A survey of the AES process

David Wagner
University of California, Berkeley
30 Sept. 1999

What's an AES?

- AES = Advanced Encryption Standard; an in-progress standards effort
  - Bulk data encryption for the masses
  - Extremely high security, high performance

$\Rightarrow$ Likely to be the international cipher of choice for the next 30+ years

. . . And, it's an interesting microcosm of the art of cipher design.

Key issues

- Challenges:
  - What are the figures of merit? (threat models, performance goals)
  - And how do we design a cipher with strong assurance that it will live up to our goals?

Making a quantitative science out of a field that's widely viewed as a black art

Organization

- Background: A history lesson
- An overview of the AES process
- Past: Round 1 candidates
- Present: Round 2 finalists
- Future: A winner?

DES: The Data Encryption Standard

- DES: The first bulk encryption standard
  - Issued in 1977, with an anticipated lifetime of 5 years
- A tremendous success...
  - Became the de facto standard world-wide
  - Partly responsible for the birth of an entire field
- ...but initially highly controversial
  - IBM's initial submission was modified by the NSA
  - Key length reduced and magic constants changed; no justification offered

DES today

- Today, DES is obsolete
  - Has exceeded its expected lifetime by a large margin
  - Researchers recently demonstrated that DES can be broken in days with a $250,000 initial investment into custom hardware
- A replacement is long overdue

Lessons from DES

Plan for the standard to be used far more widely than you think:

- Not just in government systems, but internationally
- Not just in hardware, but in software, and on crazy platforms you'd never expect
- And it will be used long past its anticipated lifetime

$\Rightarrow$ Solution: over-engineer, be terribly conservative.

More lessons

Only a totally-open process will be trusted:

- With DES, NIST had to ask the NSA for help, because the public knowledge just wasn't up to the task
- The research community has learned a lot since then
- Today, any hint of secret influence would inspire tremendous distrust

$\Rightarrow$ Solution: tap the academic research community for designs, analysis

Philosophy and organization of the AES effort

- NIST organizes the standards effort,
  - but relies heavily on input from the research community
- Goal: design an encryption standard for the federal government
  - A replacement for DES
  - Like occurred with the DES, the AES will surely be widely adopted in the commercial sector without delay
  - Will need to be secure for 50–100 years

An overview of the process

A lengthy, multiple-round process:

1997 Round 0: NIST publishes requirements, asks for submissions

1998 Round 1: everybody analyzes candidates, NIST picks ~ 5 finalists

1999 Round 2: everybody analyzes finalists, NIST picks “one or more” winner(s)

2000 NIST releases a draft standard

2001 NIST makes it official!

Requirements (Round 0)

- The AES must be free of intellectual property restrictions
  - Submitters give away all rights if they win,
    but can keep patents if they lose
- The AES must be high-performance
  - Faster than triple-DES
- The AES must support large keysizes
  - 128, 192, and 256 bit keysizes required
- The AES must be a block cipher
  - Disadvantage: other approaches might yield higher-performance
  - Benefit: more experience with block ciphers than any other approach
  - Benefit: can build other cryptographic primitives out of a block cipher

Round 1 candidates

- 15 submissions were accepted into Round 1
- Lots of diversity
  - Several high-level structures; also some novel constructions
- Different design philosophies (conservative vs. aggressive)
  - Even a surprise weapon or two: e.g., the DFC team had a new trick (‘decorrelation’) up their sleeve

Round 1 analysis

- Several weak ciphers were quickly weeded out
  - Magenta (broken in real-time at the conference where it was presented)
  - LOKI97 (differential cryptanalysis)
  - Frog (differential cryptanalysis)
  - DEAL (small flaw)
  - SAFER+ (small flaw)
- Interestingly, the weakest ciphers were also among the slowest

Analysis

- Tempting to think of the analysis process as a demolition derby
  - Last guy left standing wins?
- But that's unrealistic
- The easy attacks are always discovered first
  - And indeed, the pace has already slowed substantially
- Most submissions will remain unbroken till the end of the AES process
  - The real question is, which ones will be secure for 30 years?

