Lecture 8

Advanced Encryption Standard (AES)

CS 450/650

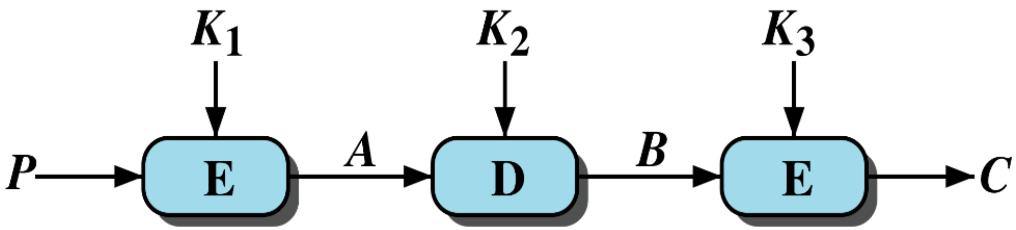
Fundamentals of Integrated Computer Security

Cracking DES

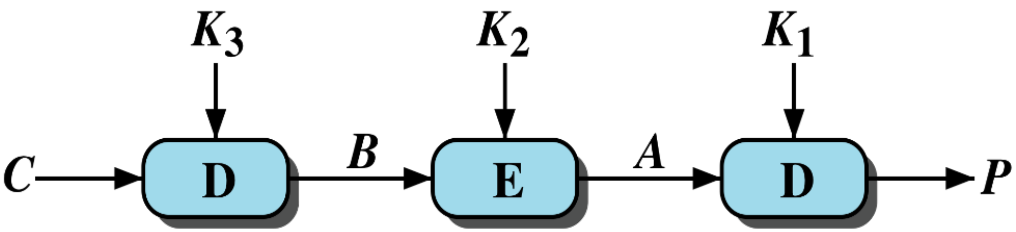
- Diffie and Hellman then outlined a "brute force" attack on DES
  - By “brute force” is meant that you try as many of the $\mathbf{2^{56}}$ (why?) possible keys to decrypt the ciphertext into a meaningful plaintext message
- cryptoanalysis—no good solution due to AE

Triple DES

- Triple-DES uses three keys and three executions of DES algorithm



(a) Encryption



(b) Decryption

Triple DES

- Keying options
  - Option 1: all three keys (K1, K2, K3) are independent: the strongest, with 3∗56=168 independent key bits
  - Option 2: K1 and K2 are independent, and K3=K1: provides less security with 2∗56=112 key bits, but stronger than pure DES
  - Option 3: all three keys are identical—equivalent of DES (why?)

Triple DES

- Attractions:
  - 168-bit (or 112-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

Introduction to AES

- 1997 - call for AES (Advanced Encryption standard by NIST)
- August 1998 - 15 algorithm submissions
- August 1999 - 15 candidates reduced to 5 finalists
- October 2nd 2000 - Rijndael alg. was chosen as the AES (by 2 young researchers from Belgium)
- AES is the most popular crypto-algorithm in the world today. browsers, atm machines, routers use it

AES

- A symmetric-key cryptosystem
- A block cipher
- Capable of supporting a block size of 128 bits
- Capable of supporting key length of 128, 192, and 256 bits

Introduction to AES

- DES uses Feistel network but AES doesn't use Feistel
- DES encrypts half of the data at every round, but AES encrypts all at every round

