Al-Farouk journal of sciences
Volume (2), Issue (1) (March, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) العدد 1 مارس 2026
ردمد: 3135-2359

دور التشفير في حماية بيانات الطلبة وأعضاء هيئة التدريس والموظفين في ظل التحول الرقمي للتعليم (دراسة ميدانية تحليلية)

The Role of Encryption in Protecting Student, Faculty, and Staff Data Amidst the Digital Transformation of Education (An Analytical Field Study Faculty of Economics, Ajilat - University of Zawiya - Libya

نشوه إسماعيل زقوت
كلية الاقتصاد العجيلات- جامعة الزاوية -ليبيا
N.zaqout@zu.edu.ly

دعاء ضو اللالي
كلية الاقتصاد العجيلات- جامعة الزاوية -ليبيا
d.allali@zu.edu.ly

تاريخ الاستلام: 2026/01/10 تاريخ المراجعة 18 / 2 / 2026 تاريخ القبول: 2026/03/11- تاريخ النشر: 22/ 03/ 2026

الملخص

هدفت الدراسة إلى استقصاء دور تقنيات التشفير في حماية بيانات الطلبة وأعضاء هيئة التدريس في ظل التحول الرقمي بالمؤسسات التعليمية الليبية (كلية الاقتصاد العجيلات نموذجاً). اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم جمع البيانات عبر استبانة إلكترونية وزعت على عينة من (100) مستجيب. أظهرت النتائج وجود وعي مرتفع بأهمية التشفير بمتوسط حسابي (4,2)، وإدراك عام لدوره في تعزيز الثقة الرقمية بمتوسط (3.90). كما كشفت النتائج أن التحديات التقنية (مثل تعقيد الأنظمة وبطء الأداء) والتحديات البشرية (نقص الكوادر المتخصصة) هي الأبرز تأثيراً على فاعلية التطبيق. وأوصت الدراسة بضرورة ترقية بروتوكولات التشفير إلى معايير (AES-256) وتفعيل المصادقة الثنائية، مع ضرورة سد الفجوة بين الوعي النظري والممارسة التطبيقية عبر برامج تدريبية متخصصة.

الكلمات المفتاحية: التشفير، الأمن السيبراني، التحول الرقمي، حماية البيانات التعليمية.

Abstract

This study investigated the role of encryption techniques in protecting student and faculty data during the digital transformation of Libyan educational institutions (Faculty of Economics, Al-Ajaylat as a case study). A descriptive-analytical approach was employed, with data collected via an electronic questionnaire from (100) participants. The findings revealed a high level of awareness regarding encryption importance (Mean: 4,2). and a strong perception of its role in enhancing digital trust (Mean: 3.90). However, the study identified significant technical challenges (e.g., system complexity and performance issues) and human challenges (e.g., lack of specialized expertise) that hinder effective implementation. The study recommends upgrading encryption protocols to (AES-256) standards, implementing Multi-Factor Authentication (MFA), and bridging the gap between theoretical awareness and practical application through specialized training programs.

Keywords:Encryption,Cybersecurity,Digital,Transformation,Educational Data.

1.1المقدمة

شهد العالم خلال السنوات الأخيرة تحولاً رقمياً متسارعاً أعاد تشكيل مفهوم العمليات في مختلف القطاعات، ولا سيما القطاع التعليمي الذي فرضت متطلبات العصر اعتماده بشكل كلي على المنصات الإلكترونية وأنظمة إدارة التعلم (Vial, 2019). وقد ترتب على هذا التحول تولد كميات ضخمة ومستمرة من البيانات الحساسة الخاصة بالطلاب وأعضاء هيئة التدريس، وتشمل هذه البيانات السجلات الأكاديمية، والأداء التقييمي، والبيانات الشخصية والمالية، مما يجعلها ثروة معلوماتية تتطلب حماية صارمة للالتزام بمعايير حماية الخصوصية عالمياً (AlHogail, 2018). غير أن هذا التبني الشامل للرقمنة فتح الباب أمام تهديدات سيبرانية متطورة؛ حيث أضحت المؤسسات التعليمية هدفاً مغرية للمخترقين بسبب ضعف البنية التحتية الأمنية لديها، مما يعرضها لهجمات التصيد الاحتيالي، وبرامج الفدية، وتسريب البيانات، وهو ما ينتهك الخصوصية ويهدم الثقة المؤسسية. ولمواجهة هذه المخاطر المتنامية، برز "التشفير" (Cryptography) كخط الدفاع الأول والأكثر موثوقية لضمان سرية وسلامة البيانات أثناء نقلها وتخزينها في قواعد البيانات السحابية أو المحلية (Stallings, 2017). إذ يعمل التشفير على تحويل البيانات المقروءة إلى نصوص مشفرة غير مفهومة، وتختلف خوارزمياته ما بين التماثل وغير التماثل، مما يجعل البيانات عديمة الفائدة للمهاجمين حتى في حال اختراق الأنظمة. ورغم الاعتراف العالمي بأهمية التشفير كأداة رادعة، إلا أن تطبيقه العملي في البيئة التعليمية لا يزال يواجه تحديات تقنية وتشريعية تستدعي التوقف عندها. ومن هنا، تبرز مشكلة هذا البحث في دراسة الدور المحوري الذي تلعبه تقنيات التشفير المختلفة في حماية خصوصية ومعلومات الطلاب وأعضاء هيئة التدريس، وتقييم مدى فاعليته كركيزة أساسية لأمن المعلومات في ظل التحول الرقمي للتعليم، وبالتالي تقديم رؤية واضحة لتعزيز منظومة الأمن السيبراني في المؤسسات التعليمية.

2.1 مشكلة البحث

على الرغم من التوسع الكبير في التحول الرقمي داخل القطاع التعليمي والاعتماد المتزايد على أنظمة إدارة التعلم (LMS)، إلا أن العديد من المؤسسات التعليمية لا تزال تعاني من قصور في بنيتها الأمنية، مما يجعل بيانات الطلاب وأعضاء هيئة التدريس عرضة للاختراقات والتهديدات السيبرانية المتطورة. وتكمن المشكلة الأساسية في الفجوة القائمة بين الحجم الهائل للبيانات الحساسة التي يتم معالجتها رقمياً، وبين مستوى الوعي والتطبيق الفعلي لتقنيات الحماية المتقدمة، وتحديداً "التشفير". فالاعتماد على وسائل الحماية التقليدية (ككلمات المرور وجدران الحماية) لم يعد كافياً لردع الهجمات الحديثة التي تستهدف الخصوصية الأكاديمية. وبناءً على ذلك، يمكن صياغة مشكلة البحث في التساؤل الرئيسي التالي:

ما دور تقنيات التشفير في حماية بيانات الطلاب وأعضاء هيئة التدريس من الهجمات السيبرانية في ظل التحول الرقمي للتعليم؟

ويتفرع من هذا التساؤل الرئيسي الأسئلة الفرعية التالية:

1- ما مستوى المعرفة والإدراك لدى الطلاب وأعضاء هيئة التدريس بمفهوم التشفير كأداة أساسية لحماية البيانات في العصر الرقمي؟

2- ما مستوى استخدام التشفير لدى الطلاب وأعضاء هيئة التدريس، وما علاقته بتعزيز أمن المعلومات وحماية الخصوصية؟

3- إلى أي مدى يسهم استخدام التشفير في تعزيز ثقة المستخدمين بالخدمات الرقمية وحماية بياناتهم؟

4- ما هي التحديات التقنية والتنظيمية التي تحد من تطبيق التشفير بكفاءة في المؤسسات التعليمية؟

3.1 أهداف البحث

الهدف الرئيسي:

التعرف على الدور الفعلي والمحوري لتقنيات التشفير في حماية خصوصية وسلامة بيانات الطلاب

وأعضاء هيئة التدريس في ظل التحول الرقمي للتعليم.

الأهداف الفرعية:

1. تحديد أبرز التهديدات والمخاطر السيبرانية التي تستهدف الأنظمة التعليمية وقواعد بيانات الطلاب وأعضاء هيئة التدريس
2. معرفة مدى مساهمة استخدام التشفير في تعزيز ثقة المستخدمين بالخدمات الرقمية وحماية بياناتهم.
3. الكشف عن التحديات التقنية والتنظيمية التي تحد من التطبيق الأمثل لأنظمة التشفير في المؤسسات التعليمية.
4. تقديم مجموعة من التوصيات والمقترحات العملية لصناع القرار والمسؤولين عن تقنية المعلومات في القطاع التعليمي لتعزيز منظومة أمن البيانات.

4.1 أهمية البحث

تنبثق أهمية هذا البحث من كونه يتناول موضوعاً حيوياً يلامس صميم العملية التعليمية في عصر رقمي تتزايد فيه المخاطر، وتتمثل أهميته في محورين رئيسيين:

أولاً: الأهمية العلمية (النظرية):

– إثراء الأدب النظري: يساهم البحث في سد فجوة معرفية في الأدبيات العربية المتعلقة بأمن المعلومات، من خلال تقديم دراسة تربط بشكل مباشر بين تقنيات التشفير المتقدمة وبيئة التعليم الرقمي.

– الإطار المفاهيمي: يقدم البحث إطاراً مرجعياً متكاملاً للباحثين والمهتمين حول طبيعة البيانات الأكاديمية الحساسة، وكيفية توظيف خوارزميات التشفير المختلفة (المتماثلة وغير المتماثلة) لحمايتها من الاختراقات.

ثانياً: الأهمية العملية (التطبيقية):

–توجيه أصحاب القرار :(توجيه صناع القرار في الجامعات لاعتماد التشفير كأولوية مالية وتقنية)

–حماية الخصوصية:(لمساهمة في حماية خصوصية الطلاب والأساتذة من التسريبات).

–دعم التخطيط الاستراتيجي:(توفير بيانات تساعد في التخطيط لتحديث البنية التحتية الأمنية).

