CSC 580
Cryptography and Computer Security

The Advanced Encryption Standard (AES)

February 7, 2017

Overview

Today:

- HW3 solution review
- Brief project phase 1 discussion (more on Thurs)
- Overview of the Java Cryptography Architecture
- AES (from handout)

To do before Tuesday:

- Study for HW3 quiz
- Start reading Chapter 7

Reminder: DES and AES for CSC 580

We will focus on *how to use block ciphers securely*.

Important to understand big picture issues:

- What parameters describe block ciphers?
- What properties does a good block cipher have?
- How do parameters affect those properties?
- How did parameters change historically as capabilities grew?

How block ciphers work (internals):

- We will view as a “black box” with certain I/O behavior
- Internals are interesting, but avoided here to save time

What's Wrong with DES?

Recall from last time:

- Can brute force a 56-bit key in a matter of days now
- Not designed for software
  - Can repeat use to increase security, but inefficient

Not discussed before: Block size

- "Collision attacks" follow "birthday problem" probabilities
  - With just 23 people, 50% chance that two have the same birthday
  - Roughly square-root of "universe size" (sqrt(365) = 19.1…
- Applies to some applications of block ciphers
  - "universe" is number of possible ciphertext outputs
  - sqrt(2^{64}) = 2^{32} - requirement for both time and space (memory)
  - Trivial by today's standards

Bottom line: Key is too small, block size is too small, and too inefficient...

Key Size

Is 128 bits enough?

2004 Estimate: $100k machine breaks 56-bit DES key in 6 hours

What about a 128-bit key?
$100k machine takes >$10^{18}$ years [the earth is <10^{10} years old]

What if we spent $100,000,000,000?
Would take >10^{12} years

What about Moore's law saying that in 20 years machines will be about 16,000 times faster?
Would take >10^{8} years

OK, what about in 40 years (machines 100 million times faster)?
Would still take >30,000 years

Do you really think Moore's law will last this long?

Block Size

Is 128 bits enough?

Birthday attack:

- Requires sqrt(2^{128}) = 2^{64} time and space
- Space is 2^{64} 128-bit entries, for a total of 16*2^{64} = 2^{68} bytes
- One terabyte is 2^{40} bytes → requires 256 million terabytes
- At $35/TB that would cost around $9 billion (plus power, …)

Seems pretty safe...

AES Selection Process

1993-1995: Clipper Chip fiasco

1997: Request for proposals for new standard block cipher

- Must use 128-bit block
- Must support 128-bit, 192-bit, and 256-bit keys
- Selection process through open evaluation

1999: 15 good submissions narrowed to 5 finalists

2000: Winner selected

- Winner was an algorithm named Rijndael (limited to 128-bit blocks)
- Invented/submitted by Vincent Rijmen and Joan Daemen (Belgians)

Important points:
- Very open, public process
- No secret modifications
- Not rushed

More trust!

AES - Some Final Points

In 20 years, no practical cryptanalytic attacks discovered

Approved for protecting classified information

- 128 bit keys for SECRET
- 192 or 256 bit keys for TOP SECRET
- Note: implementation must be approved

Efficiency

- Works on byte/word units: Efficient in software!
- Widespread standard → special fast CPU instructions now
  - Intel AES-NI instructions: over 10 gigabits/sec on a single core!
  - OpenSSL demo...
- Still simple enough for special-purpose hardware
  - 30+ Gbps possible