Performance-driven design

- You can make almost anything secure by adding more complexity,
  - but performance may suffer
- An emerging methodology: performance-driven design
  - Evaluate alternative security mechanisms in terms of their impact on the speed budget
  - No point in building a secure cipher if it's so slow that noone will use it

$\Rightarrow$ Compare AES candidates by their security-vs.-performance tradeoff

More on performance

- The catch: many measures of performance
  - Throughput (software); memory usage (smartcards); chip area (hardware); key agility (routers)

- The Twofish philosophy: the high-end just keeps getting faster, but the low-end never goes away

  $\Rightarrow$ Aim for good performance across a broad range of platforms, and give the implementor lots of tradeoffs

Round 2 finalists

NIST selected five finalists:

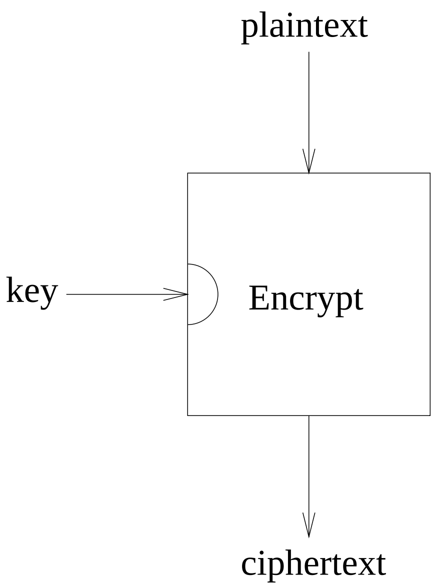
- MARS: fast, a ‘kitchen sink’—uses almost every trick in the book (IBM)
- RC6: fast, utterly simple, uses only data-dependent rotations (RSADSI)
- Rijndael: fast, elegant, unpronouncable (two top designers from Belgium)
- Serpent: ultra-conservative (three top cryptanalysts from all over)
- Twofish: fast, ‘a duct tape cipher’ (Counterpane et. al)

I’ll show you their innards in a moment.

Disclaimer: These are my opinions. I’m on the Twofish team, so I’m biased.

First: What's a block cipher?

Block cipher: encrypts data in blocks



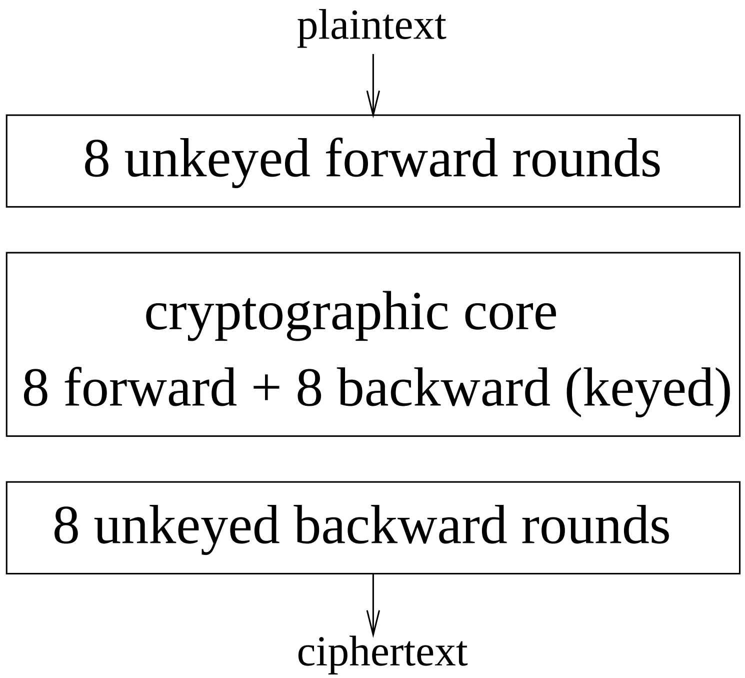
Definition of security: must resist chosen plaintext/ciphertext attack