5.1 منهجية البحث ومحدداته

"لتحقيق أهداف هذا البحث والإجابة على تساؤلاته، تم اعتماد المنهج الوصفي التحليلي، وتبرز ملاءمة هذا المنهج كون هذه الدراسة تُعد دراسة أساسية تبني إطاراً معرفياً متكاملاً. فقد استُخدم الجانب النظري لاستعراض مفاهيم التحول الرقمي وطبيعة البيانات الحساسة والتهديدات السيبرانية، بينما استُخدم الجانب التحليلي لتحليل آليات عمل تقنيات التشفير المختلفة"

6.1 حدود الدراسة:

1– "الحدود المكانية (المفاهيمية): يقتصر البحث على البيئة التعليمية الرقمية بشكل عام (الجامعات والمدارس التي تعتمد على أنظمة إدارة التعلم وقواعد البيانات السحابية أو المحلية).

2– الحدود الزمانية: 2026

3– الحدود البشرية: أعضاء هيئة التدريس و الموظفين و الطلاب بكلية الاقتصاد

7–1 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من جميع طلبة الدراسين واعضاء هيئة التدريس بكلية الاقتصاد العجيلات كما اعتمدت الدراسة على اسلوب العينة بدلا من اسلوب الحصر الشامل ويرجع ذلك بسبب ان عدد مجتمع الدراسة كبير حيث يصعب جمع البيانات بشكل دقيق، وبالتالي تم اختيار العينة الطبقية العشوائية.

8.1 الدراسات السابقة

1-**دراسة (العمري، 2023)** بعنوان "التحول الرقمي في التعليم العالي وتأثيره على خصوصية البيانات الأكاديمية واستخدم المنهج الوصفي المسحي. وأظهرت النتائج أن هناك قلقاً متزايداً لدى الطلاب حول كيفية استخدام مؤسساتهم لبياناتهم الأكاديمية، وأن السياسات الخصوصية لا تزال ضعيفة. وتتميز بملامستها للبعد القانوني والتنظيمي، لكنها قصّرت في تقديم حلول تقنية. "بحثنا يختلف بتقديمه للتشفير كحل رادع وجوهري لاختراق الخصوصية" **دراسة (Johnson & Lee, 2022)** بعنوان "Privacy Policies in E-Learning Platforms: A Critical Analysis".و استخدم المنهج التحليل المضمون لسياسات الخصوصية في المنصات وأكدت النتائج أن غالبية منصات التعلم لا تفصح بوضوح عن استخدامها لتقنيات التشفير لمستخدميها. وقدمت رؤية قانونية مهمة، لكن بحثنا يتميز بتقديم رؤية تقنية بحتة لآليات عمل هذا التشفير داخل هذه المنصات.

2-**دراسة (الحربي، 2021)** بعنوان "جاهزية المؤسسات التعليمية للأمن السيبراني في ظل جائحة كورونا". واستخدم المنهج الوصفي التحليلي وكشفت عن ضعف البنية التحتية الأمنية وارتفاع معدلات الاختراق أثناء التعلم عن بعد. وأثبتت أن المشكلة موجودة وخطيرة، مما يجعل بحثنا الحالي استكمالاً ضرورياً لها لتقديم الحل (التشفير) لهذه الجاهزية المفقودة.

3-**دراسة (Chen et al., 2023)** بعنوان "Ransomware Attacks on Educational Institutions: Vulnerabilities and Mitigation". واستخدم دراسة حالة (Case Study) لعدة جامعات تعرضت لهجمات فدية. وأكدت أن بيانات الطلاب تُباع فالويب المظلم، وأن السبب الرئيسي هو عدم تشفير قواعد البيانات. ، تعتبر دراسة ممتازة لربطها بين التهديد (الفدية) والحل (التشفير)، وقد استفاد بحثنا من هذه النتيجة لتبرير أهمية التشفير كأولوية قصوى.

4-**دراسة (السلمي، 2020)** بعنوان "اختراق الأنظمة الأكاديمية وآثاره على السجلات الدراسية للطلاب". واستخدم المنهج الوصفي. و النتائج بينت أن تلاعب الطلاب أو المخترقين بالدرجات يؤدي إلى فقدان مصداقية الشهادات الأكاديمية. وركزت على الأثر الناتج عن الاختراق، بينما يركز بحثنا على الوقاية قبل حدوث الاختراق عبر التشفير.

5-**دراسة (Kumar & Sharma, 2022)** بعنوان " Performance Evaluation of AES and DES Algorithms in Cloud-Based Educational Systems". استخدم المنهج التجريبي أثبتت أن خوارزمية (AES) المتقدمة توفر أماناً أعلى وسرعة معالجة تناسب البيانات الضخمة مقارنة بـ (DES).

. خلاصة الدراسات

يتضح من العرض السابق أن الدراسات السابقة قد تناولت موضوع أمن البيانات والتحول الرقمي بشكل منفصل، أو تناولت التشفير من زاوية حسابية بحتة. ويتميز هذا البحث عنها بكونه يدمج بين البعدين في إطار تعليمي محدد، حيث يقدم تحليلاً نقدياً مقارناً لأنواع التشفير (متماثل، غير متماثل، هجين) ويقيس فاعليتها المباشرة في حماية فئتين محددتين (الطلاب وهيئة التدريس)، وهو ما لم تُركز عليه دراسة سابقة بهذا الشكل المعمق.

1.2 التحول الرقمي في التعليم وتوليد البيانات

لا يُفهم التحول الرقمي في السياق التعليمي على أنه مجرد عملية "أتمته" (Automation) تقليدية تقتصر على استبدال الوثائق الورقية بنظيراتها الإلكترونية، بل هو تغيير جوهري وشامل في البنية التحتية والعمليات الأكاديمية والإدارية. ويُعرف التحول الرقمي في التعليم بأنه الانتقال المنهجي نحو استخدام التكنولوجيا المتقدمة لتحسين تجربة التعلم، وإدارة المؤسسة بكفاءة، واتخاذ القرارات المبنية على البيانات" (Vial, 2019). وقد فرضت متطلبات هذا التحول على المؤسسات التعليمية إعادة هندسة بيئاتها التشغيلية لتشمل اعتماد الحوسبة السحابية، وتطبيقات الاتصال في الوقت الفعلي، والأهم من ذلك: تبني أنظمة إدارة التعلم (LMS) كقلب نابض للعملية التعليمية الحديثة. وتتطلب هذه المرحلة الانتقالية توفير مقومات أساسية لنجاحها، أبرزها: بنية تحتية تقنية عالية السرعة، وكوادر بشرية قادرة على التكيف مع الأدوات الرقمية، بالإضافة إلى سياسات حوكمة واضحة تضمن استدامة هذا التحول دون التضحية بجودة المخرجات التعليمية.

2.2 طبيعة البيانات التعليمية ومدى حساسيتها:

ترتبط البنية التحتية الرقمية ارتباطاً وثيقاً بظاهرة "انفجار البيانات" (Data Explosion) داخل المؤسسات التعليمية. فمع التبني الواسع لمنصات التعلم الإلكتروني (مثل Moodle وBlackboard) وأنظمة المعلومات الطلابية (SIS)، أصبحت هذه المؤسسات مستودعات ضخمة ومستمرة التدفق لمعلومات الطلاب وأعضاء هيئة التدريس. ولتقديم صورة واضحة عن حجم المخاطر، يمكن تصنيف هذه البيانات إلى ثلاث فئات رئيسية:

1.البيانات التعريفية والشخصية: وتشمل الأسماء، وأرقام الهوية، ومعلومات الاتصال، والصور، وفي بعض الأحيان البيانات الصحية للطلاب.

2.البيانات الأكاديمية والفكرية: وتتمثل في السجلات الدراسية، الدرجات، أنماط التقييم، ومشاركات الطلاب، بالإضافة إلى الأبحاث العلمية والمحتوى Intellectual Property الخاص بأعضاء هيئة التدريس.

3.البيانات السلوكية والنظامية: وتشمل سجلات الحضور والانصراف، عادات التصفح داخل المنصة، وعناوين بروتوكولات الإنترنت (IP Addresses) الخاصة بالمستخدمين.

3.2 أنواع البيانات :

1. بيانات الطلبة (Student Data):

بيانات شخصية (اسم، عائلة، صور)، بيانات أكاديمية (علامات، حضور، غياب)، بيانات مالية (رسوم، منح). دور التشفير هو تشفير هذه البيانات في أنظمة إدارة التعلم (مثل Moodle أو Blackboard) لتجنب اختراق الحسابات وتغيير العلامات (تشفير قواعد البيانات في السكون)، وتشفير رابط الامتحانات الإلكترونية.

2. بيانات أعضاء هيئة التدريس (Faculty Data):

ملكية فكرية (محاضرات، أبحاث علمية غير منشورة)، بيانات رواتب، تقييمات أداء. ودور التشفير هو التشفير أثناء النقل (مثل تأمين نقل الملفات الثقيلة للمحاضرات عبر شبكة الجامعة)، والتوقيع الرقمي لضمان أن المحتوى لم يُعبث به من قبل الطلبة.

3–بيانات الموظفين (Staff/HR Data):

ملفات وظيفية، بيانات تأمينية وطبية، كشوف رواتب، عقود. و

هذه البيانات تمر غالباً عبر أنظمة موارد بشرية إلكترونية (HR Systems)، والتشفير هنا يحمي من تسريب البيانات الحساسة التي قد تُستخدم في الابتزاز أو الاحتيال المالي.

4.2 مفهوم الأمن السيبراني في التعليم وخصوصيته:

يتباين مفهوم الأمن السيبراني في السياق التعليمي عنه في القطاعات الأخرى كالبنوك أو المستشفيات؛ فبينما يتركز الاهتمام في تلك القطاعات بشكل أساسي على حماية الأصول المالية أو البيانات الطبية الحيوية، فإن الأمن السيبراني التعليمي يتمحور حول حماية "الخصوصية الفردية" للمستفيدين، و"الملكية الفكرية" للمؤسسة، و"سلامة العملية الأكاديمية". وتتميز الشبكات التعليمية بطبيعة فريدة تجعل تأمينها تحدياً معقداً، ألا وهي "الانفتاحية"؛ حيث يجب أن تكون الأنظمة متاحة للطلاب وأعضاء هيئة التدريس من أجهزة متعددة (حواسيب، هواتف) وشبكات مختلفة (واي فاي الجامعة، شبكات المنزل)، مما يوسع دائرة التعرض للمخاطر (Chen et al., 2023).