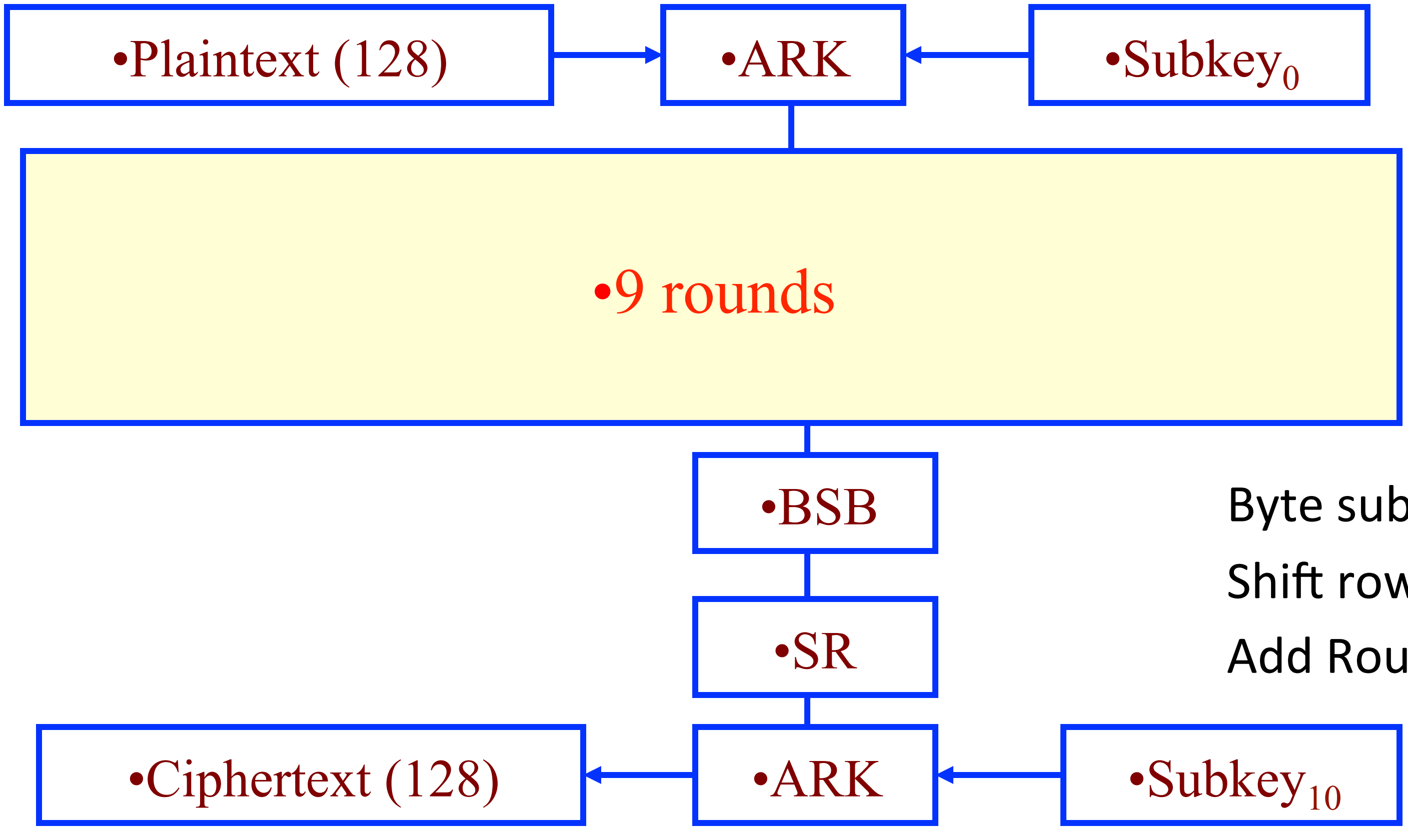
AES

- 10, 12, 14 rounds for 128, 192, 256 bit keys
  - Regular Rounds (9, 11, 13)
  - Final Round is different (10^{th}, 12^{th}, 14^{th})

- Each regular round consists of 4 steps
  - Byte substitution (BSB)
  - Shift row (SR)
  - Mix column (MC)
  - Add Round key (ARK)

