CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous class

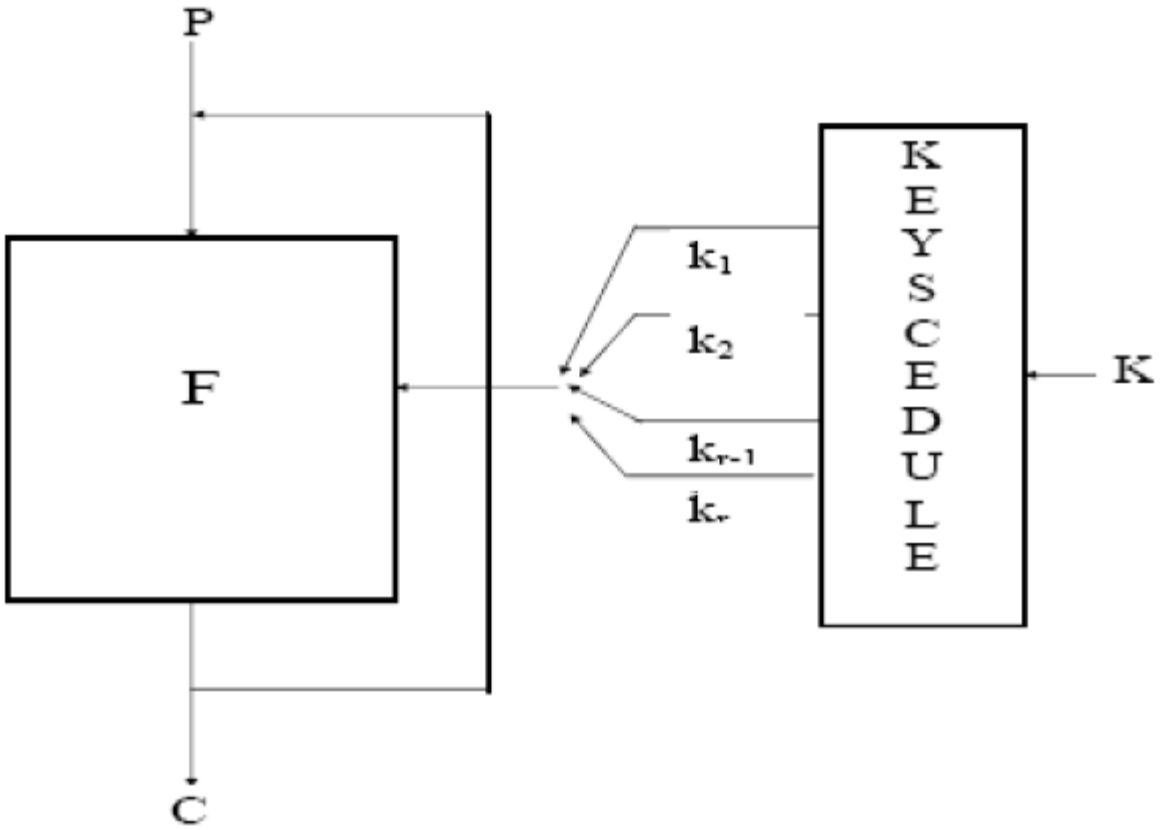
- Crypto Basics

- Cryptographic algorithms
  - important element in security services

Present class

- Crypto Basics
  - Symmetric Key encryption (Block cipher)

Iterative Block cipher



Ex.: DES, AES

Attacking Symmetric Encryption

- Cryptanalytic Attacks
  - rely on:
  - nature of the algorithm
  - plus some knowledge of the general characteristics of the plaintext
  - even some sample plaintext-ciphertext pairs
  - exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - if successful all future and past messages encrypted with that key are compromised

Brute-Force Attack

- try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - on average half of all possible keys must be tried to achieve success

