PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

APPLIED CRYPTOGRAPHY

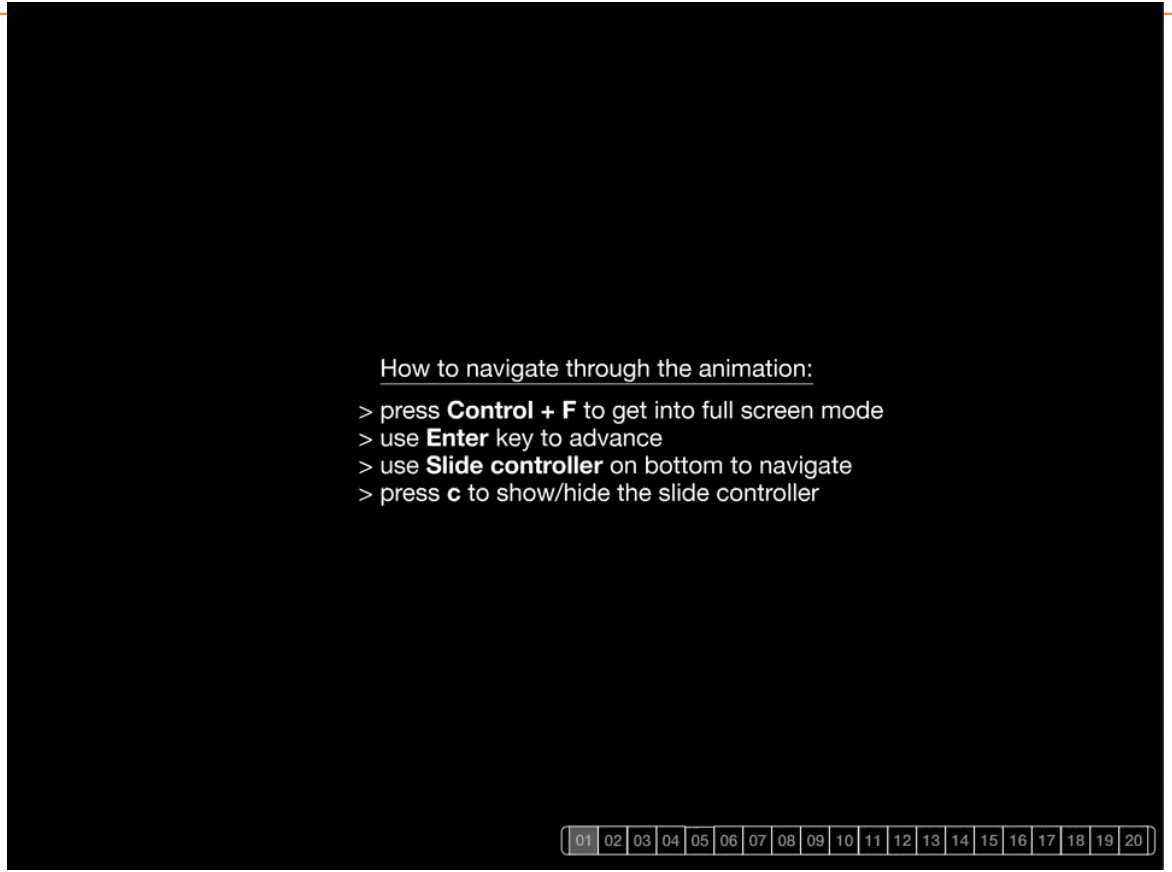
Private keys systems

Lecture 8

AES

Advanced Encryption Standard

AES animation



Origins

- A replacement for DES was needed
  - Key size is too small
- Can use Triple-DES – but slow, small block
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were shortlisted in Aug 99

AES Competition Requirements

- Private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger & faster than Triple-DES
- Provide full specification & design details
- Both C & Java implementations

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

- Found contrast between algorithms with
  - few complex rounds versus many simple rounds
  - Refined versions of existing ciphers versus new proposals