5.2 أبرز التهديدات التي تستهدف البيانات التعليمية

- **هجمات الفدية (Ransomware):** تُعد الأخطر حالياً، حيث يقوم المهاجمون باختراق أنظمة الجامعة أو المدرسة وتشفير ملفاتها بالكامل (بما فيها سجلات الطلاب وأبحاث الأساتذة)، ثم يطلبون فدية مالية لاستعادتها، مما قد يعطل العملية التعليمية لأشهر.
- **التصيد الاحتيالي (Phishing):** نظراً لكون الطلاب والمعلمين ليسوا خبراء أمنيين، يُسهل على المخترقين إرسال رسائل بريد إلكتروني مزيفة تبدو وكأنها من إدارة الجامعة، بهدف سرقة كلمات المرور والوصول المباشر إلى أنظمة إدارة التعلم (LMS).
- **تسريب البيانات (Data Breaches):** تحدث غالباً بسبب ثغرات برمجية في مواقع المؤسسة التعليمية، مما يسمح للمخترقين بسحب قواعد بيانات الطلاب وبيعها في الأسواق السوداء أو "الويب المظلم"، مما يعرضهم لجرائم انتحال الشخصية.

6.2 دوافع الاختراق للمؤسسات التعليمية

رغم خطورة التهديدات السابقة، إلا أن نجاح الهجمات على التعليم يعود لعوامل هيكلية، أبرزها:

- المساحة السطحية الواسعة للهجوم: وجود آلاف المستخدمين (طلاب وأساتذة وإداريين) يتصلون بالنظام يومياً، مما يجعل نقاط الضعف البشرية كثيرة جداً.
- محدودية الميزانيات الأمنية: غالباً ما تُعاني المؤسسات التعليمية من نقص في التمويل المخصص لتحديث البنية التحتية الأمنية مقارنة بالشركات الكبرى (Johnson & Lee, 2022).
- استخدام أنظمة قديمة (Legacy Systems): لا تزال العديد من الجامعات تعتمد على أنظمة إدارة دراسية طُورت منذ سنوات طويلة وتفتقر لمعايير الأمان الحديثة.

7.2 التشفير (Cryptography) :

يُعد التشفير العلوم والتقنيات التي تُعنى بتحويل البيانات المفهومة والقابلة للقراءة (Plaintext) إلى بيانات مشفرة وغير مفهومة (Ciphertext)، باستخدام خوارزميات رياضية معقدة ومفاتيح سرية. والهدف الجوهري من هذه العملية في البيئة التعليمية هو ضمان أنه حتى في حال تمكن مخترق من اختراق خوادم الجامعة والوصول إلى الملفات، فإنه لن يتمكن من فهمها أو الاستفادة منها (Stallings, 2017).

8.2 أهداف التشفير، (CIA Triad + Non-repudiation):

1.السرية (Confidentiality): ضمان عدم اطلاع أي جهة غير مصرح عليها (كطلاب آخرين أو مخترقين) على السجلات الأكاديمية.

2,السلامة (Integrity): التأكد من عدم حدوث أي تعديل أو تلاعب بالدرجات أو محتوى المناهج أثناء النقل أو التخزين.

3.المصادقة (Authentication): التأكد من هوية الطالب الذي يدخل الاختبار الإلكتروني، أو الأستاذ الذي يرفع المحاضرة.

4.عدم الإنكار (Non-repudiation): ضمان عدم قدرة الطالب على إنكار تسليمه لواجب معين، أو الأستاذ على إنكار إرساله لدراسة معينة

9.2 أنواع التشفير:

1. التشفير المتماثل (Symmetric Encryption)

يعتمد هذا النوع على استخدام مفتاح واحد فقط (Single Key) لعمليتي التشفير وفك التشفير. يشبه هذا الأمر "قفل الباب بمفتاح واحد"، حيث يجب أن يحتفظ كل من المرسل (نظام إدارة التعلم) والمستقبل (الطالب) بنسخة سرية من هذا المفتاح. وتُعد خوارزمية (AES - Advanced Encryption Standard) المعيار العالمي الأكثر استخداماً في هذا النوع، بينما تعتبر خوارزمية (DES) قديمة وغير آمنة (Kumar & Sharma, 2022).

و يتميز بسرعة فائقة جداً في المعالجة، مما يجعله مثالياً لتشفير قواعد البيانات الضخمة (مثل أرشيف الجامعة لبيانات الطلاب عبر سنوات الدراسة).المشكلة تكمن في كيفية إيصال المفتاح السري بأمان إلى آلاف الطلاب دون أن يتم اعتراضه من قبل المخترقين.

2.التشفير غير المتماثل (Asymmetric Encryption)

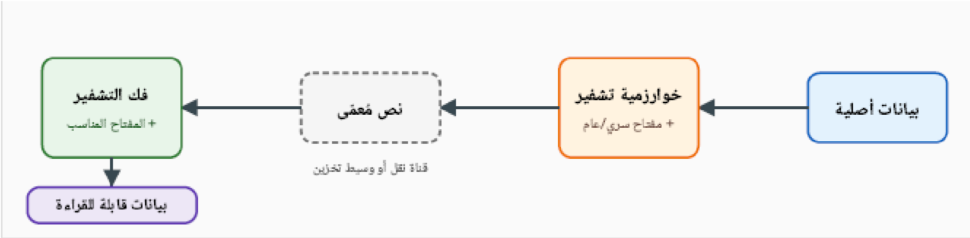
لحل مشكلة توزيع المفاتيح في النوع السابق، تم ابتكار التشفير غير المتماثل، والذي يستخدم زوجاً من المفاتيح مرتبطين رياضياً ، (كما موضح بالشكل 1)

1. المفتاح العام (Public Key): يُشارك مع الجميع (يُوضح على موقع الجامعة).
2. المفتاح الخاص (Private Key): يبقى سرياً ومخزناً بأمان لدى صاحبه فقط (مثل خادم امتحانات الجامعة). إذا أراد الطالب إرسال طلب تسجيل مشفر، يأخذ المفتاح العام للجامعة ويشفر به طلبه. لا يمكن فك هذا التشفير إلا بواسطة "المفتاح الخاص" الذي تملكه الجامعة فقط. والعكس صحيح إذا أرادت الجامعة إرسال شهادة مشفرة للطالب (الدوسري، 2021).

و من أبرز الخوارزميات: خوارزمية (RSA)، وهو يحل مشكلة التوزيع الآمن للمفاتيح تماماً.

3. دوال التجزئة (Hashing) – الحارس الصامت

تختلف دوال التجزئة عن التشفير بأنها عملية "باتجاه واحد" (One-way Function). فهي تأخذ بيانات بأي حجم (مثل كلمة مرور الطالب أو ملف الامتحان) وتُخرج نصاً ثابت الطول يُسمى "البصمة الرقمية" (Hash). و من خصائصه لا يمكن إعادة البيانات الأصلية من البصمة الرقمية، وأي تغيير بسيط جداً في الملف الأصلي (حتى حرف واحد في الدرجة) سيؤدي إلى تغير كامل في البصمة الرقمية. وتستخدم المؤسسات التعليمية الـ (Hashing) لتخزين كلمات مرور الطلاب في قواعد البيانات، بدلاً من تخزينها كنصوص واضحة، مما يمنع إداريي النظام من معرفة كلمات مرور الطلاب. كما تستخدم للتأكد من سلامة ملفات المناهج من التلاعب (Williams & Brown, 2023).



الشكل(1) مخطط يوضح عملية تشفير البيانات و فك التشفير

3-1 مصادر جمع البيانات

تم جمع البيانات من خلال مفردات العينة، ومن بيانات أساسية تم جمعها ميدانيا من خلال الاستبانة التي صممت خصيصا لهذا الغرض، والتي وزعت على عينة الدراسة المكونة من طلاب الدراسات العليا. وتم الاعتماد على الاستبانة كأداة لجمع البيانات والتي تم من خلالها الاجابة على تساؤلات الدراسة، وهي اداة شائعة لقياس الآراء والاتجاهات، ومستخدمة في كثير من الدراسات الميدانية. وتم تصميم واعداد الاستبانة من قبل الباحثتان من خلال الاعتماد على عدد من الدراسات السابقة مع اجراء بعض التعديلات بما يتماشى مع اهداف الدراسة.

وتم تقسيم الاستبانة الى خمس محاور رئيسية:

1) المحور الاول : وهو يتمثل في مجموعة من العبارات المتعلقة بالبيانات الشخصية والمستوى التعليمي.
2) المحور الثاني : وهو يتمثل في مجموعة من العبارات المتعلقة مستوى المعرفة والإدراك بالتشفير .
3) المحور الثالث: وهو يتمثل في مجموعة من العبارات المتعلقة باهمية التشفير في حماية البيانات.
4) المحور الرابع وهو يتمثل في مجموعة من العبارات المتعلقة بدور التشفير في حماية البيانات والحد من الهجمات السيبرانية .
5) المحور الخامس وهو يتمثل في مجموعة من العبارات المتعلقة بصعوبات التشفير والتحديات التي تواجهه في حماية البيانات .

بدت عملية عرض الاستبانة الالكترونيا على طلاب واعضاء هيئة التدريس بكلية الاقتصاد العجيلات خلال شهر ابريل 2026م والجدول التالي يوضح عدد الاستبانة التي تم توزيعها على عينة الدراسة: –

جدول رقم (1) يوضح عدد الاستبانة التي تم توزيعها على مجتمع الدراسة

عدد الاستبانة	عدد الاستبانة الموزعة	الاستبانات المسترجعة	غير صالحة	عدد الاستبانة الصالحة للتحليل
120	120	120	20	100

بعد ان تم عرض الاستبانة على مجتمع الدراسة والذي كان عددهم (120) والنظر في الاستبانة بعد الاجابة عليها من مجتمع الدراسة تم استبعاد عدد (20) استبانة وذلك لعدم اكتمال الاجابات بها .

