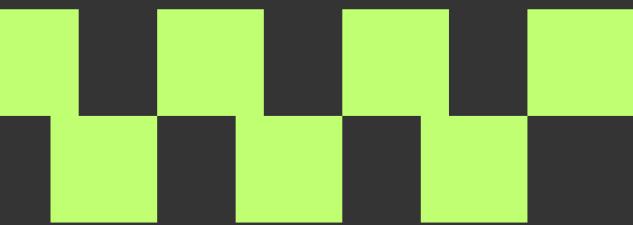
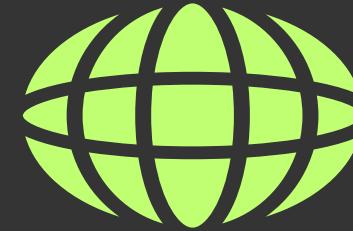
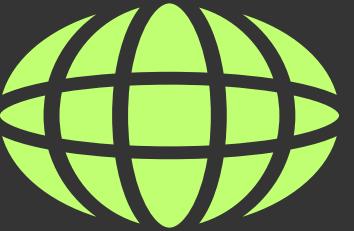
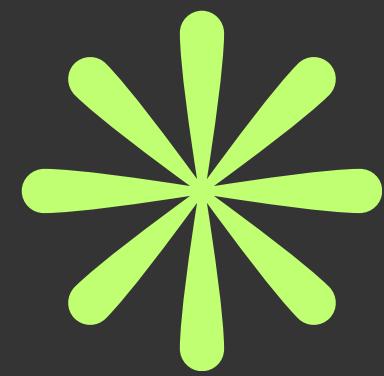


