السؤال الأول: معايير تصنيف خوارزميات التشفير

تصنف خوارزميات التشفير بناءً على عدة معايير، منها:

- **نوع المفتاح المستخدم:**
  - **التشفير المتماثل (Secret Key Cryptography):** يستخدم نفس المفتاح لتشفير وفك تشفير البيانات.
  - **التشفير غير المتماثل (Public Key Cryptography):** يستخدم مفتاحين مختلفين، أحدهما للتشفير والآخر لفك التشفير.
- **طريقة التشفير:**
  - **التشفير بالتعويض (Substitution Cipher):** يستبدل كل حرف أو مجموعة حروف بحرف أو رمز آخر.
  - **التشفير بالإبدال (Transposition Cipher):** يعيد ترتيب الحروف أو مجموعات الحروف في النص الأصلي.
  - **التشفير بالتدفق (Stream Cipher):** يشفر البيانات بتدفق مستمر من المفاتيح.
  - **تشفير الكتل (Block Cipher):** يقسم البيانات إلى كتل متساوية الحجم ويشفر كل كتلة على حدة.
- **مستوى الأمان:**
  - **خوارزميات قوية:** توفر مستوى عالٍ من الأمان، ويصعب كسرها.
  - **خوارزميات ضعيفة:** توفر مستوى أمان منخفض، ويمكن كسرها بسهولة.
- **كفاءة الخوارزمية:**
  - **سرعة التشفير وفك التشفير:** بعض الخوارزميات أسرع من غيرها.
  - **استهلاك الموارد:** بعض الخوارزميات تستهلك موارد أكثر من غيرها (مثل الذاكرة والمعالج).

السؤال الثاني: الفرق بين التشفير بالتعويض والإبدال مع أمثلة

- **التشفير بالتعويض:** يتم فيه استبدال كل حرف أو مجموعة حروف بحرف أو رمز آخر.
  - **مثال:** شيفرة قيصر، حيث يتم إزاحة كل حرف بعدد معين من المواقع في الأبجدية.
- **التشفير بالإبدال:** يتم فيه إعادة ترتيب الحروف أو مجموعات الحروف في النص الأصلي دون تغييرها.
  - **مثال:** شيفرة سكة الحديد، حيث يتم كتابة النص الأصلي في شكل سكة حديد، ثم قراءته بطريقة أخرى للحصول على النص المشفر.

السؤال الثالث: مقارنة بين تشفير الكتل وتشفير التدفق

وجه المقارنة	تشفير الكتل	تشفير التدفق
الأمان	يعتبر أكثر أمانًا بشكل عام، خاصة مع استخدام خوارزميات قوية ومفاتيح طويلة.	أقل أمانًا بشكل عام، ويمكن أن يكون عرضة لهجمات معينة إذا لم يتم استخدامه بشكل صحيح.
آلية التشفير	يقسم البيانات إلى كتل متساوية الحجم ويشفر كل كتلة على حدة.	يشفر البيانات بتدفق مستمر من المفاتيح، حرفًا بحرف أو بت.
الوقت المستهلك	قد يكون أبطأ من تشفير التدفق بسبب الحاجة إلى تقسيم البيانات إلى كتل.	أسرع من تشفير الكتل، حيث يتم تشفير البيانات بشكل مستمر دون الحاجة إلى تقسيمها.
البساطة	يعتبر أكثر تعقيدًا من تشفير التدفق، ويتطلب فهمًا أعمق لآلية التشفير.	يعتبر أبسط من تشفير الكتل، ويمكن تنفيذه بسهولة.

التصدير إلى "جداول بيانات Google"

السؤال الرابع: تشفير النص "My School is my second home"

- **شيفرة قيصر (إزاحة -٦):**
  - يتم إزاحة كل حرف ٦ مواقع إلى اليسار في الأبجدية.
  - النص المشفر: "Iw Njxxchj wn iw mxayhx hxca"
- **شيفرة تبديل سياج السكة الحديدية (٤ أسطر):**
  - يتم كتابة النص الأصلي في شكل سكة حديد بأربعة أسطر.
  - ثم يتم قراءة النص المشفر من خلال قراءة الأسطر بالتتابع.
  - النص المشفر: "MYSCH O LSIYEC ODHSCONMEO"

السؤال الخامس: فك تشفير النص "LOLNH ILQH DUWV"

- **شيفرة قيصر (إزاحة -٣):**
  - يتم إزاحة كل حرف ٣ مواقع إلى اليمين في الأبجدية.
  - النص المفكك: "KOKMG HKPG XURV"

