Republic of Yemen
Ministry of Higher Education and Scientific Research
Sana'a University
Faculty of Science

الجمهوريـــة اليمنـــية
وزارة التعليـم العـالـي والبحث العلمي
جامعة صنعاء
كلية العلوم

مواصفات مقرر: التشفير (مقرر اختياري ٢)

i. معلومات عامة عن المقرر General information about the course:

١.	اسم المقرر Course Title	التشفير (مقرر اختياري ٢)				
٢.	رمز المقرر ورقمه Course Code and Number					
	الساعات المعتمدة للمقرر Credit Hours	الساعات المعتمدة Credit Hours			الإجمالي Total	
		محاضرات Lecture	عملي Practical	سيمنار/تمارين Seminar/Tutorial		
		2	1	---	3	
	المستوى والفصل الدراسي Study Level and Semester	المستوى الثالث ـ الفصل الثاني				
	المتطلبات السابقة المقرر (إن وجدت) Pre-requisites (if any)	رياضيات – جبر خطي				
	المتطلبات المصاحبة (إن وجدت) Co-requisites (if any)	لا يوجد				
	البرنامج الذي يدرس له المقرر Program (s) in which the course is offered	بكالوريوس : تخصص رياضيات حاسوب				
	لغة تدريس المقرر Language of teaching the course	اللغة العربية / انجليزي				
	نظام الدراسة Study System	فصلي				
	معد(و) مواصفات المقرر Prepared By	د. نجران ناصر حمود				
	تاريخ اعتماد مواصفات المقرر Date of Approval	٢٠٢٠-٢٠٢١م				

ملاحظة: الساعة المعتمدة للعملي والتمارين تساوى ساعتين فعليتين خلال التدريس.

ii. وصف المقرر Course Description:

يهدف هذا المقرر إلى تعريف الطالب النظريات الأساسية لخوارزميات التشفير الحديثة التي تعتمد على الأدوات الرياضية اللازمة لبناء وتحليل طرق الحماية والامان لأنظمة التشفير المتنوعة. بحيث يتضمن هذا المقرر الموضوعات الرئيسية للتشفير المستخدمة للمفاهيم الرياضية الحديثة مثل مقدمة في التشفير الرياضي، اهمية التشفير، انواع وطرق الهجوم والتشفير، خوارزميات تشفير المفتاح المتماثل والمفتاح العام، بروتوكولات التشفير، خوارزميات الاحتمالية، ووظائف التشفير باتجاة واحد، التشفير الأمن المبرهن و التشفير الأمن الغير مشروط وخوارزميات الأمن المبرهن للتوقيع الرقمي. بحيث يكون الطالب قادرًا على تحديد مجال المعرفة التفصيلية لخوارزميات التشفير واتخاذ القرار المناسب عند بناء وتحليل آليات الامن على مستوى الانظمة التطبيقية الإلكترونية.

نائب العميد لشئون الجودة	عميد الكلية	عميدة مركز التطوير وضمان الجودة	رئيس الجامعة
أ. د. عبده الكلي	د. إبراهيم لقمان	أ.م. د. هدي على العماد	أ. د. القاسم محمد عباس

iii. مخرجات تعلم المقرر Course Intended Learning Outcomes (CILOs):

بعد الانتهاء من دراسة المقرر سوف يكون الطالب قادرا على أن:

a1 – يعرف المصطلحات والمفاهيم الأساسية لخوارزمية التشفير الرياضية التي تلائم احتياجات سوف العمل.

a2 - يحدد الخوارزميات المختلفة لانواع التشفير المتماثلة والعامة لحل المشاكل.

b1- يحلل بعض خوارزميات التشـــفير الاحتمالية والمبرهنة واحادية الاتجاة لتامين الانظمة وايجاد حلول مناسبة.

b2 - يقارن بين التشفير الأمن الغير مشروط و المبرهن و المبرهن للتوقيع الرقمي.

c1 – يسنخدم خوارزميات التشفيرالرئيسية لتطوير التقينات الامنية المستخدمة حديثاَ.

c2 - ينفذ بروتوكولات التشفير الامنة لبعض التطبيقات الحاسوبية.

c3. يطبق النظريات والمعادلات الرياضية لخوارزميات الأمن المبرهن للتوقيع الرقمي.

d1- يعمل بشكل فعال ضمن الفريق الواحد من خلال استخدام التشفير المناسبة لتامين الانظمة الالكتورنية والتطبيقات.

d2 - يكتسب المهارات المتعددة مثل كتابة التقارير الفنية والبحث العلمي ويحترم المعايير الأخلاقية.

iv. مواءمة مخرجات تعلم المقرر مع مخرجات التعلم للبرنامج:

Alignment of CILOs (Course Intended Learning Outcomes) to PILOs (Program Intended Learning Outcomes)

مخرجات التعلم المقصودة من المقرر (Course Intended Learning Outcomes)		مخرجات التعلم المقصودة من البرنامج (Program Intended Learning Outcomes)
- a1	يعرف المصطلحات والمفاهيم الأساسية لخوارزمية التشفير الرياضية التي تلائم احتياجات سوف العمل.	A1. يعبر عن معرفة عميقة بمبادئ ونظريات الرياضيات والمنطق والخوارزميات.
– a2	يحدد الخوارزميات المختلفة لانواع التشفير المتماثلة والعامة لحل المشاكل.	A2. يصف مفاهيم البرمجة ذات الصلة بمختلف فروع الرياضيات.
–b1	يحلل بعض خوارزميات التشفير الاحتمالية والمبرهنة واحادية الاتجاة لتامين الانظمة وايجاد حلول مناسبة.	B1. يحلل المشاكل الرياضية الأساسية المرتبطة بمختلف التطبيقات، وتصميم الخوارزميات لحلها.
- b2	يقارن بين التشفير الأمن الغير مشروط والمبرهن و المبرهن للتوقيع الرقمي.	B1. يحلل المشاكل الرياضية الأساسية المرتبطة بمختلف التطبيقات، وتصميم الخوارزميات لحلها.
-c1	يسنخدم خوارزميات التشفيرالرئيسية لتطوير التقينات الامنية المستخدمة حديثاَ.	C3. يستخدم التقنيات والمهارات والأدوات الحديثة اللازمة لجوانب السلامة.

-c2	ينفذ بروتوكولات التشـــفير الامنة لبعض التطبيقات الحاسوبية.	C2. يطبق الخوارزميات لحل المشاكل الرياضية.
-c3	يطبق النظريات والمعادلات الرياضية لخوارزميات الأمن المبرهن للتوقيع الرقمي.	C1. يطبق المعرفة في الحوسبة والأدوات والتقنيات لتحسين إنتاجية العمل.
-d1	يعمل بشكل فعال ضمن الفريق الواحد من خلال استخدام التشفير المناسبة لتامين الانظمة الالكترونية والتطبيقات.	D1. يعمل ويتعاون ويتواصل بصورة جماعية وبشكل فعال.
-d2	يكتسب المهارات المتعددة مثل كتابة التقارير الفنية والبحث العلمي ويحترم المعايير الأخلاقية.	D2. يكتب ويعرض التقاريرالتقنية بشكل فعال.

مواءمة مخرجات التعلم باستراتيجيات التعليم والتعلم والتقويم

Alignment of CILOs to Teaching and Assessment Strategies

أولا: مواءمة مخرجات تعلم المقرر (المعارف والفهم) باستراتيجية التعليم والتعلم والتقويم:

First: Alignment of Knowledge and Understanding CILOs

مخرجات المقرر/ المعرفة والفهم Knowledge and Understanding CILOs		استراتيجية التدريس Teaching Strategies	استراتيجية التقويم Assessment Strategies
-a1	يعرف المصـــطلحات والمفاهيم الأســـاســـية لخوارزميـة التشـــفير الريـاضـــيـة التي تلائم احتياجات سوف العمل.	المحاضرة التفاعلية + الحوار والمناقشة + التعلم الذاتي + العروض التقديمية.	الحضور+ الواجبات المنزلية + المشاركات الصفية + الامتحان النصفي+ إلإمتحان العملي+ الامتحان النهائي
-a2	يحدد الخوارزميات المختلفة لانواع التشفير المتماثلة والعامة لحل المشاكل.		

ثانيا: مواءمة مخرجات تعلم المقرر (المهارات الذهنية) باستراتيجية التدريس والتقويم:

Second: Alignment of Intellectual Skills CILOs

مخرجات المقرر/ المهارات الذهنية Intellectual Skills CILOs	استراتيجية التدريس Teaching Strategies	استراتيجية التقويم Assessment Strategies

نائب العميد لشئون الجودة	عميد الكلية	عميدة مركز التطوير وضمان الجودة	رئيس الجامعة
أ. د. عبده الكلي	د. إبراهيم لقمان	أ.م. د. هدي على العماد	أ. د. القاسم محمد عباس

-b1	يحلل بعض خوارزميات التشـــفير الاحتمالية والمبرهنـة واحـادية الاتجـاة لتـامين الانظمـة وايجاد حلول مناسبة.	المحاضرة التفاعلية + العصف الذهني + حل المشكلات + الحوار والمناقشة + التحليل والاستنتاج + المقارنة والمفاضلة	الحضور+ الواجبات المنزلية + المشاركات الصفية + التطبيقات العملية + الامتحان النصفي+ الإمتحان العملي+ الامتحان النهائي.
-b2	يقـارن بين التشـــفير الأمن الغير مشـــروط والمبرهن و المبرهن للتوقيع الرقمي.		

