جولة تثقيفية في عالم التشفير والتعمية

صادق بوروبي
أستاذ بكلية الرياضيات، جامعة هواري بومدين للعلوم والتكنولوجيا، الجزائر
bouroubis@gmail.com

مقدمة

في هذا المقال سنحاول أن نتطرق إلى نوع من أنواع الثقافة العلمية غير المنتشرة بشكل كافٍ في الأوساط العامة والخاصة، بأسلوب سلس يعالج الموضوع، قدر المستطاع، بمراعاة مهارات ومعارف القارئ الكريم، تتمثل في ثقافة علمَي التشفير والتعمية. وسنعرض هذا الموضوع دون الخوض في التفاصيل العلمية التي تُخرج المقال عن هدفه المرسوم له، وهو حصول القارئ على فكرة مجملة للموضوع تحفزه وتدفعه، إذا شاء، إلى البحث عن التفاصيل.

1. علم التشفير

التشفير هو عِلم من علوم الرياضيات التطبيقية، يهتم بحماية البيانات السرية، وينقسم إلى قسمين:

- التشفير (Cryptography)؛
- تحليل الشفرات (Cryptanalysis).

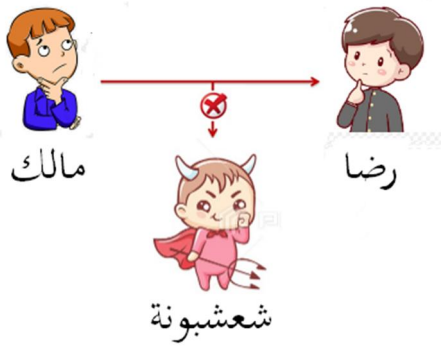
أما التشفير فهو علم يهدف إلى إنشاء أساليب علمية تعمل على حماية سرية البيانات بجعلها غير معقولة المعنى. وأما علم تحليل الشفرات فيتمثل في مجموعة تقنيات تهدف إلى فك الشفرة دون علم سابق بمفتاح الشفرة، وذلك بالبحث عن نقاط الضعف التي يمكن أن تتخلل عملية التشفير.

2. لماذا نحن بحاجة إلى التشفير؟

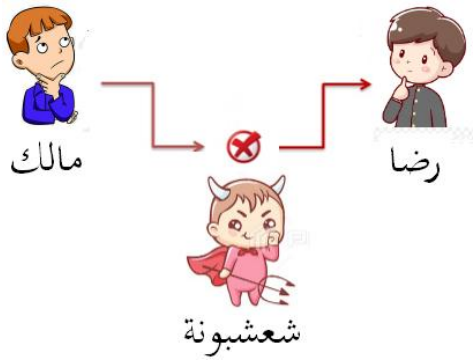
يلعب علم التشفير دورًا حاسمًا في الحفاظ على سرية وسلامة البيانات في العديد من المجالات، مثل الاتصالات عبر الإنترنت، والتحقق الإلكتروني، والأمان في البنوك، والتبادلات السياسية والعسكرية، والعديد من التطبيقات الأخرى التي تتطلب الحماية.

ولعلم التشفير أربعة أهداف أساسية، نوردها مرفقة بصور تشكيلية توضيحية كما يلي:

- **سرية البيانات**: لضمان إتاحة المعلومة ووصولها إلى المستخدمين المصرح لهم فقط لامتلاكهم مفتاح فك الشفرة، ويتم ذلك بواسطة تشويش البيانات وجعلها غير معقولة المعنى لدى المتطفلين من أمثال شعشبونة.



- **سلامة البيانات من التحريف**: لضمان عدم حصول تغيير للبيانات بوسائل مجهولة أو غير مصرح بها، ويتم ذلك بواسطة دالة البعثرة.



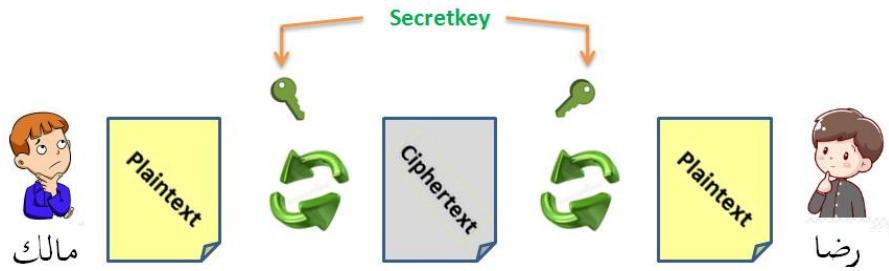
- **إثبات أصالة البيانات**: لضمان تأكيد هوية المرسل، ويتم ذلك من خلال التوقيع الإلكتروني.