Symmetric Encryption Algorithms

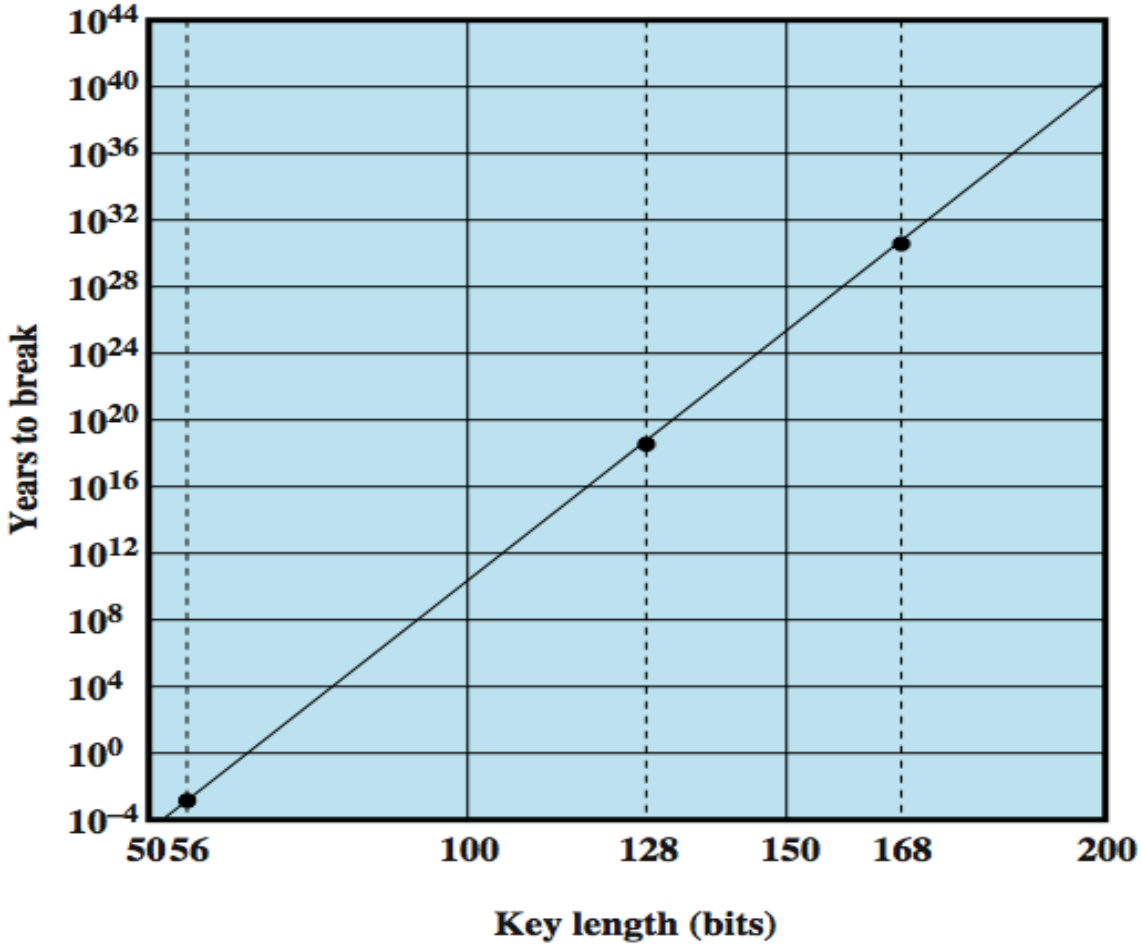
	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Data Encryption Standard (DES)

- most widely used encryption scheme
  - referred to as the Data Encryption Algorithm
  - uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
- strength concerns:
  - concerns about algorithm
    - DES is the most studied encryption algorithm in existence
  - use of 56-bit key
    - Electronic Frontier Foundation (EFF) announced in July 1998 that it had broken a DES encryption in < 3days

