IBM AES3 Comments

MARS

- Unique heterogeneous design
- Comprehensive security analysis
  - Security was primary design goal
  - Ability to analyze was an important goal (unbalanced Feistel, choice of op's, …)
  - Reflected in analyses performed to date
- High performance
- Very robust: large security margins

Performance/Complexity/Security

Cipher	Performance C Mb/sec*	Setup Clocks*	Complexity LOC*	Security R/Min R
RC6	94.2	1875	116	1.0
MARS	69.4	2134	424	1.6
Twofish	68.8	8493-15616	496	1.6
Rijndael	50.5-70.3	207-1983	449	1.3-1.8
Serpent	26.7	1296	623	1.9

* Performance numbers and lines-of-C-code refer to Brian Gladman's implementation

MARS Pseudo-Code

mixing

```
(A,B,C,D) = (A,B,C,D) + (K[0],K[1],K[2],K[3])
For i = 0 to 7 do {
        B = (B ⊕ S0[A]) + S1[A>>>8]
        C = C + S0[A>>>16]
        D = D ⊕ S1[A>>>24]
        A = (A>>>24) + B(if i=1,5) + D(if i=0,4)
        (A,B,C,D) = (B,C,D,A)
}
```

core

```
For i = 0 to 15 do {
        R = ((A<<<13) × K[2i+5]) <<< 10
        M = (A + K[2i+4]) <<< (low 5 bits of (R>>>5))
        L = (S[M] ⊕ (R>>>5) ⊕ R) <<< (low 5 bits of R)
        B = B +L(if i<8) ⊕ R(if i≥8)
        C = C + M
        D = D ⊕ R(if i<8) + L(if i≥8)
        (A,B,C,D) = (B,C,D,A<<<13)
}
```

Mixing^{-1}

```
For i = 0 to 7 do {
        A = A - B(if i=3,7) - D(if i=2,6)
        B = B ⊕ S1[A]
        C = C - S0[A<<<8]
        D = (D - S1[A<<<16]) ⊕ S0[A<<<24]
        (A,B,C,D) = (B,C,D,A<<<24)
}
(A,B,C,D) = (A,B,C,D) - (K[36],K[37],K[38],K[39])
```

Note on "Security Margins"

- Common measure: "how many more rounds than what is necessary by cryptanalysis"
- This is quite meaningless
  - Without a major breakthrough in analysis, all five candidates are secure
  - But such breakthrough will render current bounds completely useless
  - How to protect against such event?

Question your trust

- Real security margins: question the very thing in the cipher which you trust to be secure
- Example: both MARS and RC6 rely on the strength of data-dependent rotations
  - If a radically better understanding of this operation is discovered, RC6 will be most likely be broken
  - MARS probably not, since it has many fail-stop mechanisms
    - E.g., S-box, wrapper layers, …

MARS design philosophy

1. Design a strong cipher
   - Other ciphers stopped here
2. Add many fail-stop mechanisms, in case your underlying assumptions are wrong
   - As many fail-stop mechanisms as possible, while maintaining a workable solution
- Fail-stop mechanisms cost sometimes
  - MARS is still suitable for all environments

Other AES Finalists

- RC6
  - \+ High performance
  - – Security margin, “single point of failure”
- Rijndael
  - \+ Performance with 128-bit key
  - – Performance with 256-bit key
  - – Non-traditional: “algebraic structure” may lead to attack
- Serpent
  - \+ Security margin
  - – Performance
- Twofish
  - \+ Performance
  - – “Key dependent S-box”: key setup time, hard to analyze
  - – The least understood cipher. Very steep learning curve.

Best AES Choice: MARS

- Only candidate with hybrid structure
  - "Future-proof" design, many fail-stop mechanisms
- Carefully analyzed security
  - Independent analysis confirms claimed security
- Utilizes time-tested cipher methods
  - Feistel, S-box, data-dependent rotations, …
- Balanced Security/Performance