



## Course Weekly Outline

Course Instructor	Assist. Prof. Dr. Hanaa Mohsin Ahmed				
E_mail	Salmanhanna2007@yahoo.com				
Title	Cryptanalysis				
Course Coordinator					
Course Objective					
Course Description	Introduction (definition of Cryptanalysis and Cryptanalyst, Cryptanalyst position is some simple cryptosystems, Requirements of Cryptosystems), Type of Attacks on Cryptosystems, Cryptanalysis of the Classical cryptography (Transposition cryptanalysis, Keyword columnar transposition, Double transposition). substitution cryptanalysis,( additive, multiplication, affine, keyword, Polyalphabetic analysis: vigenere method, computing key length, Kasiski test, Shift itself, Percentage of coincidence, complete examples.), Statistical cryptanalysis ( unilateral frequency distribution , Letter frequency in cryptogram, roughness ,Coincidence tests, index of coincidence, Cryptanalysis for the affine using statistical cryptanalysis), Stream cipher cryptanalysis ( introduction of stream cipher, LFBSR, primitive polynomials, Matrix approach to analyzing stream cipher , examples, solve problems, , Massy algorithm , examples), DES cryptanalysis, RSA cryptanalysis .				
Textbook					
References	Cryptography: Theory and Practice, by Douglas Stinson CRC Press, CRC Press LLC, ISBN: 0849385210, Pub Date: 03/17/95 system Cryptography and Data Security, by Peter Gutmann, University of Auckland, <a href="http://www.cs.auckland.ac.nz/~pgut001">http://www.cs.auckland.ac.nz/~pgut001</a> Applied cryptanalysis' /Breaking Ciphers in the Real World/2007 PDF				
Course Assessment	Term Tests	Laboratory	Quizzes	Project	Final Exam
	(30%)	---	(10%)	----	(60%)
General Notes					



## Course weekly Outline

week	Date	Topics Covered	Lab. Experiment Assignments	Notes
1	16/9/2014	Introduction: definition of Cryptanalysis and Cryptanalyst, Cryptanalyst position is some, simple cryptosystems		
2	23/9/2014	Requirements of Cryptosystems, Type of Attacks on Cryptosystems		
3	30/9/2014	Cryptanalysis of the Classical cryptography: Transposition cryptanalysis		
4	7/10/2014	Complete examples.		
5	14/10/2014	, Keyword coalminer transposition,		
6	21/10/2014	Double transposition		
7	28/10/2014	Complete examples.		
8	4/11/2014	Substitution cryptanalysis: additive,		
9	11/11/2014	multiplication		
10	18/11/2014	, affine		
11	25/11/2014	keyword,		
12	2/12/2014	Complete examples.		
13	9/12/2014	Polyalphabetic analysis: vigenere method,		
14	16/12/2012	computing key length, Kasiski test		
15	23/12/2012	Shift itself, Percentage of coincidence		
16	30/12/2012	Complete examples.		
Half-year Break				
17	10/2/2015	Statistical cryptanalysis: unilateral frequency distribution, Letter frequency in cryptogram,		
18	17/2/2015	roughness, Coincidence tests, index of coincidence,		
19	24/2/2015	Cryptanalysis for the affine using statistical cryptanalysis		
20	3/3/2015	Complete example.		
21	10/3/2015	Stream cipher cryptanalysis: introduction of stream cipher,		
22	17/3/2015	LFBSR, primitive polynomials,		
23	24/3/2015	Complete example.		
24	31/3/2015	Matrix approach to analyzing stream cipher,		
25	7/4/2015	solve problems,		
26	14/4/2015	Complete example.		
27	21/4/2015	Massy algorithm		
28	28/4/2015	Complete example.		
29	5/5/2015	DES cryptanalysis:		
30	12/5/2015	Complete example.		
31	19/5/2015	RSA cryptanalysis:		
32	26/5/2015	Complete example.		

Instructor Signature:

Dean Signature: