CS 401

Computer Security

Dr. Samir M Hassan

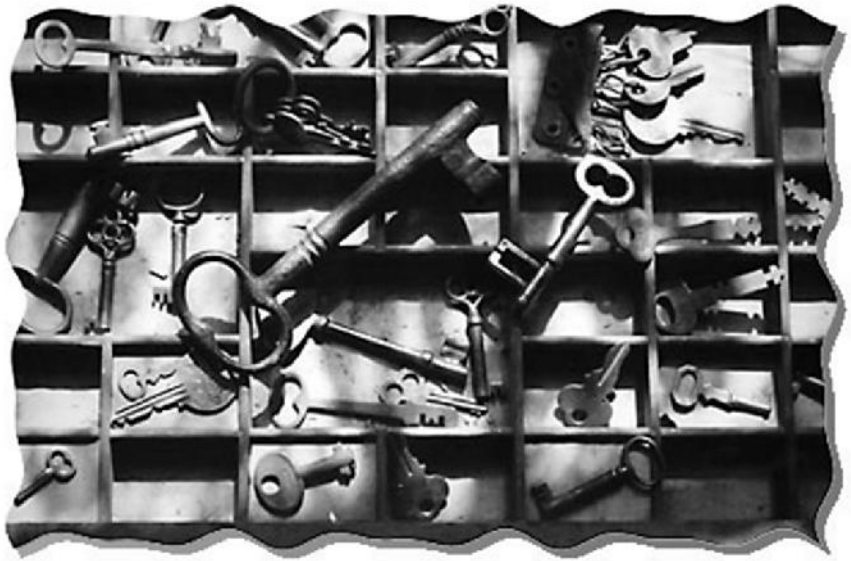
Lecturer of Communications at MSA

Member of IEEE Communications Society

Member of IEEE Computer Society

Member of IEEE Information Society

AES Project
Fall 2024



Description

Design an encryption (Encrypt/Decrypt) system based on AES algorithm with 10 rounds (128-bit key).

Clarify the behavior of the weak and semi-weak keys.

The attached document provides you with only the basic information needed to implement the AES encryption algorithm.

4 students per group.

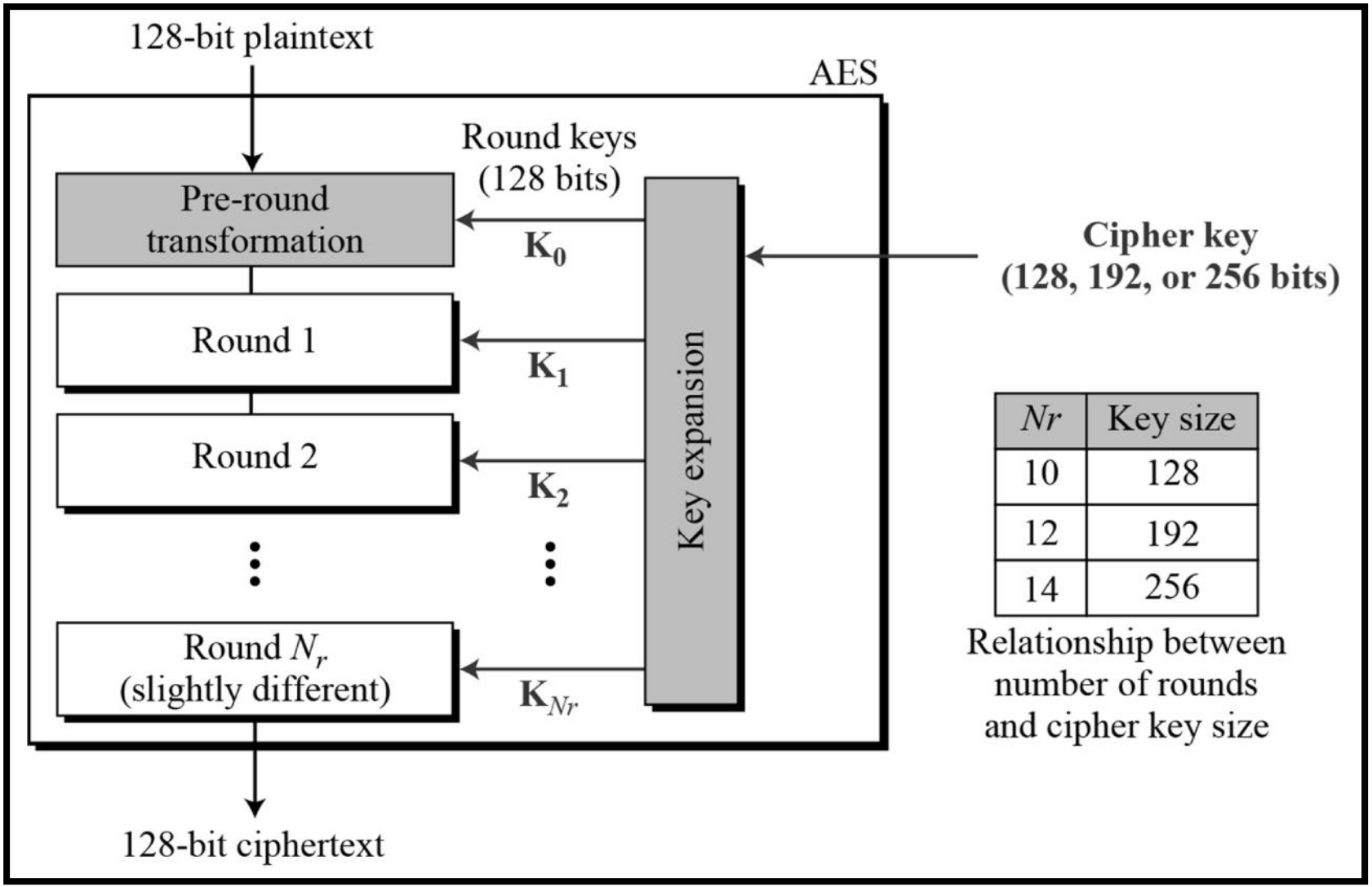
GUI is a must with check points.