Time to Break a Code



assuming 10^6 decryptions/μs

Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Triple DES (3DES)

- repeats basic DES algorithm three times using either two or three unique keys
- attractions:
  - 168-bit key length overcomes the vulnerability to brute-force attack of DES
  - underlying encryption algorithm is the same as in DES
- drawbacks:
  - algorithm is sluggish in software
  - uses a 64-bit block size

Advanced Encryption Standard (AES)

needed a replacement for 3DES

3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

should have a security strength equal to or better than 3DES

significantly improved efficiency

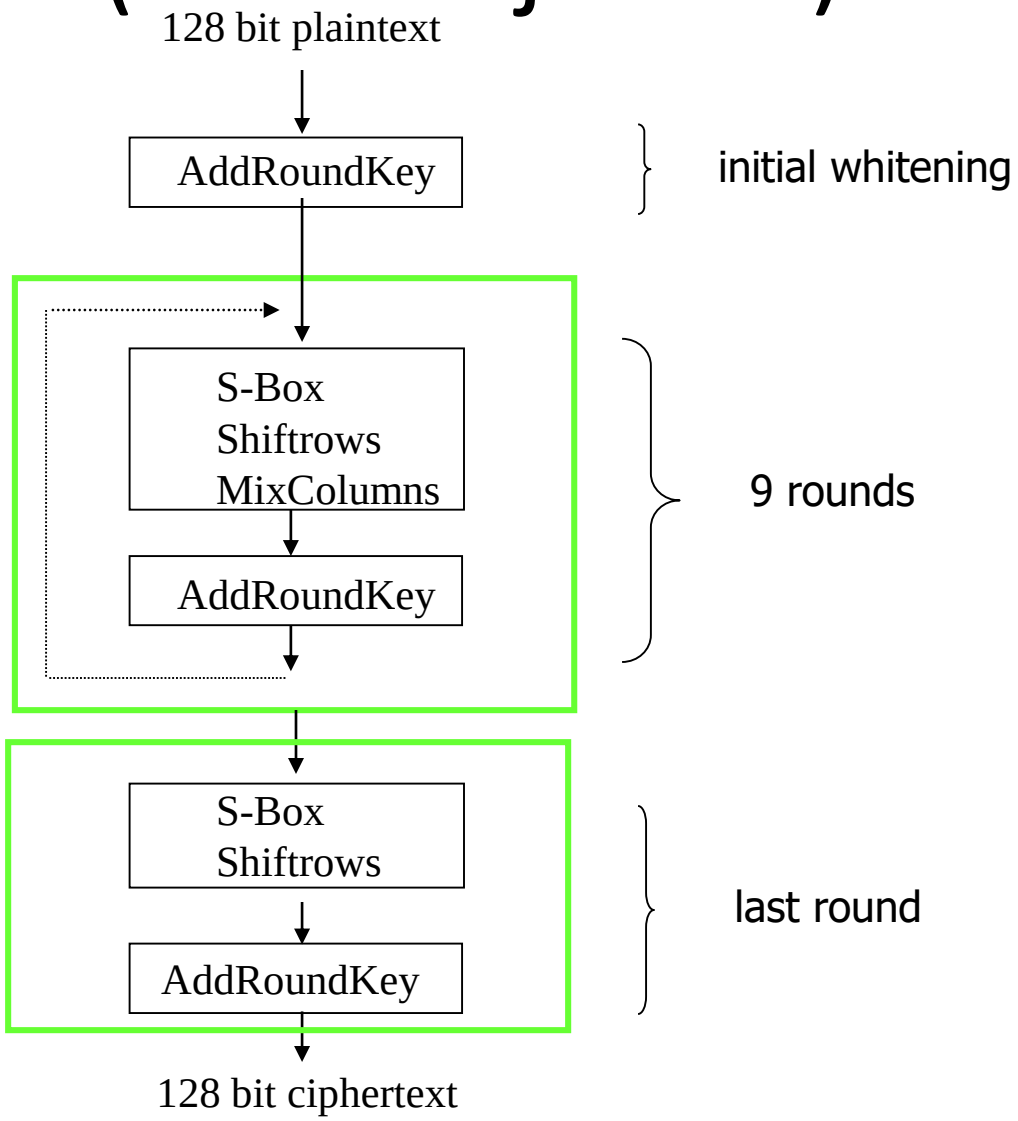