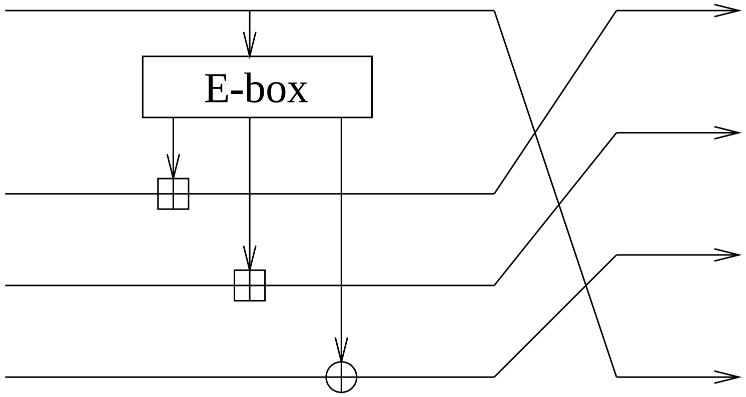
Typical internal components of a block cipher

- Confusion: non-linearity
  - S-boxes
  - Multiplies, data-dependent rotates
- Diffusion: mix up the bits
  - XOR, addition
  - MDS matrices
  - Decorrelation

And now, with that background, back to the innards of the AES finalists.