Documentation of the project with application S/W will be submitted to your class assistants.

Documentation and Presentation will be offered in lecture time on Saturday 19-5-2012.

Late submission is not allowed.

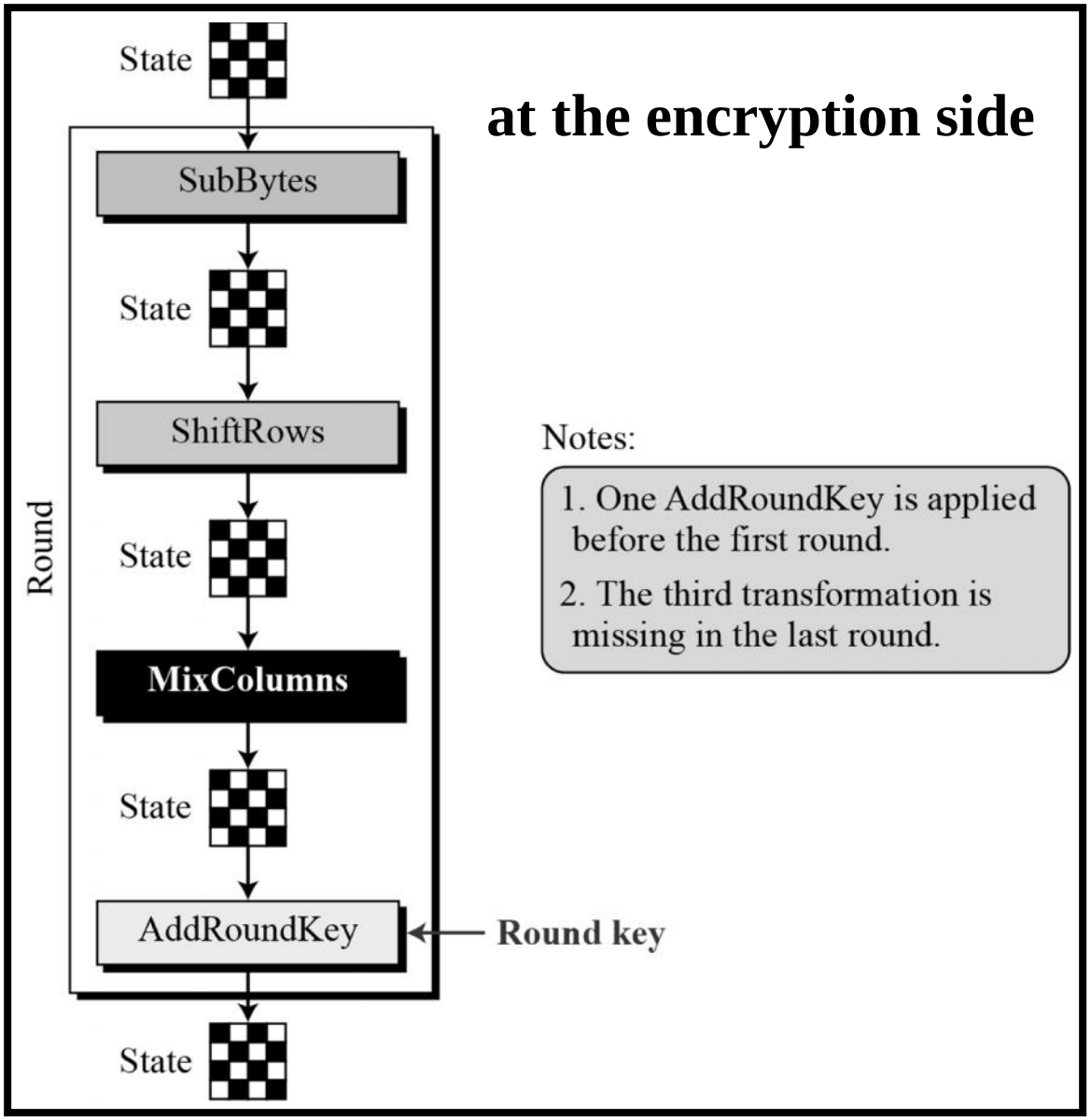
General design of AES encryption cipher



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

8.1.5 Structure of Each Round



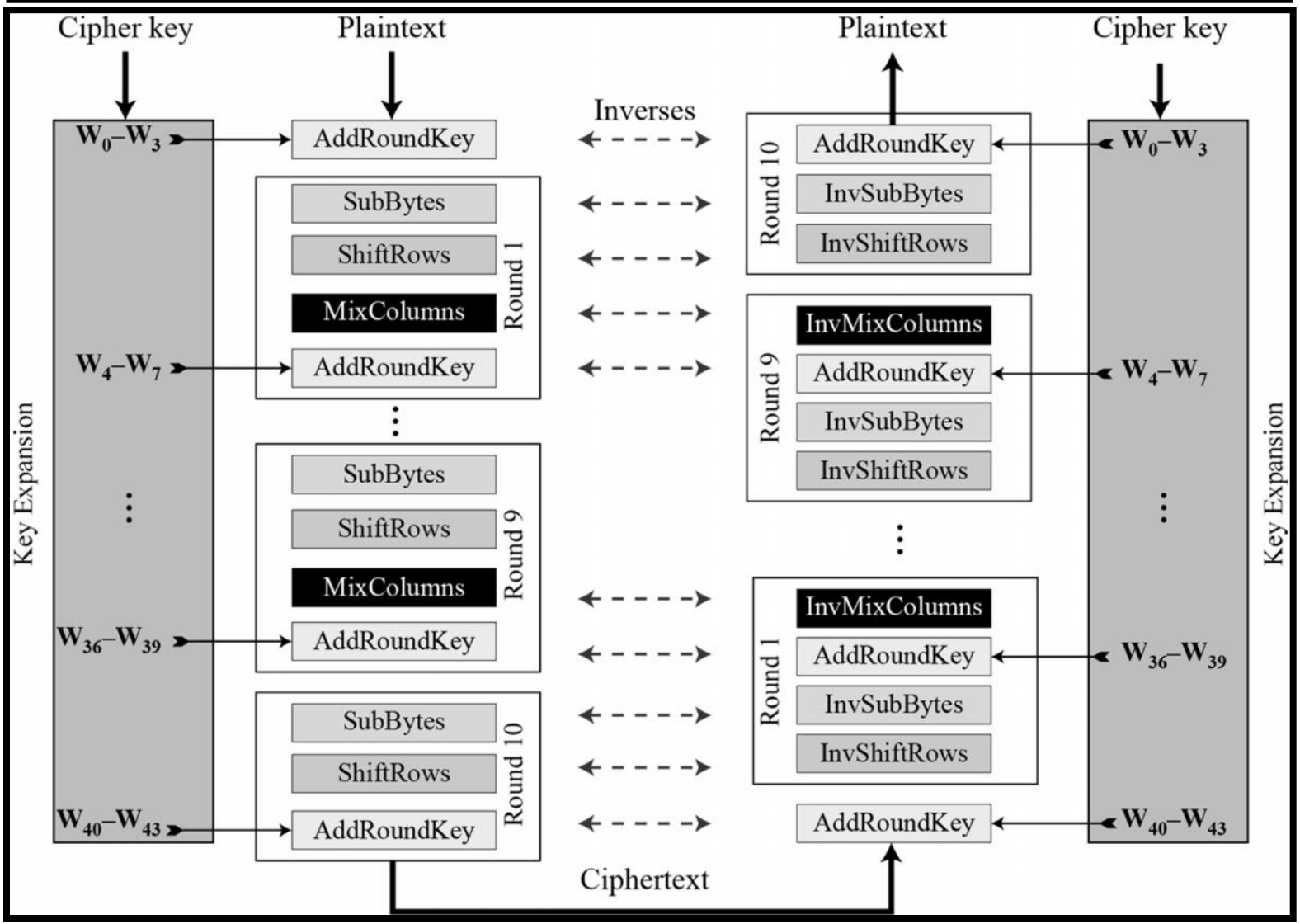
at the encryption side

Notes:

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

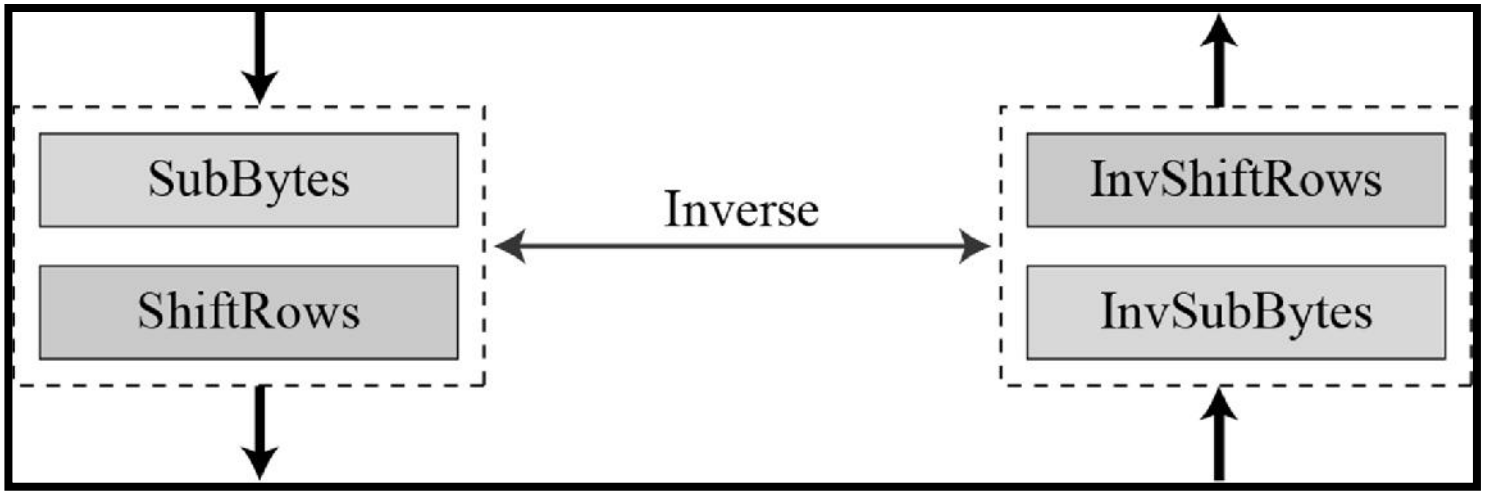
8.4.1 Original Design

Ciphers and inverse ciphers of the original design

