الفصل الثامن عشر

القوى، الجذور، والشيفرات "غير القابلة للفك"

Powers, Roots, and "Unbreakable" Codes

تعلمنا في الفصليين السابقين كيف نحسب قوى وجذور لأعداد كبيرة جداً قياس m. باختصار، نحن نعلم كيف نحسب $a^k \pmod m$ لأي قيم m, k, a، ونعلم كيف نحل $x^k \equiv b \pmod m$ بشرط أن نستطيع حساب $\phi(m)$. سنعرض الآن للفكرة الأساسية المستخدمة في كتابة وفك الرسائل المشفرة[1].

إن الخطوة الأولى في تشفير رسالة هي تحويلها إلى صف من الأرقام. سوف نستخدم أبسط طريقة متاحة لعمل ذلك. سنضع $A=11, B=12, \ldots, Z=36$.

الجدول التالي يوضح ذلك:

---

(١) ما نتكلم عنه في هذا الفصل هو التشفير cipher وليس الترميز code، لذلك فنحن نُشَفِّر enciphering ونفك تشفير deciphering الرسائل. تاريخياً، اقتصر استخدام كلمة رمز code على الطرق التي كانت تُستخدم لاستبدال جملة بكاملها بعدد أو رمز واحد، بينما الأصفار ciphers تستخدم الحروف (كل حرف على حده) كوحدات أساسية. في الآونة الأخيرة، اكتسبت كلمة ترميز code معاني رياضية أخرى في عدة مواضيع مختلفة.

A	B	C	D	E	F	G	H	I
11	12	13	14	15	16	17	18	19

J	K	L	M	N	O	P	Q	R
20	21	22	23	24	25	26	27	28

S	T	U	V	W	X	Y	Z
29	30	31	32	33	34	35	36

فعلى سبيل المثال، الرسالة "To be or not to be" (أكون أو لا أكون) تصبح :

T	O	B	E	O	R	N	O	T	T	O	B	E
30	25	12	15	25	28	24	25	30	30	25	12	15

لذلك ؛ فإن رسالتنا هي صف الخانات :

30 25 12 15 25 28 24 25 30 30 25 12 15

بالطبع، يمكن اعتبار رسالتنا الآن مشفرة؛ وذلك لأن هذا الصف من الخانات يجعل الرسالة محجوبة. ولكن حتى هاوي فك الشيفرات عنده القدرة على فك هذه الشيفرة البسيطة خلال دقائق معدودة[١].

نحن الآن مستعدون لشرح آلية كتابة وفك الشيفرة. أول شيء سنقوم به هو اختيار عددين أوليين كبيرين p , q. بعد ذلك سنوجد حاصل ضربهما لنحصل على المقياس $m = pq$. نستطيع أيضاً حساب $\phi(m)=\phi(p)\cdot\phi(q)=(p-1)(q-1)$ ، ونختار عدد k بحيث $\gcd\left(k,\phi(m)\right)=1$. يمكننا الآن الإفصاح عن الرقمين m , k لكل العالم ليعرفوه، ولكن نحتفظ بقيمة الرقمين p , q كسِر. الآن، أي شخص يريد أن يرسل لنا رسالة سيستخدم قيمة كل من m , k لتشفير رسالته وفق الآلية التالية.

في البداية، سيقومون بتحويل رسالتهم إلى صف من الخانات كما رأينا سابقاً. بعد ذلك سيقومون بتقسيم صف الخانات إلى أعداد، كل منها أقل من m. فمثلاً، إذا كان m عدداً بالملايين، فبإمكانهم كتابة رسالتهم كقائمة من أعداد كل منها مكون من 6 خانات. لذلك فإن رسالتهم الآن هي قائمة من الأعداد $a_1, a_2, \ldots, a_r$. الخطوة التالية هي استخدام التربيعات المتعاقبة لحساب:

$$a_1^k \pmod m, a_2^k \pmod m, a_3^k \pmod m, \ldots, a_r^k \pmod m$$

هذه القيم ستشكل قائمة جديدة من الأعداد $b_1, b_2, \ldots, b_r$. هذه القائمة هي الرسالة المشفرة. بمعنى أن الرسالة المرسلة لنا هي قائمة الأعداد $b_1, b_2, \ldots, b_r$.

---

(١) نستطيع تعيين رقم، مثل 99، ليشير إلى الفراغ (المسافة) بين الكلمة والأخرى، ويُمكِننا كذلك تعيين أرقام تدل على علامات متعددة. ولكن من باب التبسيط فإننا نتجاهل مثل هذه العلامات، ونكتب رسالتنا بحيث تكون جميع الأحرف ملتصقة بجانب بعضها البعض.