2.3 لأساليب الإحصائية المستخدمة في تحليل البيانات:

تم استخدام البرنامج الإحصائي SPSS (الحزم الإحصائية للعلوم الاجتماعية) في تفريغ وتحليل البيانات الواردة في استمارة الاستبيان وذلك من خلال عدد من الأساليب الإحصائية التالية:

1. النسب المئوية والتكرارات والمتوسط الحسابي: وتستخدم بشكل أساسي لأغراض معرفة تكرار فئات متغير ما ويتم الاستفادة منها في وصف عينة الدراسة.
2. الانحراف المعياري: لقياس الانحرافات في إجابات مفردات عينة الدراسة على فقرات الاستبانة.

3. معامل الارتباط بيرسون: لحساب معامل الارتباط وقياس صدق الاتساق الداخلي، وكذلك تحديد طبيعة العلاقة بين المتغيرين المستقل والتابع.
4. معامل ألفا كرونباخ: لقياس ثبات الاستبانة.

3.3 صدق وثبات اداة الدراسة (الاستبانة)

اولا:– صدق اداة الدراسة (الاستبانة)

يقصد بصدق الاستبانة ان تقيس اسئلة الاستبانة ما وضعت لقياسه، وقامت الباحثتان بالتأكد من صدق الاستبانة كالتالي:

أ– (الصدق الظاهري)

اعتمدت الدراسة في تقرير صدق الأداة على ما يعرف بالصدق الظاهري أو صدق المحكمين، حيث تم عرض الاستبيان في صورته الأولية على مجموعة من أعضاء هيئة التدريس بكلية الاقتصاد العجيلات حيث قاموا بإبداء أراءهم ومقترحاتهم وملاحظاتهم حول صياغة بعض العبارات، هذا وقد أجريت العديد من التعديلات، وتم حذف بعض العبارات وبعض الكلمات وإحلال أخرى بدلاً منها.

ب– صدق الاتساق الداخلي

–نتائج الاتساق الداخلي

1– مستوى المعرفة والإدراك بالتشفير

الجدول رقم (2) معاملات الارتباط بين فقرات مقياس مستوى المعرفة والإدراك بالتشفير والدرجة الكلية للمحور

	مستوى المعرفة والإدراك بالتشفير	معامل الارتباط	مستوى الدلالة
1	المعرفة بالتشفير " هل لديك معرفة سابقة بمفهوم التشفير"	0.642**	0.000
2	ادارك دور التشفير في بيئة الكلية (اعتقد أن نظام التعلم في الكلية يستخدم تقنيات التشفير لحماية كلمات المرور)	0.571**	0.000
3	ادارك دور التشفير في بيئة الكلية [تشعر بالثقة في أن بياناتك الأكاديمية مشفرة ومحمية]	0.637**	0.000
4	ادارك دور التشفير في بيئة الكلية [التشفير يقلل بشكل كبير من احتمالية استفادة المخترقين من بيانات الطلاب وهيئة التدريس]	0.598**	0.000
5	ادارك دور التشفير في بيئة الكلية [المؤسسات التعليمية التي تعتمد على التشفير المتقدم هي أكثر أمانا	0.528**	0.000
6	ادارك دور التشفير في بيئة الكلية [التشفير يساهم في حماية خصوصيتي الرقمية ومنع التلاعب بسجلاتي]	0.606**	0.000

يوضح الجدول رقم (2) والذي يضم (6) فقرات أن معامل الارتباط بين كل فقرة من فقرات البعد الأول والدرجة الكلية للبعد وهو مستوى المعرفة والإدراك بالتشفير، حيث جاءت كل نتائج فقرات البعد الاول للمتغير الفرعي الاول موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الفرعي الاول زادت المعرفة والإدراك بالتشفير .وبذلك تعتبر فقرات هذا البعد يجمع بينها عناصر مشتركة تجعلها أكثر تجانساً وصادقة لما وضعت لقياسه في هذا البعد وبالتالي يعتبر المتغير صادقا لما وضع لقياسه.

2– اهمية التشفير في حماية البيانات.

الجدول رقم (3) معاملات الارتباط بين فقرات اهمية التشفير في حماية البيانات والدرجة الكلية للمحور

	اهمية التشفير في حماية البيانات	معامل الارتباط	مستوى الدلالة
1	هل تعتقد ان التشفير مهم لحماية البيانات	**0.645	0.000
2	هل سبق لك استخدام تطبيقات تعتمد على التشفير	**0.547	0.000
3	التقييم العام [التشفير ضروري في العصر الرقمي]	**0.613	0.000
4	التقييم العام [يجب زيادة التوعية بأهمية التشفير]	**0.486	0.000
5	التقييم العام [المؤسسات في ليبيا تهتم كفاية بأمن البيانات]	**0.523	0.000
6	ما مدى فاعلية التشفير في حماية البيانات من الاختراق	0.476	0.000

يوضح الجدول رقم (3) والذي يضم (6) فقرات أن معاملات الارتباط بين كل فقرة من فقرات البعد الثاني والدرجة الكلية للبعد وهي اهمية التشفير في حماية البيانات ، حيث جاءت كل نتائج فقرات البعد الثاني للمتغير الفرعي الثاني موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الفرعي الثاني زادت فاعلية اهمية التشفير في حماية البيانات. وبذلك تعتبر فقرات هذا البعد يجمع بينها عناصر مشتركة تجعلها أكثر تجانساً وصادقة لما وضعت لقياسه في هذا البعد وبالتالي يعتبر المتغير صادقا لما وضع لقياسه.

وتؤكد النتائج وجود إدراك مرتفع ومترابط لأهمية التشفير في حماية البيانات، حيث ترتبط جميع الفقرات بشكل إيجابي ودال إحصائيًا، مع بروز القناعة بأهمية التشفير كأحد أهم أدوات الأمن الرقمي، رغم وجود تفاوت نسبي في تقييم فعاليته التطبيقية ومستوى الاهتمام المؤسسي به.

3- استخدام التشفير

الجدول رقم (4) معاملات الارتباط بين فقرات مقياس نتائج استخدام التشفير والدرجة الكلية للمقياس.

	نتائج استخدام التشفير	معامل الارتباط	مستوى الدلالة
1	استخدام التشفير [استخدم التشفير لحماية بيانتي]	**0.615	0.000
2	استخدام التشفير [التشفير يقلل الاختراق]	**0.541	0.000
3	استخدام التشفير [المؤسسات التي تستخدم التشفير أكثر أمانا]	**0.631	0.000
4	استخدام التشفير [أشعر بالثقة عند استخدام خدمات تعتمد على التشفير]	**0.545	0.000
5	استخدام التشفير [التشفير يساعد في حماية الخصوصية الرقمية]	**0.496	0.000
6	يساعد التشفير في حماية المعلومات	**0.456	0.000

يوضح الجدول رقم (4) والذي يضم (6) فقرات أن معاملات الارتباط بين كل فقرة من فقرات البعد الثالث والدرجة الكلية للبعد وهي نتائج استخدام التشفير ، حيث جاءت كل نتائج فقرات البعد الثالث موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الثالث زاد نتائج استخدام التشفير. وبذلك تعتبر فقرات هذا البعد يجمع بينها عناصر مشتركة تجعلها أكثر تجانساً وصادقة لما وضعت لقياسه في هذا البعد وبالتالي يعتبر المتغير صادقا لما وضع لقياسه.

وتشير النتائج إلى أن جميع الفقرات ترتبط إيجابيًا بالمتغير الكلي، مما يدل على اتساق داخلي جيد حيث ان أقوى العوامل المرتبطة باستخدام التشفير هي الاستخدام الفعلي للتشفير ودوره في تعزيز أمن المؤسسات بينما الجوانب المرتبطة بحماية الخصوصية وهي الحماية العامة للمعلومات جاءت بدرجة أقل نسبيًا، لكنها لا تزال مؤثرة.

4- الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير

يمكن حساب معامل الارتباط بين كل فقرة من فقرات البعد الرابع والدرجة الكلية للبعد وهي الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير

الجدول رقم (5) معاملات الارتباط بين فقرات مقياس الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير والدرجة الكلية للمقياس.

	الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير	معامل الارتباط	مستوى الدلالة
1	هل تعتقد أن هناك صعوبات في استخدام التشفير؟	**0.743	0.000
2	ماهم التحديات التي تواجه استخام التشفير؟	**0.803	0.000
3	تواجه المؤسسة صعوبة في تطبيق تقنيات التشفير بسبب تعقيدها الفني	**0.638	0.000
4	يؤدي استخدام التشفير إلى بطء في أداء الأنظمة.	**0.883	0.000
5	عدم توفر بنية تحتية تقنية كافية يحد من تطبيق التشفير	*0.528	0.000
6	ضعف الوعي لدى الموظفين بأهمية التشفير يؤثر على استخدامه	**0.860	0.000
7	نقص الكوادر المؤهلة في مجال التشفير يمثل تحديًا كبيرًا.	**0.747	0.000

يوضح الجدول رقم (5) والذي يضم (7) فقرات أن معاملات الارتباط بين كل فقرة من فقرات المتغير الفرعي الرابع والدرجة الكلية للمتغير وهي الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير، حيث جاءت كل نتائج فقرات المحور الفرعي الرابع للمتغير موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير زادت الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير. وبذلك تعتبر فقرات هذا البعد يجمع بينها عناصر مشتركة تجعلها أكثر تجانساً وصادقة لما وضعت لقياسه في هذا البعد وبالتالي يعتبر المتغير صادقا لما وضع لقياسه.

تؤكد نتائج معاملات الارتباط وجود علاقة قوية ودالة إحصائيًا بين مختلف التحديات التي تواجه استخدام التشفير، مما يدل على أن هذه العوامل مترابطة وتشكل منظومة متكاملة تؤثر على مستوى تطبيق التشفير، مع بروز العوامل التقنية والبشرية كأكثر العوامل تأثيرًا.