AES Overview

128-bit AES

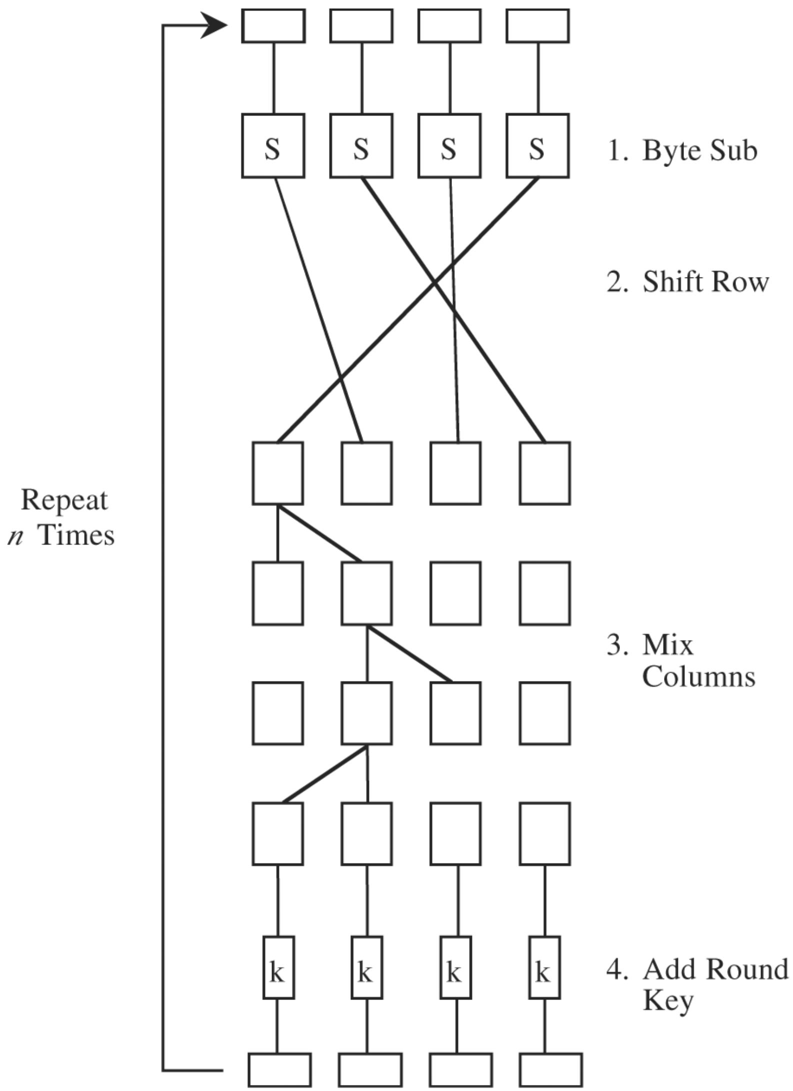


Byte substitution (BSB)

Shift row (SR)

Add Round key (ARK)

Round *i* operations



- 128-bit substitution boxes
- transposition step of circular shift
- Left shift and XOR of bits
- portion of key is XORed
- Subkey$_i$

Four Operations

1. *Byte Substitution*
   – predefined substitution table s[i,j] → s' [i,j]
2. *Shift Row*
   – left circular shift
3. *Mix Columns*
   – 4 elements in each column are multiplied by a polynomial
4. *Add Round Key*
   – Key is derived and added to each column

Four Operations

1. *Byte Substitution*
   – predefined substitution table s[i,j] → s' [i,j]
2. *Shift Row*
   – left circular shift
3. *Mix Columns*
   – 4 elements in each column are multiplied by a polynomial
4. *Add Round Key*
   – Key is derived and added to each column

Substitution table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	BE	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	84	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Exercise

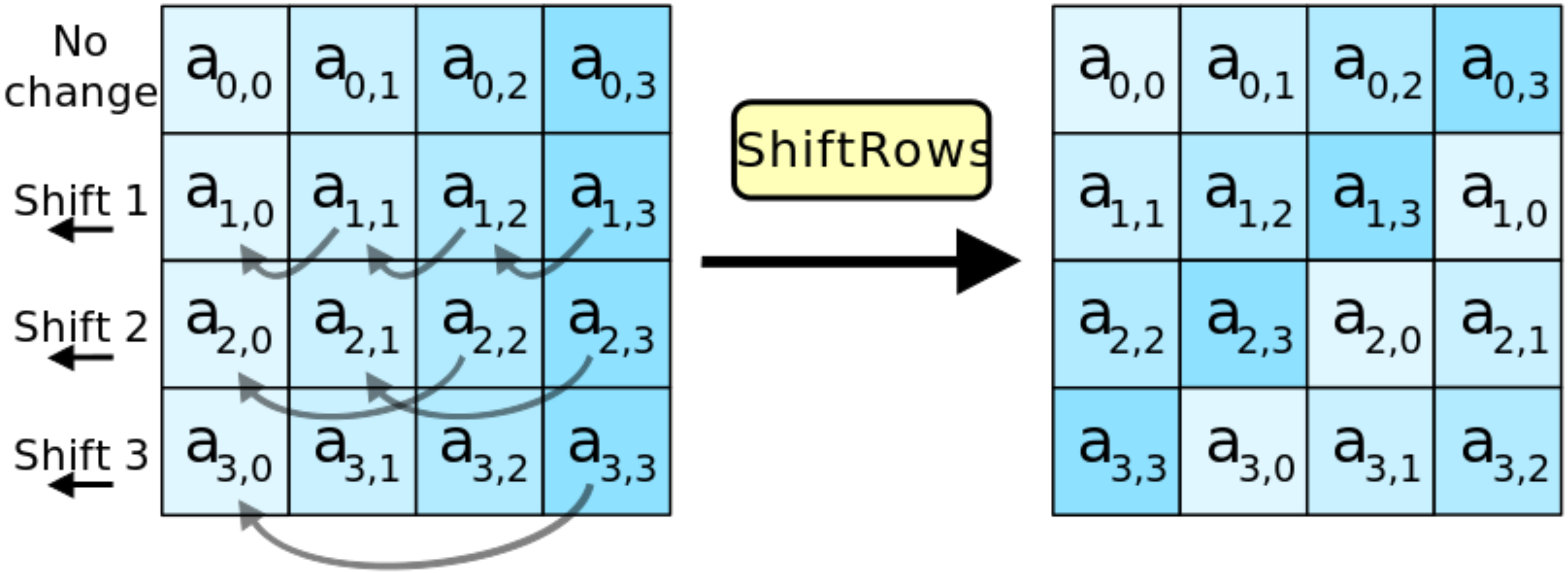
- Using the table, find the substitution of