كيف نفك شيفرة الرسالة عندما نستلمها؟

أرُسِل لنا الأرقام $b_1, b_2, \ldots, b_r$ ، ونحتاج لمعرفة الأرقام $a_1, a_2, \ldots, a_r$. كل b_i يطابق $a_i^k \pmod m$ ، لذلك لإيجاد a_i نحتاج لحل التطابق $x^k \equiv b_i \pmod m$.

هذه بالضبط هي المسألة التي قمنا بحلها في الفصل السابق، على اعتبار أننا قادرون على حساب $\phi(m)$. لكننا نعلم قيمة كل من p , q ، وحيث $m = pq$ ، فإننا بسهولة نحسب:

$$\begin{aligned}\phi(m) &= \phi(p)\cdot\phi(q)\\ &= (p-1)(q-1)\\ &= pq - p - q + 1\\ &= m - p - q + 1\end{aligned}$$

الآن نحن بحاجة فقط إلى تطبيق الطريقة الواردة في الفصل السابع عشر لحل كل تطابق $x^k \equiv b_i \pmod m$. الحلول هي الأرقام $a_1, a_2, \ldots, a_r$ ، وبعد ذلك فإنه من السهل أخذ هذا الصف من الخانات والكشف عن الرسالة الأصلية.

لقد بينا إجراء تشفير وفك تشفير رسالة مع العددين الأوليين $p = 12553, q = 13007$. نقوم بضربهم لنحصل على $m = pq = 163276871$ ، وأيضاً نسجل لاستخدامه فيما بعد:

$$\phi(m) = (p-1)(q-1) = 163251312$$

نحتاج كذلك لاختيار عدد k بحيث $\gcd(k, \phi(m)) = 1$ ؛ لذلك نأخذ $k = 79921$. خلاصة ما سبق أنا قمنا باختيار:

$$p=12553 \quad , \quad q=13007 \ , \ m=pq=163276871 \ , \ k=79921$$

لنفرض الآن أننا نريد إرسال الرسالة "To be or not to be". كما رأينا سابقاً، فإن هذه الرسالة تصبح صف الخانات:

30 25 12 15 25 28 24 25 30 30 25 12 15

العدد m طوله 9 خانات؛ لذلك نقوم بتقسيم الرسالة إلى أعداد طول كل منهم حتى 8 خانات:

30251215 25282425 30302512 15

بعد ذلك نستخدم طريقة التربيعات المتعاقبة لرفع كل رقم من هذه الأرقام إلى القوة k^{th} قياس m.

$$30251215^{79921} \equiv 149419241 \pmod{163276871}$$

$$25282425^{79921} \equiv 62721998 \pmod{163276871}$$

$$30302512^{79921} \equiv 118084566 \pmod{163276871}$$

$$15^{79921} \equiv 40481382 \pmod{163276871}$$

الرسالة المشفرة هي قائمة الأرقام:

149419241 , 62721998 , 118084566 , 40481382

دعنا الآن نحاول فك شيفرة رسالة جديدة.

إنه بعد منتصف الليل، سَمِعتَ طرقاً خفيفاً على باب بيتك، فتحتَ الباب فإذا برجل ملثم يعطيك رسالة غامضة كتب فيها:

145387828 , 47164891 , 152020614 , 27279275 , 35356191

بدون أن تتردد للحظة ، ستقفز بسرعة وتتناول كتاب نظرية الأعداد وتبدأ بالعمل. ستستخدم الطريقة الواردة في الفصل السابع عشر لحل التطابقات :

$$x^{79921} \equiv 145387828 \pmod{163276871} \Rightarrow x = 30182523$$

$$x^{79921} \equiv 47164891 \pmod{163276871} \Rightarrow x = 26292524$$

$$x^{79921} \equiv 152020614 \pmod{163276871} \Rightarrow x = 19291924$$

$$x^{79921} \equiv 27279275 \pmod{163276871} \Rightarrow x = 30282531$$

$$x^{79921} \equiv 35356191 \pmod{163276871} \Rightarrow x = 122215$$

وهذا يعطي صف الخانات :

$$30182523262925241929192430282531122215$$

سوف نستخدم الآن جدول تعويض الأرقام بالحروف لإنهاء الخطوة الأخيرة لفك الشيفرة.

30	18	25	23	26	29	25	24	19	29
T	*H*	*O*	*M*	*P*	*S*	*O*	*N*	*I*	*S*

19	24	30	28	25	31	12	22	15
I	*N*	*T*	*R*	*O*	*U*	*B*	*L*	*E*

بتقطيع هذه الأحرف إلى كلمات ستحصل على الجملة :

"Thompson is in trouble" (ثومسون في مأزق)

وستذهب مباشرة لمساعدته.

