Cryptography and Network Security

ADVANCED ENCRYPTION STANDARD

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	4 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Introduction

- AES Selection process
- AES Encryption & Decryption details
- Details of every round structure
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
- Implementation Aspects

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Origin

- clear a replacement for DES was needed
  - have theoretical attacks that can break it
  - have demonstrated exhaustive key search attacks
- can use Triple-DES – but slow, has small blocks
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were shortlisted in Aug-99
- Rijndael was selected as the AES in Oct-2000
- issued as FIPS PUB 197 standard in Nov-2001

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

AES Requirements

- private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- stronger & faster than Triple-DES
- active life of 20-30 years (+ archival use)
- provide full specification & design details
- both C & Java implementations
- NIST have released all submissions & unclassified analyses

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

AES Evaluation Criteria

- initial criteria:
  - security – effort for practical cryptanalysis
  - cost – in terms of computational efficiency
  - algorithm & implementation characteristics
- final criteria
  - general security
  - ease of software & hardware implementation
  - implementation attacks
  - flexibility (in en/decrypt, keying, other factors)

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

AES Shortlist

- after testing and evaluation, shortlist in Aug-99:
  - MARS (IBM) - complex, fast, high security margin
  - RC6 (USA) - v. simple, v. fast, low security margin
  - Rijndael (Belgium) - clean, fast, good security margin
  - Serpent (Euro) - slow, clean, v. high security margin
  - Twofish (USA) - complex, v. fast, high security margin
- then subject to further analysis & comment
- saw contrast between algorithms with
  - few complex rounds verses many simple rounds
  - which refined existing ciphers verses new proposals

