Lecture 6:
Two Fish on the Rijndael

The algorithm might look haphazard, but we did everything for a reason. Nothing is in Twofish by chance. Anything in the algorithm that we couldn't justify, we removed. The result is a lean, mean algorithm that is strong and conceptually simple.

Bruce Schneier

CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Menu

- Clipper
- AES Program
- RC6
- Blowfish
- AES Winner - Rijndael

Breaking Grades File

- Not in my office or any UVA computer
  - Do not try to break into any UVA computer
- Home PC: C:\cs588\grades.txt (encrypted)
  - If you obtain that file, it tells you what to do next
- Adelphia Cable Modem
- My browser is set to disallow ActiveX, allow Java and JavaScript

Clipper

- 1993 – AT&T markets secure telephony device
- Law enforcement: US courts can authorize wire taps, must be able to decrypt
- NSA proposes Clipper Chip
  - Secret algorithm (Skipjack), only implemented in hardware

Key Escrow

- NSA has copy of special key, can get with a court order
- Sender transmits $E(M, k) \| LEAF$ ("law enforcement agents' field")
- Holder of special key can decrypt LEAF to find message key and decrypt message

LEAF

f known by FBI

$LEAF = E((E(k, u) \| n \| a), f)$

k = message key

u = 80-bit special key (unique to chip)

n = 30-bit identifier (unique to chip)

a = escrow authenticator

f = 80-bit key (same on all chips)

Wire Tap

- FBI investigating Alice, intercepts Clipper communication
- Uses f to decrypt LEAF:

  $D(E((E(k, u) \| n \| a), f)) = E(k, u) \| n \| a$
- Delivers n and court order to 2 escrow agencies, obtains u
- Decrypts $E(k, u)$ to obtain message key and decrypt message

Two Escrow Agencies

- Proposal didn't specify who (one probably NSA)
- Divide u so neither one can decrypt messages on their own (even if they obtain f)

One gets $u \oplus X$, other gets X

Clipper Security

- How do you prevent criminals from transmitting wrong LEAF?
  - NSA solution: put it in hardware, inspect all Clipper devices
    - Still vulnerable to out-of-the box device

Clipper Politics

- Not widely adopted, administration backed down
  - Secret algorithm
  - Public relations disaster
    - Didn't involve academic cryptographers early
    - Proposal was rushed, in particular hadn't figured out who would be escrow agencies
- See http://www.eff.org/pub/Privacy/Key_escrow/Clipper/
- Future?: Senators have called for new Clipper-like restrictions on cryptography
- Lessons learned well for AES process

AES

- 1996: NIST initiates program to choose Advanced Encryption Standard to replace DES
- Requests algorithm submissions: 15
- Requirements:
  - Secure for next 50-100 years
  - Performance: faster than 3DES
  - Support 128, 192 and 256 bit keys
    - Brute force search of 2^{128} keys at 1 trillion keys/second would take 10^{18} years (10^8 * age of universe)
  - Must be a block cipher

AES Process

- Open Design
  - DES: design criteria for S-boxes kept secret
- Many good choices
  - DES: only one acceptable algorithm
- Public cryptanalysis efforts before choice
  - Heavy involvements of academic community, leading public cryptographers
- Conservative (but quick): 4 year+ process

AES Round 1

- 15 submissions accepted
- Weak ciphers quickly eliminated
  - Magenta broken at conference!
- 5 finalists selected: MARS (IBM), RC6 (Rivest, et. al.), Rijndael (top Belgium cryptographers), Serpent (Anderson, Biham, Knudsen), Twofish (Schneier, et. al.)
  - Security v. Performance is main tradeoff
    - How do you measure security?
  - Simplicity v. Complexity
    - Need complexity for confusion
    - Need simplicity to be able to analyze and implement efficiently

Breaking a Cipher

- Real World Standard
  - Attacker can decrypt secret messages
  - Reasonable amount of work, actual amount of ciphertext
- "Academic" Standard
  - Attacker can determine something about the message
  - Given unlimited number of chosen plaintext - ciphertext pairs
  - Can perform a very large number of computations, up to, but not including, 2^n, where n is the key size in bits (i.e. assume that the attacker can't mount a brute force attack, but can get close)

AES Evaluation Criteria

1. Security
   Most important, but hardest to measure
   Resistance to cryptanalysis, randomness of output
2. Cost and Implementation Characteristics
   Licensing, Computational, Memory
   Flexibility (different key/block sizes), hardware implementation

From RC5 to RC6 in seven easy steps

From Rivest's RC6 talk, http://www.rsasecurity.com/rsalabs/aes/

Description of RC6

- RC6-*w*/*r*/*b* parameters:
  - *Word size* in bits: w (32) (lg(w) = 5)
  - Number of *rounds*: r (20)
  - Number of *key bytes*: b (16, 24, or 32)
- Key Expansion:
  - Produces array S[0, ... $2r + 3$] of w-bit *round keys*.
- Encryption and Decryption:
  - Input/Output in 32-bit registers A,B,C,D

Design Philosophy

- Leverage experience with RC5: use *data-dependent rotations* to achieve a high level of security.
- Adapt RC5 to meet AES requirements
- Take advantage of a new primitive for increased security and efficiency: *32x32 multiplication*, which executes quickly on modern processors, to compute rotation amounts.