هل هذه إستراتيجية آمنة لتشفير رسالة؟ لنفترض أن رسالة مشفرة وقعت في يدك، وأنت تعلم أنها شُفِّرت بمنسوب إليه m وأس k. ما مدى صعوبة أن تقوم بفك الشيفرة وقراءة الرسالة؟ حتى هذه اللحظة، فإن الطريقة الوحيدة لفك الشيفرة هي إيجاد قيمة $\phi(m)$ ومن ثم استخدام آلية فك الشيفرة المشروحة سابقاً. إذا كان m هو حاصل ضرب عددين أوليين p , q ، فإن:

$$\phi(m)=(p-1)(q-1)=pq-p-q+1=m-p-q+1$$

وحيث إنك تعرف قيمة m ، فإنك بحاجة فقط لإيجاد قيمة $p+q$. ولكن إذا كنت تستطيع إيجاد $p+q$ ، عندها فإنك تستطيع أيضاً تحديد قيمة كل من p , q ، لأنهما جذري المعادلة التربيعية:

$$X^2-(p+q)X+m=0$$

لذلك لكي تقوم بفك شيفرة هذه الرسالة، فإنك بحاجة ماسة لإيجاد عاملي m وهما p , q .

إذا كان m ليس بالعدد الكبير جداً، مكوناً من 5 أو 10 خانات، فإن الكمبيوتر على الأغلب سيقوم بإيجاد العوامل خلال لحظات. إذا أردنا استخدام طرق متقدمة في نظرية الأعداد، فإن الرياضيين ابتكروا طرقاً قادرة على تحليل أرقام ضخمة، مثل الأرقام التي لها 50 أو حتى 100 خانة. لذلك إذا أخذت عددين أوليين p , q كل منهما عدد خاناته أقل من 50 خانة، فإن رسالتك المشفرة لن تكون بأمان. على كل حال، إذا أخذت عددين أوليين عدد خانات كل منهما 100 خانة مثلاً، فإن أحداً حتى هذه اللحظ لن يتمكن من فك تشفير رسائلك إلا إذا أخبرتهم بقيمة p , q. طبعاً، من الممكن أن يتمكن الرياضيون مستقبلاً على جعل

الناس قادرة على تحليل أرقام لها 200 خانة، ولكن عندها فإنك بحاجة إلى أخذ عددين أوليين كل منهما له 200 خانة، وسيصبح العدد ذو الـ 400 خانة المنسوب إلى m قادراً مرة أخرى على جعل رسالتك آمنة. إن الفكرة الأساسية في آلية التشفير هي ببساطة: إنه من السهل ضرب أعداد كبيرة مع بعضها البعض، ولكن من الصعب تحليل عدد كبير.

إن طريقة كتابة رسالة سرية بالشيفرة والموصوفة في هذا الفصل تسمى "نظام التعمية ذو المفتاح المعلن" *(public key cryptosystem)*. إن هذا الاسم يعكس حقيقة أن مفتاح تشفير الرسالة يكمن في أن المقياس والأس يمكن نشر قيمة كل منهما بين جميع الناس بينما طريقة فك الشيفرة يبقى سراً. هذه الفكرة، وهي أن معرفتك لآلية التشفير لا تمكنك من فك الشيفرة، أعلن عنها العالمان (وايتفيلد ديفي) Whitfield Diffie و (مارتن هيلمان) Martin Hellman في سنة 1976. ديفي وهيلمان قدما وصفاً نظرياً عن كيفية عمل نظام التعمية ذي المفتاح المعلن، وفي السنة التي بعدها قدم العلماء (رون ريفست) Ron Rivest، (آدي شامير) Adi Shamir و (ليونارد أدلمان) Leonard Adleman وصفاً تطبيقياً لنظام التعمية ذي المفتاح المعلن. إن فكرتهم، والتي قمنا بوصفها في هذا الفصل، تسمى RSA "نظام التعمية ذو المفتاح المعلن" *(public key cryptosystem)* نسبة إلى مخترعيها الثلاثة.

تمارين

(١٨.١) فك شيفرة الرسالة التالية، والتي أُرسلت باستخدام المقياس $m = 7081$ والأس $k = 1789$. (لاحظ أنك تحتاج أولاً لتحليل m).

5192 , 2604 , 4222

(١٨,٢) قد يبدو أن طريقة RSA لفك الشيفرة لا تعمل إذا لم تكن محظوظ بما يكفي لاختيار رسالة a لا يكون أوليًّا نسبياً مع m. إذا كان $m = pq$ و p و q كبيرين، فإن هذا مستبعد الحدوث.

