Modern Block Ciphers

Dr Rosanne English

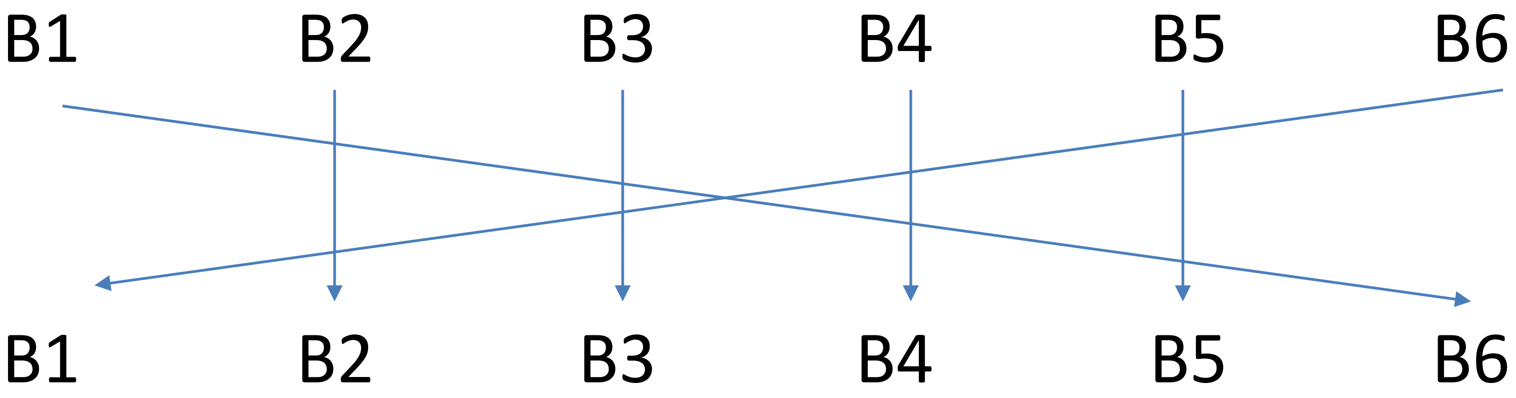
S Box Example

INPUT - 101001

4 middle bits																	
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
	01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
	10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
	11	0101	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

OUTPUT - 0100

P-Box Example (Straight)



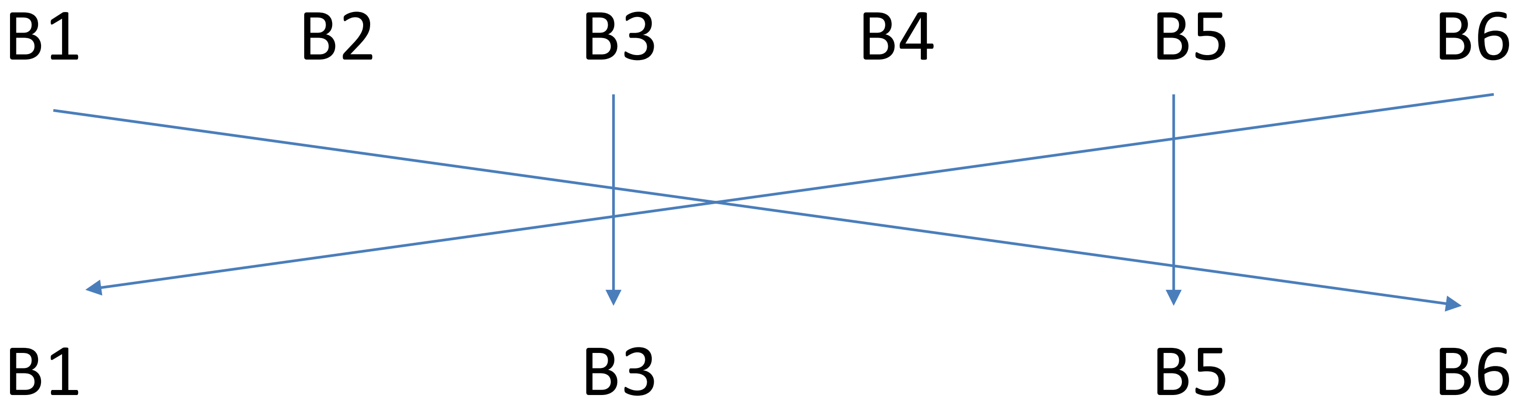
B1 B2 B3 B4 B5 B6

B1 B2 B3 B4 B5 B6

B6 B2 B3 B4 B5 B1

Straight P-box Permutes only

P-Box Example (Compression)