الدرس الثالث
الأمن السيبراني
CYBER SECURITY



عناصر الدرس

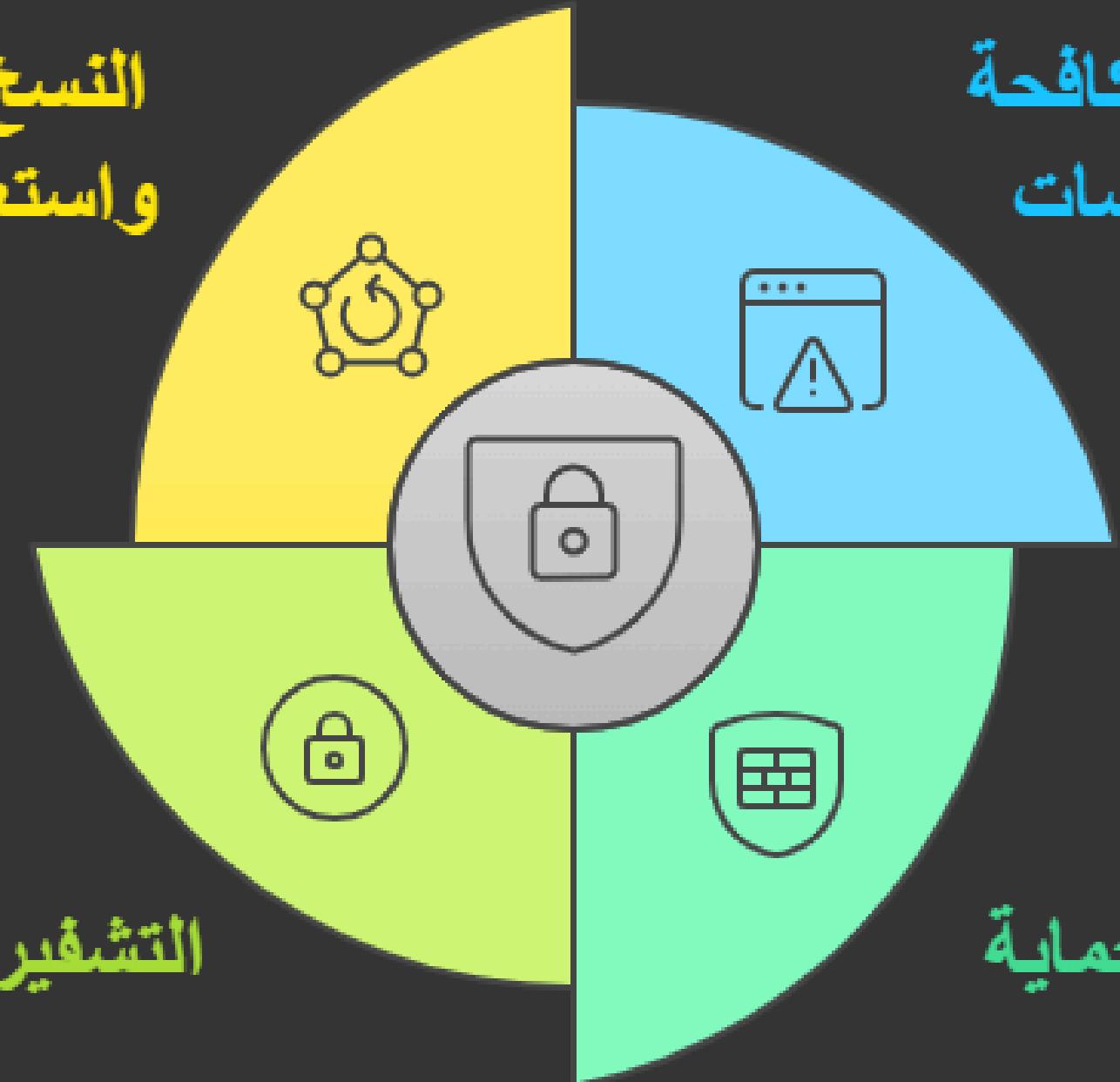


النسخ الاحتياطي
واستعادة البيانات

التشفير

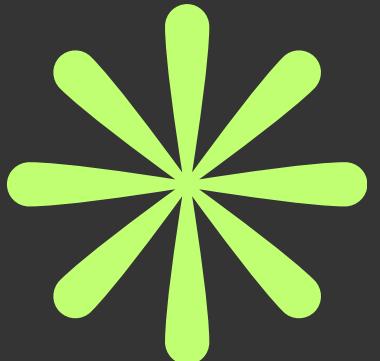
برامج مكافحة
الفيروسات

جدران الحماية



برامج مكافحة الفيروسات (Antivirus Software)

برامج مكافحة الفيروسات هي أدوات أو تطبيقات تُستخدم لحماية أجهزة الكمبيوتر والهواتف الذكية من البرمجيات الخبيثة (Malware) مثل:

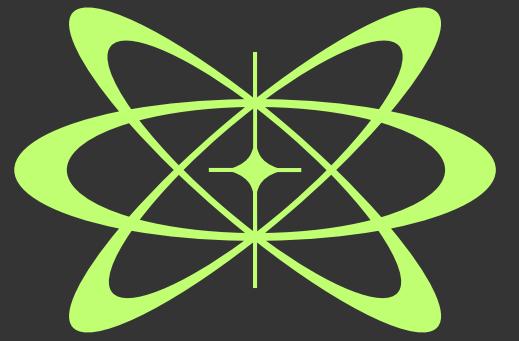


- الفيروسات (Viruses)
- الديدان (Worms)
- أحصنة طروادة (Trojans)
- برامج التجسس (Spyware)
- برامج الفدية (Ransomware)

تُعد برامج مكافحة الفيروسات الخط الأول في الدفاع عن الأجهزة ضد البرمجيات الخبيثة.

وظيفتها الرئيسية هي اكتشاف، وحذف، ومنع البرمجيات الضارة من التسلل إلى النظام.

وتعمل من خلال فحص الملفات والبرامج بشكل دوري، ومراقبة السلوك غير الطبيعي للأنظمة.



وظائف برامج مكافحة الفيروسات

المراقبة في الوقت الحقيقي (Real-time Protection)

راقب كل الأنشطة التي تتم على الجهاز لحظة بلحظة، ويمنع أي محاولة لاختراق أو تثبيت ملف ضار.

العزل (Quarantine)

عندما يكتشف البرنامج ملفاً مشبوهاً، يعزله في مكان آمن حتى يقرر المستخدم ما إذا كان سيرذفه أو يستعيده.

الفحص (Scanning)

يقوم البرنامج بفحص ملفات النظام، والبرامج المثبتة، والأقراص الخارجية بحثاً عن أي أ Kovad أو ملفات ضارة.

التحديث التلقائي (Automatic Updates)

لأن الفيروسات تتطور باستمرار، يقوم البرنامج بتحديث قاعدة بياناته بانتظام للتعرف على أحدث أنواع التهديدات.

