3.4 شيفرتي II

شيفرة סהר

نسخ **סהר** أحجية من الإنترنت لتلاميذ صفّه، وقد حصل على السّطر الآتي:

"ינא המכ תב .ותוא תוביכרמה תורפסה יתש תלפכמם סיילפכ אוה יליג"

?ינא המכ תב

تبدو له هذه الأحجية شيفرة، لكنّه فكّها بسرعة.

أوحت هذه الحالة له بفكرة لاختراع شيفرة أصعب كي يتراسل بواسطتها مع أصدقائه.

فيما يلي الشيفرة التي اخترعها:

المرحلة أ: لاءَم **סהר** عددًا لكلّ حرف كالتّالي:

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
1	2	3	4	5	6	7	8	9	10	11

ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
12	13	14	15	16	17	18	19	20	21	22

المرحلة ب: عوّض كلّ عدد في التّعبير $2x - 10$.

المرحلة ت: سجّل **סהר** الحرف المناسب لنتيجة التّعويض.

إذا لم يحصل على نتيجة التّعويض في الجدول فقد أضاف أو طرح 22،

حتّى حصل على نتيجة موجودة في الجدول.

مثال: شيفرة الاسم "סהר" هي: "רתח" حسب الحساب الآتي:

ר ← ס

$2 \cdot 15 - 10 = 20$

ת ← ה

$2 \cdot 5 - 10 = 0 \rightarrow 0 + 22 = 22$

ח ← ר

$2 \cdot 20 - 10 = 30 \rightarrow 30 - 22 = 8$

נשفِّر ونفكّ شيفرة نصوص بطريقة تشفير סהר ونبحث هذه الطّريقة.

1. شيفرة الاسم "סהר" هي: "רתח".
   حاولوا أنْ تفكّوا شيفرة الحروف רתח بواسطة التّعبير الجبريّ.
   ما هي الإمكانيّات الّتي حصلتم عليها بالإضافة إلى סהר؟

2. أ. **شفِّروا** اسم تلميذ أو تلميذة في الصّفّ حسب شيفرة **סהר**.
   ب. **فكّوا شيفرة** اسم زميلكم.

3. اسم والد **סהר** هو اسم من التوراة. اسمه المشفَّر هو **עית**. **فكّوا شيفرة** اسم الأب.

بحث طريقة تشفير סהר

اعملوا مع زميل أو زميلة

4. أ. هل يوجد حرف إذا شفّرناه بهذه الطّريقة فسيعطينا الحرف ذاته؟ ما هو الحرف؟
هل يوجد حرف إضافيّ كهذا؟ علّلوا.

ب. أيّة حروف يعطينا تعويضها أعدادًا موجودة في الجدول؟ اِشرحوا كيف وجدتم ذلك؟

ت. أيّة حروف يعطينا تعويضها أعدادًا يجب أنْ نضيف إليها 22 كي نجد العدد في الجدول؟

ث. أيّة حروف يعطينا تعويضها أعدادًا يجب أنْ نطرح منها 22 كي نجد العدد في الجدول؟

5. هل يمكن لكلّ حرف أنْ يظهر في النّص المشفَّر حسب طريقة تشفير סהר؟
إذا كانت الإجابة بلا، فأيّة حروف لا تظهر أبدًا في النّص المشفَّر حسب هذه الطّريقة؟

6. أ. هل تشفير كلّ حرف هو وحدة؟ إذا كانت الإجابة بلا فكم حرفًا في الشّيفرة يناسب كلّ حرف؟

ب. هل فكّ الشّيفرة لكلّ حرف هو منفرد؟ إذا كانت الإجابة بلا فكم حرفًا أصليًّا يناسب كلّ حرف مشفَّر؟

زاوية الحاسوب

7. أ. حضِّروا في الإكسل (*Excel*) جدول تناظر كي يساعدكم في تشفير وفكّ شيفرة نص حسب شيفرة סהר.
استعملوا صيغة رياضيّة للعمود C.

	A	B	C	D	E
1	**الحرف الأصليّ**	**العدد المناسب للحرف الأصليّ**	**العدد بعد التّعويض في التّعبير** $2x-10$	**إضافة أو طرح العدد** 22	**الحرف في الشّيفرة**
2					
3					
4					

ب. اِفحصوا إجابتكم عن الأسئلة السّابقة.

8. أ. **شفِّروا** رسالة قصيرة لا تتجاوز خمس كلمات حسب شيفرة סהר.

ب. **فكّوا شيفرة** رسالة زميلكم.

هل تعلمون؟

في الحرب العالمية الثّانية استعمل الألمان وحلفاؤهم الإيطاليون آلات تشفير وفكّ شيفرات رسائل. هذه العائلة من الآلات سُميت **أنيجما**. معنى الكلمة في اليونانيّة أُحجية أو سرّ.