The AES Cipher - Rijndael

- Rijndael was selected as the AES in Oct-2000
  - Designed by Vincent Rijmen and Joan Daemen in Belgium
  - Issued as FIPS PUB 197 standard in Nov-2001

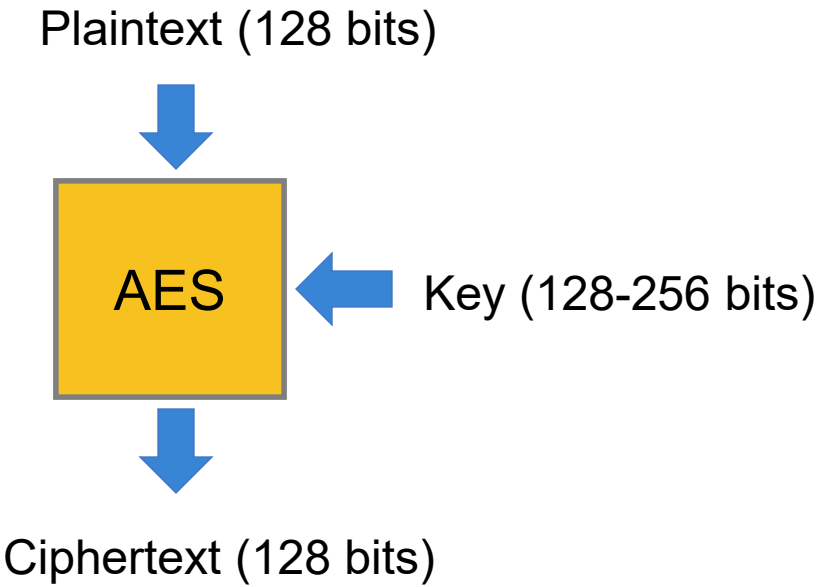
- An **iterative** rather than **Feistel** cipher
  - processes data as block of 4 columns of 4 bytes (128 bits)
  - operates on entire data block in every round

- Rijndael design:
  - simplicity
  - has 128/192/256 bit keys, 128 bits data
  - resistant against known attacks
  - speed and code compactness on many CPUs

