Symmetric Encryption: AES

Yan Huang

Credits: David Evans (UVA)

Advanced Encryption Standard

- 1997: NIST initiates program to choose Advanced Encryption Standard to replace DES

- Why not just use 3DES?

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 Requirements

- Secure for next 50-100 years
- Royalty free
- 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^{19} years (10^{9} * age of universe)

AES Round 1

- 15 submissions accepted
- Weak ciphers quickly eliminated
  - Magenta broken at conference!
- 5 finalists selected:
  - MARS (IBM)
  - RC6 (Rivest, et. al.)
  - Rijndael (Belgian cryptographers)
  - Serpent (Anderson, Biham, Knudsen)
  - Twofish (Schneier, et. al.)

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

AES Criteria Tradeoffs

- Security v. Performance
  - 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

- Intuitive Impression
  - Attacker can decrypt secret messages
  - Reasonable amount of work, actual amount of ciphertext
- "Academic" Ideology
  - 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)

Choosing AES

(Table from Twofish Paper)

Cipher	Speed (32)	Speed (8)	Safety Factor	Simplicity (code size)
Serpent	62	69	3.56	341 KB
MARS	23	34	1.90	85 KB
RC6	15	43	1.18	48 KB
Rijndael	18	20	1.11	98 KB
Twofish	16	18	2.67	104 KB

(cycles/byte encrypt)

Attempt to measure security = number of rounds / max rounds breakable

(academic breaks count)

AES Winner: Rijndael

Invented by Joan Daemen and Vincent Rijmen

Rijndael. A variant of Square, the chief drawback to this cipher is the difficulty Americans have pronouncing it.

Bruce Schneier

Selected as AES, October 2000

Choosing AES

(Table from Twofish Paper)

Cipher	Speed (32)	Speed (8)	Safety Factor	Simplicity (code size)
Serpent	62	69	3.56	341 KB
MARS	23	34	1.90	85 KB
RC6	15	43	1.18	48 KB
Rijndael	18	20	1.11	98 KB
Twofish	16	18	2.67	104 KB

(cycles/byte encrypt)

Attempt to measure security = number of rounds / max rounds breakable

(academic breaks count)

Rijndael Overview

- Key sizes: 128, 192, 256 bits
- Block sizes: 128, 192, 256 bits
- 10 rounds (including initial AddKey)
  - Academic break on 9 rounds, 256-bit key gives safety factor of 10/9 = 1.11
    - Requires 2^{39} work and 2 chosen related-key plaintexts [BKN09, CRYPTO]

"Our results have no practical significance for anyone using the full Rijndael."

Rijndael Design

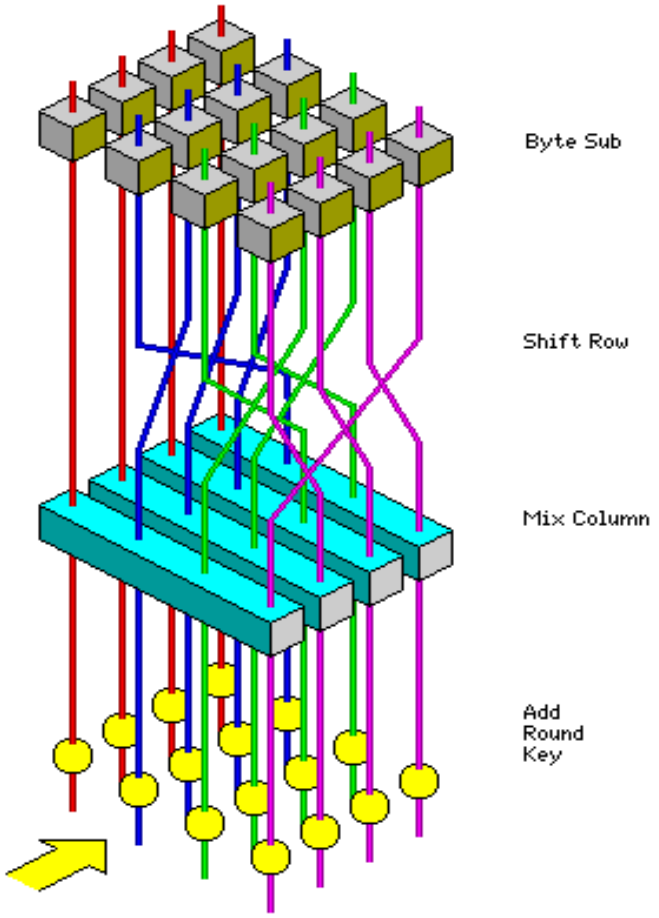
- View bytes as elements in finite field