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

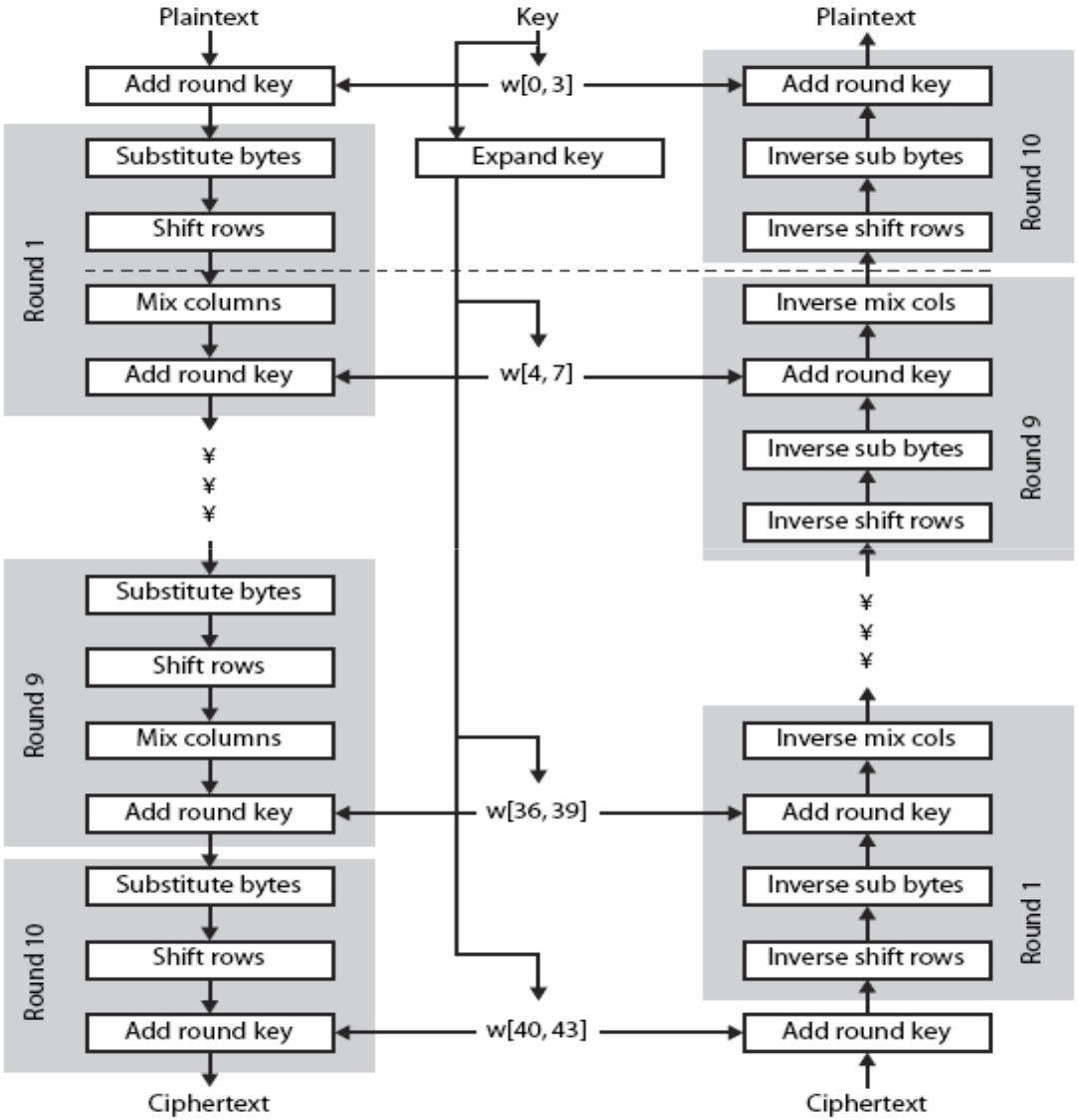
The AES Cipher - Rijndael

- designed by Rijmen-Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- an **iterative** rather than **feistel** cipher
  - processes data as block of 4 columns of 4 bytes
  - operates on entire data block in every round
- designed to be:
  - resistant against known attacks
  - speed and code compactness on many CPUs
  - design simplicity

Rijndael

- data block of 4 columns of 4 bytes is state
- key is expanded to array of words
- has 9/11/13 rounds in which state undergoes:
  - byte substitution (1 S-box used on every byte)
  - shift rows (permute bytes between groups/columns)
  - mix columns (subs using matrix multipy of groups)
  - add round key (XOR state with key material)
  - view as alternating XOR key & scramble data bytes
- initial XOR key material & incomplete last round
- with fast XOR & table lookup implementation

Rijndael


Plaintext
Key
Plaintext
Add round key
w[0, 3]
Add round key
Substitute bytes
Expand key
Inverse sub bytes
Shift rows
Inverse shift rows
Round 1
Round 10
Mix columns
Inverse mix cols
Add round key
w[4, 7]
Add round key
Inverse sub bytes
Round 9
Inverse shift rows
Substitute bytes
Shift rows
Inverse mix cols
Mix columns
Add round key
w[36, 39]
Add round key
Round 9
Substitute bytes
Inverse sub bytes
Shift rows
Inverse shift rows
Round 1
Add round key
w[40, 43]
Add round key
Round 10
Ciphertext
Ciphertext
(a) Encryption
(b) Decryption