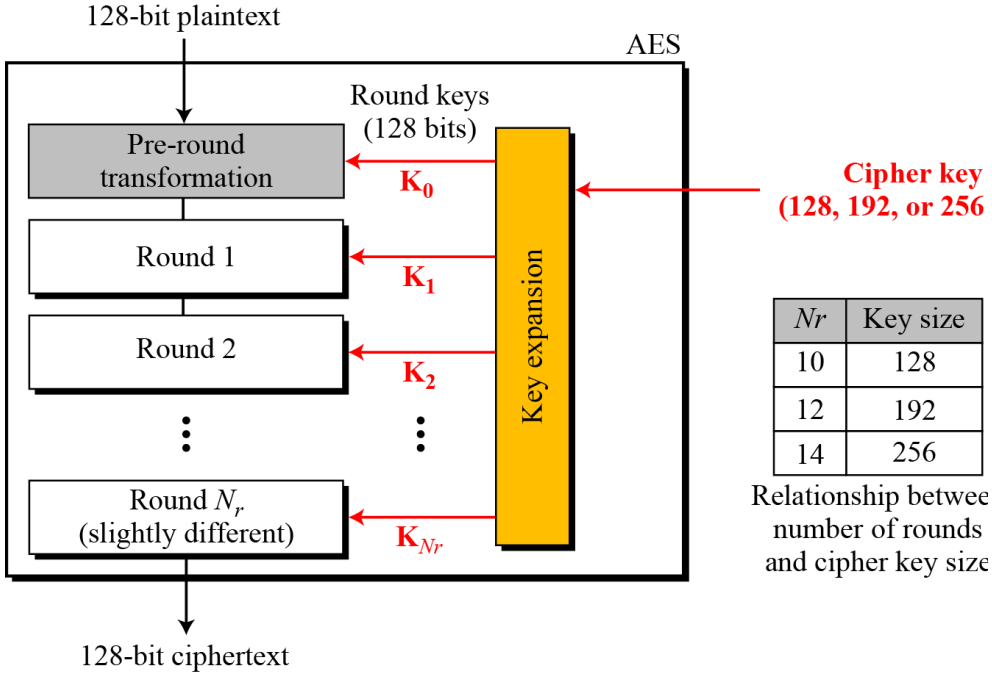
V. Rijmen

J. Daemen

AES Conceptual Scheme



Multiple rounds



Nr	Key size
10	128
12	192
14	256

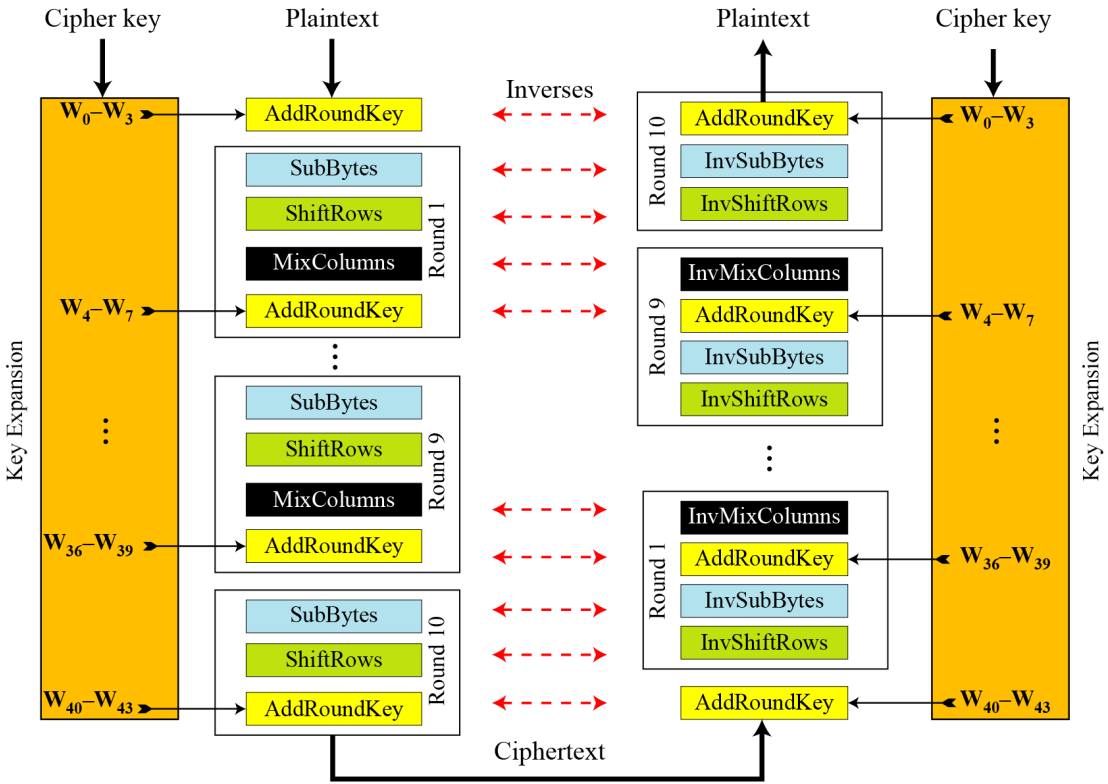
Relationship betwee
number of rounds
and cipher key size

- Rounds are (almost) identical
- First and last round are a little different

High Level Description

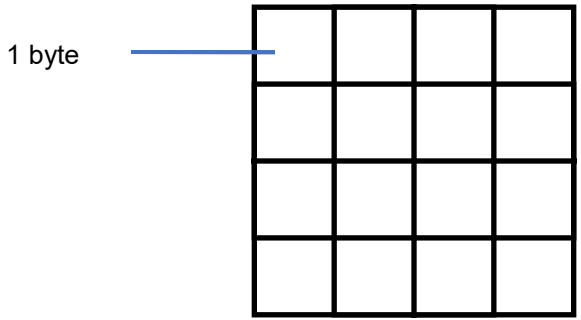
- Key Expansion: Round keys are derived from the cipher key using Rijndael's key schedule
- Initial Round: AddRoundKey : Each byte of the state is combined with the round key using bitwise xor
- Rounds
  - SubBytes : non-linear substitution step
  - ShiftRows : transposition step
  - MixColumns : mixing operation of each column.
  - AddRoundKey
- Final Round:
  - SubBytes
  - ShiftRows
  - AddRoundKey