ثانيا: ثبات اداة الدراسة (الاستبانة)

يقصد بثبات اداة الدراسة، ان تعطي اداة جمع البيانات (الاستبانة) نفس النتائج اذا ما تم استخدامها مرة اخرى، وتحت ظروف مماثلة وقد تم استخدام معامل (ألفا كرونباخ) وذلك من اجل قياس تناسق وثبات الاستبانة لكل محور من محاورها.

تم استخدام طريقة معامل الفا كرونباخ لقياس ثبات الاستبانة لكل محور من محاورها، وكانت معاملات الثبات تتمتع بدلالات ثبات مقبولة لغايات البحث العلمي، حيث وجد ان قيمة معامل الفا كرونباخ للبنود، تقترب من الواحد الصحيح، وبذلك يكون قد تأكد من صدق وثبات الاستبانة، وتكون الاستبانة في صورتها النهائية قابلة للتحليل والنتيجة موضحة في الجدول (6).

الجدول 6 يبين معاملات الثبات للاستبانة باستخدام طريقة الفا كرونباخ

ت	البند	عدد الفقرات	معامل الثبات
1	مستوى المعرفة والإدراك بالتشفير	6	0.729
2	اهمية التشفير في حماية البيانات	6	0.854
3	استخدام التشفير	6	0.798
4	الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير	7	0.821

يتضح من خلال نتائج الجدول (6) أن معاملات الثبات (ألفا كرونباخ) لجميع أبعاد الاستبانة جاءت مرتفعة ومقبولة إحصائيًا، حيث تراوحت القيم بين (0.854 – 0.729)، وهو ما يدل على أن أداة الدراسة تتمتع بدرجة عالية من الاتساق الداخلي والموثوقية.

4.3 عرض وتحليل البيانات الاولية للدراسة

يتناول هذا الجزء عرض وتحليل البيانات الاولية للدراسة وفقا للترتيب التالي :

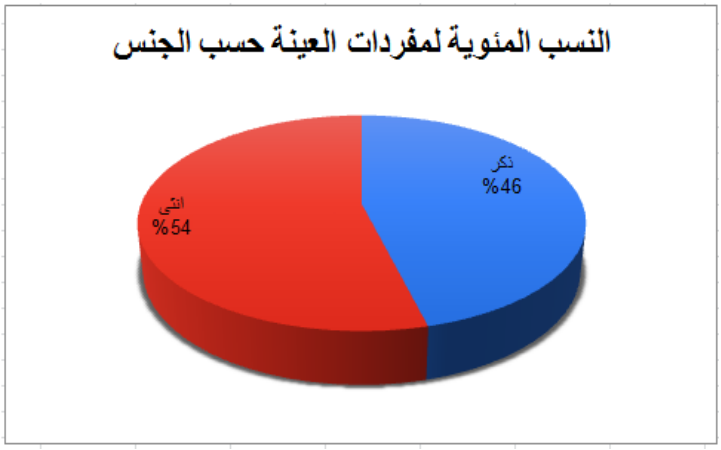
3-4-1 خصائص عينة الدراسة ووصف متغيراتها

اولا: خصائص عينة الدراسة

1- الجنس

ت	الجنس	التكرار	النسبة %
1	ذكر	46	%46
2	انثى	54	%54
المجموع		100	%100

الجدول (7) يبين التوزيع التكراري لمفردات العينة حسب الجنس



الشكل البياني رقم (1) يبين النسبة المئوية لمفردات العينة حسب الجنس

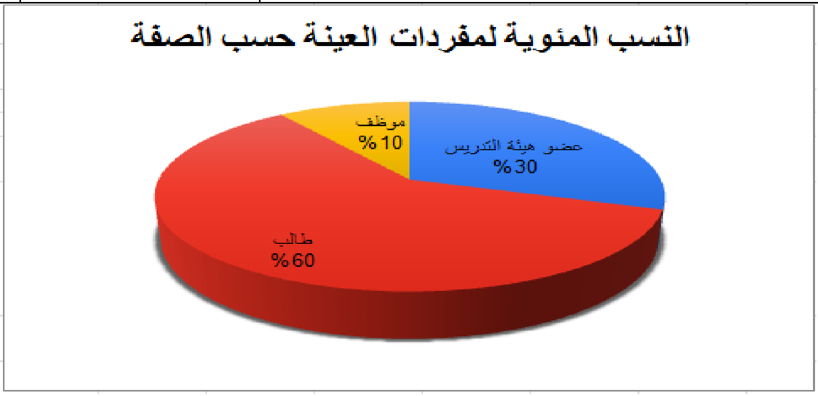
تبين من خلال البيانات الواردة في الجدول والاشكال البيانية السابقة، ان اغلب مفردات عينة الدراسة هم فئة الاناث بنسبة (54%) بينما يشكل فئة الذكور اقل نسبة حيث كانت (46%).

ويعكس هذا التوزيع أن نتائج الدراسة حول دور التشفير في حماية البيانات تمثل وجهات نظر متنوعة لكلا الجنسين، مما يعزز من موضوعية ومصداقية النتائج. كما يدل التقارب بين النسب على أن الوعي باستخدام التشفير وأهميته في حماية البيانات لا يقتصر على فئة معينة، بل هو موضوع مشترك بين الذكور والإناث.

2- الصفة

الجدول (8) يبين التوزيع التكراري لمفردات العينة حسب المستوى الدراسي

الرقم	الصفة	التكرار	النسبة %
1	عضو هيئة التدريس	30	%30
2	طالب	60	%60
3	موظف	10	%10
المجموع		100	%100



الشكل البياني رقم (2) يبين النسب المئوية لمفردات العينة حسب الصفة

يتضح من خلال بيانات الجدول أن غالبية أفراد عينة الدراسة هم من الطلاب بنسبة (60%)، يليهم أعضاء هيئة التدريس بنسبة (30%)، ثم الموظفون بنسبة (10%) ويعكس هذا التوزيع تركّز العينة بشكل أساسي في الفئة الطلابية، مع تمثيل جيد لأعضاء هيئة التدريس، مقابل تمثيل محدود للفئة الإدارية.وتشير النسبة المرتفعة للطلاب (60%) إلى أن النتائج تعكس بدرجة كبيرة وجهة نظر المستخدمين الرئيسيين للأنظمة التعليمية الرقمية، مما يعزز أهمية تقييم مستوى استخدام التشفير من منظور المستخدم النهائي. أما أعضاء هيئة التدريس (30%)، فيمثلون فئة تمتلك وعيًا أكاديميًا وتقنيًا أعلى نسبيًا، مما يساهم في إعطاء تقييم أكثر عمقًا لدور التشفير في حماية البيانات. في حين أن انخفاض نسبة الموظفين (10%) قد يعني ضعف تمثيل الفئة الإدارية، رغم أهميتها في تطبيق السياسات الأمنية وإدارة الأنظمة التقني

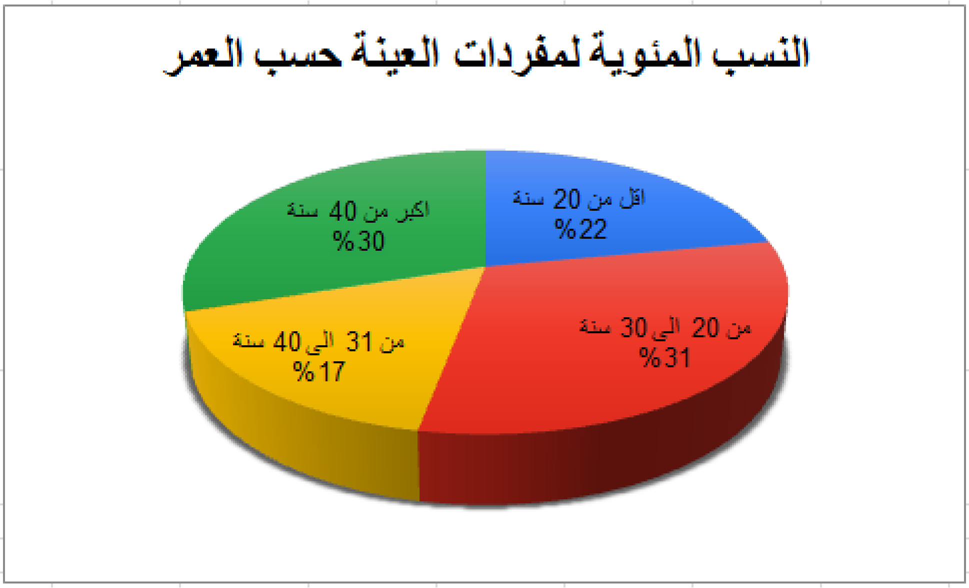
ويوضح توزيع العينة أن نتائج الدراسة حول استخدام التشفير في حماية البيانات تستند بشكل أساسي إلى آراء الطلاب، مع دعم من أعضاء هيئة التدريس، مما يوفر تصورًا جيدًا عن مستوى الوعي والاستخدام، إلا أنه يستدعي الحذر عند تعميم النتائج على الجوانب الإدارية والتقنية نظرًا لانخفاض تمثيل الموظفين.

3-

4- العمر

الجدول (9) يبين التوزيع التكراري والنسب المئوية لمفردات العينة حسب العمر

الرقم	العمر	التكرار	النسبة %
1	اقل من 20 سنة	22	%22
2	من 20 الى 30 سنة	31	%31
3	من 31 الى 40 سنة	17	%17
4	اكبر من 40 سنة	30	%30
المجموع		100	%100



الشكل البياني رقم (3) يبين النسب المئوية لمفردات العينة حسب العمر

يتضح من خلال البيانات الواردة في الجدول أن عينة الدراسة تتوزع على مختلف الفئات العمرية، حيث جاءت الفئة العمرية من 20 إلى 30 سنة في المرتبة الأولى بنسبة (31%)، تليها فئة أكبر من 40 سنة بنسبة (30%)، ثم فئة أقل من 20 سنة بنسبة (22%)، وأخيرًا فئة من 31 إلى 40 سنة بنسبة (17%). ويشير هذا التوزيع إلى وجود تنوع عمري مقبول داخل عينة الدراسة، مما يعزز من مصداقية النتائج ويعكس وجهات نظر مختلفة حول موضوع التشفير وحماية البيانات.

