جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جهاز الاشراف والتقويم العلمي

أسم الجامعه: الجامعة التكنولوجية
أسم الكليه: علوم الحاسبات
أسم القسم: أمنيه بيانات
أسم المحاضر: د. علاء كاظم فرحان
اللقب العلمي: أستاذ مساعد
المؤهل العلمي: دكتوراه
مكان العمل:الجامعة التكنولوجية/قسم علوم الحاسبات

جدول الدروس الاسبوعي

الاسم	**د. علاء كاظم فرحان**
البريد الالكتروني	**dralaa_cs@yahoo.com**
اسم المادة	**خوارزميات المفتاح المتناظر والشتفير الانسيابي** **المرحله الثانيه**
مقرر الفصل	
اهداف المادة	تهدف هذه المادة إلى تعليم الطالب على كيفية استخدام خوارزميات التشفير زبرمجتها بشكل ملائم لتشفير النصوص الهامه والسريه وتعليمهم على اساس رياضي وتطيقهابشكل عملي لخوارزميات التشفير المفتاح المعلن او خوارزمات التشفير الانسيابي
التفاصيل الاساسية للمادة	Chapter One: Basic Concepts of The Cryptography Block cipher Algorithm of block cipher
الكتب المنهجية	H. Boker & F. Piper, " Cipher System, The Protection of Communications ", Northwood Books, Landon, 1982.
المصادر الخارجية	B. Schneier, "**Applied Cryptography**", 2nd ed., John Wiley & Sons, Inc., 1996. ANSI X9.44, "**Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using RSA**", 1994. Diffie: Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976. William, S.," ***Cryptography and Network Security: Principles and Practice."***, Three Edition. Prentice Hall, 2002.

	الفصل الدراسي	**المختبر**	**الامتحانات اليومية**	**المشروع**	**الامتحان النهائي**

تقديرات الفصل	%20	%20	%10	-	%50
معلومات اضافية	Visual basic.net 2013				

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جهاز الاشراف والتقويم العلمي

أسم الجامعه: الجامعة التكنولوجية
أسم الكليه: علوم الحاسبات
أسم القسم: أمنيه البيانات
أسم المحاضر: د. علاء كاظم فرحان
اللقب العلمي: استاذ مساعد
المؤهل العلمي: دكتوراه
مكان العمل:الجامعة التكنولوجية/قسم علوم الحاسبات

جدول الدروس الاسبوعي

الاسبوع	التاريخ	المادة النظرية	المادة العلمية	الملاحظات
1	22/9/2014	Intoductionof Cryptography Complexity Theory	Designing simple vb.net program.(GCD)	
2	30/9/2014	Types of cryptography .	Designing simple vb.net program.(LCM)	
3	7/10/2014	attackers	Euler's program	
4	14/10/2014	Principles of Public-Key Cryptosystems Diffie and Hellman Public key VS private key	Fast program	
5	21/10/2014	Asymmetric Public-key Cryptosystems	Model program of all function	
6	28/10/2014	RSA public key algorithm	RSA algorithm program	
7	4/11/2014	Signature of RSA	Signature of RSA program	
8	11/11/2014	Security of RSA	Complete program RSA	
9		ELGamal algorithm	ELGamal algorithm program	
10	18/11/2014	Signature of ElGamal algorithm	Signature of ElGamal algorithm program	

	Security of ElGamal algorithm program	**Security of ElGamal algorithm**		
	review	**review**	**25/11/2014**	**11**
	Exam in program	**Exam**	**2/12/2014**	**21**
	Knapsack of algorithm	**Knapsack of algorithm**	**9/12/2014**	**13**
	Complete program Knapsack	**example of algorithm**	**16/12/2014**	**14**
	Review.	**review**	**23/12/2014**	**15**
	Review	**Exam**	**30/12/2014**	**16**
عطلة نصف السنة				
	McEliece of public key program	**McEliece of public key**	**17/2/2015**	**18**
	Program to stream cipher	**Stream Cipher Structure Important element for design a stream cipher**	**24/2/2015**	**19**
	Program to stream cipher	**Types of stream ciphers**	**3/3/2015**	**20**
	Program to Polynomial	**Polynomial**	**10/3/2015**	**21**
	Program to Arithmetic of Polynomial	**Arithmetic of Polynomial**	**17/3/2015**	**22**
	Program to Shift register	**Shift register**	**24/3/2015**	**23**
	Counties program to SR	**Types of shift register**	**31/3/2015**	**24**
	review	**Review**	**7/4/2015**	**25**
	Exam	**Exam**	**14/4/2015**	**26**
	Nonlinear Shfit Register program	**Nonlinear Shfit Register**	**21/4/2015**	**27**
	Five Basic Tests program	**Five Basic Tests**	**28/4/2015**	**28**
	Counties	**exam**	**5/5/2015**	**29**
	----------	**Review and Exam**	**12/5/2015**	**30**
	----------	**Final course Exam**	**19/5/2015**	**31**

توقيع الاستاذ : **توقيع العميد :**