جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جهاز الاشراف والتقويم العلمي

الجامعة : ديالى
الكلية : الهندسة
القسـم : الحاسوب والبرامجيات
المرحلة : الرابعة
اسم المحاضر الثلاثي : هدى محمد صالح
اللقب العلمي : مدرس مساعد
المؤهل العلمي : ماجستير
مكان العمل : قسم الحاسبات

استمارة انجاز الخطة التدريسية للمادة

الاسم	**هدى محمد صالح**
البريد الالكتروني	**Hoopoe٢٠٠٨٠@hotmail.com**
اسم المادة	**تشفير وأمنية معلومات**
مقرر الفصل	
اهداف المادة	**تعريف الطالب بالمبادئ الاساسية لمادة التشفير وأمنيه البيانات، تمكين الطالب من معرفه وتميز طرق التشفير وخوارزمياتها الكلاسيكيه والحديثه، طرق حمايه البيانات المخزونه والمرسله عبر الشبكه.**
التفاصيل الاساسية للمادة	**دراسة طرق التشفير بأنواعها الحديثه منها والكلاسيكية. توفير امنية للمعلومات والبيانات المخزونه في انظمه الحاسبه وفي قواعد البيانات والمرسلة عبر شبكة الانترنيت.**
الكتب المنهجية	**References:** **١. Applied Cryptography by Schneier, B. ٢٠٠٩** **٢. Security in Computing, Textbook by Pfleege ٢٠١٢.**
المصادر الخارجية	**Data Base Security By Pfleege.** **Network Security by Pfleege.**

تقديرات الفصل	**الفصل الدراسي الاول**	**نصف السنة**	**الفصل الدراسي الثاني**	**العملي**	**الامتحان النهائي**
	% ١٠	**% ٢٠**	**% ١٠**	**%١٠**	**% ٥٠**

معلومات اضافية	

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جهاز الاشراف والتقويم العلمي

الجامعة : ديالى
الكلية : الهندسة
القسـم : الحاسوب والبرامجيات
المرحلة : الرابعة
اسم المحاضر الثلاثي : هدى محمد صالح
اللقب العلمي : مدرس مساعد
المؤهل العلمي : ماجستير
مكان العمل : قسم الحاسبات

استمارة الخطة التدريسية للمادة

الأسبوع	التاريخ	المادة النظرية	المادة العلمية	الملاحظات
١	٢٠١٤/١٠/٠٦	**Introduction to encryption and Data security:**		
٢	٢٠١٤/١٠/١٣	**١.١ Characteristics of Computer intrusion**		
٣	٢٠١٤/١٠/٢٠	**١.٢ Kinds of Security Breaches**		
٤	٢٠١٤/١٠/٢٧	**١.٣ The points of security Vulnerability - Attacks on Hardware- Attacks on Software - Attacks on Data**		
٥	٢٠١٤/١١/٠٣	**١.٤ The people involved**		
٦	٢٠١٤/١١/١٠	**١.٥ Methods of defense**		
٧	٢٠١٤/١١/١٧	**Classification of cipher system** **١.٦ Secret key systems.** **١.٦.١ Conventional System (classical)** **١.٦.٢ Modern Systems**		
٨	٢٠١٤/١١/٢٤	**١.٧ Public key Systems**		
٩	٢٠١٤/١٢/٠١	**١.٧.١ RSA** **١.٧.٢ Knapsack.**		
١٠	٢٠١٤/١٢/٠٨	**٢.١ Encryption systems:** **٢.١ Monoaphabetic cipher (substitution)**		
١١	٢٠١٤/١٢/١٥	**٢.٢ Transposition (permutation)**		

		٢.٣ Stream and block cipher	٢٠١٤/١٢/٢٢	١٢
		٢.٤ Characteristics of Good ciphers	٢٠١٤/١٢/٢٩	١٣
		Holiday	٢٠١٥/٠١/٠٥	١٤
		--	--	١٥
		--	--	١٦
عطلة نصف السنة				
		٢.٥ Cryptanalysis	١٧/٠٢/٢٠١٥	١٧
		Secure encryption systems:	٢٤/٠٢/٢٠١٥	١٨
		٣.١ Define & Type of such system	٠٣/٠٣/٢٠١٥	١٩
		٣.١ Prosperities of Arithmetic	١٠/٠٣/٢٠١٥	٢٠
		٣.٢ Public key systems Intoduction	١٧/٠٣/٢٠١٥	٢١
		٣.٢ Public key systems Algorithms	٢٤/٠٣/٢٠١٥	٢٢
		٣.٣ Rivest-Shamir-Adelman (RSA) Encryption review.	٣١/٠٣/٢٠١٥	٢٣
		٣.٣ Rivest-Shamir-Adelman (RSA) Encryption Algorithm	٠٧/٠٤/٢٠١٥	٢٤
		٣.٤ Single key (Conventional) Systems	١٤/٠٤/٢٠١٥	٢٥
		٣.٤ Single key (Conventional) Systems ٢	٢١/٠٤/٢٠١٥	٢٦
		٣.٥ The Data Encryption Standard(DES)	٢٨/٠٤/٢٠١٥	٢٧
		٣.٦ Security involving programs	٠٥/٠٥/٢٠١٥	٢٨
		٣.٧ Protection Services for users of operating systems	١٢/٠٥/٢٠١٥	٢٩
		٣.٨.Data Base security	١٩/٠٥/٢٠١٥	٣٠
		٣.٩ Computer network security	٢٦/٠٥/٢٠١٥	٣١
		٣.١٠ Communication Security	٠٢/٠٦/٢٠١٥	٣٢

توقيع الاستاذ :

توقيع العميد :

Republic of Iraq

The Ministry of Higher Education

& Scientific Research

University: Diyala
College: Engineering
Department: Computer and S/W
Stage: ٤th class
Lecturer name: Huda M. Saleh
Academic Status:Asst.Lecturer
Qualification: MSc.
Place of work: Computer Dept.

Flow up the implementation of course syllabus

Course Instructor	Huda Mohammed Saleh				
E_mail	Hoopoe٢٠٠٨٠@hotmail.com				
Title	Cryptography & Data security				
Course Coordinator					
Course Objective	Introduce students to the basic principles of Cryptography & Data security. Introduce students to the different type of cryptography Algorthims (Classic & Modern Method)				
Course Description	Study the different of Cryptography type, as well as the study of different type of cryptography Algorthims (Classic & Modern Method). Data Security for storded data & (Data Base) & Secure Data Transmited through Networks.				
Textbook	References: ١. Applied Cryptography by Schneier, B. ٢٠٠٩ ٢. Security in Computing, Textbook by Pfleege ٢٠١٢. Data Base Security By Pfleege. Network Security by Pfleege.				
Course Assessment	First Term	Mid-Year	٢nd Term	Project	Final Exam
	١٠ %	٢٠ %	١٠ %	١٠ %	٥٠ %
General Notes					

Republic of Iraq

The Ministry of Higher Education

& Scientific Research

University: Diyala
College: Engineering
Department: Computer and S/W
Stage: Fourth Class
Lecturer name: Huda M. Saleh
Academic Status: Asst. Lecturer
Qualification: MSc.
Place of work: Computer Dept.

Course Weekly Outline

week	Date	Topics Covered	Lab. Experiment Assignments	Notes
١	٢٠١٤/١٠/٠٦	**Introduction to encryption and Data security:**		
٢	٢٠١٤/١٠/١٣	**١.٢ Characteristics of Computer intrusion**		
٣	٢٠١٤/١٠/٢٠	**١.٢ Kinds of Security Breaches**		
٤	٢٠١٤/١٠/٢٧	**١.٣ The points of security Vulnerability - Attacks on Hardware- Attacks on Software - Attacks on Data**		
٥	٢٠١٤/١١/٠٣	**١.٤ The people involved**		
٦	٢٠١٤/١١/١٠	**١.٥ Methods of defense**		
٧	٢٠١٤/١١/١٧	**Classification of cipher system** **١.٦ Secret key systems.** **١.٦.١ Conventional System (classical)** **١.٦.٢ Modern Systems**		
٨	٢٠١٤/١١/٢٤	**١.٧ Public key Systems**		
٩	٢٠١٤/١٢/٠١	**١.٧.١ RSA** **١.٧.٢ Knapsack.**		

١٠	٢٠١٤/١٢/٠٨	٢.١ Encryption systems: ٢.١ Monoaphabetic cipher (substitution)		
١١	٢٠١٤/١٢/١٥	٢.٢ Transposition (permutation)		
١٢	٢٠١٤/١٢/٢٢	٢.٣ Stream and block cipher		
١٣	٢٠١٤/١٢/٢٩	٢.٤ Characteristics of Good ciphers		
١٤	٢٠١٥/٠١/٠٥	Holiday		
١٥	--	--		
١٦	--	--		
Half-Year Break				
١٧	١٧/٠٢/٢٠١٥	٢.٥ Cryptanalysis		
١٨	٢٤/٠٢/٢٠١٥	Secure encryption systems:		
١٩	٠٣/٠٣/٢٠١٥	٣.١ Define & Type of such system		
٢٠	١٠/٠٣/٢٠١٥	٣.١ Prosperities of Arithmetic		
٢١	١٧/٠٣/٢٠١٥	٣.٢ Public key systems Intoduction		
٢٢	٢٤/٠٣/٢٠١٥	٣.٢ Public key systems Algorithms		
٢٣	٣١/٠٣/٢٠١٥	٣.٣ Rivest-Shamir-Adelman (RSA) Encryption review.		
٢٤	٠٧/٠٤/٢٠١٥	٣.٣ Rivest-Shamir-Adelman (RSA) Encryption Algorithm		
٢٥	١٤/٠٤/٢٠١٥	٣.٤ Single key (Conventional) Systems		
٢٦	٢١/٠٤/٢٠١٥	٣.٤ Single key (Conventional) Systems ٢		
٢٧	٢٨/٠٤/٢٠١٥	٣.٥ The Data Encryption Standard(DES)		

٢٨	٠٥/٠٥/٢٠١٥	**٣.٦ Security involving programs**		
٢٩	١٢/٠٥/٢٠١٥	**٣.٧ Protection Services for users of operating systems**		
٣٠	١٩/٠٥/٢٠١٥	**٣.٨.Data Base security**		
٣١	٢٦/٠٥/٢٠١٥	**٣.٩ Computer network security**		
٣٢	٠٢/٠٦/٢٠١٥	**٣.١٠ Communication Security**		

Instructor Signature: **Dean Signature:**