أنواع برامج مكافحة الفيروسات

البرامج المدفوعة (Paid) (Antivirus)

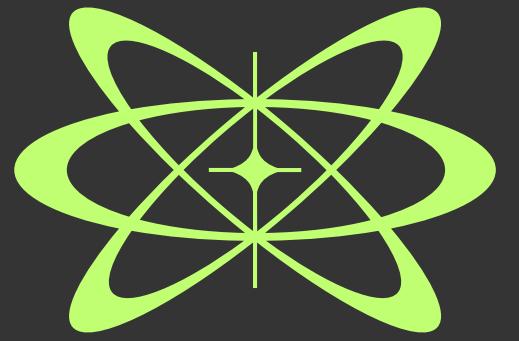
تقدم حماية شاملة تشمل الإنترن特 والبريد الإلكتروني والشبكة، مثل:

- Kaspersky Internet Security
- Bitdefender Total Security
- Norton Antivirus
- McAfee Security

البرامج المجانية (Free) (Antivirus)

تقدم حماية أساسية فقط ضد الفيروسات الشائعة، مثل:

- Windows Defender (موجود في نظام ويندوز)
- Avast Free Antivirus



أهمية برامج مكافحة الفيروسات لطلاب تكنولوجيا التعليم

1. حماية الأجهزة التعليمية من الملفات المصابة أثناء تحميل البرامج أو المشاريع.
2. تأمين البيانات الشخصية والمشروعات البحثية من السرقة أو التلف.
3. ضمان استمرار عمل المنصات التعليمية دون تعطيل أو اختراق.
4. زيادة الوعي بأهمية الأمان الرقمي في بيئات التعلم الإلكتروني.

ما هو جدار الحماية (Firewall)

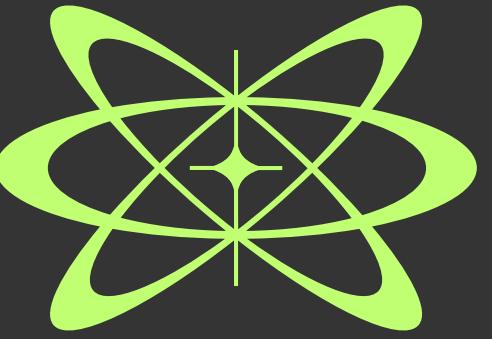
جدار الحماية هو برنامج أو جهاز يُستخدم للتحكم في تدفق حركة البيانات (Traffic) بين شبكتين — عادةً بين شبكة داخلية آمنة (زي شبكة المدرسة أو البيت) والإنترنت الخارجي.

وظيفته الأساسية هي السماح أو منع الاتصالات بناءً على مجموعة من القواعد والسياسات الأمنية المحددة مسبقاً.

بمعنى أبسط:

جدار الحماية يعمل مثل "حارس البوابة" الذي يراقب كل ما يدخل ويخرج من الشبكة، ويعمل أي اتصال مشبوه أو غير مصرح به.





طريقة عمل جدار الحماية



عندما يحاول أي برنامج أو جهاز الاتصال بالإنترنت، يقوم جدار الحماية بما يلي:

يفحص كل طلب اتصال (Packet) يدخل أو يخرج من الجهاز أو الشبكة.

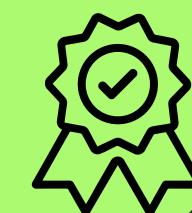


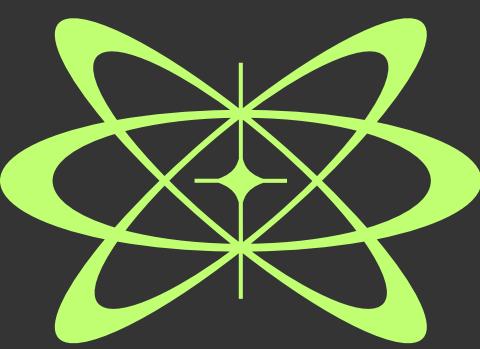
يقارن هذا الطلب بالقواعد المحددة مسبقاً (مثلاً: السماح لمتصفح الإنترنت، منع برامج غير معروفة).



طريقة عمل جدار الحماية

يقرر السماح أو المنع بناءً على ما إذا كان الاتصال آمناً أم لا.





أنواع جدران الحماية

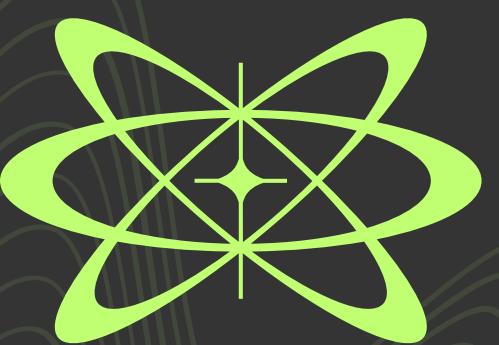


جدار الحماية المادي (Firewall)

- هاز مستقل يُركب بين الشبكة الداخلية والمودم أو الراوتر.
- يحمي مجموعة أجهزة أو شبكة كاملة في وقت واحد.
- يُستخدم في المؤسسات والجامعات والمراكز الكبيرة.