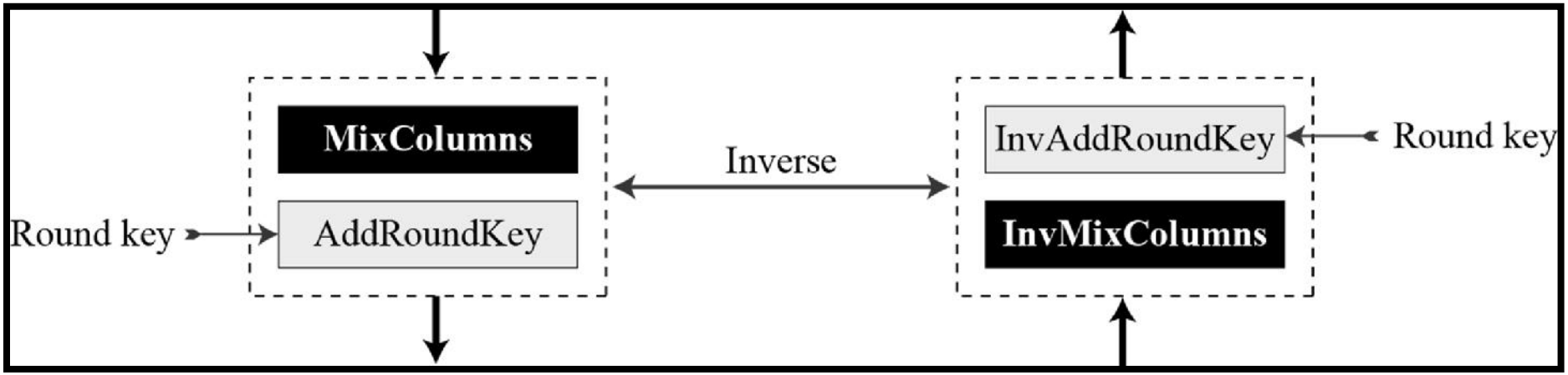


8.4.2 Alternative Design

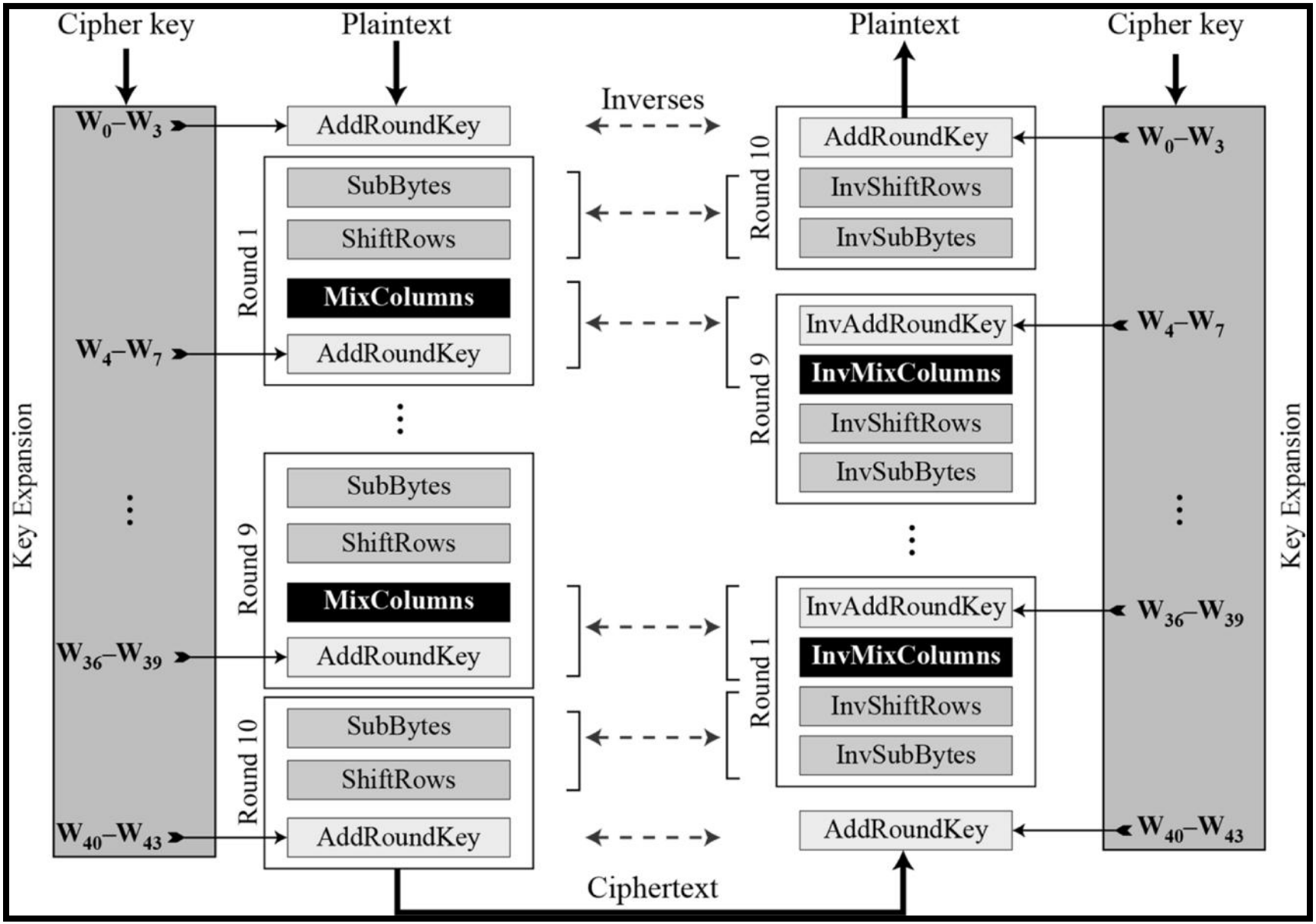
Invertibility of SubBytes and ShiftRows combinations