6b, ff, 6e, 09

Four Operations

1. *Byte Substitution*
   – predefined substitution table s[i,j] → s' [i,j]
2. *Shift Row*
   – left circular shift
3. *Mix Columns*
   – 4 elements in each column are multiplied by a polynomial
4. *Add Round Key*
   – Key is derived and added to each column

Shift Row (128-bit)



Four Operations

1. *Byte Substitution*
   – predefined substitution table s[i,j] → s' [i,j]
2. *Shift Row*
   – left circular shift
3. *Mix Columns*
   – 4 elements in each column are multiplied by a polynomial
4. *Add Round Key*
   – Key is derived and added to each column

Mix Column

$$\begin{bmatrix} S'_{0,i} \\ S'_{1,i} \\ S'_{2,i} \\ S'_{3,i} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} S_{0,i} \\ S_{1,i} \\ S_{2,i} \\ S_{3,i} \end{bmatrix}$$

$i=0\ldots3$

- Multiplying by 1 → no change
- Multiplying by 2 → shift left one bit
- Multiplying by 3 → shift left one bit and XOR with original value

Exercise

$$\begin{bmatrix} S'_{0,I} \\ S'_{1,I} \\ S'_{2,I} \\ S'_{3,i} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} e5 \\ a8 \\ 6f \\ 33 \end{bmatrix}$$

Four Operations

1. *Byte Substitution*
   – predefined substitution table s[i,j] → s' [i,j]
2. *Shift Row*
   – left circular shift
3. *Mix Columns*
   – 4 elements in each column are multiplied by a polynomial
4. *Add Round Key*
   – Enc key is derived and added to each column