MARS

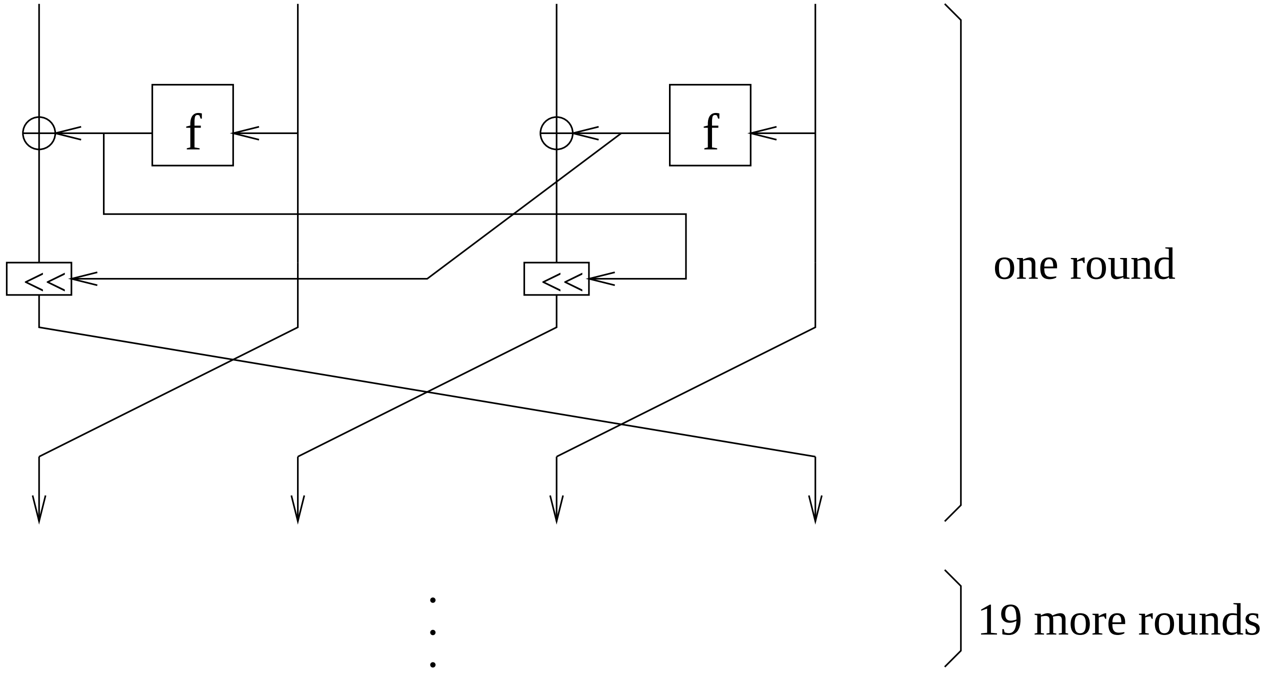




one forward round

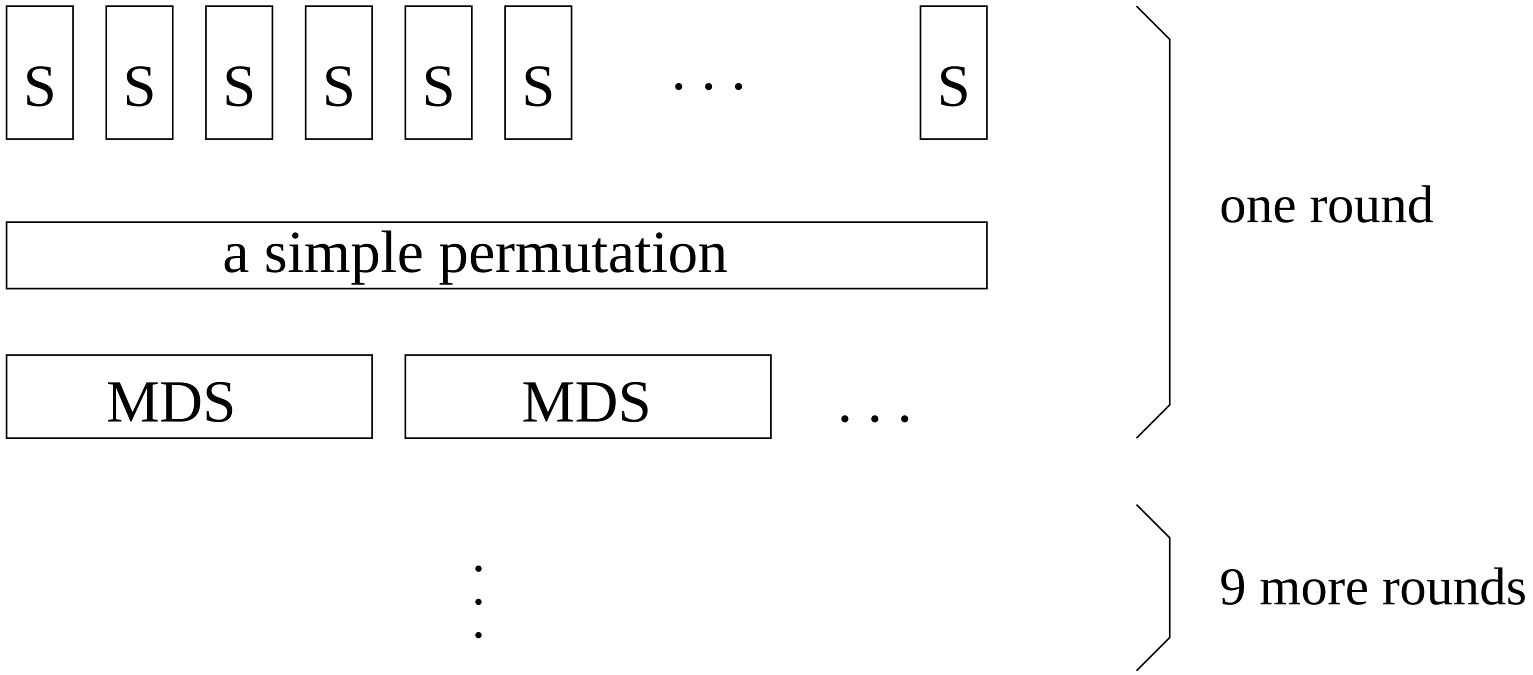
Uses: data-dependent rotations, multiplies, S-boxes, additions, XORs.