جدار الحماية البرمجي (Firewall)

- يثبت داخل نظام التشغيل على جهاز الكمبيوتر.
- يحمي الجهاز الفردي من الاتصالات المشبوهة.
- مثال: Windows Defender .ZoneAlarm Firewall
- يُستخدم عادة في المنازل والمدارس أو الأجهزة الشخصية.

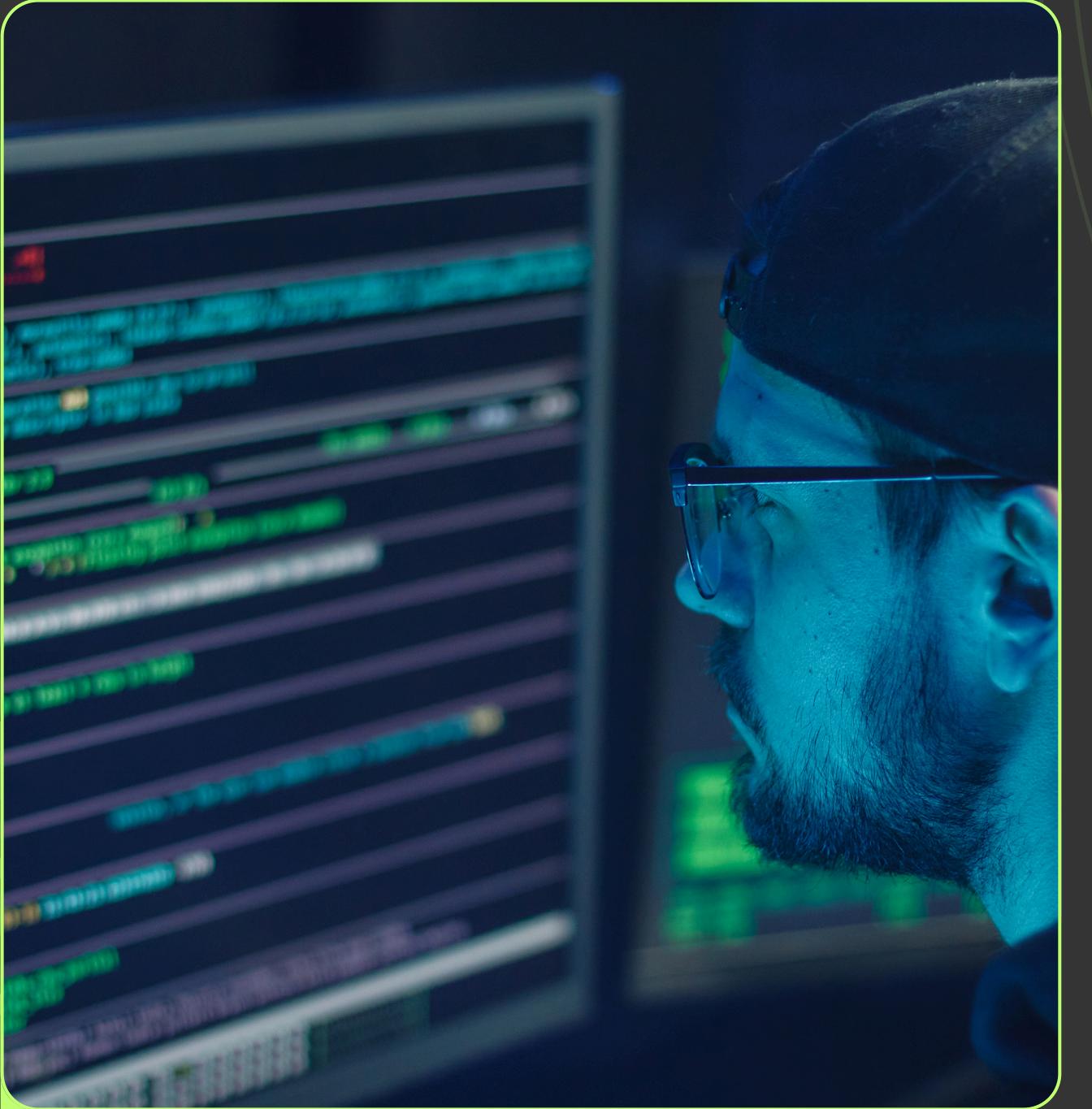


أهمية جدار الحماية في بيئات التعليم الإلكتروني



1. حماية أجهزة المعلمين والطلاب من الهجمات الخارجية أثناء استخدام الإنترنت أو المنصات التعليمية.
2. منع المواقع الضارة أو غير التعليمية داخل شبكة المدرسة أو الجامعة.
3. مراقبة حركة البيانات لتجنب تسرب المعلومات أو دخول برمجيات خبيثة.
4. ضمان استقرار الشبكة وعدم انقطاع الخدمات التعليمية الإلكترونية.
5. توفير بيئة تعلم رقمية آمنة تحمي خصوصية الطالب والملفات الدراسية.

