

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جهاز الاشراف والتقويم العلمي

جدول الدروس الاسبوعي

أ.م.د. سكيانة حسن هاشم					الاسم
soukaena_hassan@yahoo.com					البريد الإلكتروني
Data Security					اسم المادة
30 محاضرة كل محاضرة 2 ساعات					مقرر الفصل
تعريف الطالب بأمنية الحاسبات والبيانات، ثم الدخول الى تدرسيهم الرياضيات المتعلقة بأمنية البيانات وبالذات مايتعلق بالتشفير ثم الدخول الى تفاصيل خوارزميات التشفير ابتداء من التشفير التقليدي القديم الى احداث خوارزميات التشفير.					اهداف المادة
Introduction to Data Security, Mathematical Background, Classical Encryption, Data Encryption Standard (DES), <u>Exponential Cipher</u> , Stream Cipher, data hiding					التفاصيل الاساسية للمادة
1- William Stallings, <i>Cryptography and Network Security, (Principles and Practice)</i> , 2003 2- William Stallings, <i>Cryptography and Network Security, (Principles and Practice)</i> , 2011					الكتب المنهجية
1- Managing Cisco Network Security: Building Rock-Solid Networks, 2000					المصادر الخارجية
الامتحان النهائي	المشروع	الامتحانات اليومية	المختبر	الفصل الدراسي	تقديرات الفصل
60%	-	10%	لا يوجد	30%	
					معلومات اضافية



الجامعة : التكنولوجيا
الكلية : العلوم-علوم الحاسوب
القسم : برامجيات- نظم- ذكاء-وسائط
المرحلة : الرابعة
اسم المحاضر الثلاثي : سكيبة حسن هاشم
اللقب العلمي : استاذ مساعد
المؤهل العلمي : الدكتوراه
مكان العمل : الجامعة التكنولوجية / علوم الحاسوب

جدول الدروس الاسبوعي

الاسبوع	التاريخ	المادة النظرية	المادة العلمية	الملاحظات
1	2/10/2016 5/10/2016	Security, Confidentiality, Threats to confidentiality, Integrity, Availability, Authentication, Non-repudiation, Security Attack, Basic Terminology, Basic Cryptographic Algorithms	VB.net lectures	
2	9/10/2016 12/10/2016	Cryptographic Random Number Generators, Strength of Cryptographic Algorithms,	VB.net lectures	
3	16/10/2016 19/10/2016	Cryptanalysis and Attacks on Cryptosystems	Implement algorithms in VB.net	
4	23/10/2016 26/10/2016	Information hiding (steganography and water marking)	Implement algorithms in VB.net	
5	30/10/2016 2/11/2016	Mathematical Background, Prim Numbers , Greatest Common Divisor(GCD), (LCM) Least Common Multiple, Modular, Euler Function,	Implement algorithms in VB.net	
6	6/11/2016 9/11/2016	Inverse Algorithm (inv), Fast Exponential.	Implement algorithms in VB.net	
7	13/11/2016 16/11/2016	Classical Encryption, Transposition Ciphers, Keyless Transposition Ciphers, Keyed Transposition Ciphers, Combining Two Approaches, Double Transposition Ciphers,	Implement algorithms in VB.net	
8	20/11/2016 23/11/2016	Monoalphabetic Ciphers, Additive Cipher , Shift Cipher and Caesar	Implement algorithms in VB.net	

		Cipher, Multiplicative Ciphers , Affine Ciphers , polybious cipher		
	Implement algorithms in VB.net	Polyalphabetic Ciphers, Autokey Cipher, Vigenere Cipher, Beaufort Cipher , Running Key Cipher	27/11/2016 30/11/2016	9
	Implement algorithms in VB.net	Polygraphic Ciphers, Playfair Cipher, Hill Cipher,	4/12/2016 7/12/2016	10
	Implement algorithms in VB.net	Other Ciphers and Codes, Ascci Beale Cipher, Book Cipher,	11/12/2016 14/12/2016	11
	Implement algorithms in VB.net	Data Encryption Standardx (DES), , Block Cipher, ECB Operation Mode , CBC Operation Mode , Output Feedback Mode (OFM), Product Cipher , Iterated Block Cipher , Feistel Cipher ,	18/12/2016 21/12/2016	12
	Implement algorithms in VB.net	DES Cipher , Data Encryption Standard (DES), DES (Data Encryption Standard) history, Description of DES, Outline of the Algorithm ,	25/12/2016 28/12/2016	13
	Implement algorithms in VB.net	The Initial Permutation, The Key Transformation, The Expansion Permutatio, The S-Box Substitution , The P-Box Permutation, The Final Permutation, Decrypting DES.	1/1/2017 4/1/2017	14
		التقييم للفصل الاول	8/1/2017 11/1/2017	15
		امتحانات نصف السنة + العطلة الربيعية		16
	Implement algorithms in VB.net	Exponential Cipher, Introduction, Public-Key Cryptography, Public-Key Applications, Security of Public Key Schemes,	19/2/2017 22/2/2017	17
	Implement algorithms in VB.net	Exponentiation Ciphers, Pohlig-Hellman Scheme, RSA description and algorithm, Key Generation Algorithm, Encryption, Decryption,	26/2/2017 1/3/2017	18
	Implement algorithms in VB.net	A simple example of RSA encryption, Security Concern,	5/3/2017 8/3/2017	19
	Implement algorithms in VB.net	Secrecy And Authenticity	12/3/2017 15/3/2017	20
	Implement algorithms in VB.net	Merkle-Hellman Knapsacks, MH Knapsack,	19/3/2017 22/3/2017	21

	Implement algorithms in VB.net	Diffie-Hellman knapsack	26/3/2017 29/3/2017	22
	Implement algorithms in VB.net	Stream Cipher, One-Time Pad or Vernam Cipher, Drawback, Solution , Randomness , Pseudo-randomness ,	2/4/2017 5/4/2017	23
	Implement algorithms in VB.net	Synchronous Stream Ciphers , Self-Synchronizing Stream Ciphers ,	9/4/2017 12/4/2017	24
	Implement algorithms in VB.net	Linear feedback shift registers, Nonlinear combination , Generators	16/4/2017 19/4/2017	25
	Implement algorithms in VB.net	Nonlinear Filter Generator , Example (Geffe Generator),	23/4/2017 26/4/2017	26
	Implement algorithms in VB.net	Randomness key tests	30/4/2017 3/5/2017	27
		التقييم للفصل الاول	7/5/2017 10/5/2017	28
		الامتحانات النهائية		29
				30
				31
				32

توقيع العميد :

توقيع الاستاذ :