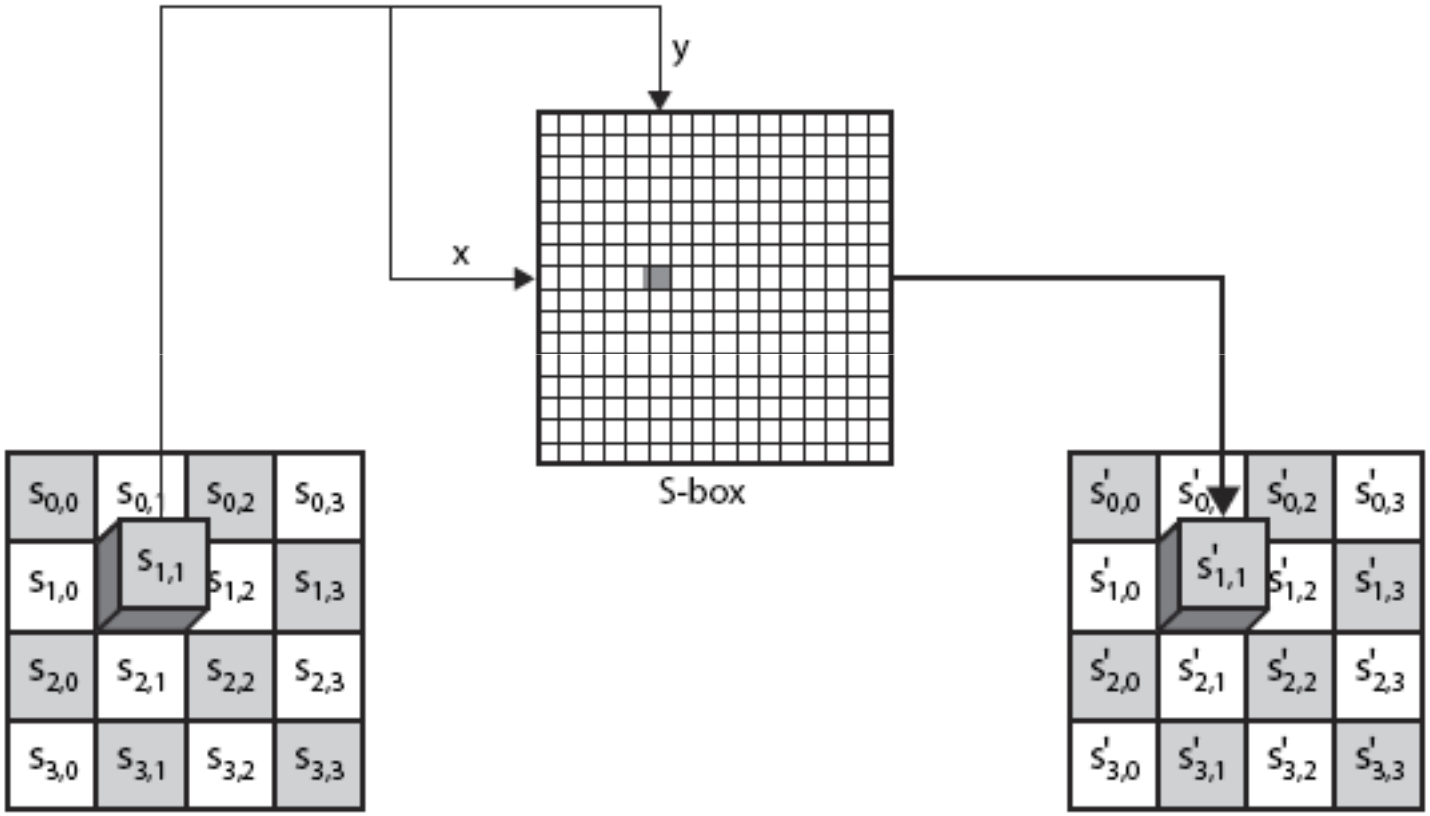
Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Byte Substitution

- a simple substitution of each byte
- uses one table of 16x16 bytes containing a permutation of all 256 8-bit values
- each byte of state is replaced by byte indexed by row (left 4-bits) & column (right 4-bits)
  - eg. byte {95} is replaced by byte in row 9 column 5
  - which has value {2A}
- S-box constructed using defined transformation of values in GF(2^8)
- designed to be resistant to all known attacks

Byte Substitution



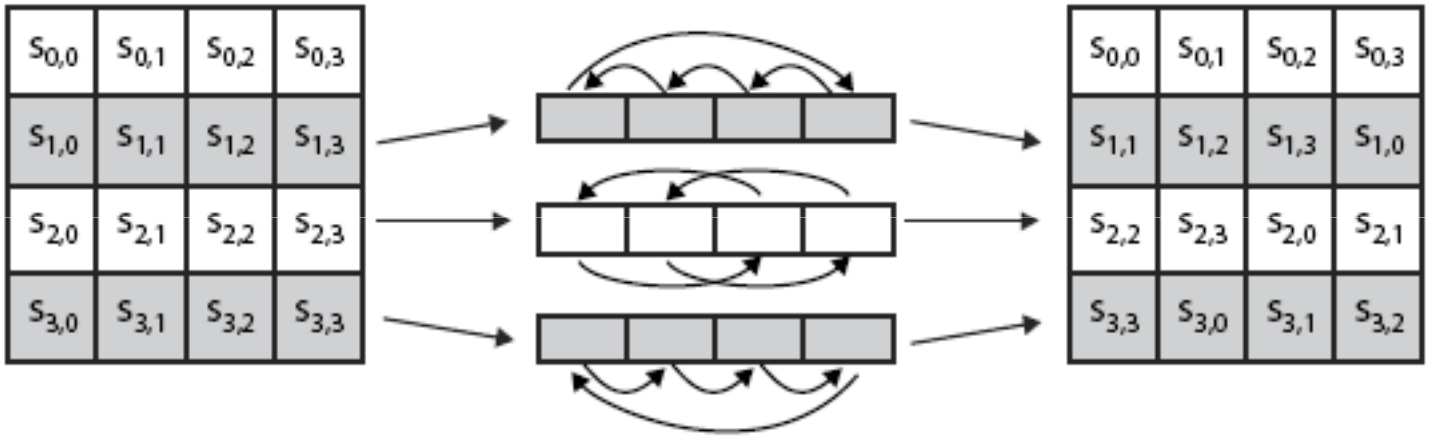
Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Shift Rows

- a circular byte shift in each each
  - 1st row is unchanged
  - 2nd row does 1 byte circular shift to left
  - 3rd row does 2 byte circular shift to left
  - 4th row does 3 byte circular shift to left
- decrypt inverts using shifts to right
- since state is processed by columns, this step permutes bytes between the columns

Shift Rows


$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,1}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

Agenda

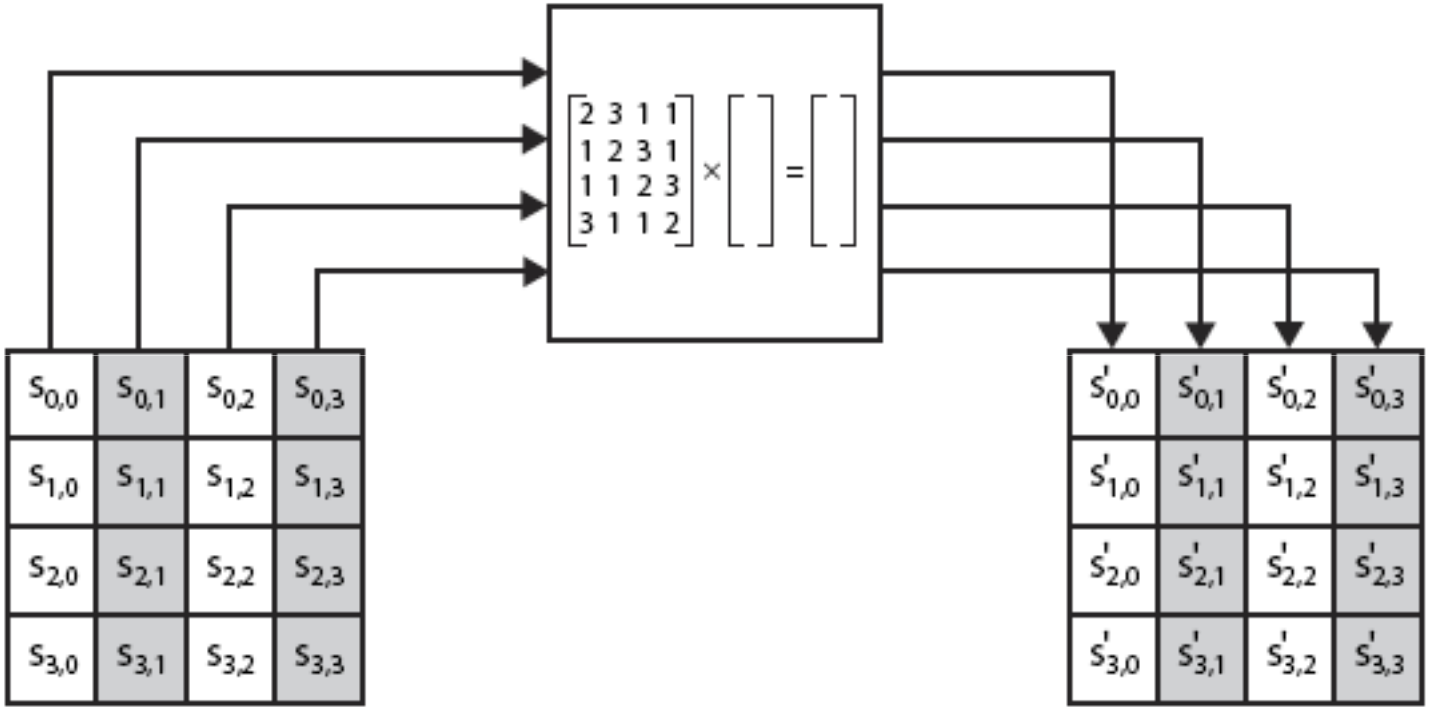
- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Mix Columns