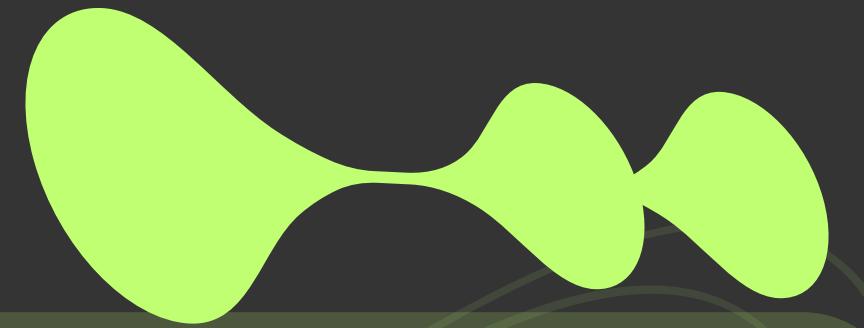
التشفير (Encryption)



التشفير هو عملية تحويل البيانات أو المعلومات من شكلها المقرؤء والمفهوم (Plain Text) إلى شكل غير مفهوم أو رموز مشفرة (Cipher Text)، بحيث لا يمكن لأي شخص غير مخول قراءتها أو استخدامها إلا إذا كان يمتلك مفتاح فك التشفير (Decryption Key) يُستخدم في حماية الرسائل، والملفات، والمعاملات الإلكترونية.

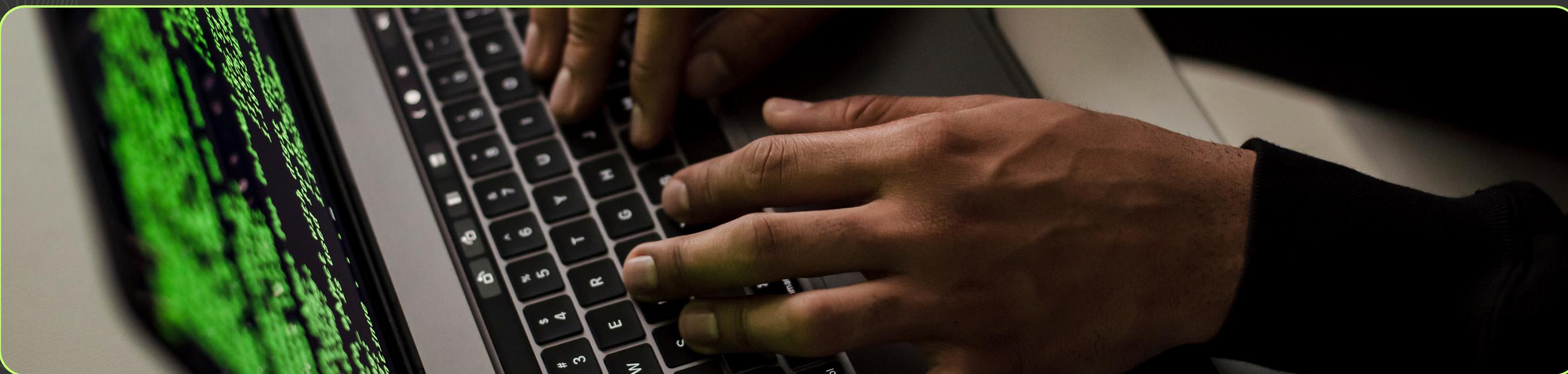
بمعنى بسيط:
التشفير يجعل البيانات "مغلقة" بمفتاح رقمي، ولا يستطيع فتحها أو فهمها إلا الشخص الذي يملك هذا المفتاح.

كيف يعمل التشفير؟



1. المستخدم يكتب أو يرسل معلومة عادية مثل كلمة سر أو رسالة.
2. خوارزمية التشفير تقوم بتحويل هذه المعلومة إلى رموز غير مفهومة.
3. يرسل النص المشفر عبر الإنترنت أو يخزن في النظام.
4. عند وصوله إلى الشخص المصرح له، يتم فك التشفير باستخدام مفتاح خاص ليعود النص إلى حالته الأصلية.