السؤال الأول: المقارنة بين طرق التشفير المختلفة

يمكنك اتباع الخطوات التالية لإنشاء إنفوجرافيك باستخدام Canva:

1. **البحث وجمع المعلومات:** ابحث عن طرق التشفير المختلفة التي تعلمتها في الدرس، مثل:
   - التشفير المتماثل (DES, AES)
   - التشفير غير المتماثل (RSA)
   - التشفير بالتجزئة (MD5, SHA)
2. **تصميم الإنفوجرافيك:** استخدم Canva لإنشاء تصميم جذاب وسهل الفهم. يمكنك استخدام القوالب الجاهزة أو إنشاء تصميم خاص بك.
3. **تنظيم المعلومات:** قم بتنظيم المعلومات في الإنفوجرافيك بشكل منطقي، مع استخدام العناوين والصور والرسوم البيانية لتوضيح أوجه التشابه والاختلاف بين طرق التشفير المختلفة.
4. **مشاركة الإنفوجرافيك:** قم بتنزيل الإنفوجرافيك ومشاركته على Padlet، مع إضافة تعليق قصير يشرح أهم النقاط.

مثال على جدول المقارنة في الإنفوجرافيك

طريقة التشفير	نوع المفتاح	السرعة	الأمان	الاستخدام
DES	متماثل	سريع	ضعيف	نادر الاستخدام
AES	متماثل	سريع	قوي	شائع الاستخدام
RSA	غير متماثل	بطيء	قوي	توقيع رقمي، تبادل المفاتيح

MD5	تجزئة	سريع	ضعيف	التحقق من سلامة الملفات
SHA	تجزئة	متوسط	قوي	توقيع رقمي، تخزين كلمات المرور

التصدير إلى "جداول بيانات Google"

السؤال الثاني: البحث عن طرق تشفير أخرى

يمكنك البحث عن طرق تشفير أخرى من خلال:

- **محركات البحث:** استخدم كلمات مفتاحية مثل "أنواع التشفير" أو "خوارزميات التشفير الحديثة".
- **المواقع الإلكترونية:** ابحث في المواقع المتخصصة في الأمن السيبراني والتشفير.
- **الدورات التدريبية:** يمكنك الالتحاق بدورات تدريبية لتعلم المزيد عن التشفير.

أمثلة على طرق تشفير أخرى

- **تشفير المنحنى الإهليلجي (ECC):** يعتمد على خصائص المنحنيات الإهليلجية لتوفير مستوى عالٍ من الأمان باستخدام مفاتيح قصيرة.
- **تشفير البلوفيش (Blowfish):** خوارزمية تشفير متماثل قوية وسريعة، تستخدم على نطاق واسع في التطبيقات المختلفة.
- **تشفير Twofish:** خوارزمية تشفير متماثل أخرى قوية ومرنة، تعتبر من أفضل الخوارزميات المتاحة.

السؤال الثالث: التشفير وحماية البيانات الحساسة

- **هل التشفير وسيلة قوية لحماية البيانات الحساسة؟** نعم، التشفير يعتبر وسيلة قوية لحماية البيانات الحساسة، حيث يحول البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام المفتاح الصحيح.
- **هل يكفي التشفير لحماية البيانات؟** لا، التشفير ليس كافيًا لحماية البيانات بشكل كامل. يجب اتخاذ إجراءات أخرى، مثل:
  - التحكم في الوصول إلى البيانات.
  - استخدام كلمات مرور قوية.
  - تحديث البرامج بانتظام.
  - توعية المستخدمين بأهمية الأمن السيبراني.
- **هل توجد طرق أخرى للحماية؟** نعم، هناك طرق أخرى لحماية البيانات، مثل:
  - النسخ الاحتياطي للبيانات.
  - استخدام برامج مكافحة الفيروسات.
  - جدران الحماية.
  - المراقبة الأمنية.

القيم والاتجاهات: تصميم بوستر للتوعية بأهمية حماية البيانات

بالتعاون مع زملائك، يمكنكم تصميم بوستر جذاب ومفيد، يتضمن:

- **عنوانًا catchy:** مثل "بياناتك الشخصية كنز ثمين، حافظ عليه!"
- **معلومات مبسطة:** عن أهمية حماية البيانات الشخصية، ومخاطر فقدانها أو سرقتها.
- **دور التشفير:** في حماية البيانات، مع شرح مبسط لكيفية عمله.
- **مقترحات لتشفير بسيط:** مثل استخدام كلمات مرور قوية، وتشفير الملفات الهامة.
- **دعوة للنشر:** في مواقع التواصل الاجتماعي للمدرسة، لزيادة الوعي بين الأهل والزملاء.