symmetric block cipher

128 bit data and 128/192/256 bit keys

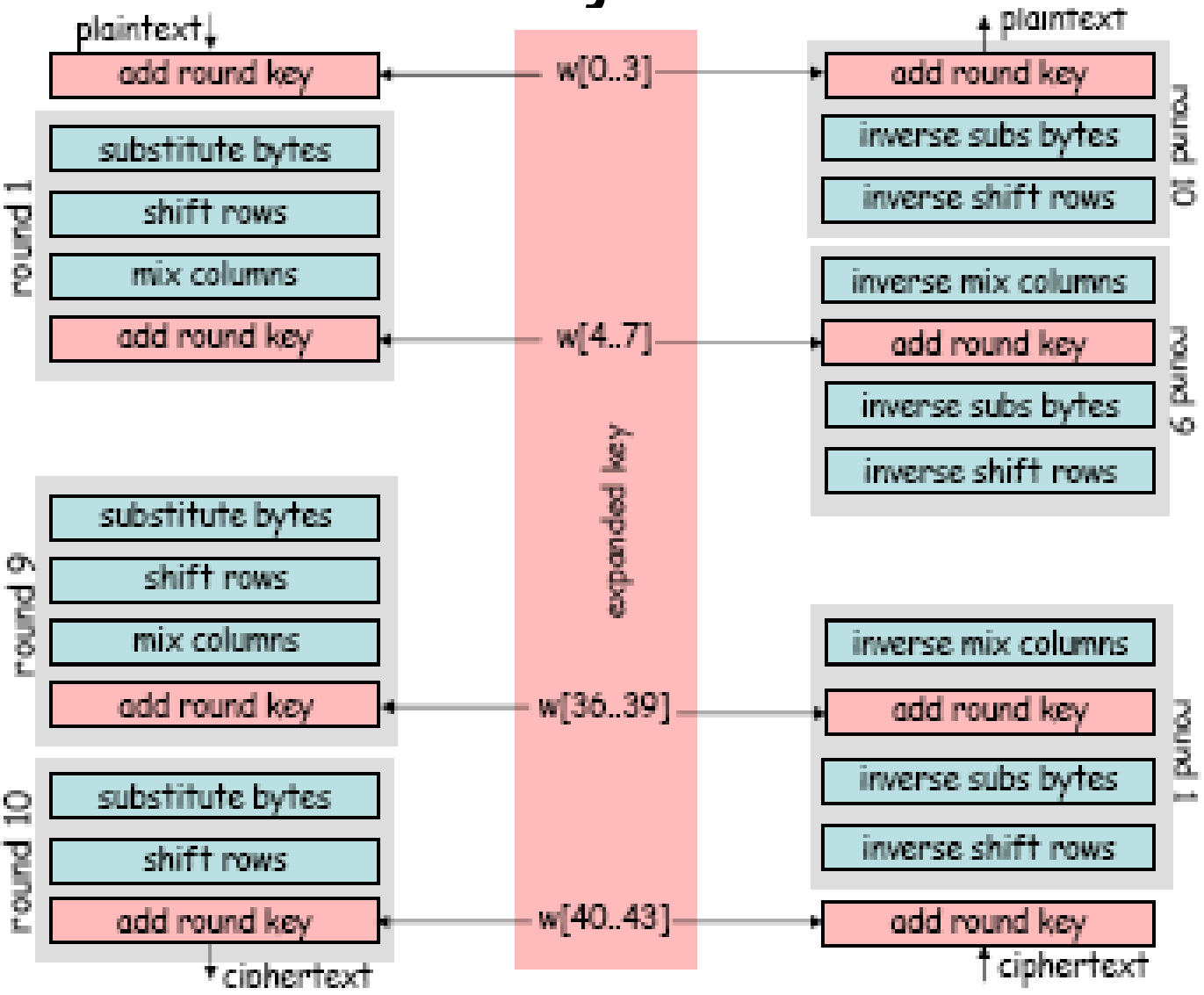
selected Rijndael in November 2001

published as FIPS 197

Symmetric key Block cipher (AES – Rijndael)

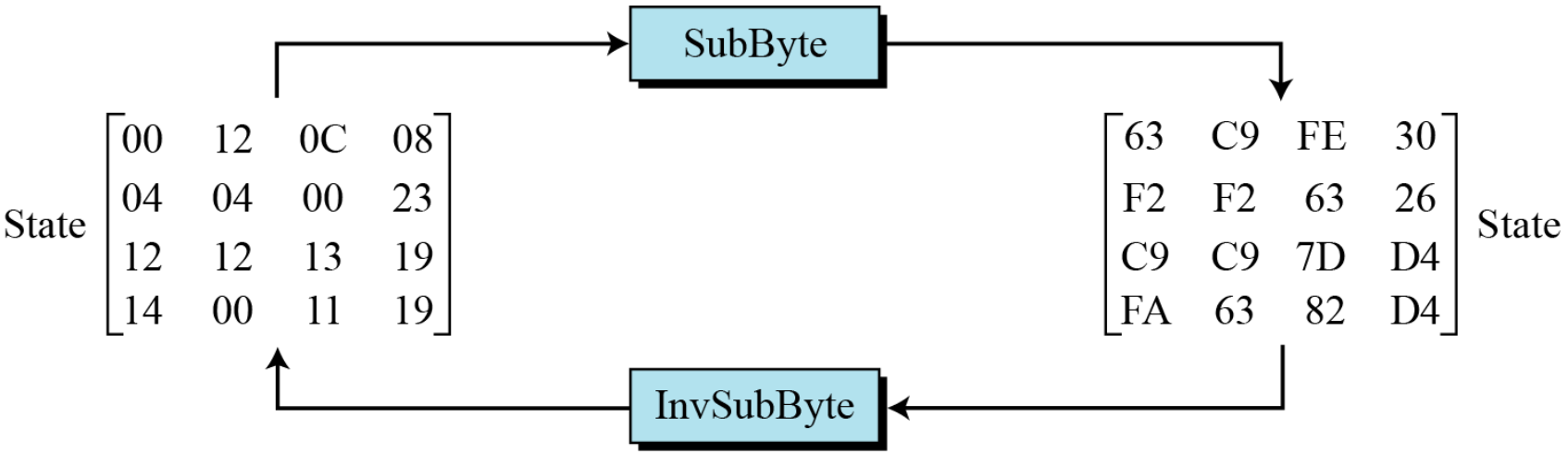


AES-Rijndael



AES Round Function Components:

Byte Substitution



Shift Rows

A:

sij is a byte

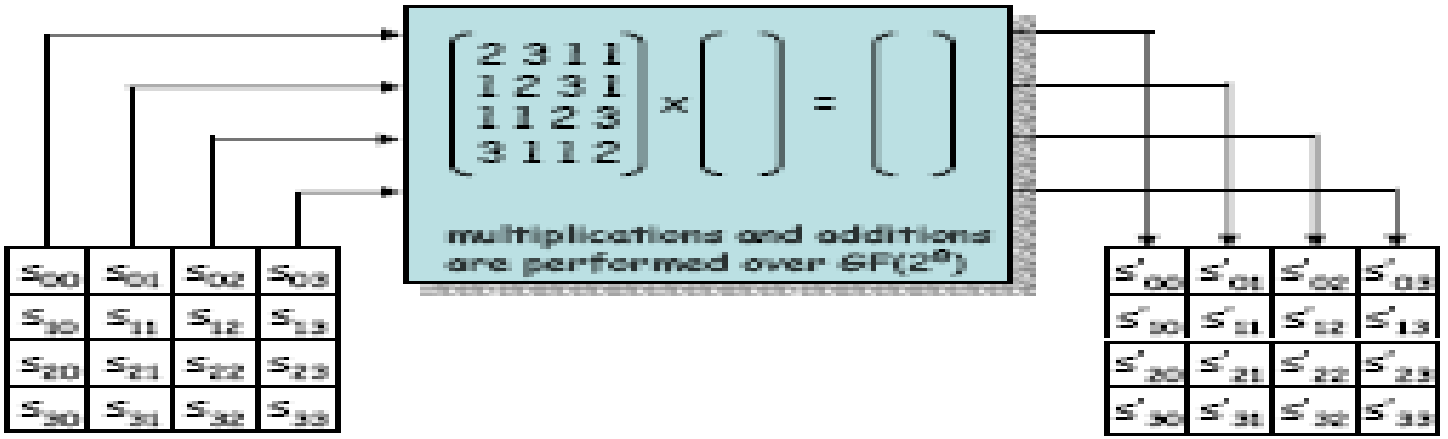
s00	s01	s02	s03
s10	s11	s12	s13
s20	s21	s22	s23
s30	s31	s32	s33

Shift row i
i positions
(i = 0 to 3)

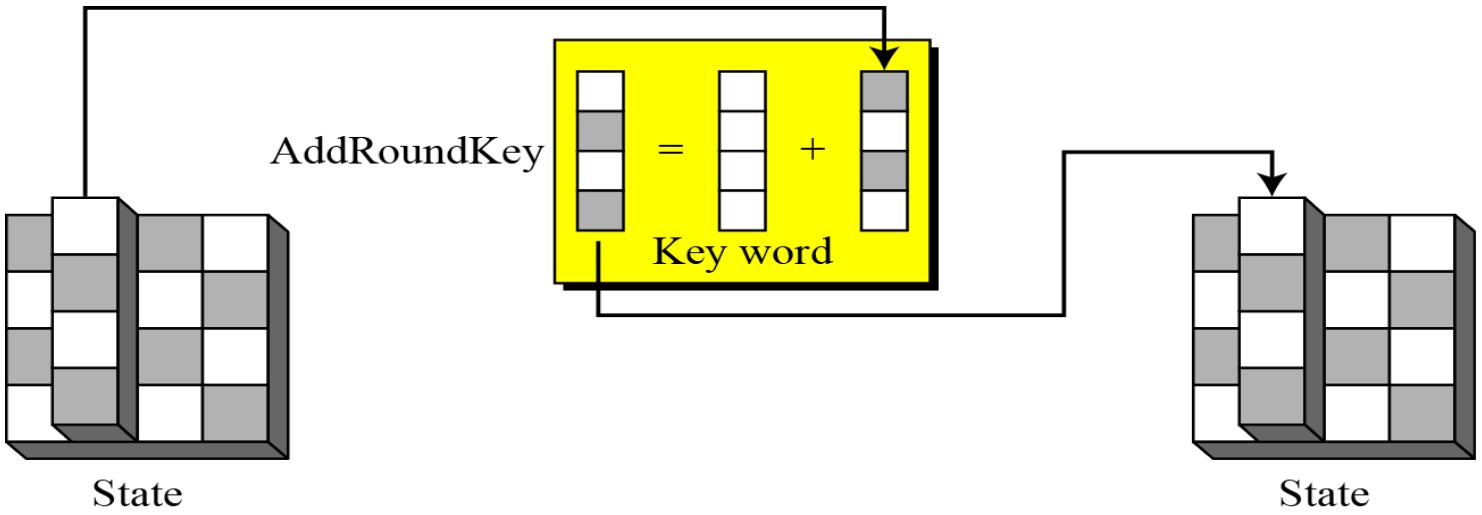
s00	s01	s02	s03
s11	s12	s13	s10
s22	s23	s20	s21
s33	s30	s31	s32