- each column is processed separately
- each byte is replaced by a value dependent on all 4 bytes in the column
- effectively a matrix multiplication in GF(2^8) using prime poly $m(x) = x^8+x^4+x^3+x+1$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

Mix Columns


2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
×
=
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Mix Columns

- can express each col as 4 equations
  - to derive each new byte in col
- decryption requires use of inverse matrix
  - with larger coefficients, hence a little harder
- have an alternate characterisation
  - each column a 4-term polynomial
  - with coefficients in GF(2^8)
  - and polynomials multiplied modulo (x^4+1)

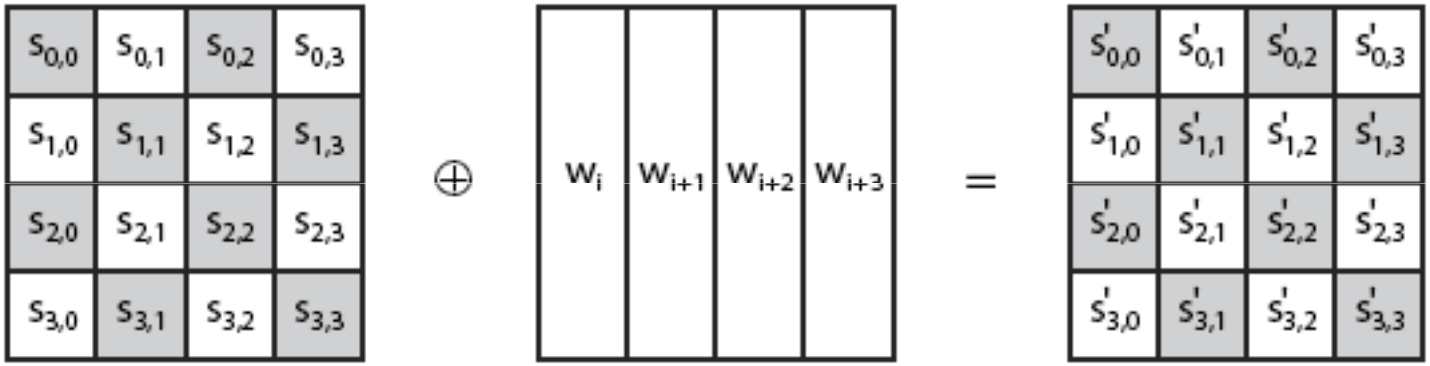
Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