ثالثا: مواءمة مخرجات تعلم المقرر (المهارات المهنية والعملية) باستراتيجية التدريس والتقويم:

Third: Alignment of Professional and Practical Skills CILOs

مخرجات المقرر/ المهارات المهنية والعملية Professional and Practical Skills CILOs		استراتيجية التدريس Teaching Strategies	استراتيجية التقويم Assessment Strategies
-c1	يستخدم خوارزميات التشفيرالرئيسية لتطوير التقنيات الامنية المستخدمة حديثاً.	المحاكاة والعروض العملية +التدريب العملي + حل المشكلات + دراسة حالة + التعلم التعاوني + التعلم الذاتي	الحضور+ التكليفات المختلفة (الخطط + البرامج + التقارير + المشاريع) + مراقبة التطبيقات العملية + الامتحان النصفي + الإمتحان العملي+ الامتحان النهائي .
-c2	ينفذ بروتوكولات التشفير الامنة لبعض التطبيقات الحاسوبية.		
-c3	يطبق النظريات والمعادلات الرياضية لخوارزميات الأمن المبرهن للتوقيع الرقمي.		

رابعا: مواءمة مخرجات تعلم المقرر (المهارات العامة) باستراتيجية التدريس والتقويم:

Fourth: Alignment of Transferable (General) Skills CILOs

مخرجات المقرر Transferable (General) Skills CILOs	استراتيجية التدريس Teaching Strategies	استراتيجية التقويم Assessment Strategies

نائب العميد لشئون الجودة	عميد الكلية	عميدة مركز التطوير وضمان الجودة	رئيس الجامعة
أ. د. عبده الكلي	د. إبراهيم لقمان	أ.م. د. هدي على العماد	أ. د. القاسم محمد عباس

-d1	يعمل بشكل فعال ضمن الفريق الواحد من خلال استخدام التشفير المناسبة لتامين الانظمة الالكترونية والتطبيقات.	المشروعات والمهام والتكاليف + الحوار والمناقشة + التعلم التعاوني + التعلم الذاتي + تبادل الخبرات بين الزملاء	تقييم الحوار والمناقشة + التكليفات المختلفة (الخطط + البرامج + التقارير + المشاريع) + مراقبة التطبيقات العملية + الامتحان النصفي + إلإمتحان العملي+ الامتحان النهائي .
-d2	يكتسب المهارات المتعددة مثل كتابة التقارير الفنية والبحث العلمي ويحترم المعايير الأخلاقية.		

v. موضوعات محتوى المقرر Course Content

أولا: موضوعات الجانب النظري Theoretical Aspect

الرقم Order	الموضوعات الرئيسة/ الوحدات Topic List / Units	الموضوعات التفصيلية Sub Topics List	عدد الأسابيع Number of Weeks	الساعات الفعلية Contact Hours	رموز مخرجات التعلم للمقرر (CILOs)
1	المقدمة Introduction	▪ Cryptography Concepts, Cryptography History, Encryption and Secrecy, the Objectives of Cryptography, Attacks, services, Cryptographic Protocols, Provable Security. Algebra and Number and Information Theory	1	2	a1,
2	تشفير المفتاح المتماثل Symmetric-Key Cryptography	▪ **Symmetric - Key Encryption:** Stream Ciphers, Block Ciphers, DES, ٣DES, AES. ▪ **Modes of Operation Cryptographic Hash Functions:** Security Requirements for Hash Functions, Construction of Hash Functions, Data Integrity and Message Authentication, Hash Functions as Random Functions.	2	4	a1, a2, c1,

a1, a2, c1,	4	2	▪ The Concept of Public - Key Cryptography. ▪ **Modular Arithmetic**: RSA, the Discrete Logarithm, Homomorphic Encryption Algorithms, Elliptic Curve Cryptography.	تشفير المفتاح العام **Public-Key Cryptography**	**3**
a1, c1,c2,c3	2	1	▪ **Cryptographic Protocols:** Key Exchange and Entity Authentication, Identification Schemes, Commitment Schemes, Secret Sharing, Verifiable Electronic Elections, Mix Nets and Shuffles, Receipt-Free and Coercion-Resistant Elections, Digital Cash.	بروتوكولات التشفير **Cryptographic Protocols**	**4**
a2, b1, c1, c2, d1	٤	٢	▪ **Provably Secure Encryption :** Classical Information-Theoretic Security, Perfect Secrecy and Probabilistic Attacks, Public-Key One-Time Pads , Passive Eavesdroppers , Chosen-Ciphertext Attacks , A Security Proof in the Random Oracle Model , Security Under Standard Assumptions.	االخوارزميات الاحتمالية **Probabilistic Algorithms**	**5**
a2, b1, c1, c2, d1	2	1	▪ **Probabilistic Algorithms:** Coin-Tossing Algorithms, Monte Carlo and Las Vegas Algorithms.	االخوارزميات الاحتمالية **Probabilistic Algorithms**	**6**
a2, b1, c1, d1	2	1	▪ The Basic Assumptions and concepts, Bit Security algorithms, Pseudo randomness.	وظائف أحادية الاتجاه **One-Way Functions**	**7**
a2, b1,b2, c1,d1	2	1	▪ Classical Information - Theoretic Security, Perfect Secrecy and Probabilistic Attacks , Public-Key One-Time	التشفير الأمن المبرهن **Provably Secure Encryption**	**8**