AES Round Function Components:

Mix Columns

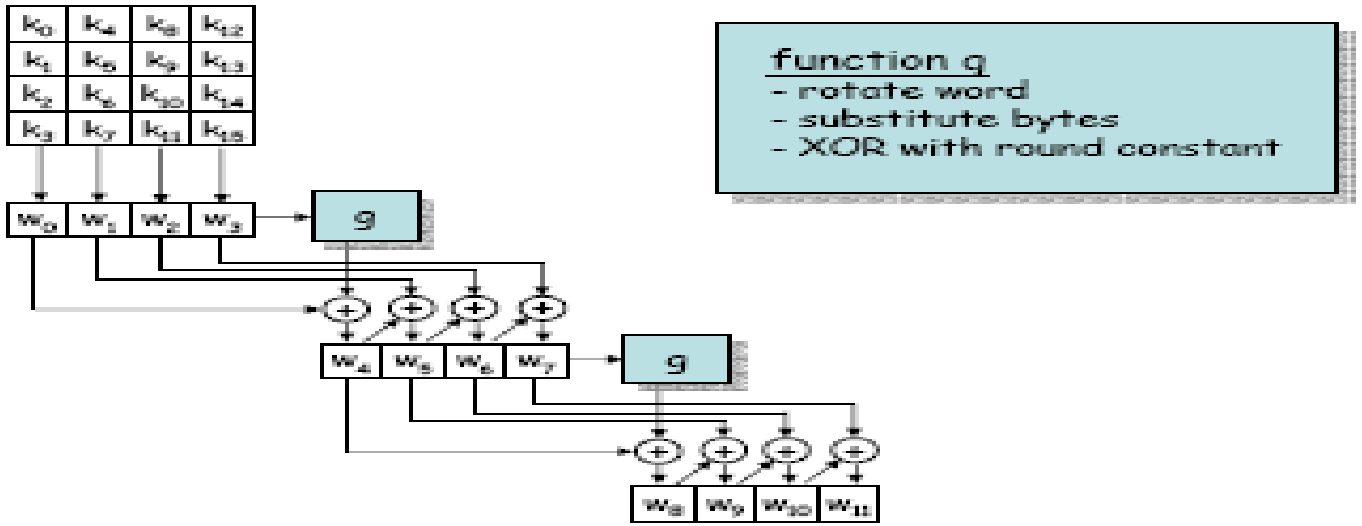


Add Round Key



AES Key Expansion

- takes 128/192/256-bit (16/24/32-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 and 4 places back
  - in 3 of 4 cases just XOR these together
  - every 4th has S-box + rotate + XOR constant of previous before XOR together



AES Diffusion: Single Byte

Round 1

s00	s01	s02	s03
s10	s11	s12	s13
s20	s21	s22	s23
s30	s31	s32	s33

Input

s00	s01	s02	s03
s11	s12	s13	s10
s22	s23	s20	s21
s33	s30	s31	s32

After ShiftRows

s'00	s'01	s'02	s'03
s'11	s'12	s'13	s'10
s'22	s'23	s'20	s'21
s'33	s'30	s'31	s'32

After MixColumns

Round 2

s'00	s'01	s'02	s'03
s'12	s'13	s'10	s'11
s'20	s'21	s'22	s'23
s'32	s'33	s'30	s'31

s''00	S''01	s''02	s''03
s''12	s''13	s''10	s''11
s''20	s''21	s''22	s''23
s''32	s''33	s''30	s''31

Note: AddRoundKey has no impact on diffusion

Thanks