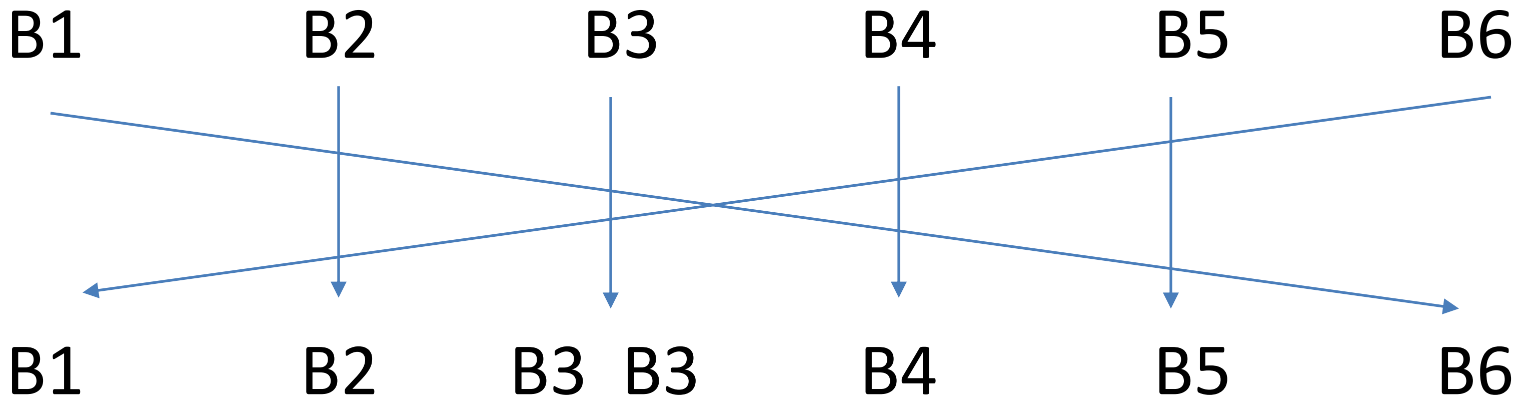
B1 B2 B3 B4 B5 B6

B1 B3 B5 B6

B6 B3 B5 B1

Compression Pbox permutes and can remove blocks

P-Box Example (Expansion)



B1 B2 B3 B4 B5 B6

B1 B2 B3 B3 B4 B5 B6

B6 B2 B3 B3 B4 B5 B1

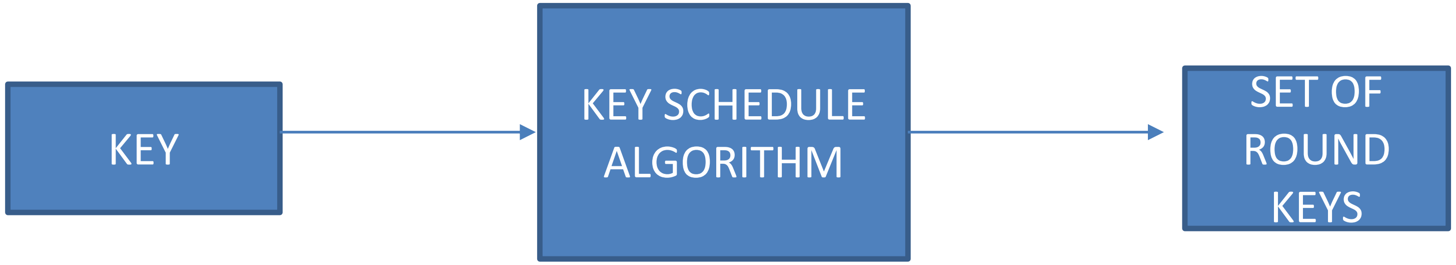
Expansion P-box permutes and can expand by duplication

Confusion and Diffusion

- Confusion – each bit of the ciphertext is dependent on multiple parts of the key
- Diffusion – if one bit of the plaintext is altered, multiple bits from the ciphertext should also be altered

Key Schedule

- Algorithm which takes a key and generates multiple keys for use in rounds
- Older key schedules have been composed of permutations etc., but in modern crypto they are often more complex