			Pads, Passive Eavesdroppers, Chosen-Ciphertext Attacks		
a2, b1,b2, c1,d1	2	1	▪ The Bounded Storage Model, The Noisy Channel Model, Unconditionally Secure Message Authentication, Collision Entropy and Privacy Amplification, Quantum Key Distribution.	التشفير الأمن الغير مشروط **Unconditional Security of Cryptosystems**	**9**
a2, b1,b2, c1,c3, d1	4	2	▪ Provably Secure Digital Signatures Attacks and Levels of Security, Claw-Free Pairs and Collision-Resistant Hash Functions, Authentication-Tree-Based Signatures, A State-Free Signature Scheme, Algebra and Number Theory	الأمن المبرهن للتوقيع الرقمي **Provably Secure Digital Signatures**	**10**
	28	**14**	**اجمالي عدد الأسابيع والساعات الفعلية** **Number of Weeks /and Contact Hours Per Semester**		

ثانيا: موضوعات الجانب العملي Practical Aspect

رموز مخرجات التعلم Course ILOs	الساعات الفعلية Contact Hours	عدد الأسابيع Number of Weeks	التجارب العملية/ تدريبات Practical / Tutorials topics	الرقم Order
b2, c1, c2, c3,d1	**4**	**2**	▪ Implementation of Symmetric-Key Encryption and decryption: Stream Ciphers, Block Ciphers.	١
a2, b1, d1,d2	**4**	**2**	▪ Symmetric Ciphers (DES, AES, RC4)	٢
a2, b1, d1,d2	**2**	**1**	▪ Public-key Ciphers (RSA, Diffie-Hellman Key Exchange)	٣
c2, d1	**2**	**1**	▪ Cryptographic Protocols.	٤
b1, c1, c3,d1	**2**	**1**	▪ Probabilistic Algorithms	**5**
b1, c1, c3,d1	**2**	**1**	▪ Implement of One-Way Functions	**6**
b1, c1, c3,d1	**2**	**1**	▪ Implement Provably Secure Encryption	**7**

8	▪ Implement Unconditional Security of Cryptosystems	1	2	b2, c1, c3,d1
9	▪ Implement Provably Secure Digital Signatures	2	4	b2, c1,c3, d1, d2
	اجمالي الأسابيع والساعات الفعلية Number of Weeks /and Contact Hours Per Semester	12	24	===

استراتيجيات التدريس Teaching Strategies:

- المحاضرة التفاعلية Lectures
- الحوار والمناقشة discussion
- العصف الذهني Brainstorming
- حل المشكلات Problem solving
- المحاكاة والعروض العملية Practical presentations& Simulation Method
- التطبيق العملي (Lab works) Practical in computer Lab
- المشروعات والمهام والتكاليف projects
- التعلم الذاتي Self-learning
- التعلم التعاوني Cooperative Learning
- تبادل الخبرات بين الزملاء

vi. الأنشطة والتكليفات Tasks and Assignments:

م No	الأنشطة / التكليف Assignments/ Tasks	نوع التكليف (فردي/ تعاوني)	الدرجة المستحقة Mark	أسبوع التنفيذ Week Due	مخرجات التعلم CILOs (symbols)
١	الواجبات المنزلية و المشاركات الصفية.	فردي	10	أسبوعياً	a1, a2, b1, b2,
٢	التكليفات المختلفة (التطبقات العملية + تقييم الحوار والمناقشة + التحليل + البرامج + التقارير + المشاريع+مراقبة التطبيقات العملية)	فردية أو جماعية	10	الثاني عشر والثالث عشر	c1, c2,c3, d1,d2
	إجمالي الدرجة Total Score		20	==	===

vii. تقييم التعلم Learning Assessment:

الرقم No.	أنشطة التقييم Assessment Tasks	أسبوع التقييم Week due	الدرجة Mark	نسبة الدرجة إلى الدرجة النهائية Proportion of Final Assessment	مخرجات التعلم CILOs (symbols)
١	الواجبات والمشاركات	أسبوعياً	10	% 6.67	a1, a2, b1, b2,
٢	التكليفات كوز(١) Quiz	السادس	5	% 3.33	b1, b2, c3, d1,d2

نائب العميد لشئون الجودة
أ. د. عبده الكلي

عميد الكلية
د. إبراهيم لقمان

عميدة مركز التطوير وضمان الجودة
أ.م. د. هدي على العماد

رئيس الجامعة
أ. د. القاسم محمد عباس

٣	اختبار نصف الفصل (نظري) Midterm Exam	الثامن	20	% 13.33	a1, a2, b1, b2, d2
٤	التكليفات كوز (٢) Quiz	العاشر	5	% 3.33	b1, b2, c3, d1,d2
٥	اختبار نهاية الفصل (عملي) Final Exam (practical)	الرابع عشر	٥٠	% 33.34	c1, c2,c3, d2,
٦	اختبار نهاية الفصل (نظري) Final Exam (theoretical)	السادس عشر	60	% 40	a1, a2, b1, b2, d2
	الإجمالي Total		١٥٠	%100	===

مصادر التعلم Learning Resources: كتابة المراجع للمقرر (اسم المؤلف، سنة النشر، اسم الكتاب، دار النشر، بلد النشر).