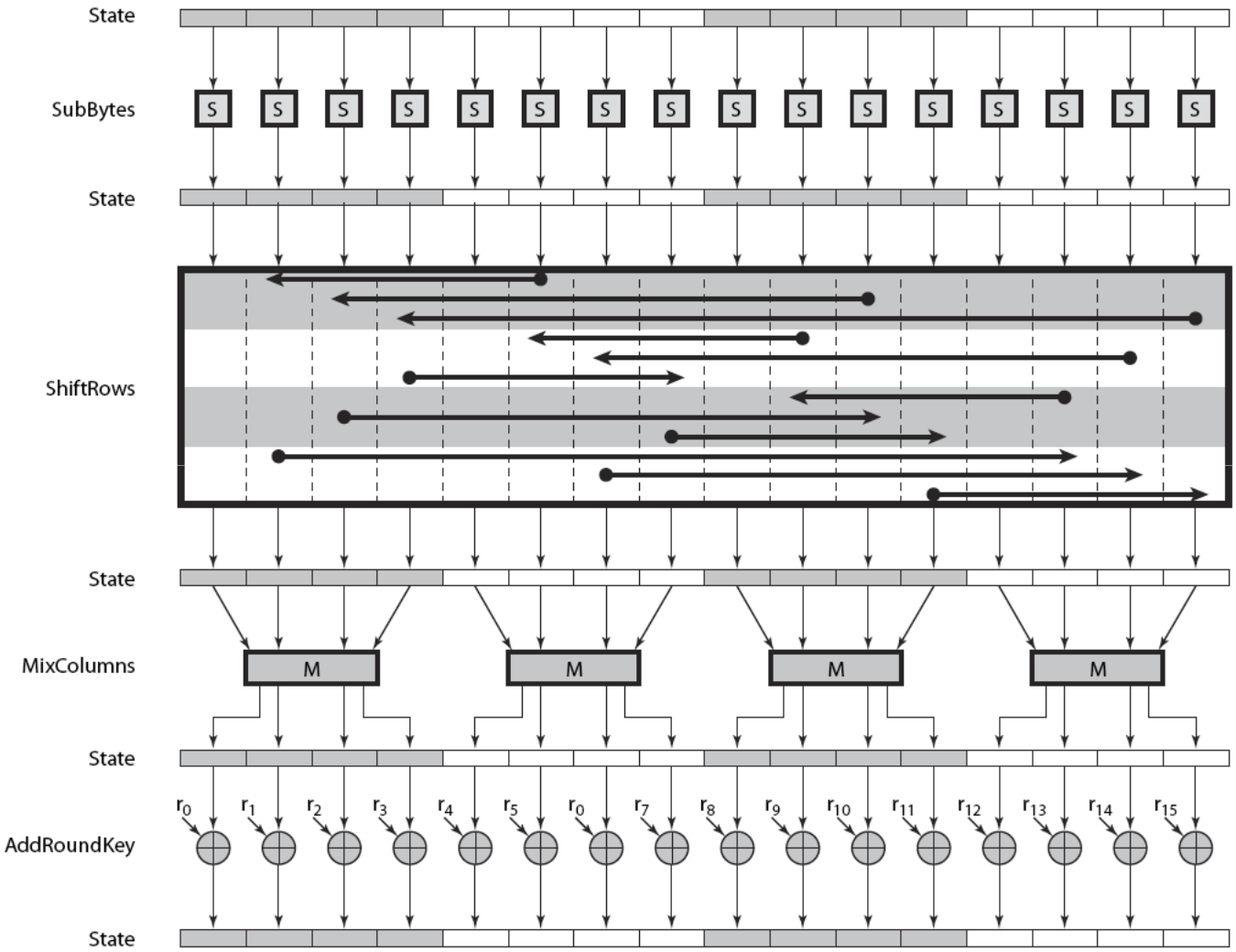
Add Round Key

- XOR state with 128-bits of the round key
- again processed by column (though effectively a series of byte operations)
- inverse for decryption identical
  - since XOR own inverse, with reversed keys
- designed to be as simple as possible
  - a form of Vernam cipher on expanded key
  - requires other stages for complexity / security

Add Round Key



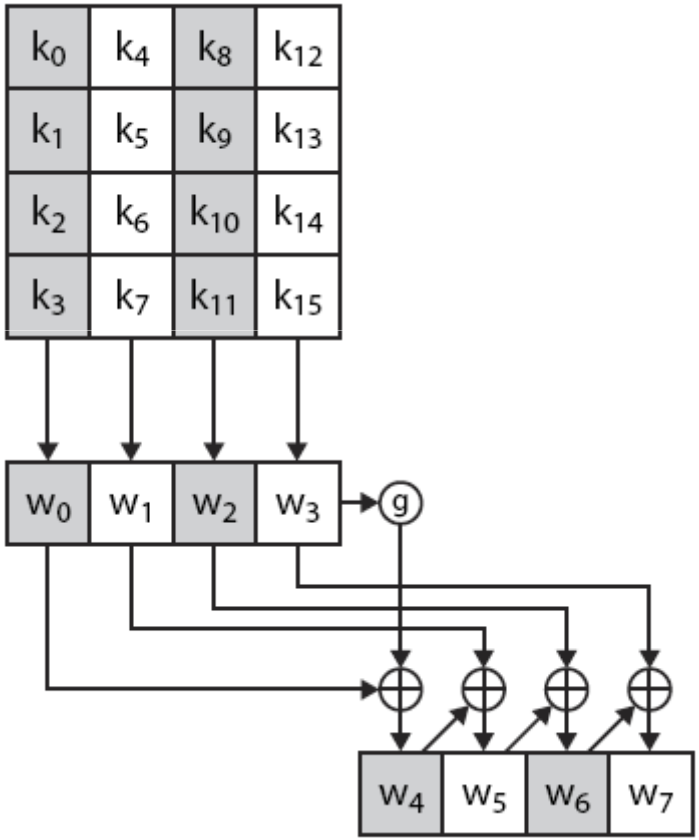
AES Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r0 r1 r2 r3 r4 r5 r0 r7 r8 r9 r10 r11 r12 r13 r14 r15
State