RC6



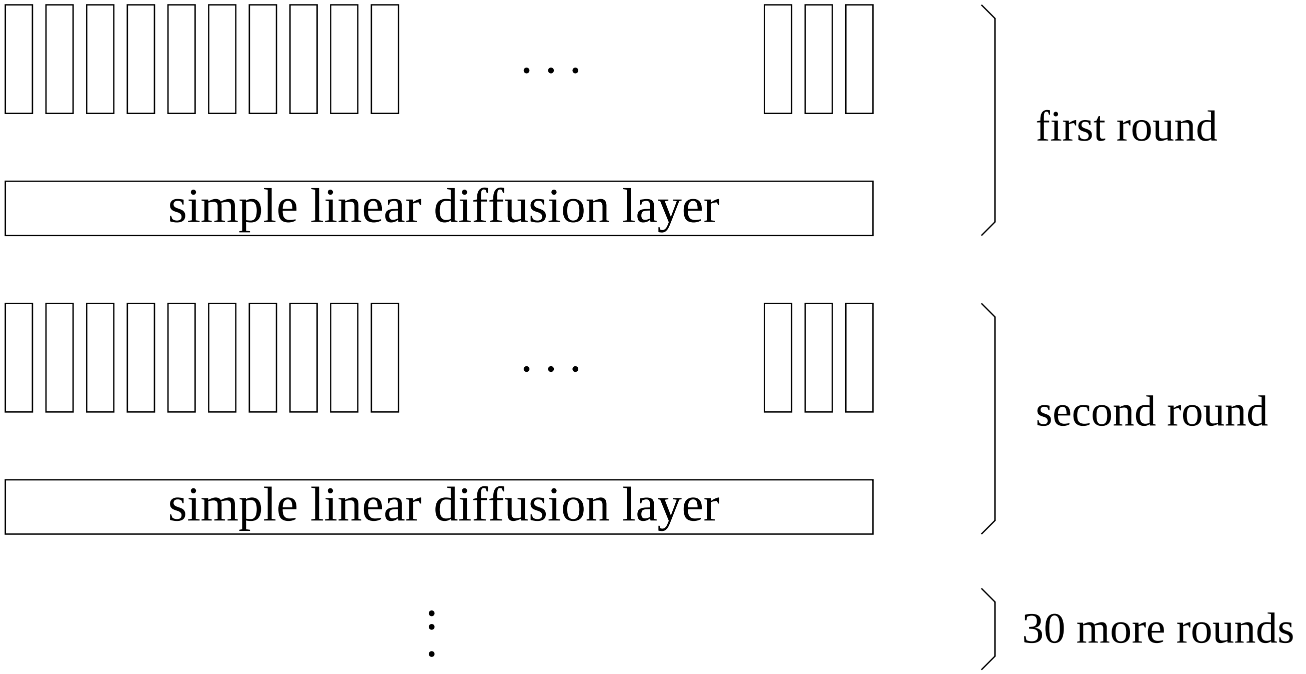
Uses: data-dependent rotations, multiplies.

Rijndael



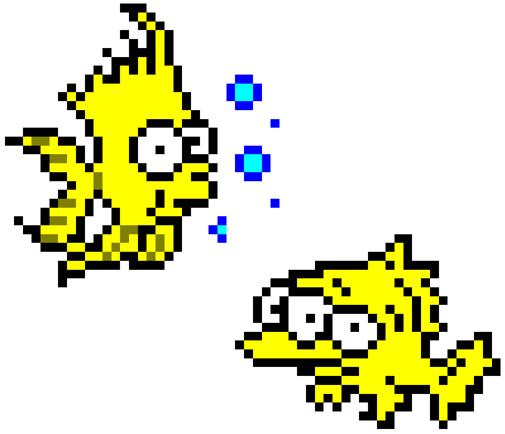
Uses: 8-bit S-boxes, MDS matrices.