Invertibility of MixColumns and AddRoundKey combination



Cipher and reverse cipher in alternate design



Examples

Plaintext:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Cipher Key:	24	75	A2	B3	34	75	56	88	31	E2	12	00	13	AA	54	87
Ciphertext:	63	2C	D4	5E	5D	56	ED	B5	62	04	01	A0	AA	9C	2D	8D

Plaintext 1:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Plaintext 2:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
Ciphertext 1:	63	2C	D4	5E	5D	56	ED	B5	62	04	01	A0	AA	9C	2D	8D
Ciphertext 2:	26	F3	9B	BC	A1	9C	0F	B7	C7	2E	7E	30	63	92	73	13

Plaintext:	00	04	12	14	12	04	12	00	0c	00	13	11	08	23	19	19
Cipher Key:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Ciphertext:	5A	6F	4B	67	57	B7	A5	D2	C4	30	91	ED	64	9A	42	72

Input String	Key	Output String (HEX)
ABCDEFGHIJKLMNOP	112233445566778899 00AABBCCDDEEFF	BC4784A37D6F46452656B993D53393F5
ABCDEFGHIJKLMNOP	012233445566778899 00AABBCCDDEEFF	855866490543FDF6504FC84088FEDCA0
ABCDEFFHIJKLMNOP	112233445566778899 00AABBCCDDEEFF	372CCA446C0D391C4381392344630EE1

Input String(HEX)	Key	Output String (HEX)
00000000000000000000000000000000	00000000000000000000000000000000	66E94BD4EF8A2C3B884CFA59CA342B2E
00000000000000000000000000000000	00000000000000000000000000000001	0545AAD56DA2A97C3663D1432A3D1C84
00000000000000000000000000000001	00000000000000000000000000000001	A17E9F69E4F25A8B8620B4AF78EEFD6F

Proposed GUI

MSA at October City

Faculty of Computer Science

Computer Security (CS 401) Final Project

AES Block Cipher

By:

Aaaaaaaaa

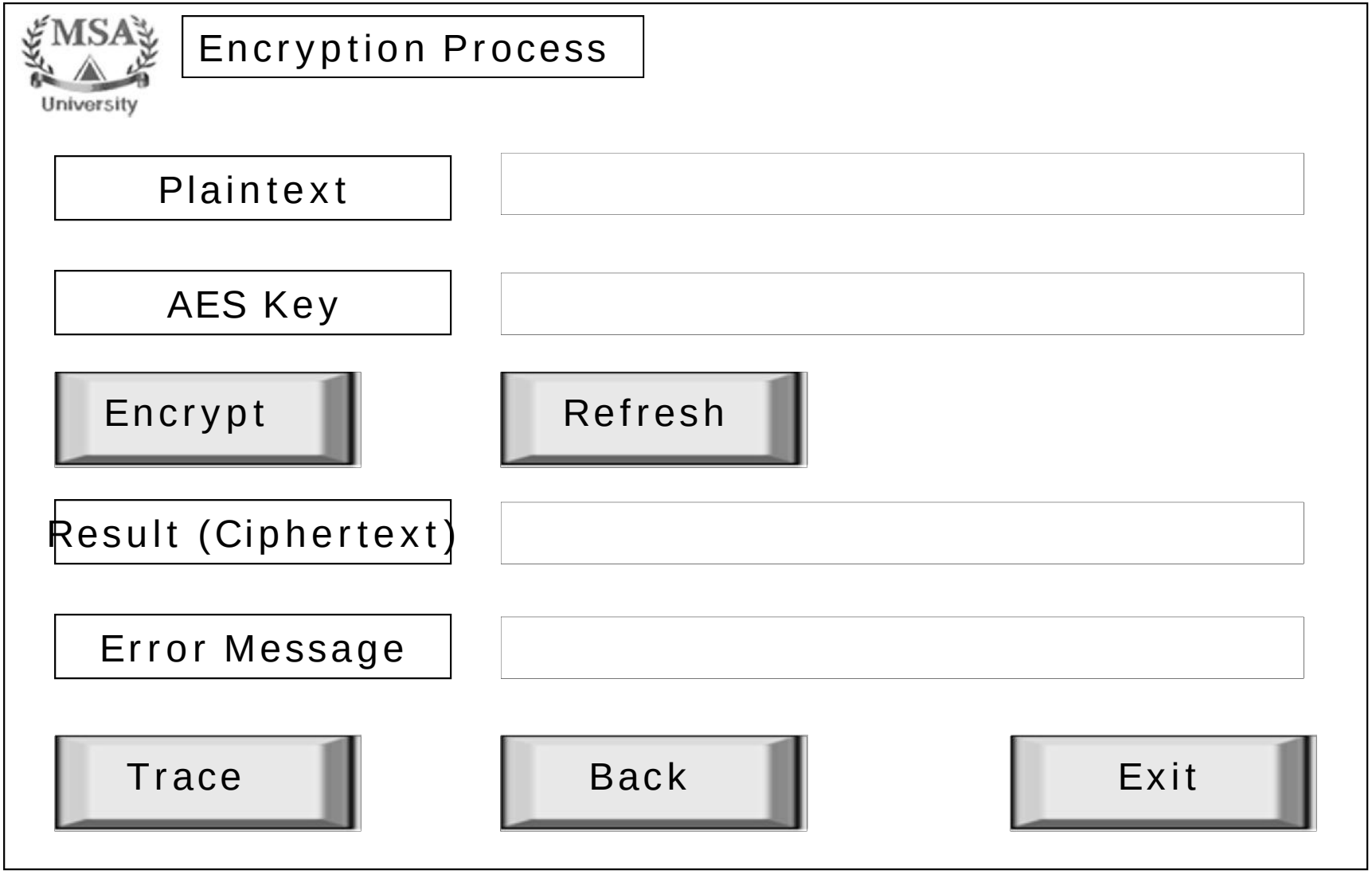
Bbbbbbbbb

Ccccccccccc

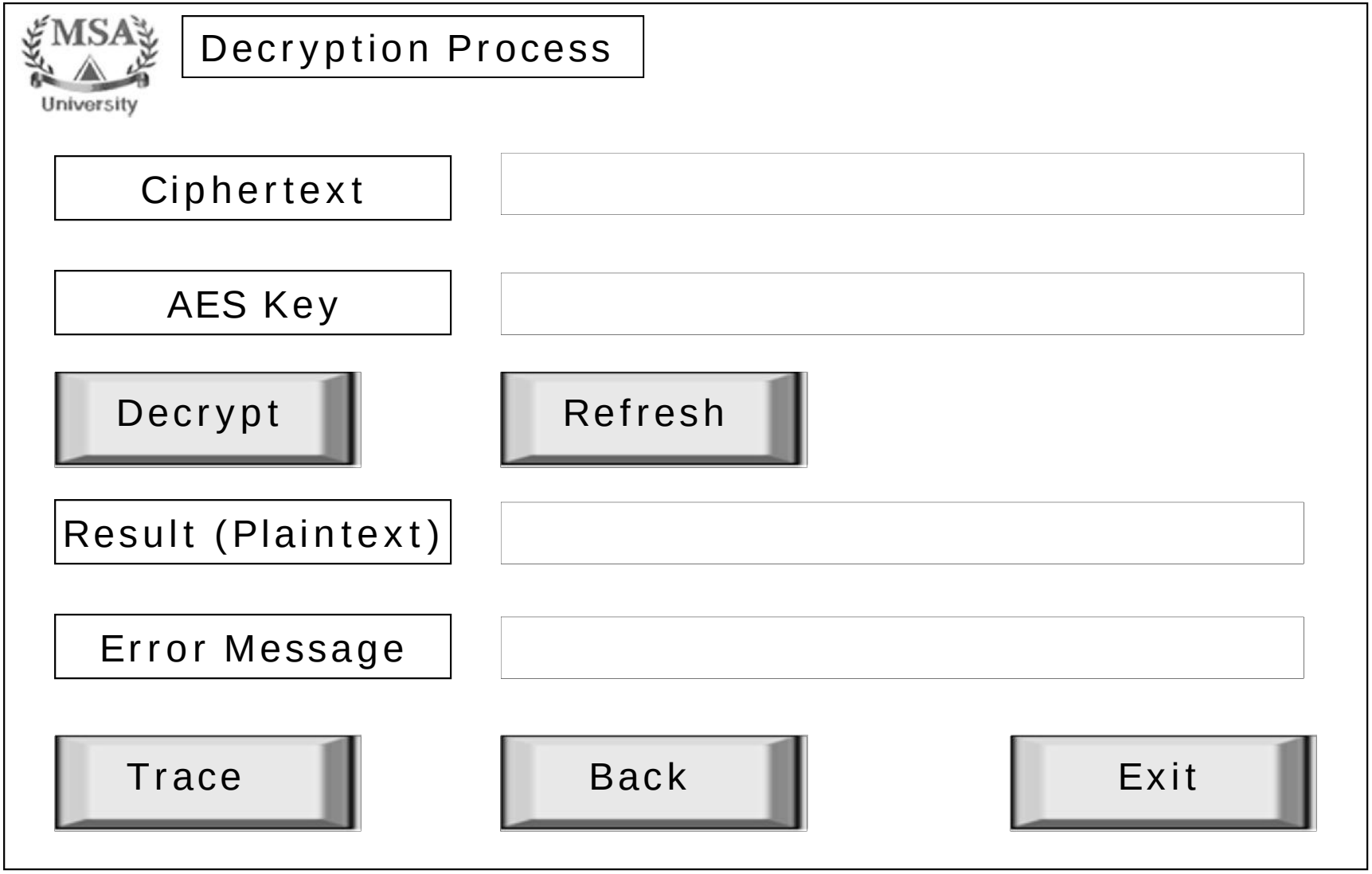
Ddddddddd

Encrypt | Decrypt | About | Exit

Proposed GUI; cont.



Proposed GUI; cont.



Proposed GUI; cont.

Trace of Encryption Process

Plaintext	abcdabcdabcdabcd
AES Key	
Ciphertext	f8db7cd33da5798a

```
IP:     L0=aa00aaff, R0=ff55ff55
Rnd1    f(R0=ff55ff55,    SK1=04 00 02 08 11 00 01 00 )    = c97a5158
Rnd2    f(R1=637afba7,    SK2=04 00 22 00 10 08 01 00 )    = f089b81e
Rnd3    f(R2=0fdc474b,    SK3=04 02 20 00 10 08 10 08 )    = f5be7d2d
Rnd4    f(R3=96c4868a,    SK4=00 02 10 04 02 01 10 08 )    = 6ab50a0d
Rnd5    f(R4=65694d46,    SK5=10 00 10 04 02 05 00 20 )    = d91e50a5
.
Rnd13   f(R12=327cf516, SK13=01 20 04 01 08 22 00 01 )    = b91db080
Rnd14   f(R13=39b680c3,         SK14=02 30 00 01 08 20 04 02 )    =
a9dd5518
Rnd15   f(R14=9ba1a00e,         SK15=02 10 02 08 01 00 04 02 )    =
92c35749
Rnd16   f(R15=ab75d78a,                  02 08 01 00
d4fe9474
FP:     L=f8db7cd3, R=3da5798a
Ciphertext: f8db7cd33da5798a
```

Back

Exit

Proposed GUI; cont.

Trace of Decryption Process

Ciphertext	f8db7cd33da5798a
AES Key	
Plaintext	abcdabcdabcdabcd

```
IP:     L0=4f5f347a, R0=ab75d78a
Rnd1    f(R0=ab75d78a,  SK16=00 10 02 08 01 00 05 00 )    = d4fe9474