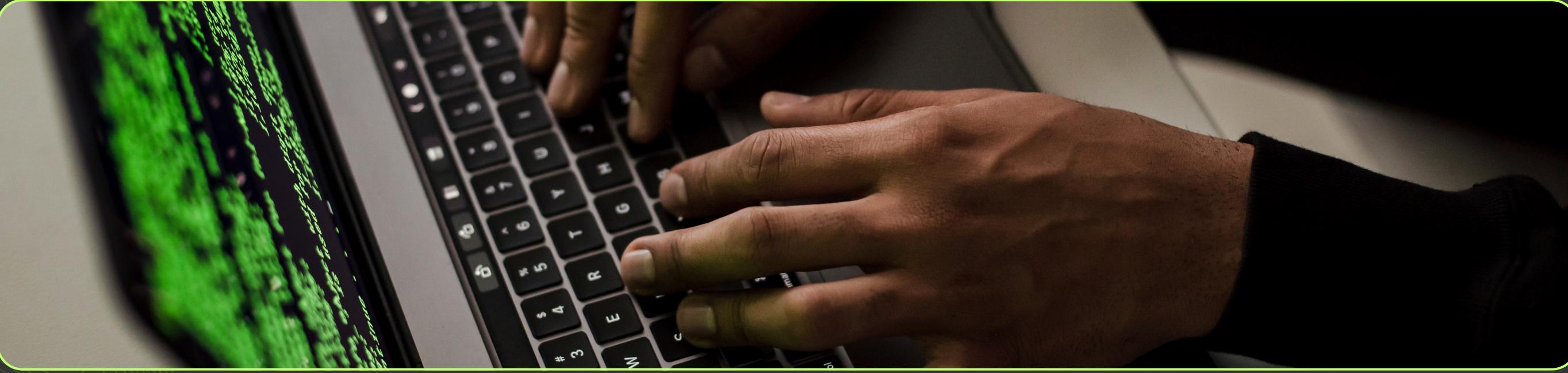
العملية تشمل مراحلتين أساسيتين



فك التشفير
(Decryption)

التشفير (Encryption)