في سنة 1918 اخترع **الأنيجما** مهندس كهرباء ألماني اسمه أرتور شربيوس (Arthur Scherbius). اعتمدت الأنيجما على شيفرة التّبديل لكلّ حرف من حروف الإرسال الّتي يجب تشفيرها. تمَّ التّبديل بواسطة قرص شيفرة استُعمل خلال مئات السّنين. أنتج شربيوس صيغة كهربائيّة للقرص، وهكذا نَتَجت الوسيلة الآليّة الأولى الّتي استُعملت للتشفير. هناك أفضليّة إضافيّة لطريقته وهي أنّ كلّ تغيير لشيفرة التّبديل بعد كلّ حرف كان بواسطة نظام أقراص تدور. أدت إمكانية تغيير ترتيب الأقراص ووضعها الإبتدائي إلى صعوبة أكبر في فك الشّيفرة.

بفضل الاتصال المشفَّر بواسطة الأنيجما نجح الأسطول الألماني وخاصة أسطول الغواصات في أنْ يطوّق الجيش البريطانيّ بنجاعة، وقد منع هذا الطّوق من نقل الغذاء ووسائل القتال إلى الأسطول البريطانيّ.

بذل الرياضيون جهدًا كبيرًا لفكّ الشّيفرة، وبنوا الحاسوب الأول كولوسوس (Colossus)، وفي نهاية الأمر نجحوا في فكّ الشّيفرة. حُفظت قدرة فكّ رسائل العدو بسريّة تامّة، وقد زوّدت الأسطول البريطانيّ أفضلية مهمة في الحرب ضد القوات البحريّة الألمانيّة.

نحافظ على لياقة رياضيّة

سجِّلوا، لكلّ تعبير، جميع الأعداد الصّحيحة الّتي تكون نتيجة تعويضها في التّعبير عددًا صحيحًا يقع بين 1 إلى 22 (يشمل).

أ. $5x+1$

ب. $6x-6$

ت. $4x+10$

ث. $15-7x$

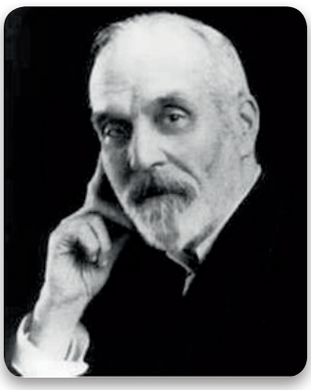
ج. $2-5x$

ح. $-x$

خ. $4x+\frac{1}{4}$

د. $2\frac{1}{3}x+3$

ذ. $5\frac{1}{4}x-3$



الحروف والأعداد هي أُحجية تعرض عملية حسابيّة، وقد بُدّلت أرقامها بالحروف. يجب على الشّخص الّذي يحلّ الأحجية أنْ يفكّ الشّيفرة، وهذا يعني أنْ يجد الأرقام الممثَّلة بواسطة حروف.

في سنة 1924 نشر هنري دودين(Henry Dudeney) أُحجية معروفة مكوَّنة من أعداد وحروف.

	S	E	N	D
+	M	O	R	E
M	O	N	E	Y

هل تعلمون؟

خيبة أمل في إنكلترا

في شهر أكتوبر - تشرين أوّل 2012 وجد مواطن بريطانيّ خلال تنظيف رفّ الموقد في بيته حمامة زاجلة ماتت قبل حوالي 70 سنة، وقد كان مربوطًا بعظامها وعاء أحمر صغير يحتوي على رسالة مشفَّرة مكوَّنة من 27 "كلمة" كلّ واحدة منها مكوَّنة من خمسة حروف. نقل المواطن الرّسالة إلى مُتحف الحمام في ببلتشلي بارك (Bletchley Park)، وقد نُقلت فيما بعد إلى GCHQ – الوكالة المركزيّة لجمع الاستخبارات الإلكترونيّة على أمل أنْ يستطيعوا فكّ الشّيفرة.

اعترفت الوكالة بعد مرور شهر أنّها لم تنجح في فكّ الشّيفرة، ومن المعقول الافتراض أنّهم لن ينجحوا دون معلومات إضافيّة. يقدِّرون في إنكلترا أنّ الجيش البريطانيّ في فرنسا هو الذي كان قد أرسل الحمامة، وقد كان ذلك حول يوم الإنزال في النورماندي سنة 1944. " على الرّغم من خيبة الأمل من أنّنا لم نستطع أنْ نقرأ الرّسالة التي حملتها الحمامة الزّاجلة الشّجاعة، إلا أنّ ذلك فخر واعتزاز بقدرات الأشخاص الّذين بنوا الشّيفرة في أيام الحرب الّتي عملوا فيها في ظروف ضغط كبيرة، ونجحوا في اختراع شيفرة لا يمكن فكّها حتّى اليوم، هكذا أُرسل من GCHQ.

لكن في متحف الحمام في ببلتشلي بارك، الّذي أُقيم في المكان الّذي جلس فيه مختصو التّشفير البريطانيّ خلال الحرب، يرفضون الاستسلام. قال كولين هيل إنّه يشكّ في الجهد الّذي تبذله وكالة GCHQ في فكّ الشّيفرة، وهو مستمرّ في محاولة معرفة هُوِيّة الحمامة النافقة، على أمل أنْ يحلّ اللّغز من خلال ذلك.

استنادًا إلى مقال من Ynet في تاريخ 24.11.2012