Serpent



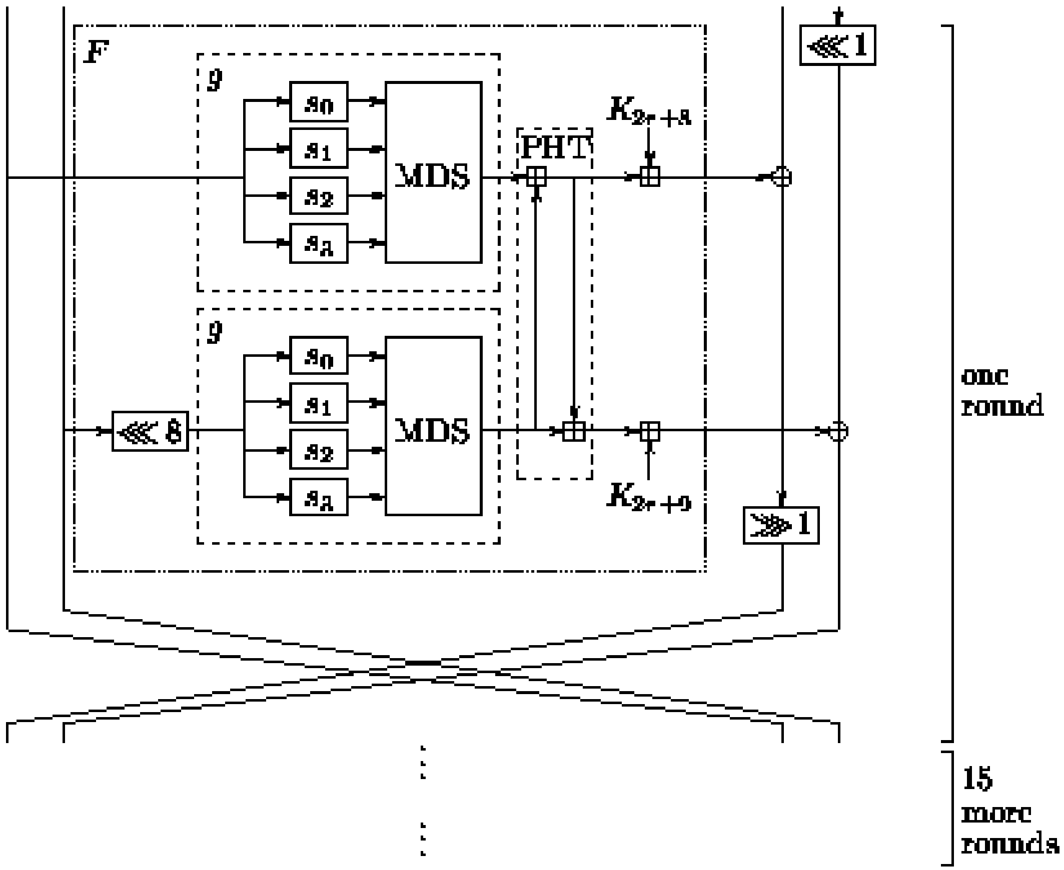
Uses: 4-bit S-boxes, XORs. Bitslice implementation tricks.

Twofish



Eats: snakes, planets, tasty Belgian after-dinner treats.

Twofish



Uses: 8-bit key-dependent S-boxes, pseudo-Hadamard, addition, XORs.

Tradeoffs

Each finalist aims for a different sweet spot:

- MARS: fast on targeted platforms but complex
- RC6: simple and fast on targeted platforms, but low security margin
- Rijndael: fast everywhere, simple, and decent security margin
- Serpent: huge security margin, but comparatively slow
- Twofish: fast everywhere, large security margin, but a bit complicated

More details below.

A breakdown of the finalists

Cipher	Speed	Speed	Security margin	Elegance	Smartcards?
Serpent	62	69	huge	pretty	yes
MARS	23	34	medium	kitchen sink	barely
RC6	15	43	small	very simple	iffy
Rijndael	18	20	medium	gorgeous	yes
Twofish	16	18	large	duct tape	yes

Speeds are measured in cycles/byte. All other data is purely subjective.

Round 2 analysis

- Cryptanalysis results on round 2 finalists are far and few between
  - Best result is an attack on 15 of 20 rounds of RC6
  - One exception: implementation attacks (only relevant on smartcards)
- Don't expect this to change too much

- Also some forward-looking performance analysis
  - Rijndael screams on future platforms; Twofish also does very well

Looking to the future

My personal favorites, for those keeping score at home:

- I like Rijndael best of all.
  - It sacrifices almost nothing
  - Its only weak spot is its unexceptional security margin
- Honorable mention to Twofish.
- But watch Serpent closely.
  - Its ultra-conservative design could win the day

Summary

- The AES will have a broad impact on information security
  - Side effect: it is bringing together the academic research community, and helping to advance the state of the art
- This is your standard! Vote early, vote often.