ويمكن تفسير الجدول على ان الفئة (20–30 سنة) تمثل الشريحة الأكثر استخدامًا للتكنولوجيا، وبالتالي يُتوقع أن يكون لديها وعي أكبر بتقنيات التشفير وأهميتها في حماية البيانات. أما الفئة (أكبر من 40 سنة)، والتي تشكل نسبة مرتفعة أيضًا، فمن المحتمل أن تمتلك خبرة عملية وإدارية تساعد في تقييم سياسات التشفير من منظور تنظيمي واستراتيجي. في حين أن الفئة (أقل من 20 سنة) قد تعكس مستوى وعي تقني ناشئ، خاصة في ظل الاستخدام المتزايد للتكنولوجيا الحديثة. أما انخفاض نسبة الفئة (31–40 سنة) فقد يشير إلى ضعف تمثيل هذه الفئة، لكنها تظل فئة مهمة لكونها تجمع بين الخبرة والقدرة التقنية.

5.3 التحليل الاحصائي لمتغيرات الدراسة.

تم استخدم الدراسة اساليب الاحصاء الوصفي (المتوسط الحسابي، الانحراف المعياري) لجميع متغيرات الدراسة، وذلك للتعرف على معدل تواجد كل متغير في عينة الدراسة ومعدل تشتتها، بالإضافة تم تحليل واستخلاص النتائج حول مدى دور تقنيات التشفير في حماية بيانات الطلاب وأعضاء هيئة التدريس من الهجمات السيبرانية في ظل التحول الرقمي للتعليم.

1– **التحليل الوصفي (مستوى المعرفة والإدراك بالتشفير)**

تم احتساب المتوسط الحسابي لكل فقرات المحور الاول معا وكذلك الانحراف المعياري حيث جاءت النتائج على النحو الموضح بالجدول التالي:

الجدول رقم (10) يبين المتوسط الحسابي والانحراف المعياري لمستوى المعرفة بالتشفير

ت	العبارة	المتوسط الحسابي	الانحراف المعياري	مدى التوفر
1	المعرفة بالتشفير " هل لديك معرفة سابقة بمفهوم التشفير"	4,2	0.279	مرتفع

يتضح من خلال نتائج الجدول رقم (10) أن المتوسط الحسابي لعبارة: "هل لديك معرفة سابقة بمفهوم التشفير" بلغ(2،4) بانحراف معياري قدره (0.279)، وقد تم تصنيف مستوى التوفر بأنه مرتفع.

ويشير المتوسط الحسابي (4,2) إلى أن أفراد عينة الدراسة يمتلكون مستوى جيد من المعرفة بالتشفير، مما يعكس وجود إدراك عام بأهمية هذا المفهوم في حماية البيانات. كما أن قيمة الانحراف المعياري (0.279) تُعد منخفضة نسبيًا، مما يدل على تقارب إجابات أفراد العينة وعدم وجود تباين كبير بينهم، أي أن هناك اتفاقًا واضحًا حول مستوى المعرفة بالتشفير.

الجدول رقم (11) يبين المتوسط الحسابي والانحراف المعياري لمستوى الادراك بالتشفير

ت	العبارة	المتوسط الحسابي	الانحراف المعياري	مدى التوفر
1	ادارك دور التشفير في بيئة الكلية (اعتقد أن نظام التعلم في الكلية يستخدم تقنيات التشفير لحماية كلمات المرور)	3.21	0.385	متوسط
2	ادارك دور التشفير في بيئة الكلية [تشعر بالثقة في أن بياناتك الأكاديمية مشفرة ومحمية]	3.44	0.246	مرتفع
3	ادارك دور التشفير في بيئة الكلية [التشفير يقلل بشكل كبير من احتمالية استفادة المخترقين من بيانات الطلاب وهيئة التدريس]	4.12	0.447	مرتفع
4	ادارك دور التشفير في بيئة الكلية [المؤسسات التعليمية التي تعتمد على التشفير المتقدم هي أكثر أمانا	4.55	0.262	مرتفع
5	ادارك دور التشفير في بيئة الكلية [التشفير يساهم في حماية خصوصيتي الرقمية ومنع التلاعب بسجلاتي]	4.19	0.321	مرتفع
المتوسط الحسابي ككل		3.902	0.3322	مرتفع

يتضح من نتائج الجدول رقم (11) أن المتوسط الحسابي العام لمستوى الإدراك بالتشفير بلغ (3.902)بانحراف معياري (0.3322)، وهو ما يشير إلى أن مستوى الإدراك لدى أفراد عينة الدراسة مرتفع، مع وجود درجة جيدة من الاتفاق بين إجاباتهم.

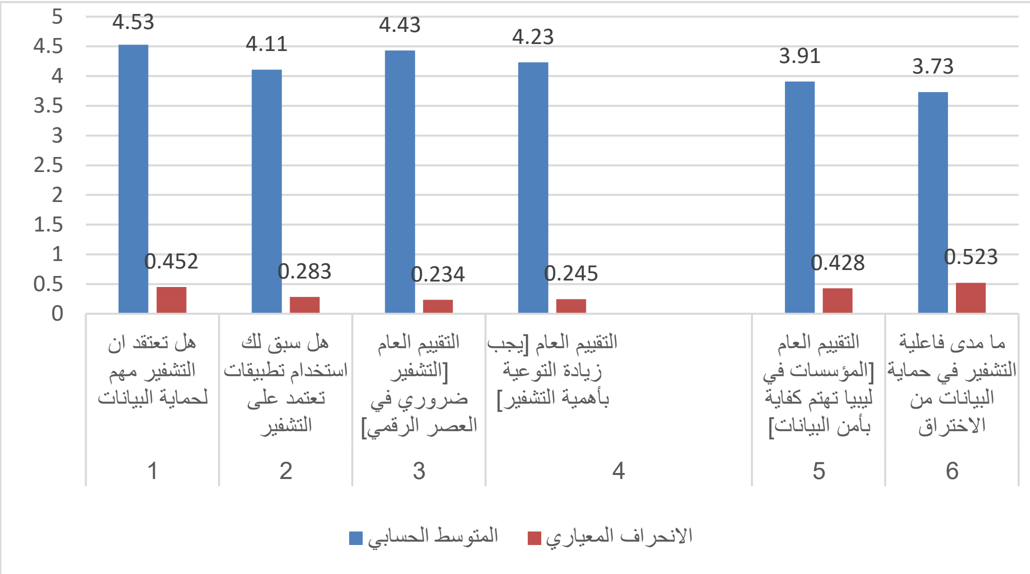
وجاءت الفقرة الأولى بمتوسط حسابي (3.21) وانحراف معياري (0.385) وبمستوى متوسط، مما يدل على أن إدراك المبحوثين لاستخدام الكلية لتقنيات التشفير في حماية كلمات المرور ليس مرتفعًا بشكل كافٍ، وقد يعكس ذلك نقصًا في وضوح أو شفافية الأنظمة التقنية المستخدمة داخل المؤسسة . أما الفقرة الثانية فقد سجلت متوسطًا (3.44) وانحرافًا (0.246)وبمستوى مرتفع، مما يشير إلى أن المبحوثين لديهم ثقة جيدة نسبيًا في أن بياناتهم الأكاديمية مشفرة ومحمية .

وجاءت الفقرة الثالثة بمتوسط (4.12) وانحراف معياري (0.447)، مما يعكس إدراكًا عاليًا لدى أفراد العينة بأن التشفير يحد من استفادة المخترقين من البيانات، وهو مؤشر على وعي أمني متقدم . وسجلت الفقرة الرابعة أعلى متوسط حسابي (4.55) وانحراف (0.262)، مما يدل على اتفاق قوي جدًا بين أفراد العينة على أن المؤسسات التي تعتمد على التشفير

المتقدم تكون أكثر أمانًا، وهو ما يعكس فهمًا نظريًا واضحًا لأهمية التشفير .كما جاءت الفقرة الخامسة بمتوسط (4.19) وانحراف معياري (0.321)، مما يشير إلى إدراك مرتفع لدور التشفير في حماية الخصوصية الرقمية ومنع التلاعب بالبيانات.

2- التحليل الوصفي (اهمية التشفير في حماية البيانات)

تم التحليل الوصفي لمعرفة اهمية التشفير في حماية البيانات، وتم ايجاد المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات المحور الثاني كما موضح بالشكل البياني رقم (4)



الشكل البياني رقم (4) يبين المتوسط الحسابي والانحراف المعياري لأهمية التشفير في حماية البيانات

تُظهر نتائج أن المتوسط الحسابي العام بلغ (4.242) بانحراف معياري (0.3284)، وهو ما يدل على أن مستوى تقييم أفراد عينة الدراسة لأهمية وفاعلية التشفير في حماية البيانات جاء مرتفعًا، مع وجود درجة جيدة من الاتفاق والتقارب في آرائهم.

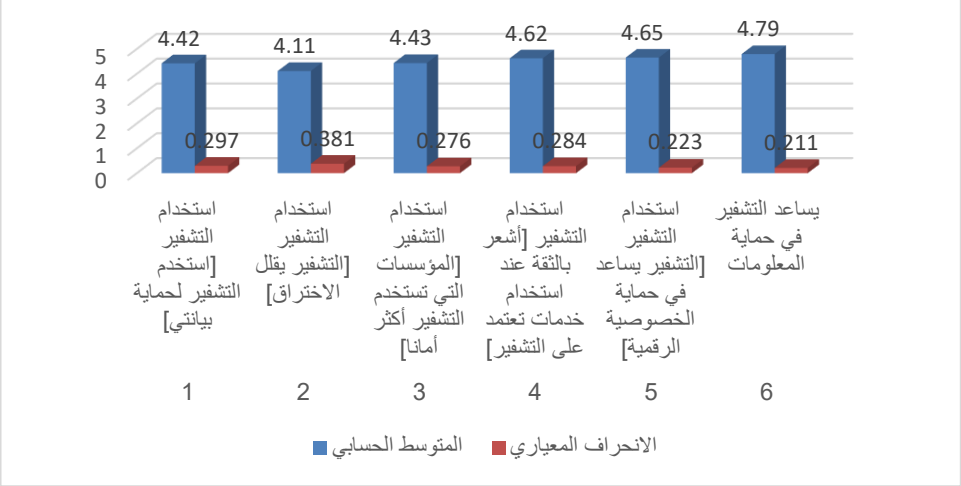
لقد سجلت الفقرة الأولى أعلى متوسط حسابي (4.53) بانحراف معياري (0.452)، مما يشير إلى اتفاق قوي جدًا بين أفراد العينة على أن التشفير عنصر أساسي في حماية البيانات، وهو ما يعكس إدراكًا واضحًا لأهميته. وجاءت الفقرة الثانية بمتوسط (4.11) وانحراف (0.283)، مما يدل على أن غالبية المبحوثين لديهم تجربة فعلية في استخدام تطبيقات تعتمد على التشفير، وهو مؤشر إيجابي على الانتشار العملي لهذه التقنيات. أما الفقرة الثالثة فقد سجلت متوسطًا (4.43) وانحرافًا (0.234)، وهو ما يعكس قناعة راسخة بأن التشفير أصبح ضرورة في العصر الرقمي. كما أظهرت الفقرة الرابعة متوسطًا (4.23) وانحرافًا (0.245)، مما يشير إلى إدراك مرتفع لأهمية تعزيز التوعية بالتشفير، وهو ما يعكس وجود حاجة مستمرة للتثقيف في هذا المجال. وسجلت الفقرة الخامسة متوسطًا (3.91) بانحراف معياري (0.428)، وهو مستوى مرتفع نسبيًا، لكنه أقل مقارنة ببقية الفقرات، مما يدل على أن المبحوثين يرون أن اهتمام المؤسسات في الكلية بأمن البيانات جيد لكنه ليس بالمستوى المطلوب. أما الفقرة السادسة فقد سجلت أدنى متوسط حسابي (3.73) وانحراف (0.523)، مما يشير إلى أن تقييم فاعلية التشفير في الحماية من الاختراق مرتفع ولكن بدرجة أقل، وقد يعكس ذلك وجود بعض الشكوك أو التباين في الآراء حول كفاءته المطلقة.

وتشير النتائج إلى أن أفراد عينة الدراسة يمتلكون وعيًا مرتفعًا جدًا بأهمية التشفير وضرورته في البيئة الرقمية، سواء من حيث الاستخدام أو من حيث القناعة بأهميته في حماية البيانات. وفي المقابل، يظهر تفاوت نسبي في تقييم الفاعلية الفعلية للتشفير ووجود تحفظات حول مستوى اهتمام المؤسسات بأمن البيانات وهذا يعكس فجوة بين الإدراك النظري العالي

و الثقة الكاملة في التطبيق العملي. وتؤكد النتائج أن التشفير يُعد عنصرًا أساسيًا في حماية البيانات من وجهة نظر المبحوثين، مع وجود وعي مرتفع بأهميته، إلا أن هناك حاجة لتعزيز الثقة في فعاليته التطبيقية ورفع مستوى اهتمام المؤسسات بأمن المعلومات.

3- استخدام التشفير

تم التحليل الوصفي لمعرفة الغرض من استخدام التشفير عند عينة الدراسة، وتم ايجاد المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات المحور الثالث. كما موضح بالشكل البياني رقم (5)



الشكل البياني رقم (5) يبين المتوسط الحسابي والانحراف المعياري للمحور استخدام التشفير

تُظهر نتائج أن المتوسط الحسابي العام لمتغير استخدام التشفير بلغ (4.503) بانحراف معياري (0.278)، مما يدل على أن مستوى استخدام التشفير لدى أفراد عينة الدراسة مرتفع جدًا، مع وجود درجة عالية من التجانس والتقارب في الإجابات.

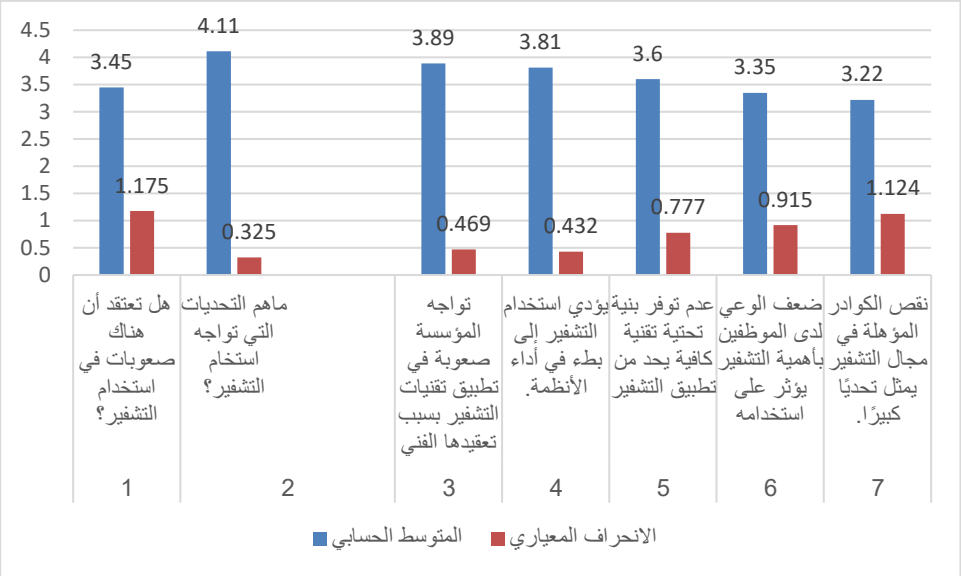
وجاءت الفقرة الأولى بمتوسط (4.42)وانحراف معياري (0.297)، مما يشير إلى أن أفراد العينة يستخدمون التشفير بشكل فعلي لحماية بياناتهم، وهو مؤشر على وعي تطبيقي مرتفع .وسجلت الفقرة الثانية متوسطًا (4.11) وانحرافًا (0.381)، مما يعكس اتفاقًا واضحًا على أن التشفير يساهم في تقليل مخاطر الاختراق. أما الفقرة الثالثة فقد بلغت (4.43) بانحراف (0.276)، مما يدل على إدراك قوي بأن المؤسسات التي تعتمد على التشفير تتمتع بمستوى أمان أعلى. وجاءت الفقرة الرابعة بمتوسط (4.62) وانحراف (0.284)، مما يشير إلى أن التشفير يعزز مستوى الثقة لدى المستخدمين عند التعامل مع الخدمات الرقمية . كما سجلت الفقرة الخامسة متوسطًا (4.65) وانحرافًا (0.223)، مما يعكس إدراكًا عاليًا لدور التشفير في حماية الخصوصية الرقمية. وسجلت الفقرة السادسة أعلى متوسط حسابي (4.79) وانحراف معياري (0.211)، وهو ما يدل على اتفاق شبه كامل بين أفراد العينة على أن التشفير عنصر أساسي في حماية المعلومات .

تشير هذه النتائج بشكل عام إلى أن أفراد عينة الدراسة لا يقتصرون على إدراك أهمية التشفير نظريًا فحسب، بل يمتد ذلك إلى مستوى استخدام فعلي مرتفع، مما يعكس نضجًا في السلوك الرقمي ووعيًا متقدمًا بأمن المعلومات. كما تعكس النتائج أن التشفير يعزز الثقة في الأنظمة الرقمية ويساهم في حماية الخصوصية ويقلل من المخاطر الأمنية

تؤكد النتائج أن استخدام التشفير يُعد ممارسة شائعة وفعالة لدى أفراد العينة، مع وجود مستوى مرتفع جدًا من الثقة في دوره في حماية البيانات والخصوصية، مما يعزز من أهمية تعميم هذه التقنيات في مختلف المؤسسات.

4- التحليل الوصفي (الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير)

لقد استخدمت الباحثتان التحليل الوصفي لمعرفة الصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير وذلك من خلال حساب المتوسط الحسابي والانحراف المعياري حيث كانت النتائج كما موضحة بالشكل البياني (6) على النحو الاتي: -



الشكل البياني (6)يبين المتوسط الحسابي والانحراف المعياري للصعوبات التي تحد من مستوى استخدام التشفير والتحديات التي تواجه التشفير

تشير نتائج هذا البُعد إلى أن أفراد عينة الدراسة يرون وجود مستوى متوسط إلى مرتفع من الصعوبات التي تواجه استخدام التشفير، حيث تراوحت المتوسطات الحسابية بين **(4.11 – 3.22)**، مع تباين ملحوظ في الانحرافات المعيارية، مما يدل على اختلاف وجهات النظر بين المبحوثين.