(a) بين حقيقة أن طريقة RSA لفك التشفير تعمل لجميع الرسائل a، بغض النظر عما إذا كان لها عامل مشترك مع m أم لا.

(b) بشكل عام، بيّن أن طريقة RSA لفك التشفير تعمل مع جميع الرسائل a طالما أن m هو حاصل ضرب أعداد أولية مختلفة.

(c) أعط مثالاً فيه $m = 18$ و $a = 3$ بحيث لا يمكن تطبيق RSA لفك التشفير.

(تذكر، يجب أن تختار k ليكون أوليًّا نسبياً مع $\Phi(m) = 6$).

(١٨,٣) اكتب تقريراً قصيراً عن واحد أو أكثر من الموضوعات التالية:

(a) التطور التاريخي لمفتاح كتابة الشيفرة العام.

(b) نظام التعمية ذو المفتاح المعلن RSA.

(c) مفتاح التواقيع الرقمية العام.

(d) التبعات السياسية والاجتماعية لإتاحة شيفرات رخيصة غير قابلة للفك ورد الحكومة على ذلك.

(١٨,٤) هنا رسالتان طويلتان يمكن فكهما إذا رغبت في استخدام كمبيوتر.

(a) استلمت الرسالة التالية:

5272281348, 21089283929, 3117723025, 26844144908, 22890519533
26945939925, 27395704341, 2253724391, 1481682985, 2163791130
13583590307, 5838404872, 12165330281, 28372578777, 7536755222

هذه الرسالة شُفّرت باستخدام:

$p=187963$, $q=163841$, $m=pq=30796045883$, $k=48611$

فك شيفرة الرسالة.

(b) وقعت بيدك الرسالة التالية، والتي تعرف أنها شُفّرت باستخدام المقياس

$$m=95633199200784355265260442503137669036 7$$

والأس $k=12398737$. جزء الشيفرة وفكها.

821566670681253393182493050080875560504,

870741731290463997209497869585113910 52,

552100909946781566365272088688468880029,

491078995197839451033115784866534122828,

172219665767314444215921020847762293421.

(مادة هذا التمرين متاحة على الموقع الإلكتروني لهذا الكتاب والمذكور في المقدمة).

(١٨,٥) اكتب برنامجاً ينفذ نظام تشفير RSA. اكتب برنامجك بشكل بسيط قدر الإمكان. وبشكل خاص، الشخص الذي يقوم بتشفير الرسالة يجب أن يكون قادراً على طباعتها بالكلمات وتحوي المسافات وعلامات الترقيم، نفس الشيء بالنسبة لمن يحل الشيفرة، يجب أن يتمكن من رؤية الرسالة بالكلمات والمسافات وعلامات الترقيم.

(١٨,٦) مسألة تحليل الأرقام الكبيرة إلى عواملها تمت دراستها بشكل مكثف في السنوات الأخيرة بسبب أهمية تشفير الرسائل. ابحث في طرق التحليل التالية واكتب تقريراً قصيراً عن كيفية عملها.

(يمكن أن تجد معلومات عن هذه الطرق في كتب نظرية الأعداد أو في بعض المواقع الإلكترونية).

(a) طريقة "ρ بولارد" Pollard's ρ (حرف لاتيني يُقرأ رو).

(b) طريقة $p-1$ بولارد.

(c) طريفة "تحليل المُنْخُل التربيعي" Quadratic sieve factorization.

(d) طريقة "تحليل منحنى لنسترا الناقص" Lenstra's elliptic curve factorization.

(e) "مُنْخُل حقل العدد" The number field sieve.

(الطريقتان الأخيرتان تحتاجان إلى أفكار متقدمة ؛ لذلك أنت بحاجة إلى أن تتعلم عن المنحنيات الناقصية أو عن حقول العدد لفهم تلك الطرق). إن طريقة مُنْخُلْ حقل العدد هي أكثر طرق التحليل فاعلية حتى الآن. من خلال هذه الطريقة يمكن تحليل أرقام يصل عدد خاناتها إلى 150 خانة.

(١٨,٧) اكتب برنامج كمبيوتر لتنفيذ إحدى طرق التحليل التي قمت بدراستها في التمارين السابقة، مثل طريقة ρ بولارد، طريقة $p-1$ بولارد، أو طريقة مُنْخُل التربيعي. استخدم برنامجك لتحليل الأرقام التالية :

(a) 47386483629775753

(b) 1834729514979351371768185745442640443774091