١. المراجع الرئيسة Required Textbook(s): (لا تزيد عن مرجعين)

1. Hans Delfs and Helmut Knebl, et al, "Introduction to Cryptography Principles and Applications," Third Edition ©Springer-Verlag Berlin Heidelberg 2015.

٢. المراجع المساندة Essential References:

1. William Stallings, 201٣, "Cryptography and Network Security: Principles and Practice", ٦th Edition, Prentice Hal.
2. Jeffrey Hoffstein and Jill Pipher, et al, "An Introduction to Mathematical Cryptography," Second Edition© Springer Science + Business Media New York, 2014

٣. المصادر الإلكترونية ومواقع الإنترنت... Electronic Materials and Web Sites *etc.*

1. https://docs.microsoft.com/en-us/windows/win32/seccrypto/about-cryptography
2. https://www.tutorialspoint.com/cryptography/index.htm
3. https://sites.google.com/site/ddmwsst/cryptography-concepts

viii. الضوابط والسياسات المتبعة في المقرر Course Policies

بعد الرجوع إلى لوائح الجامعة يتم كتابة السياسة العامة للمقرر فيما يتعلق بالآتي:

١	سياسة حضور الفعاليات التعليمية Class Attendance: - يلتزم الطالب بحضور ٧٥% من المحاضرات ويحرم في حال عدم الوفاء بذلك. - يقدم أستاذ المقرر تقريرا بحضور وغياب الطلاب للقسم ويحرم الطالب من دخول الامتحان في حال تجاوز الغياب ٢٥% ويتم اقرار الحرمان من مجلس القسم.
٢	الحضور المتأخر Tardy: - يسمح للطالب حضور المحاضرة إذا تأخر لمدة ربع ساعة لثلاث مرات في الفصل الدراسي، وإذا تأخر زيادة عن ثلاث مرات يحذر شفويا من أستاذ المقرر، وعند عدم الالتزام يمنع من دخول المحاضرة.
٣	ضوابط الامتحان Exam Attendance/Punctuality:

	- لا يسمح للطالب دخول الامتحان النهائي إذا تأخر مقدار (٢٠) دقيقة من بدء الامتحان - إذا تغيب الطالب عن الامتحان النهائي تطبق اللوائح الخاصة بنظام الامتحان في الكلية.
٤	**التعيينات والمشاريع Assignments & Projects:** - يحدد أســتاذ المقرر نوع التعيينات في بداية الفصــل ويحدد مواعيد تســليمها وضــوابط تنفيذ التكليفات وتسليمها. - إذا تأخر الطالب في تسليم التكليفات عن الموعد المحدد يحرم من درجة التكليف الذي تأخر في تسليمه.
٥	**الغش Cheating:** - في حال ثبوت قيام الطالب بالغش في الامتحان النصفي أو النهائي تطبق عليه لائحة شؤون الطلاب. - في حال ثبوت قيام الطالب بالغش او النقل في التكليفات والمشاريع يحرم من الدرجة المخصصة للتكليف.
6	**الانتحال Plagiarism:** - في حالة وجود شخص ينتحل شخصية طالب لأداء الامتحان نيابة عنه تطبق اللائحة الخاصة بذلك
7	**سياسات أخرى Other policies:** - أي سياسات أخرى مثل استخدام الموبايل أو مواعيد تسليم التكليفات ..... الخ

العام الجامعي: ٢٠٢٠-٢٠٢١م

خطة مقرر: التشفير (مقرر اختياري ٢)

i. معلومات عن أستاذ المقرر Information about Faculty Member Responsible for the Course

الاسم Name	د. نجران ناصر حمود	الساعات المكتبية (أسبوعيا) Office Hours					
المكان ورقم الهاتف Location &Telephone No.	صنعاء - ٧٧٥٣٧٧٠٨٠	السبت SAT	الأحد SUN	الاثنين MON	الثلاثاء TUE	الأربعاء WED	الخميس THU
البريد الإلكتروني E-mail	Meetnajran@gmail.com						

ii. معلومات عامة عن المقرر General information about the course:

اسم المقرر Course Title	التشفير (مقرر اختياري ٢)			
رمز المقرر ورقمه Course Code and Number				
الساعات المعتمدة للمقرر Credit Hours	الساعات المعتمدة Credit Hours			المجموع Total
	محاضرات Lecture	عملي Practical	سيمنار/تمارين Seminar/Tutorial	
	2	1	---	3

نائب العميد لشئون الجودة أ. د. عبده الكلي	عميد الكلية د. إبراهيم لقمان	عميدة مركز التطوير وضمان الجودة أ.م. د. هدي على العماد	رئيس الجامعة أ. د. القاسم محمد عباس

	المستوى والفصل الدراسي Study Level and Semester	المستوى الثالث - الفصل الثاني
	المتطلبات السابقة للمقرر (إن وجدت) Pre-requisites	رياضيات – جبر خطي
	المتطلبات المصاحبة (إن وجدت)– Co requisite	لا يوجد
	البرنامج/ البرامج التي يتم فيها تدريس المقرر Program (s) in which the course is offered	بكالوريوس : تخصص رياضيات حاسوب
	لغة تدريس المقرر Language of teaching the course	اللغة العربية / انجليزي
	مكان تدريس المقرر Location of teaching the course	قسم الرياضيات بكلية العلوم