وجاءت الفقرة العامة "هل تعتقد أن هناك صعوبات في استخدام التشفير؟ "بمتوسط (3.45)وانحراف معياري مرتفع نسبيًا (1.175)، مما يشير إلى تباين واضح في آراء المبحوثين حول وجود هذه الصعوبات وسجلت فقرة "ما هي التحديات التي تواجه استخدام التشفير؟ "أعلى متوسط (4.11) وانحراف (0.325)، وهو ما يعكس اتفاقًا مرتفعًا على وجود تحديات حقيقية تعيق تطبيق التشفير. أما فقرة تعقيد التشفير الفني فقد بلغت (3.89) بانحراف (0.469)، مما يدل على أن الجانب التقني يمثل أحد أبرز العوائق . كما أظهرت فقرة بطء الأنظمة نتيجة التشفير متوسطًا (3.81)، مما يشير إلى وجود تخوفات عملية تتعلق بالأداء . وسجلت فقرة ضعف البنية التحتية التقنية متوسطًا (3.60) وانحرافًا مرتفعًا نسبيًا (0.777)، مما يدل على أن هذه المشكلة موجودة ولكن بدرجات متفاوتة بين المؤسسات . أما فقرة ضعف الوعي لدى الموظفين فقد جاءت بمتوسط (3.35)، مما يشير إلى أن العامل البشري يمثل تحديًا متوسط التأثير. وجاءت فقرة نقص الكوادر المؤهلة بأدنى متوسط (3.22)وانحراف مرتفع (1.124)، وهو ما يعكس اختلافًا كبيرًا في تقييم هذه المشكلة بين المبحوثين. وضحت النتائج أن التحديات التي تواجه استخدام التشفير يمكن تصنيفها إلى تحديات تقنية مثل تعقيد التشفير وتأثيره على أداء الأنظمة، والتحديات تنظيمية والتي ضعف البنية التحتية وغياب الإمكانيات التقنية الكافية

واما تحديات بشرية ضعف الوعي نقص الكفاءات. كما تشير النتائج إلى أن التحديات التقنية هي الأكثر وضوحًا وتأثيرًا، تليها التحديات التنظيمية، ثم البشرية ورغم وجود مستوى مرتفع من الوعي باستخدام التشفير وأهميته، إلا أن هناك مجموعة

من التحديات التقنية والتنظيمية والبشرية التي تعيق التطبيق الكامل والفعال لهذه التقنيات، مما يستدعي تدخلًا متكاملًا لمعالجتها.

النتائج

من خلال التحليل الاحصائي توصل الباحثتان الى الاجابة على تساؤل الدراسة من خلال التحليل الاحصائي حيث تبين ان هناك دور كبير للتشفير في حماية البيانات والحد من الهجمات السبرانية وترى الباحثتان بان من المميزات هذه الدراسة هو التفاعل الذي تم مع عينة الدراسة اثناء جمع البيانات والنقاشات التي تمت حول تناول ابعاد جديدة في المستقبل تتم دراستها .

بعد ان قامت الباحثتان بجمع البيانات وعرضها وتحليلها فان الباحثتان قد توصلتا في هذه الدراسة الى مجموعة من النتائج تتخلص في النقاط الاتية :-

1- أثبتت الدراسة وجود علاقة إيجابية قوية بين استخدام التشفير ومستوى حماية البيانات، مع وجود وعي مرتفع بأهميته، يقابله بعض التحديات التقنية والبشرية التي تحد من التطبيق الكامل له.
2- أظهرت النتائج وجود مستوى مرتفع من المعرفة والإدراك بالتشفير لدى أفراد العينة.
3- تبيّن أن المعرفة الأساسية بالتشفير تُعد عاملًا رئيسيًا في تعزيز الإدراك الأمني.
4- اظهرت النتائج وجود تحديات حقيقية تواجه استخدام التشفير رغم ارتفاع أهميته. وكانت التحديات التقنية والبشرية كانت الأكثر تأثيرًا.
5- وجود توازن نسبي بين الذكور والإناث مما يعزز موضوعية النتائج كما ان أغلب افراد العينة من الطلاب، مما يعكس الجانب التطبيقي والاستخدامي للتشفير.
6- تؤكد النتائج أن الاستخدام الفعلي للتشفير مرتبط بتحسين أمن المعلومات.
7- اظهرت النتائج ان التشفير يعزز الثقة والخصوصية والحماية من الاختراق.
8- اظهرت النتائج الى وجود إدراك مرتفع جدًا لأهمية التشفير كما يُنظر إليه كـ ضرورة في العصر الرقمي وليس خيارًا.

التوصيات

1. التوصيات التقنية (البنية التحتية):اعتماد بروتوكولات التشفير الحديثة: ضرورة انتقال المؤسسات التعليمية من أنظمة التشفير القديمة إلى معايير التشفير المتقدمة مثل (AES-256) لحماية قواعد البيانات الساكنة، وتفعيل بروتوكول (TLS 1.3) لتأمين البيانات أثناء انتقالها عبر المنصات التعليمية.تطبيق المصادقة الثنائية (FA2): عدم الاكتفاء بتشفير كلمات المرور فقط، بل إلزام أعضاء هيئة التدريس والطلاب باستخدام المصادقة الثنائية لضمان عدم اختراق الحسابات حتى في حال تسرب بيانات الدخول.

2. التوصيات التنظيمية والإدارية:صياغة سياسة خصوصية واضحة: يجب على الكلية والمؤسسة التعليمية نشر وثيقة "سياسة حماية البيانات" توضح للمستخدمين (طلاب وموظفين) أنواع التشفير المستخدمة وكيفية حماية بياناتهم، لتعزيز الثقة الرقمية التي أظهرت الدراسة أهميتها .تخصيص ميزانية للأمن السيبراني: التوصية بزيادة الدعم المالي لتحديث السيرفرات (Servers) والأنظمة القديمة (Legacy Systems) التي أشار البحث إلى أنها تمثل ثغرة أمنية كبيرة.

3. التوصيات البشرية (التوعية والتدريب):برامج تدريبية متخصصة: تنظيم دورات دورية ليست "عامة" بل "تقنية" للموظفين والإداريين حول كيفية التعامل مع البيانات المشفرة وتجنب هجمات التصيد الاحتيالي (Phishing) التي تستهدف تجاوز التشفير .دمج الثقافة الرقمية: إدراج وحدة تعليمية مصغرة ضمن مقررات الحاسوب للطلاب الجدد تتناول "أمن المعلومات الشخصية" وكيفية حماية ملفاتهم الأكاديمية.

4. التوصيات المستقبلية (للباحثين):

- توسيع نطاق الدراسة: إجراء دراسات مقارنة بين الجامعات الليبية لتقييم مدى التباين في جاهزية الأمن السيبراني.
- دراسة الأثر القانوني: بحث التشريعات **الليبية المنظمة لحماية البيانات الرقمية ومدى مواءمتها للتحول الرقمي السريع في قطاع التعليم**.

المراجع العربية

–الحربي، م. (2019). بناء استراتيجيات مؤسسية للأمن السيبراني لدعم التحول الرقمي في مؤسسات التعليم العالي وضمان استمراريته. مجلة الدراسات التربوية والإدارية، 15(2)، 45–68.

–الحربي، (2021). جاهزية المؤسسات التعليمية للأمن السيبراني في ظل جائحة كورونا. (دراسة وصفية تحليلية).

–السلمي، (2020). اختراق الأنظمة الأكاديمية وآثاره على السجلات الدراسية للطلاب. (دراسة وصفية).

–العربي، أ. (2021). الأمن السيبراني: المفاهيم الأساسية وأمن الشبكات والمنصات الرقمية. دار النشر والتوزيع الأكاديمي.

–العتيبي، ف. (2021). أثر تطبيق سياسات الأمن السيبراني على رفع ثقة الطلاب في استخدام أنظمة التعليم الإلكتروني في الجامعات السعودية. مجلة بحوث التعليم العالي، 33(1)، 112–134.العمري، (2023). التحول الرقمي في التعليم العالي وتأثيره على خصوصية البيانات الأكاديمية. (دراسة وصفية مسحية).

–عياد، ر. (2020). جاهزية البنية التحتية الأمنية كعائق أمام تبني التعليم الإلكتروني في الجامعات العربية وانعكاسها على جودة الخدمات. مجلة تكنولوجيا التعليم، 28(4)، 89–110.

–الغرياني، س. (2022). حماية البيانات وأمن المعلومات في المؤسسات الحديثة: نحو بيئة رقمية آمنة. مركز النشر العلمي بالجامعات.

–الموسوي، ع. (2018). الارتباط بين تطبيق معايير الأمن السيبراني وجودة التعليم الإلكتروني وفق نظام ضمان الجودة الشامل. مجلة البحوث الأكاديمية، 12(3)، 77–98.

–الميعة، م. أ، الخسافنة، أ، والثنيبات، أ. (2020). التحديات الحرجة والعوامل المؤثرة على استخدام نظام التعليم الإلكتروني خلال جائحة كوفيد–19. مجلة تقنيات التعليم والمعلومات، 25(6)، 5261–5280.

المراجع الأجنبية

–Aldawood, H., & Skinner, G. (2019). Educating and raising awareness on cybersecurity within educational institutions. Information and Computer Security, 27(3), 316-329.

-Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing factors affecting student adoption and usage of cloud computing: A systematic review of challenges and solutions. International Journal of Information Management, 37(3), 245-256.

-AlHogail, A. (2018). Improving cybersecurity awareness in higher education: A conceptual framework. Journal of Information Security and Applications, 40, 157–164.

-Almaiah, M., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. Education and Information Technologies, 25(6), 5261-5280.

-Ali, A., & Hassan, N. (2020). The role of cybersecurity in enhancing trust in digital services and supporting sustainable development. Journal of Digital Security, 4(1), 22-35.

-Chen, et al. (2023). Ransomware Attacks on Educational Institutions: Vulnerabilities and Mitigation. (Case Study).

-González-Zamar, M. D., Abad-Segura, E., López-Meneses, E., & Gómez-Galán, J. (2020). Managing ICT for sustainable education: An overview in the context of higher education. Sustainability, 12(19), 8254.

-Ifinedo, P. (2021). Examining students' perception of e-learning cybersecurity, trust, and satisfaction. Education and Information Technologies, 26(4), 4567–4585.
-Johnson, C. (2021). Cybersecurity: Principles, practices, and predictive intelligence for digital environments. Wiley Publications.
- Lee, & Johnson. (2022). Privacy Policies in E-Learning Platforms: A Critical Analysis. (Content Analysis).
-Miranda, J., et al. (2021). The core components of education 4.0 in higher education: Three case studies in engineering education. Computers in Human Behavior, 119, 106715.
-Sharma, & Kumar. (2022). Performance Evaluation of AES and DES Algorithms in Cloud-Based Educational Systems. (Experimental Study).
-Smith, R. (2019). Cybersecurity and critical infrastructure protection: National strategies and legal frameworks. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 12-25.