AES Key Expansion

- takes 128-bit (16-byte) key and expands into array of 44/52/60 32-bit words
- start by copying key into first 4 words
- then loop creating words that depend on values in previous & 4 places back
  - in 3 of 4 cases just XOR these together
  - 1st word in 4 has rotate + S-box + XOR round constant on previous, before XOR 4th back

AES Key Expansion



Key Expansion Rationale

- designed to resist known attacks
- design criteria included
  - knowing part key insufficient to find many more
  - invertible transformation
  - fast on wide range of CPU's
  - use round constants to break symmetry
  - diffuse key bits into round keys
  - enough non-linearity to hinder analysis
  - simplicity of description

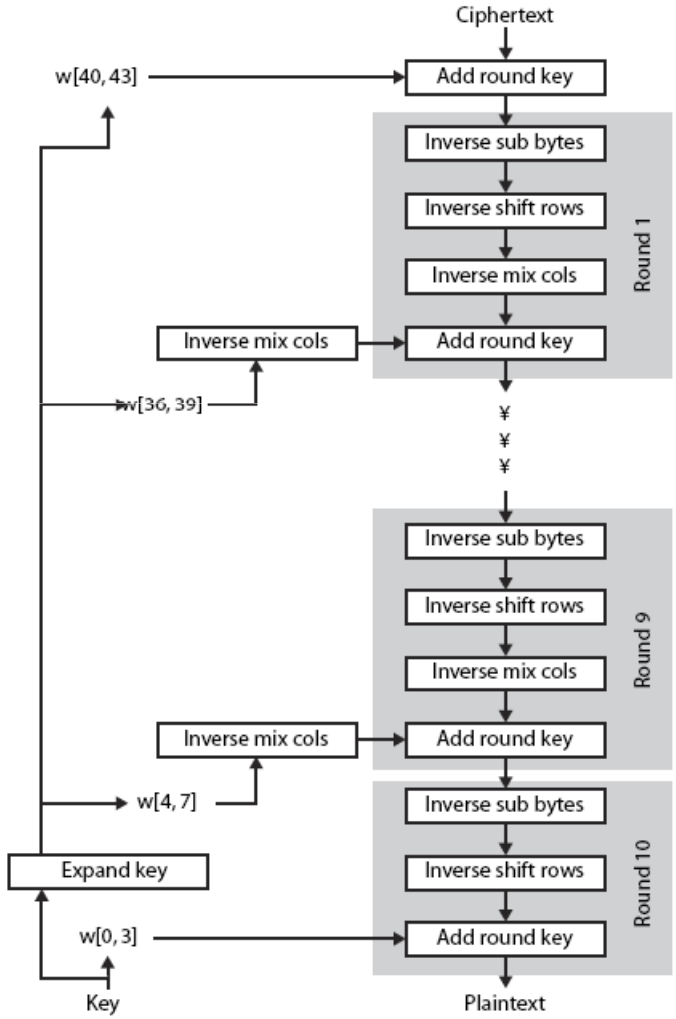
Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

AES Decryption

- AES decryption is not identical to encryption since steps done in reverse
- but can define an equivalent inverse cipher with steps as for encryption
  - but using inverses of each step
  - with a different key schedule
- works since result is unchanged when
  - swap byte substitution & shift rows
  - swap mix columns & add (tweaked) round key

AES Decryption



Implementation Aspects

- can efficiently implement on 8-bit CPU
  - byte substitution works on bytes using a table of 256 entries
  - shift rows is simple byte shift
  - add round key works on byte XOR's
  - mix columns requires matrix multiply in GF(2^8) which works on byte values, can be simplified to use table lookups & byte XOR's

Implementation Aspects

- can efficiently implement on 32-bit CPU
  - redefine steps to use 32-bit words
  - can precompute 4 tables of 256-words
  - then each column in each round can be computed using 4 table lookups + 4 XORs
  - at a cost of 4Kb to store tables
- designers believe this very efficient implementation was a key factor in its selection as the AES cipher

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Summary

- have considered:
  - the AES selection process
  - the details of Rijndael – the AES cipher
  - looked at the steps in each round
  - the key expansion
  - implementation aspects

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

Test your understanding

1. Explain AES algorithm in detail.
2. What are the basic building blocks of AES cipher.

Agenda

- Introduction
  - Origin
  - AES requirement
  - AES evaluation criteria
  - AES Shortlist
- AES
  - Substitute bytes
  - Shift rows
  - Mixing columns
  - Add round key
  - Decryption
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.