أنواع التشفير

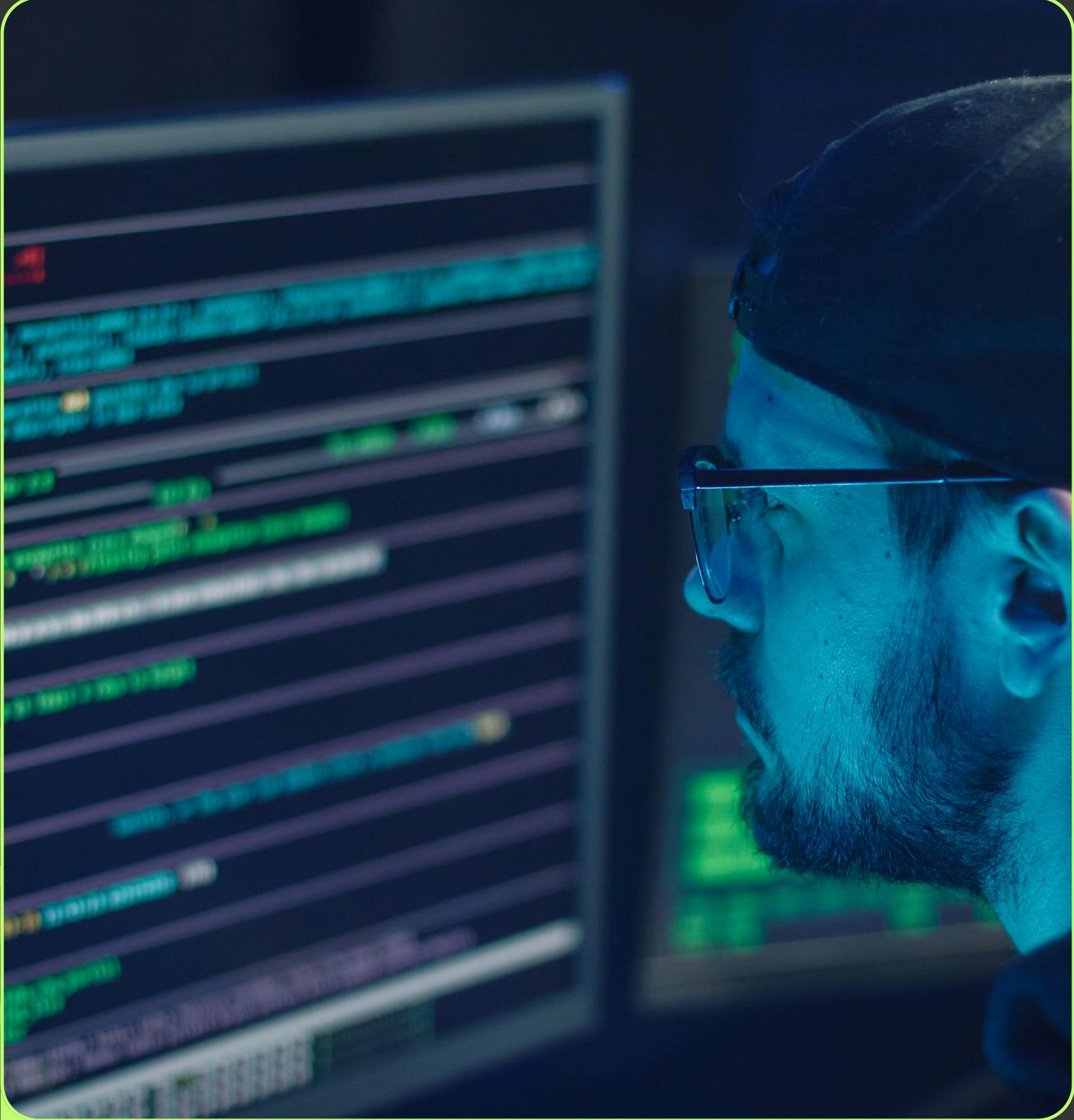


التشفيـر غير
المتماثـل
Asymmetric)
(Encryption

التشـفـير المـتمـاثـل
Symmetric)
(Encryption

التشغیر المتماثل (Encryption)

Symmetric



1. يستخدم نفس المفتاح في عملية التشفير وفك التشفير.

2. سريع في الأداء، لكنه أقل أماناً إذا تم تسريب المفتاح.

3. مثال: خوارزمية AES (Advanced Encryption Standard)

مثال: إذا أرسلت ملفاً مشفرًا بكلمة مرور، فالشخص الآخر يحتاجنفس الكلمة لفك التشفير. 

التشغيل غير المتماثل (Encryption)



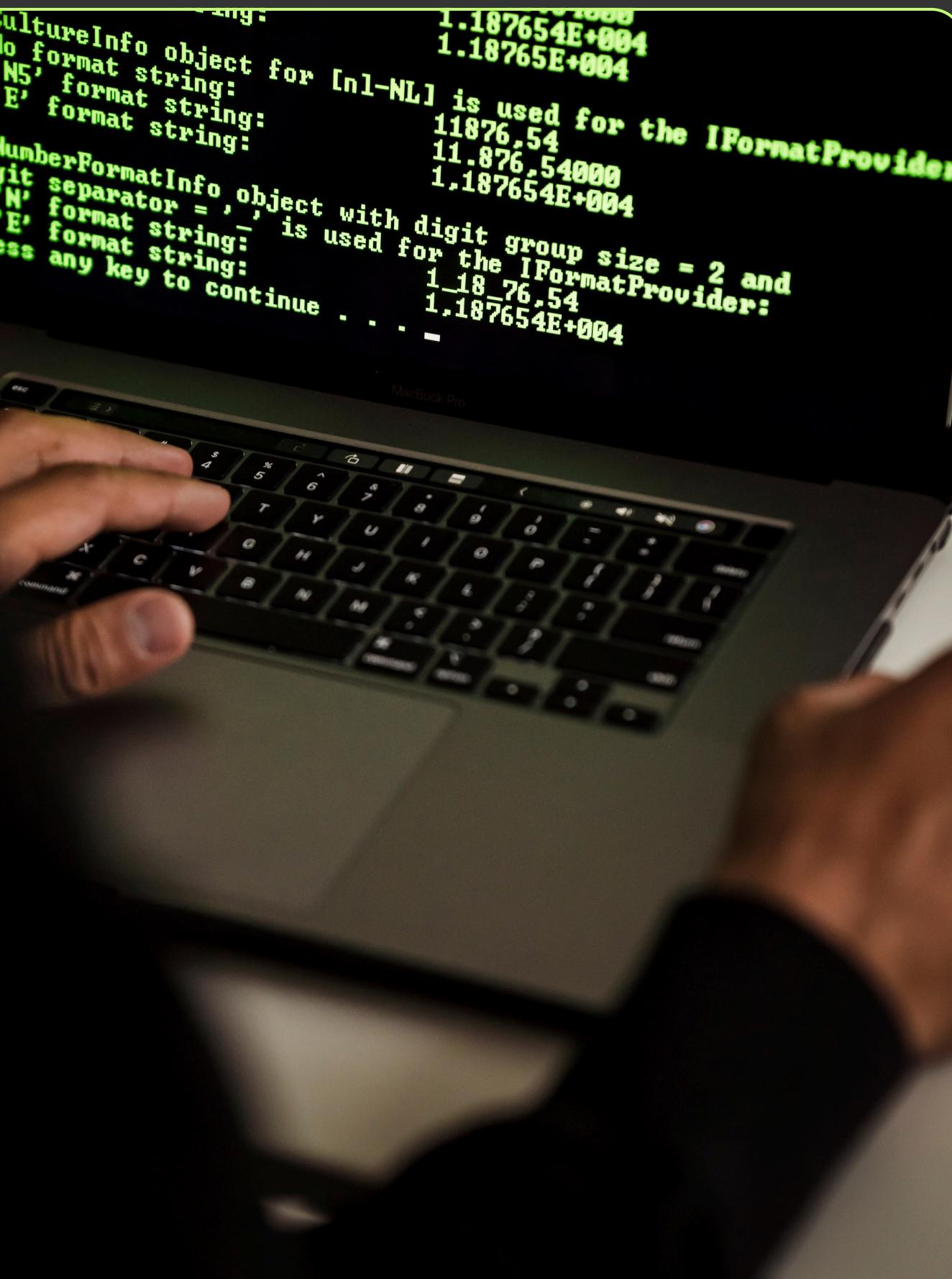
- يعتمد على مفتاحين مختلفين:
- مفتاح عام (Public Key): يُستخدم لتشغيل البيانات.
- مفتاح خاص (Private Key): يُستخدم لفك التشفير.
- حتى لو عرف أحد المفتاح العام، لا يمكنه فك التشفير بدون المفتاح الخاص.
- مثال: تشفير البريد الإلكتروني، وتشغيل المواقع (HTTPS).
- مثال: عند الدخول لموقع يبدأ بـ `https://`, فإن بياناتك تُشفّر باستخدام المفتاح العام للموقع، ولا يمكن لأحد قراءتها إلا الخادم الذي يملك المفتاح الخاص.