Add Key

b0	b4	b8	b12
b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15

k0	k4	k8	k12
k1	k5	k9	k13
k2	k6	k10	k14
k3	k7	k11	k15

$$\boxed{b'_x} = \boxed{b_x} \text{ XOR } \boxed{k_x}$$

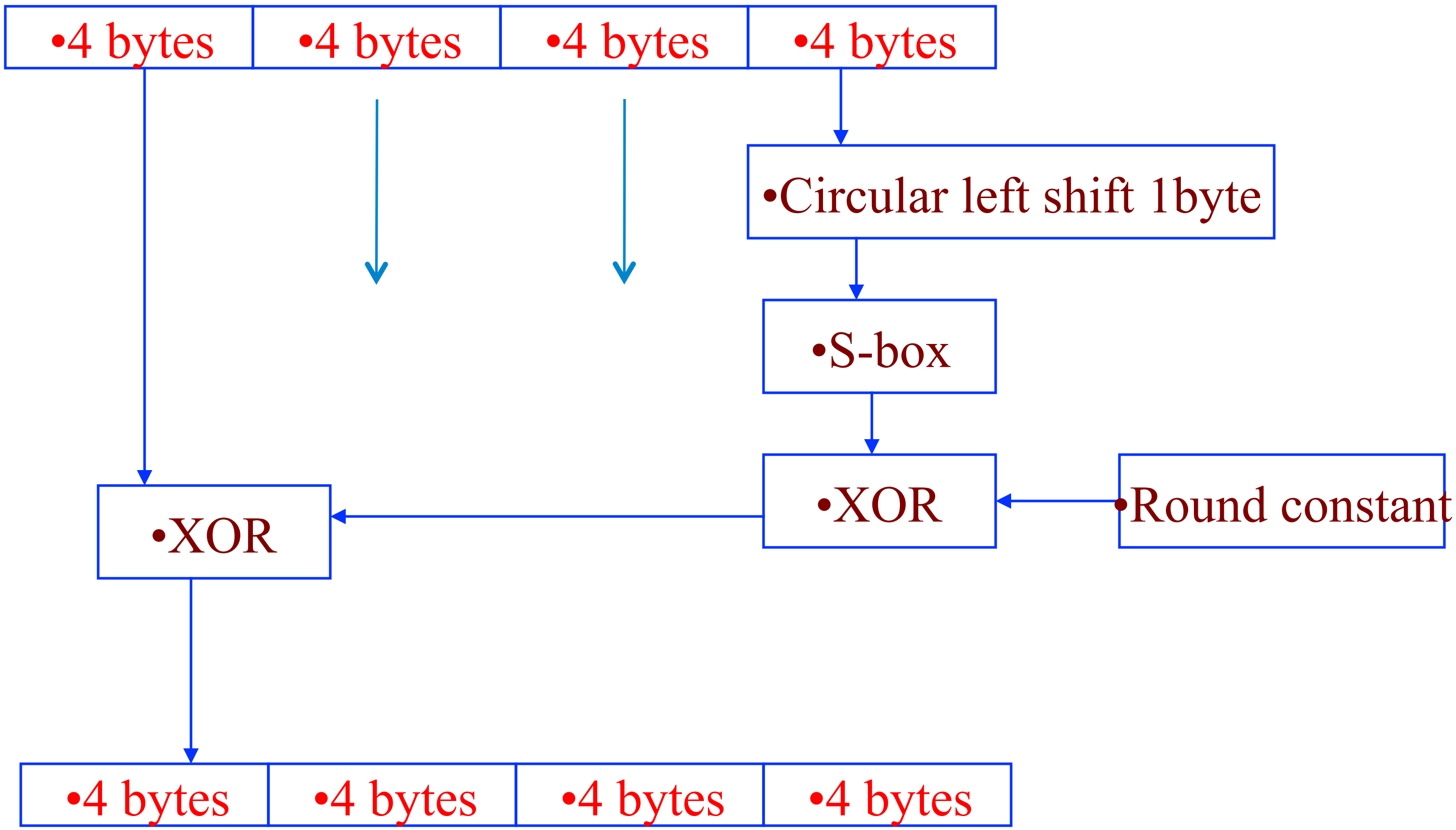
Example

k = 1f 34 0c da 5a 29 bb 71 6e a3 90 f1 47 d6 8b 12

B = e5 a8 6f 33 0a 52 31 9c c2 75 f8 1e b0 46 de 3a

B’= fa 9c 63 9e 50 7b 8a ed ac d6 68 ef f7 90 55 28

Key Generation for Each Round

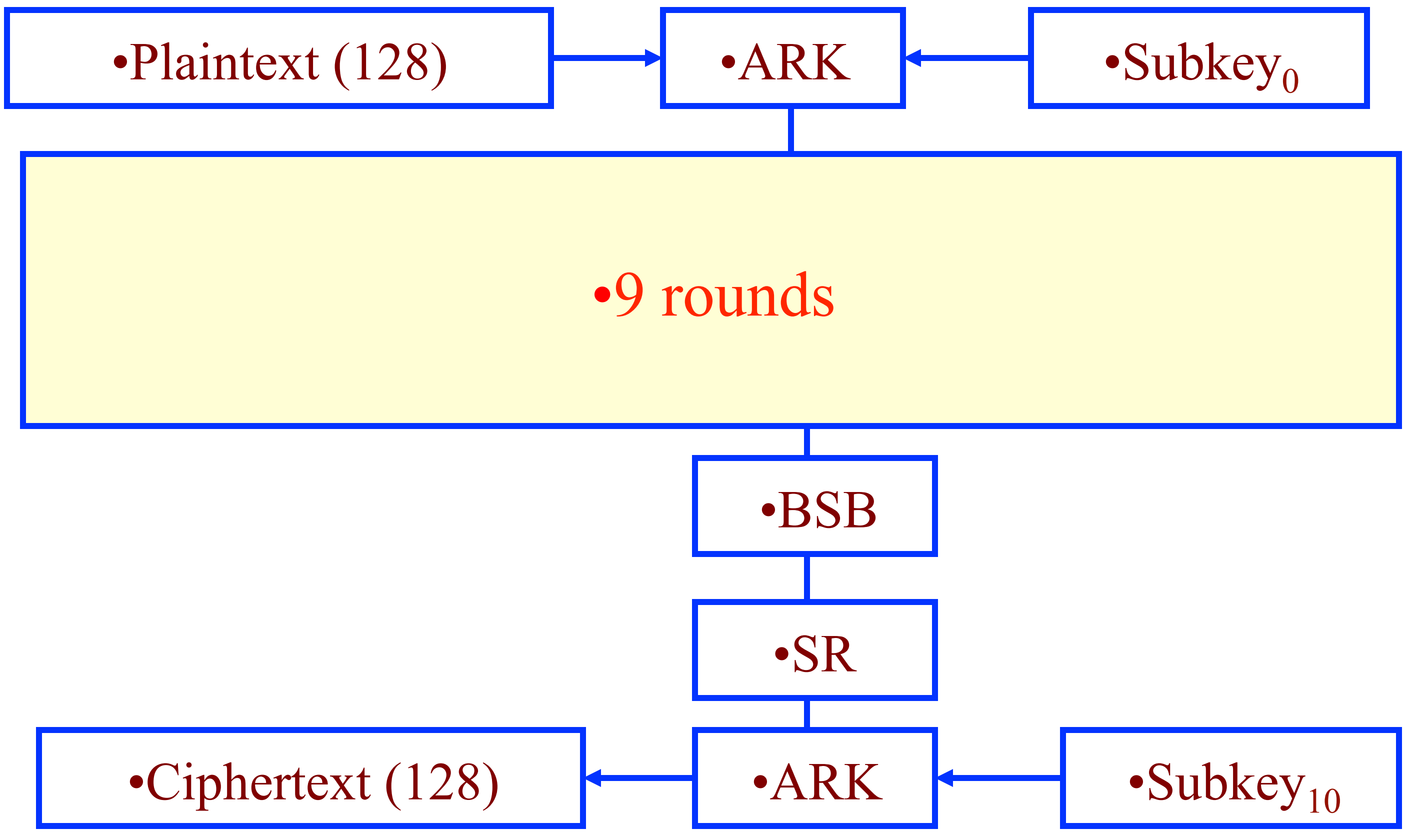


Round Constant Table

Round	Round Constant (hex)
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1b 00 00 00
Final	36 00 00 00

AES Overview

128-bit AES



DES vs AES

	DES	AES
Date	1976	1999
Block size	64 bits	128 bits
Key length	56 bits	128, 192, 256, … bits
Encryption primitives	Substitution and permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion and diffusion	Confusion and diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret (accepted public comment)
Source	IBM, enhanced by NSA	Belgian cryptographers

Rivest-Shamir-Adelman (RSA)

CS 450/650

Fundamentals of Integrated Computer Security

Two kinds of Cryptography

Symmetric

1) Alice and Bob agree on a cryptosystem
2) Alice and Bob agree on a key
3) Alice takes her plaintext message and encrypts it using the encryption algorithm and the key. This creates a ciphertext message
4) Alice sends the ciphertext message to Bob
5) Bob decrypts the ciphertext message with the same algorithm and key and reads it

Asymmetric

1) Alice and Bob agree on a public-key cryptosystem
2) Bob sends Alice his public key
3) Alice encrypts her message using Bob's public key and sends it to Bob
4) Bob decrypts Alice's message using his private key

RSA

- **RSA** is one of the first practical public-key cryptosystems and is widely used for secure data transmission.
- The encryption key is public and differs from the decryption key which is kept secret (asymmetric cipher)
- Its security is based on the practical difficulty of doing some mathematical operations
  - RSA: factoring the product of two large prime numbers, the factoring problem

- Mid-term review Oct. 15
- Mid-term Oct. 17