n) = +1$ or -1

- Jacobi symbol is multiplicative

$$J(ab, n) = J(a, n)J(b, n)$$

- Of the four square roots modulo n , two are Jacobi $+1$ and two are Jacobi -1

- If you know a Jacobi $+1$ root **and** a Jacobi -1 root of $t \in (1, n)$, then **you can factor** n and find the private key d

Fair RSA

- Alice chooses primes p and q
- $n = pq$ and $p, q = 3 \pmod{4}$
- Alice chooses 5 Jacobi $+1$ integers

$$x_1, x_2, x_3, x_4, x_5 \in Z_n^*$$

where Z_n^* is set of integers modulo n , which are relatively prime to n

- Let $x = \prod x_i \pmod{n}$ and $s = \prod x_i^2 \pmod{n}$

- Alice computes y , a Jacobi -1 root of s
- $y^2 = s = \prod x_i^2 = (\prod x_i)^2 = x^2$
- x and y are Jacobi $+1$ and Jacobi -1 roots of s , respectively
- Anyone who knows x and y can factor n
- Alice sends x_i and y to trustee i
- Trustee i checks that x_i is Jacobi $+1$ and that y is Jacobi -1

- By sharing the x_i^2 s, trustees can verify that

$$\prod x_i^2 = y^2$$

and thus that $\prod x_i$ is a Jacobi +1 root of $s = y^2$

- Trustees together can produce a Jacobi +1 and a Jacobi -1 root of s
- Therefore, trustees can factor n , and recover private key
- Cooperation of all 5 trustees is necessary to factor n

EES versus FPKC

EES:

- Requires users to trust key generation center
- Requires secure hardware
- No software implementations
- Automatic key registration
- Process is invisible to users
- Possible abuse by authorities, not users

EES versus FPKC

FPKC:

- Users generate own keys
- No secure hardware is needed
- Software implementations are possible
- Key registration is more complicated
- Users have more responsibility
- Abuse by users more of a concern

Additional Features in FPKC

- A subset of trustees can reconstruct private key in case a trustee loses data
 - Example: 4 out of 5
- Time-limited access
 - Keys with expiration periods

Needs of Customers and Suppliers

- Customers:
 - good enough security
 - interoperability
 - data recovery
- Suppliers:
 - customer's needs
 - exportability
 - single product line

Concerns of Government

- surveillance capability
- legal issues
- key certification authority
- algorithm certification authority
- standards

Policy Issues

- Key escrowing is ineffective against criminals unless ordinary cryptography is illegal
- Will ordinary cryptography become illegal?
- Ordinary cryptography would be legal but unusual and unsupported
- Criminals will use unescrowed keys or super-encryption even if it is illegal to do so

Desired Properties of Escrowed Encryption

- Multiple algorithms
 - compatibility
 - evaluation
 - certification
 - variable key size
 - flexible structures (e.g., S-boxes)
- Software and hardware implementation

- Secure communication for ordinary user
- Access to message by an authorized party
- Audit trail: No undetectable wiretaps
- Resistant to abuse by users or authorities
- Time-limited access

Open Questions

- Ownership of digital data
- Hierarchy of key escrow systems
 - Within a corporation
 - Nationwide
- Cryptographic locksmith
- Crypto-anarchy