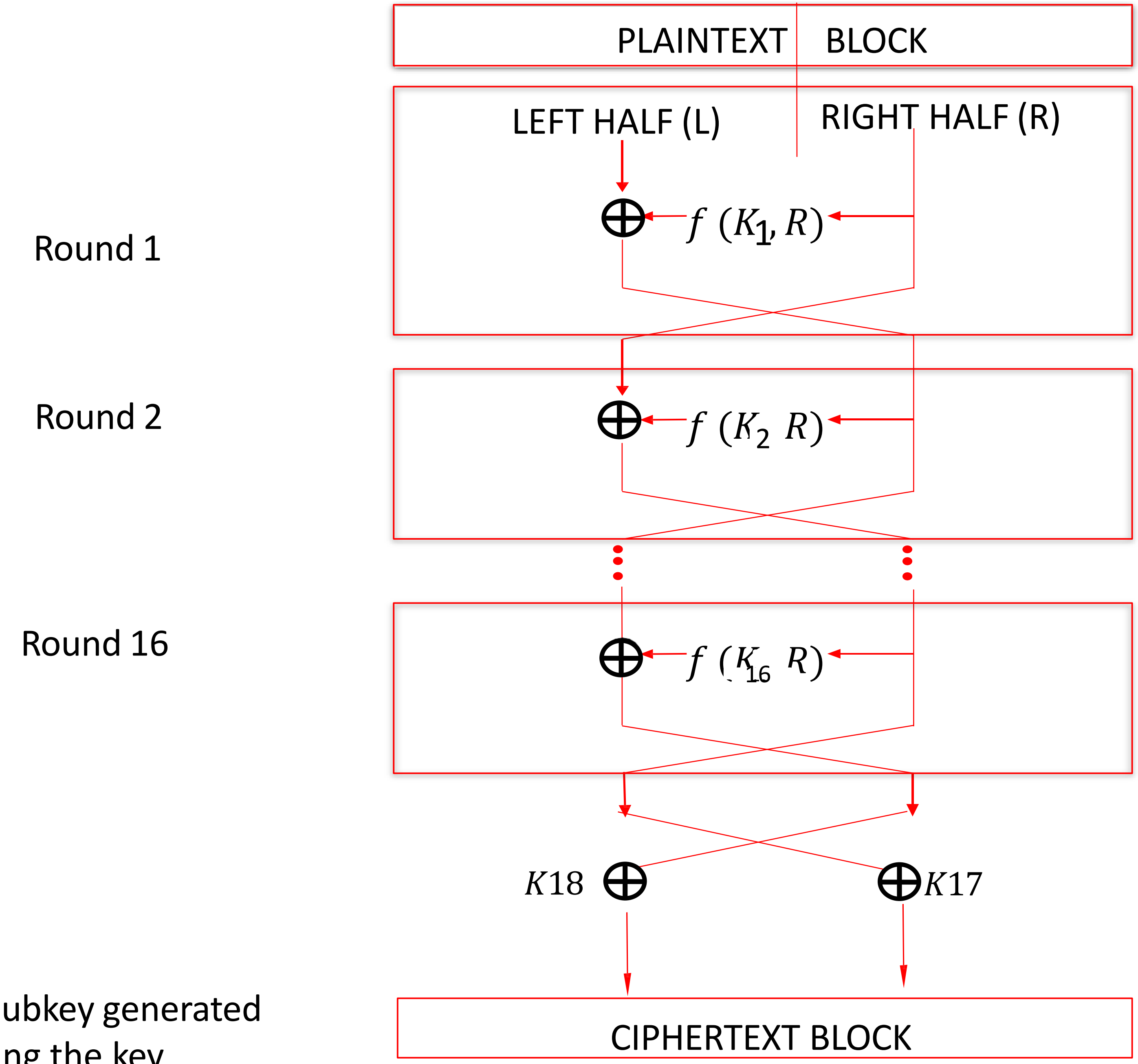


KEY

KEY SCHEDULE ALGORITHM

SET OF ROUND KEYS

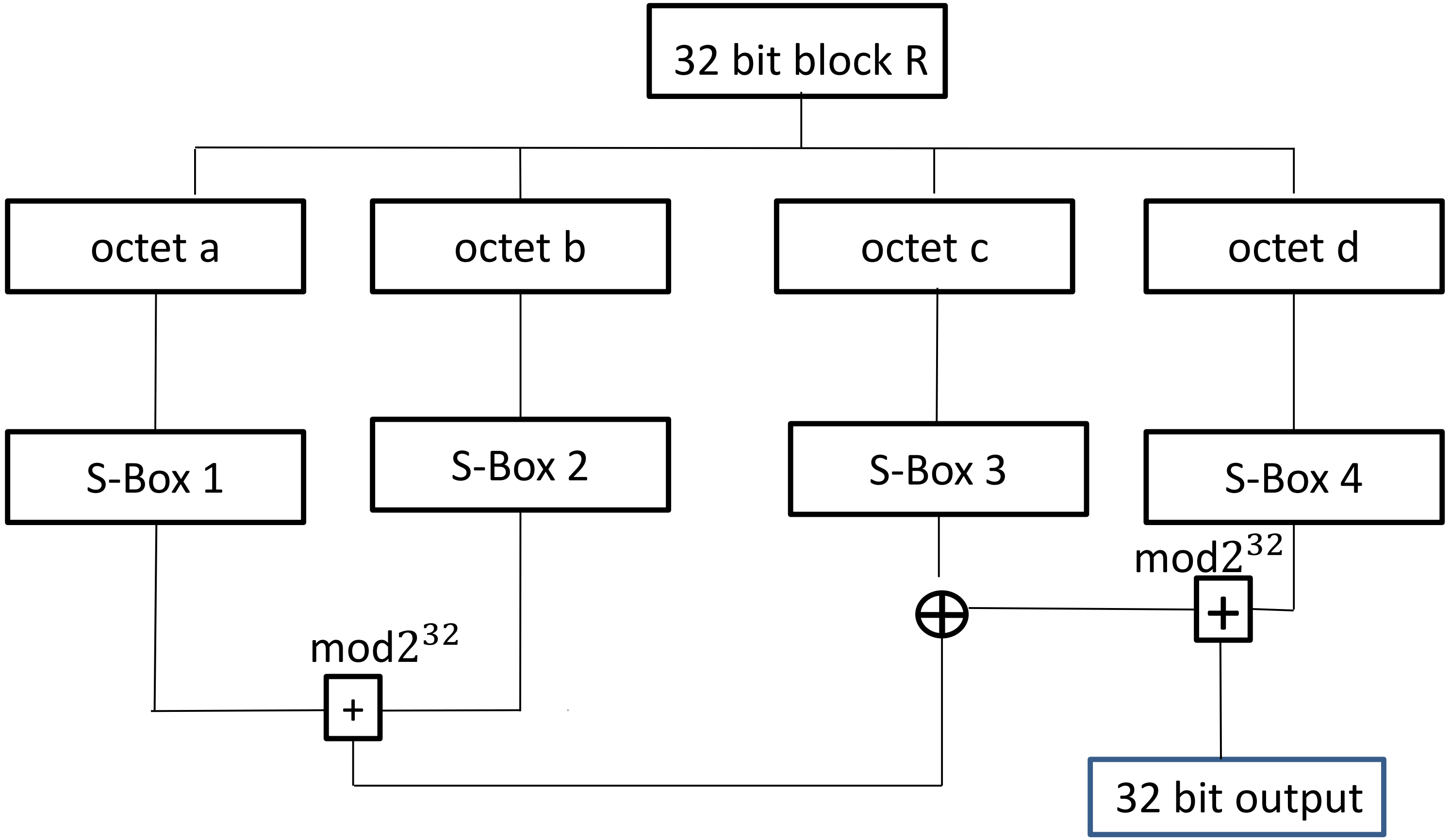
Blowfish



K_i = subkey generated using the key schedule

Dr Rosanne English

F in Blowfish



Advance Encryption Standard

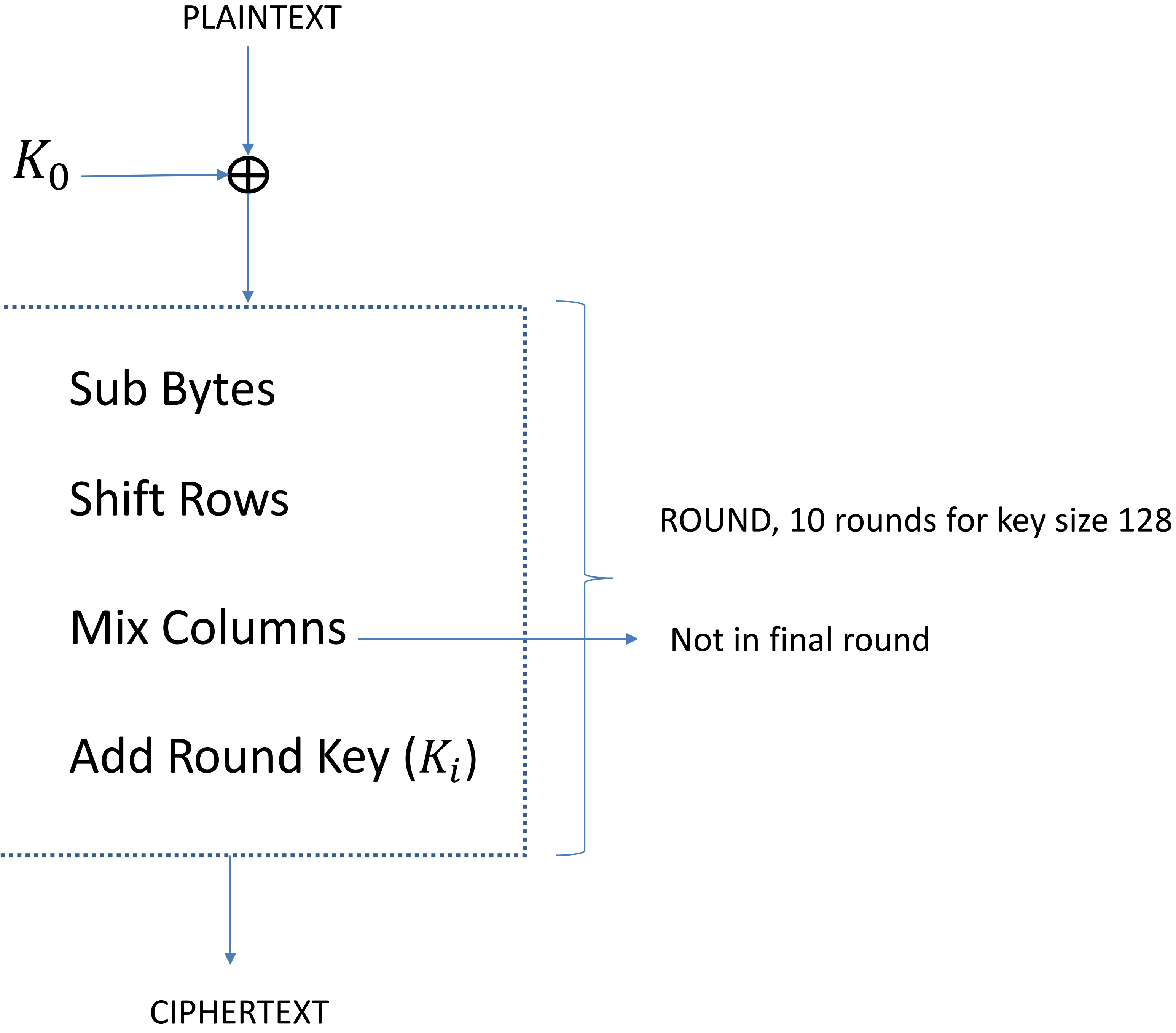
128 bits plaintext split into a 4x4 matrix each position containing a byte

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte 16

Byte 1	Byte 5	Byte 9	Byte 13
Byte 2	Byte 6	Byte 10	Byte 14
Byte 3	Byte 7	Byte 11	Byte 15
Byte 4	Byte 8	Byte 12	Byte 16

AES

Byte 1	Byte 5	Byte 9	Byte 13
Byte 2	Byte 6	Byte 10	Byte 14
Byte 3	Byte 7	Byte 11	Byte 15
Byte 4	Byte 8	Byte 12	Byte 16



PLAINTEXT

K_0 $\oplus$

Sub Bytes

Shift Rows

Mix Columns

Add Round Key (K_i)

ROUND, 10 rounds for key size 128

Not in final round

CIPHERTEXT

Modes of Operation

- Electronic Code Book (ECB)
  - Each block is encrypted separately

- Cipher Block Chaining (CBC)
  - Each block is XOR’d with the output of previous block before encryption
  - Requires initialisation vector and padding

- What’s the drawback of ECB?