



## Course Weekly Outline

Course Instructor	Dr. Alaa Kadhim				
E_mail	dralaa_cs@yahoo.com				
Title	Block cipher				
Course Coordinator	Dr. Alaa Kadhim				
Course Objective	The aim if this subject to learn the students how to programming the algorithm of block cipher and the basic principle to encryption the cipher text.				
Course Description	Chapter One: Basic Concepts of The Cryptography Block cipher Algorithm of block cipher				
Textbook	H. Boker & F. Piper, “ Cipher System, The Protection of Communications “ , Northwood Books, Landon, 1982.				
References	B. Schneier, “ <b>Applied Cryptography</b> ”, 2nd ed., John Wiley & Sons, Inc., 1996.  ANSI X9.44, “ <b>Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using RSA</b> ”, 1994.  Diffie: Whitfield Diffie and Martin Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory, Nov 1976.  William, S.," <i>Cryptography and Network Security: Principles and Practice.</i> ", Three Edition. Prentice Hall, 2002.				
Course Assessment	Term Tests	Laboratory	Quizzes	Project	Final Exam
	(20%)	(20%)	(10%)	----	(50%)
General Notes	Programming in VB.net				



## Course weekly Outline

week	التاريخ	Topics Covered		Notes
1	22/9/2014	Symmetric Cipher Model.	Designing simple vb.net program.	
2	30/9/2014	Confusion and Diffusion.	Designing simple vb.net program.	
3	7/10/2014	Feistel Mode .	S-P-Box	
4	14/10/2014	Data Encryption Standard DES	f-Function in DESDES	
5	21/10/2014	Key of DES algorithm	Permutation tables of DES algorithm	
6	28/10/2014	Example of DES	DES algorithm	
7	4/11/2014	Type of DES	Key of DES algorithm	
8	11/11/2014	CAST algorithm	CAST algorithm program	
9		Key generator of cost	Key generator of cost program	
10	18/11/2014	GOST algorithm	GOST algorithm program	
		Key generator of Gost	Key generator of Gost	

		of Gost	program	
<b>11</b>	<b>25/11/2014</b>	Example of gost	Key generator of Gost	
<b>21</b>	<b>2/12/2014</b>	RC5 algorithm	Functions algorithm program	
<b>13</b>	<b>9/12/2014</b>	Key Generator of RC5	RC5 program program	
<b>14</b>	<b>16/12/2014</b>	example of RC5	Key Generator of RC5	
<b>15</b>	<b>23/12/2014</b>	review	Review.	
<b>16</b>	<b>30/12/2014</b>	Exam	review	
<b>18</b>	<b>17/2/2015</b>	Feal algorithm	Functions of Feal algorithm	
<b>19</b>	<b>24/2/2015</b>	Key of feal	Feal algorithm program	
<b>20</b>	<b>3/3/2015</b>	blowfish	Blowfish algorithm program	
<b>21</b>	<b>10/3/2015</b>	Key of blowfish	Key of blowfish	
<b>22</b>	<b>17/3/2015</b>	example	Complete blowfish program	
<b>23</b>	<b>24/3/2015</b>	AES	Functions of AES algorithm	
<b>24</b>	<b>31/3/2015</b>	Key of AES	AES rounds program	
<b>25</b>	<b>7/4/2015</b>	Example of AES	Complete program of AES	
<b>26</b>	<b>14/4/2015</b>	review	Complete program of AES	
<b>27</b>	<b>21/4/2015</b>	Half Exam	Half Exam	
<b>28</b>	<b>28/4/2015</b>	serpent	Functions of serpent programs	
<b>29</b>	<b>5/5/2015</b>	Key of serpent	Key of serpents algorithm	
<b>30</b>	<b>12/5/2015</b>	Example of serpent	-----	
<b>31</b>	<b>19/5/2015</b>	Final course Exam	-----	

**Instructor Signature:**

**Dean Signature:**