Rnd2    f(R1=9ba1a00e,  SK15=02 10 02 08 01 00 04 02 )    = 92c35749
Rnd3    f(R2=39b680c3,  SK14=02 30 00 01 08 20 04 02 )    = a9dd5518
Rnd4    f(R3=327cf516,  SK13=01 20 04 01 08 22 00 01 )    = b91db080
Rnd5    f(R4=80ab3043,  SK12=01 04 04 10 00 02 02 01 )    = b16080be
.
Rnd13   f(R12=96c4868a,         SK4=00 02 10 04 02 01 10 08 )     =
6ab50a0d
Rnd14   f(R13=0fdc474b, SK3=04 02 20 00 10 08 10 08 )     = f5be7d2d
Rnd15   f(R14=637afba7, SK2=04 00 22 00 10 08 01 00 )     = f089b81e
Rnd16   f(R15=ff55ff55,  SK1=04 00 02 08 11 00 01 00 )     = c97a5158
FP:     L=abcdabcd, R=abcd
returns abcdabcdabcdabcd
```

Back

Exit

Evaluation Criteria

Computer Security CS401

Evaluation Sheet of Final Project

ID	Name	Evaluation														Remarks
		Report 20				Testing the application 50			Presentation 15			Participation of each member	Adding extra features	Quality of the project	Total	
		Report content	References	Formatting	Report presentation	User interface	Robustness	Creativity	Understanding	Skills	Language					
		5	5	5	5	15	20	15	5	5	5	5	5	5	100	

References

- Lecture 8
- FIPS 197, "Advanced Encryption Standard"
- Advanced Encryption Standard (AES)
  http://www.ratchkov.com/vpn/aes/aes.html
- RIJNDAEL
  http://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html
- The Laws of Cryptography
  http://www.cs.utsa.edu/~wagner/laws/

Thanks