ملاحظة: الساعة المعتمدة للعملي وللتمارين تساوى ساعتين فعليتين خلال التدريس.

iii. وصف المقرر Course Description:

يهدف هذا المقرر إلى تعريف الطالب النظريات الأساسية لخوارزميات التشفير الحديثة التي تعتمد على الأدوات الرياضية اللازمة لبناء وتحليل طرق الحماية والامان لأنظمة التشفير المتنوعة. بحيث يتضمن هذا المقرر الموضوعات الرئيسية للتشفير المستخدمة للمفاهيم الرياضية الحديثة مثل مقدمة في التشفير الرياضي، اهمية التشفير، انواع وطرق الهجوم والتشفير، خوارزميات تشفير المفتاح المتماثل والمفتاح العام، بروتوكولات التشفير، خوارزميات الاحتمالية، ووظائف التشفير باتجاة واحد، التشفير الأمن المبرهن و التشفير الأمن الغير مشروط وخوارزميات الأمن المبرهن للتوقيع الرقمي. بحيث يكون الطالب قادرًا على تحديد مجال المعرفة التفصيلية لخوارزميات التشفير واتخاذ القرار المناسب عند بناء وتحليل آليات الامن على مستوى الانظمة التطبيقية الإلكترونية.

iv. مخرجات تعلم المقرر Course Intended Learning Outcomes (CILOs):

بعد الانتهاء من دراسة المقرر سوف يكون الطالب قادرا على أن:

a1 – يعرف المصطلحات والمفاهيم الأساسية لخوارزمية التشفير الرياضية التي تلائم احتياجات سوف العمل.

a2 - يحدد الخوارزميات المختلفة لانواع التشفير المتماثلة والعامة لحل المشاكل.

b1- يحلل بعض خوارزميات التشـــفير الاحتمالية والمبرهنة واحادية الاتجاة لتامين الانظمة وايجاد حلول مناسبة.

b2 - يقارن بين التشفير الأمن الغير مشروط و المبرهن و المبرهن للتوقيع الرقمي.

c1 – يستخدم خوارزميات التشفيرالرئيسية لتطوير التقينات الامنية المستخدمة حديثاَ.

c2 - ينفذ بروتوكولات التشفير الامنة لبعض التطبيقات الحاسوبية.

c3. يطبق النظريات والمعادلات الرياضية لخوارزميات الأمن المبرهن للتوقيع الرقمي.

d1- يعمل بشكل فعال ضمن الفريق الواحد من خلال استخدام التشفير المناسبة لتامين الانظمة الالكتورنية والتطبيقات.

d2 - يكتسب المهارات المتعددة مثل كتابة التقارير الفنية والبحث العلمي ويحترم المعايير الأخلاقية.

v. محتوى المقرر Course Content:

أولا: الموضوعات النظرية Theoretical Aspect:

الرقم Order	الوحدات (الموضوعات الرئيسة) Units	الموضوعات التفصيلية Sub Topics	الأسبوع Week Due	الساعات الفعلية Con. H
1	المقدمة Introduction	▪ Cryptography Concepts, Cryptography History, Encryption and Secrecy, the Objectives of Cryptography, Attacks, services, Cryptographic Protocols, Provable Security. Algebra and Number and Information Theory	W١	2
2	تشفير المفتاح المتماثل Symmetric-Key Cryptography	▪ **Symmetric - Key Encryption:** Stream Ciphers, Block Ciphers, DES, ٣DES, AES. ▪ **Modes of Operation Cryptographic Hash Functions:** Security Requirements for Hash Functions, Construction of Hash Functions, Data Integrity and Message Authentication, Hash Functions as Random Functions.	W2	2
3	تشفير المفتاح المتماثل Symmetric-Key Cryptography	▪ **Symmetric - Key Encryption:** Stream Ciphers, Block Ciphers, DES, ٣DES, AES. ▪ **Modes of Operation Cryptographic Hash Functions:** Security Requirements for Hash Functions, Construction of Hash Functions, Data Integrity and Message Authentication, Hash Functions as Random Functions.	W3	2
4	تشفير المفتاح العام Public-Key Cryptography	▪ The Concept of Public - Key Cryptography. ▪ **Modular Arithmetic**: RSA, the Discrete Logarithm, Homomorphic Encryption Algorithms, Elliptic Curve Cryptography.	W٤	2
5	تشفير المفتاح العام Public-Key Cryptography	▪ The Concept of Public - Key Cryptography. ▪ **Modular Arithmetic**: RSA, the Discrete Logarithm, Homomorphic Encryption Algorithms, Elliptic Curve Cryptography.	W٥	2