Overall Structure

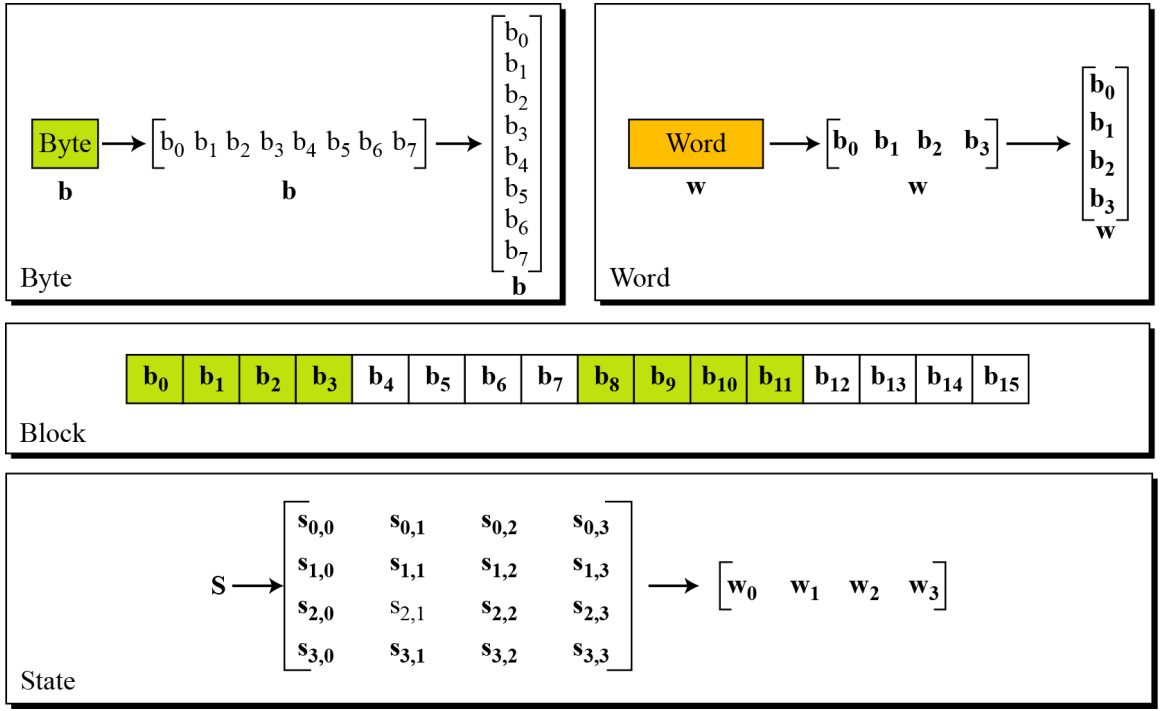


128-bit values

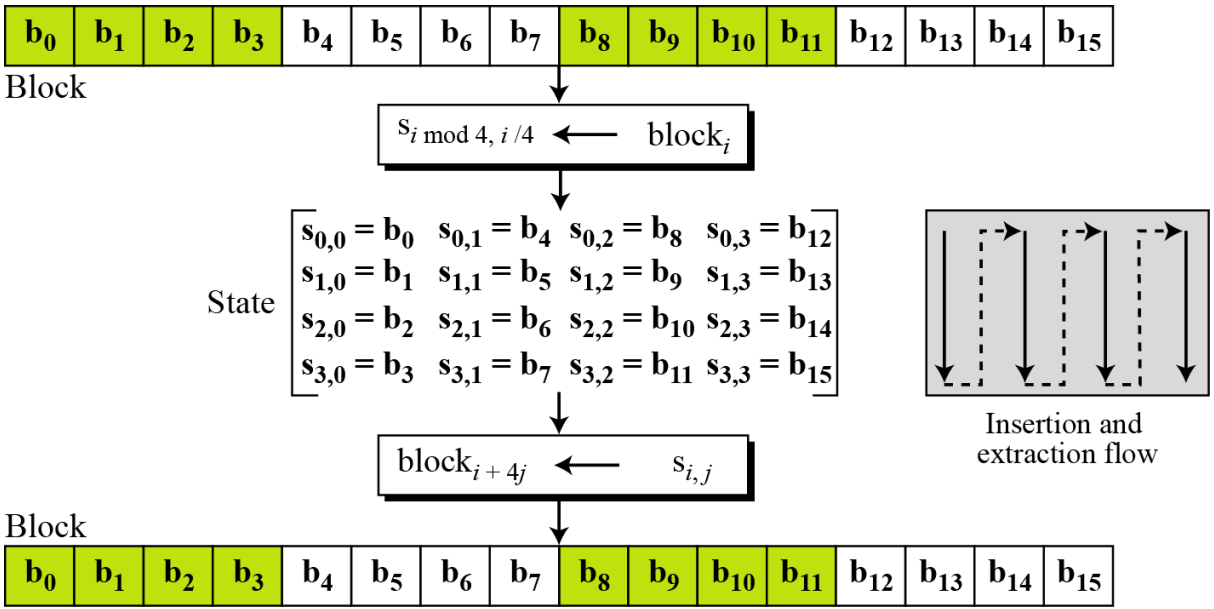
- Data block viewed as 4-by-4 table of bytes
- Represented as 4 by 4 matrix of 8-bit bytes.
- Key is expanded to array of 32 bits words



Data Unit



Unit Transformation



AES

Plaintext: AES USES MATRIX = 14 characters = 14*8 = 112

Converting plaintext to state which is 128 bits. 128-112 = 16bits needed

So add 2 extra character

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