أهمية التشفير في بيئة التعليم الإلكتروني

1. حماية بيانات الطلاب والمعلمين مثل الدرجات والمشروعات والرسائل الإلكترونية.
2. منع سرقة أو تعديل الملفات التعليمية أثناء إرسالها أو تخزينها على المنصات الإلكترونية.
3. ضمان سرية الاتصالات داخل أنظمة إدارة التعليم (LMS) مثل Moodle أو Blackboard.
4. الحفاظ على الخصوصية الرقمية للطلاب للنavigating the internet أو استخدام الذكاء الاصطناعي التعليمية.
5. تأمين عمليات الدفع الإلكتروني في حالة شراء مواد تعليمية أو اشتراكات رقمية.



أمثلة واقعية على التشفير



- عند رفع اختبار إلكتروني إلى منصة تعليمية، يُشفر الملف تلقائياً حتى لا يتمكن أي طالب من الإطلاع عليه قبل الموعود المحدد.
- تطبيقات مثل Zoom Meeting تسخدم التشفير لحماية المحادثات من أي محاولة تجسس أو تسجيل غير مصرح.
- عند إرسال مشروع بحثي عبر البريد الإلكتروني، يمكن حمايته بكلمة مرور أو ملف مضغوط مشفر.

النسخ الاحتياطي واستعادة البيانات (Backup & Recovery)



النسخ الاحتياطي هو تخزين نسخة من البيانات في مكان آمن لاستخدامها عند فقدان البيانات الأصلية بسبب أخطاء أو هجمات إلكترونية. ويُعتبر من أهم مكونات الأمن السيبراني لأنه آخر وسيلة لحماية البيانات بعد وقوع الحوادث.

أنواع النسخ الاحتياطي



1. **نسخ محلي (Local Backup):** تخزين على أقراص صلبة خارجية أو أجهزة USB.
2. **نسخ سحابي (Cloud Backup):** تخزين على الإنترنت عبر خدمات مثل Google Drive, OneDrive.
3. **نسخ تلقائي (Automated Backup):** يتم بشكل دوري دون تدخل المستخدم.

نحوان النسخ الاحتياطي الآمن



1. تحديد الملفات المهمة.
2. اختيار وسيلة تخزين آمنة.
3. جدولة عملية النسخ بشكل أسبوعي أو يومي.
4. اختبار عملية الاستعادة للتأكد من سلامة النسخ.

THANK YOU