  $10110010 = x^7 + x^5 + x^4 + x^1$

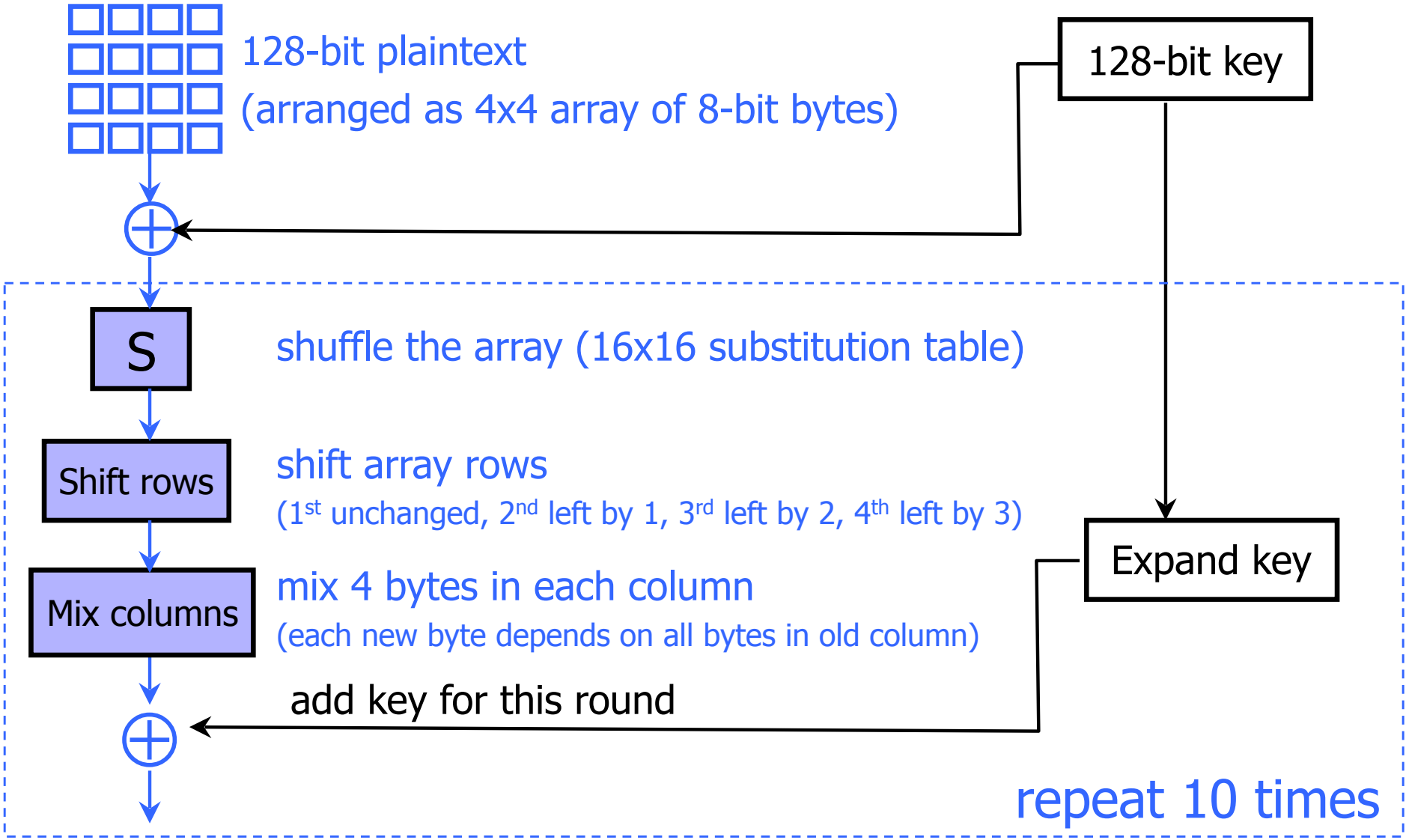
- More complex than RC6, but still simple:
  - Specification of cipher is < 8 pages (big type and diagrams)
- Not a Feistel cipher: each round operates on all bits
- 10-14 rounds depending on key and block size
  - 3DES ~ 48 rounds

Rijndael Round

1. Byte substitution using non-linear S-Box (independently on each byte)
2. Shift rows (square)
3. Mix columns – matrix multiplication by polynomial
4. XOR with round key



Basic Structure of Rijndael



Will AES survive until 2050?

- XSL Algebraic Attacks [Courtois & Pieprzyk 2002]
- 128-bit AES can be written as a system of 8000 quadratic equations with 1600 unknowns
  - Solving those equations breaks AES!
  - Only a few known plaintexts required (but $\sim 2^{100}$ work)

"The XSL attack is not an attack. It is a dream."

Vincent Rijmen (co-designer of AES)