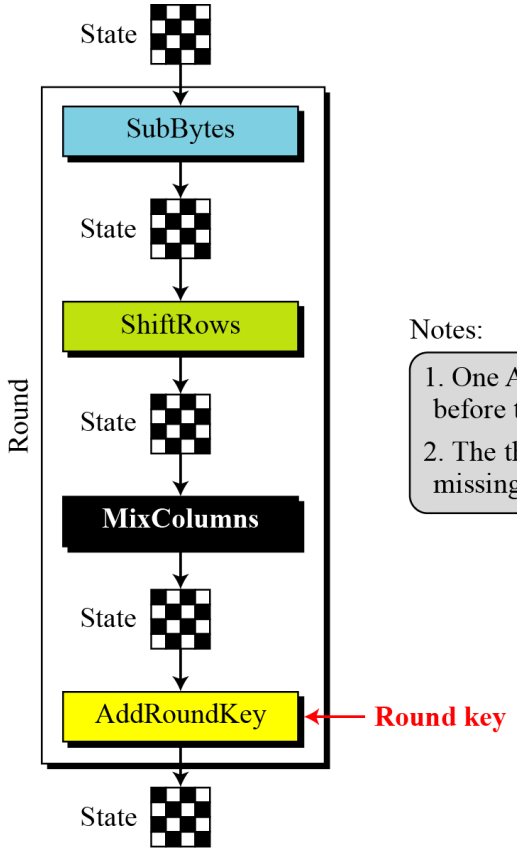
Changing Plaintext to State

Text	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	08	17	19	19

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 17 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}$$ State

Reference 2: example 7.1

Details of Each Round



Notes:

1. One AddRoundKey is applied before the first round.
2. The third transformation is missing in the last round.

Reference 2: figure 7.5

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT PESU Center for Internet of Things