جمهورية العراق
وزارة التعليم العالي والبحث العلمي
قسم جهاز الاشراف والتقويم والمتابعة

أسم الجامعة: الجامعة التكنولوجية
أسم الكلية: علوم الحاسبات
أسم القسم: أمنيه بيانات
أسم المحاضر: م. ايناس طارق خضير
اللقب لعلمي: مدرس
المؤهل العملي: ماجستير
مكان العمل: الجامعة التكنولوجية/قسم علوم الحاسبات

جدول الدروس الاسبوعي 2023-2024

الاسم	م. ايناس طارق خضير
البريد الالكتروني	Enas.T.Khudir@uotechnology.edu.iq
اسم المادة	خوارزميات المفتاح المعلن اللامتناظر المرحلة الثالثة- كورس الاول
مقرر الفصل	
اهداف المادة	تهدف هذه المادة إلى تعليم الطالب على كيفية استخدام خوارزميات التشفير برمجتها بشكل ملائم لتشفير النصوص الهامه والسرية وتعليمهم على اساس رياضي وتطبيقهابشكل عملي لخوارزميات التشفير المفتاح المعلن
التفاصيل الاساسية للمادة	**Chapter One: Basic Concepts of The Cryptography** **Algorithm of block cipher** **Public key algorithm**
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.

تقديرات الفصل	الفصل الدارسي	المختبر	الامتحانات اليومية	المشروع	الامتحان النهائي
	%20	%20	%10	-	%60
معلومات اضافية	Visual basic.net 2013				

جمهورية العراق
وزارة التعليم العالي والبحث
العلمي
قسم جهاز الاشراف والتقويم والمتابعة

أسم الجامعة: الجامعة التكنولوجية
أسم الكلية: علوم الحاسبات
أسم القسم: أمنيه بيانات
أسم المحاضر: م. ايناس طارق خضير
اللقب لعلمي: مدرس
المؤهل العلمي: ماجستير
مكان العمل: الجامعة التكنولوجية/قسم علوم الحاسبات

جدول الدروس الاسبوعي

الاسبوع	التاريخ	المادة النظرية	المادة العلمية	الملاحظات
1	1/10/2023	Introduction of Cryptography Complexity Theory	Designing simple vb.net program. (GCD)	
2	8/10/2023	Types of cryptography .	Designing simple vb.net program. (LCM)	
3	15/10/2023	attackers	Euler's program	
4	29/10/2023	Principles of Public-Key Cryptosystems Diffie and Hellman Public key VS private key	Fast program	
5	5/11/2023	Asymmetric Public-key Cryptosystems	The model program of all function	
6	12/11/2023	RSA public key algorithm	RSA algorithm program	
7	19/11/2023	Signature of RSA	Signature of RSA program	
	26/11/2023			
8		Security of RSA	Complete program RSA	

	ElGamal algorithm program	**ElGamal algorithm**	3/**12**/**20**23	**9**
	Signature of ElGamal algorithm program	**Signature of ElGamal algorithm**	10/**12**/**20**23	**10**
	Security of the ElGamal algorithm program	**Security of ElGamal algorithm**	17/1**2**/**20**23	**11**
	Knapsack of algorithm	**Knapsack of algorithm**	24/**12**/**20**23	**12**
	Complete program Knapsack	**example of algorithm**	31/**12**/**20**23	**13**
	McEliece of public key program	**McEliece of public key**	7/**1**/**20**23	**14**
Review and examination				**15**

توقيع الاستاذ: **توقيع العميد:**

م. ايناس طارق خضير

Republic of Iraq
The Ministry of Higher Education
& Scientific Research

Lecturer name: Enas Tariq Khudair

Academic Status: Lecturer
Qualification: MSc
Place of work: University of Technology
College: computer science
Stage: Third Class

Course Weekly Outline

Course Instructor	Enas Tariq Khudair
Email	Enas.T.Kudir@uotechnology.edu.iq
Title	Public key and stream cipher
Course Coordinator	
Course Objective	The aim of this subject is to teach the students how to program the algorithm of public key with a basic principle to encryption the cipher text.
Course Description	Chapter One: Basic Concepts of Cryptography. Algorithm of block cipher. Public key algorithm.
Textbook	H. Boker & F. Piper, "Cipher System, The Protection of Communications ", Northwood Books, Landon, 1982.
References	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.

Course Assessment	Term Tests	Laboratory	Quizzes	Project	Final Exam
	(20%)	(20%)	(10%)	----	(50%)

General Notes	Programming in VB.net

Republic of Iraq
The Ministry of Higher Education
& Scientific Research

Lecturer name: Enas Tariq Khudair

Academic Status: Lecturer
Qualification: MSc
Place of work: University of Technology
College: computer science
Stage: Third Class

Course weekly Outline

Note	Piratical	Theoretical	Data	Week
	Designing simple vb.net program. (GCD)	Introduction of Cryptography Complexity Theory	1/10/2023	1
	Designing simple vb.net program. (LCM)	Types of cryptography .	8/10/2023	2
	Euler's program	attackers	15/10/2023	3
	Fast program	Principles of Public-Key Cryptosystems Diffie and Hellman Public key VS private key	29/10/2023	4
	The model program of all function	Asymmetric Public-key Cryptosystems	5/11/2023	5
	RSA algorithm program	RSA public key algorithm	12/11/2023	6
	Signature of RSA program	Signature of RSA	19/11/2023	7
	Complete program RSA	Security of RSA	26/11/2023	8
	ElGamal algorithm program	ElGamal algorithm		9

	Signature of ElGamal algorithm program	**Signature of ElGamal algorithm**	3/**12**/**20**23	**10**
	Security of ElGamal algorithm program	**Security of ElGamal algorithm**	10/**12**/**20**23	**11**
	Knapsack of algorithm	**Knapsack of algorithm**	17/1**2**/**20**23	**12**
	Complete program Knapsack	**example of algorithm**	24/**12**/**20**23	**13**
	McEliece of public key program	**McEliece of public key**	31/**12**/**20**23	**14**
Review and examination				**15**

Instructor Signature: **Dean Signature:**