2	W٦	▪ **Cryptographic Protocols:** Key Exchange and Entity Authentication, Identification Schemes, Commitment Schemes, Secret Sharing, Verifiable Electronic Elections, Mix Nets and Shuffles, Receipt-Free and Coercion-Resistant Elections, Digital Cash.	بروتوكولات التشفير **Cryptographic Protocols**	6
2	W7	▪ **Provably Secure Encryption:** Classical Information-Theoretic Security, Perfect Secrecy and Probabilistic Attacks, Public-Key One-Time Pads, Passive Eavesdroppers , Chosen-Ciphertext Attacks , A Security Proof in the Random Oracle Model , Security Under Standard Assumptions.	االخوارزميات الاحتمالية **Probabilistic Algorithms**	7
	W8	الأختبار النصفي **Midterm Exam**		8
2	W9	▪ **Provably Secure Encryption:** Classical Information-Theoretic Security, Perfect Secrecy and Probabilistic Attacks, Public-Key One-Time Pads, Passive Eavesdroppers , Chosen-Ciphertext Attacks , A Security Proof in the Random Oracle Model , Security Under Standard Assumptions.	االخوارزميات الاحتمالية **Probabilistic Algorithms**	9
2	W10	▪ **Probabilistic Algorithms:** Coin-Tossing Algorithms, Monte Carlo and Las Vegas Algorithms.	االخوارزميات الاحتمالية **Probabilistic Algorithms**	10
2	W11	▪ The Basic Assumptions and concepts, Bit Security algorithms, Pseudo randomness.	وظائف أحادية الاتجاه **One-Way Functions**	11
2	W12	▪ Classical Information - Theoretic Security, Perfect Secrecy and Probabilistic Attacks , Public-Key One-Time Pads, Passive Eavesdroppers, Chosen-Ciphertext Attacks	التشفير الأمن المبرهن **Provably Secure Encryption**	12
2	W13	▪ The Bounded Storage Model, The Noisy Channel Model, Unconditionally Secure Message Authentication, Collision Entropy and Privacy Amplification, Quantum Key Distribution.	التشفير الأمن الغير مشروط **Unconditional Security of Cryptosystems**	13
2	W14	▪ Provably Secure Digital Signatures Attacks and Levels of Security, Claw-Free Pairs and Collision-Resistant Hash Functions, Authentication-Tree-Based Signatures, A State-Free Signature Scheme, Algebra and Number Theory	الأمن المبرهن للتوقيع الرقمي **Provably Secure Digital Signatures**	14

15	الأمن المبرهن للتوقيع الرقمي Provably Secure Digital Signatures	▪ Provably Secure Digital Signatures Attacks and Levels of Security, Claw-Free Pairs and Collision-Resistant Hash Functions, Authentication-Tree-Based Signatures, A State-Free Signature Scheme, Algebra and Number Theory	W15	2
16	اختبار نهاية الفصل (نظري)		W16	
عدد الأسابيع والساعات الفعلية Number of Weeks /and Contact Hours Per Semester			14	28

ثانيا: خطة تنفيذ الجانب العملي Training/ Tutorials/ Exercises Aspects:

الرقم Order	المهام / التمارين Tutorials/ Exercises	الأسبوع Week Due	الساعات الفعلية Cont. H
1	▪ Implementation of Symmetric-Key Encryption and decryption: Stream Ciphers, Block Ciphers.	W١	2
2	▪ Implementation of Symmetric-Key Encryption and decryption: Stream Ciphers, Block Ciphers.	W2	2
3	▪ Symmetric Ciphers (DES, AES, RC4)	W3	2
4	▪ Symmetric Ciphers (DES, AES, RC4)	W٤	2
5	▪ Public-key Ciphers (RSA, Diffie-Hellman Key Exchange)	W٥	2
6	▪ Cryptographic Protocols.	W٦	2
7	اختبار نصف الفصل (Midterm Exam)	W٧	
8	▪ Probabilistic Algorithms	W8	2
9	▪ Implement of One-Way Functions	W9	2
10	▪ Implement Provably Secure Encryption	W10	2
11	▪ Implement Unconditional Security of Cryptosystems	W11	2
12	▪ Implement Provably Secure Digital Signatures	W12	2
13	▪ Implement Provably Secure Digital Signatures	W13	2
14	اختبار نهاية الفصل (عملي) Final Exam	W14	
اجمالي الأسابيع والساعات الفعلية Number of Weeks /and Contact Hours Per Semester		W12	H24

vi. استراتيجيات التدريس Teaching Strategies:

- المحاضرة التفاعلية Lectures
- الحوار والمناقشة discussion
- العصف الذهني Brainstorming
- حل المشكلات Problem solving
- المحاكاة والعروض العملية Practical presentations& Simulation Method
- التطبيق العملي Practical in computer Lab (Lab works)

نائب العميد لشئون الجودة	عميد الكلية	عميدة مركز التطوير وضمان الجودة	رئيس الجامعة
أ. د. عبده الكلي	د. إبراهيم لقمان	أ.م. د. هدي على العماد	أ. د. القاسم محمد عباس

- المشروعات والمهام والتكاليف projects
- التعلم الذاتي Self-learning
- التعلم التعاوني Cooperative Learning
- تبادل الخبرات بين الزملاء

VII . الأنشطة والتكليفات Tasks and Assignments:

م No	النشاط/ التكليف Assignments	نوع التكليف (فردي/ تعاوني)	الدرجة المستحقة Mark	أسبوع التنفيذ Week Due
١	الواجبات المنزلية و المشاركات الصفية.	فردي	10	أسبوعياً
٢	التكليفات المختلفة (التطبيقات العملية + تقييم الحوار والمناقشـــة + التحليل + البرامج + التقارير + المشاريع+ مراقبة التطبيقات العملية)	فردية أو جماعية	10	الثاني عشر والثالث عشر
	إجمالي الدرجة Total Score		20	

vii. تقويم التعلم Learning Assessment :

م No	أساليب التقويم Assessment Method	موعد(أسبوع) التقويم Week Due	الدرجة Mark	الوزن النسبي% Proportion of Final Assessment
1	والواجبات والمشاركات	أسبوعياً	10	% 6.67
2	التكليفات كوز(١) Quiz	السادس	5	% 3.33
3	اختبار نصف الفصل (نظري) Midterm Exam	الثامن	20	% 13.33
4	التكليفات كوز(٢) Quiz	العاشر	5	% 3.33
5	اختبار نهاية الفصل (عملي) Final Exam (practical)	الرابع عشر	٥٠	% 33.34
6	اختبار نهاية الفصل (نظري) Final Exam (theoretical)	السادس عشر	60	% 40
	المجموع Total		١٥٠	%100

viii. مصادر التعلم Learning Resources: (اسم المؤلف، سنة النشر، اسم الكتاب، دار النشر، بلد النشر).

١. المراجع الرئيسة Required Textbook(s): (لا تزيد عن مرجعين)

1. Hans Delfs and Helmut Knebl, et al, "Introduction to Cryptography Principles and Applications," Third Edition ©Springer-Verlag Berlin Heidelberg 2015.

٢. المراجع المساندة Essential References:

نائب العميد لشئون الجودة	عميد الكلية	عميدة مركز التطوير وضمان الجودة	رئيس الجامعة
أ. د. عبده الكلي	د. إبراهيم لقمان	أ.م. د. هدي على العماد	أ. د. القاسم محمد عباس

1. William Stallings, 201٣, "Cryptography and Network Security: Principles and Practice", ٦th Edition, Prentice Hal.
2. Jeffrey Hoffstein and Jill Pipher, et al, "An Introduction to Mathematical Cryptography," Second Edition© Springer Science + Business Media New York, 2014

٣. المصادر الإلكترونية ومواقع الإنترنت... Electronic Materials and Web Sites *etc.*

1. https://docs.microsoft.com/en-us/windows/win32/seccrypto/about-cryptography
2. https://www.tutorialspoint.com/cryptography/index.htm
3. https://sites.google.com/site/ddmwsst/cryptography-concepts

ix. الضوابط والسياسات المتبعة في المقرر Course Policies

بعد الرجوع إلى لوائح الجامعة يتم كتابة السياسة العامة للمقرر فيما يتعلق بالآتي:

١	**سياسة حضور الفعاليات التعليمية Class Attendance:** - يلتزم الطالب بحضور ٧٥% من المحاضرات ويحرم في حال عدم الوفاء بذلك. - يقدم أستاذ المقرر تقريرا بحضور وغياب الطلاب للقسم ويحرم الطالب من دخول الامتحان في حال تجاوز الغياب ٢٥% ويتم اقرار الحرمان من مجلس القسم.
٢	**الحضور المتأخر Tardy:** - يسمح للطالب حضور المحاضرة إذا تأخر لمدة ربع ساعة لثلاث مرات في الفصل الدراسي، وإذا تأخر زيادة عن ثلاث مرات يحذر شفويا من أستاذ المقرر، وعند عدم الالتزام يمنع من دخول المحاضرة.
٣	**ضوابط الامتحان Exam Attendance/Punctuality:** - لا يسمح للطالب دخول الامتحان النهائي إذا تأخر مقدار (٢٠) دقيقة من بدء الامتحان - إذا تغيب الطالب عن الامتحان النهائي تطبق اللوائح الخاصة بنظام الامتحان في الكلية.
٤	**التعيينات والمشاريع Assignments & Projects:** - يحدد أستاذ المقرر نوع التعيينات في بداية الفصل ويحدد مواعيد تسليمها وضوابط تنفيذ التكليفات وتسليمها. - إذا تأخر الطالب في تسليم التكليفات عن الموعد المحدد يحرم من درجة التكليف الذي تأخر في تسليمه.
٥	**الغش Cheating:** - في حال ثبوت قيام الطالب بالغش في الامتحان النصفي أو النهائي تطبق عليه لائحة شؤون الطلاب. - في حال ثبوت قيام الطالب بالغش او النقل في التكليفات والمشاريع يحرم من الدرجة المخصصة للتكليف.
6	**الانتحال Plagiarism:** - في حالة وجود شخص ينتحل شخصية طالب لأداء الامتحان نيابة عنه تطبق اللائحة الخاصة بذلك
7	**سياسات أخرى Other policies:** - أي سياسات أخرى مثل استخدام الموبايل أو مواعيد تسليم التكليفات ..... الخ