- **عدم القدرة على التنصل**: لضمان قطع الطريق، في مجال المعاملات الرقمية، على كل من يريد أن يموّه أو يتنكّر من تلقي أو نشر البيانات، ويتم ذلك بواسطة شهادة رقمية.

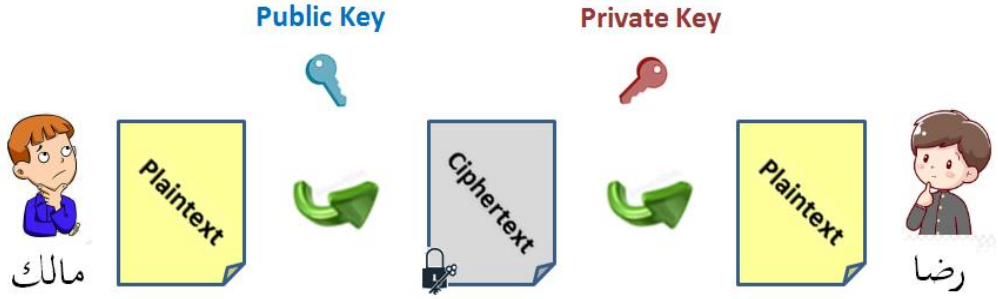
3. أنواع أنظمة التشفير

للتشفير ثلاثة أنظمة أساسية جارٍ بها العمل إلى يومنا هذا وتشمل:

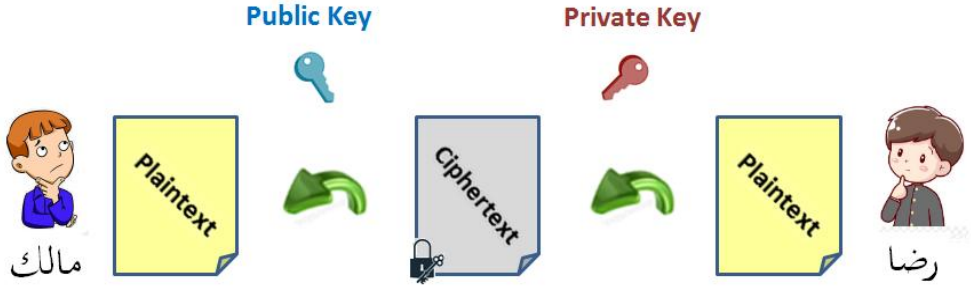
- **النظام المتماثل**: وهو الذي يكون فيه مفتاح الشفرة وفك الشفرة واحد. أحد أشهر الأنظمة المتماثلة هو نظام تشفير الكتلة AES (Advanced Encryption Standard).



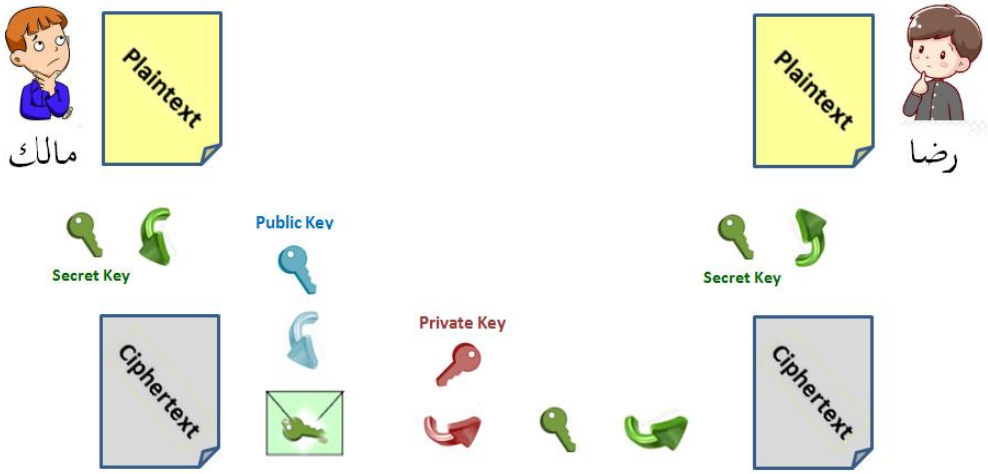
- **النظام غير المتماثل**: والمعروف أيضًا باسم تشفير المفتاح العام، وهو الذي يكون فيه مفتاح الشفرة خاصا ويسمى المفتاح الخفي، ويكون مختلفا عن مفتاح فك الشفرة المسمى بالمفتاح العام. أحد أنظمة التشفير غير المتماثلة الشائعة هو RSA، القائم على مسألة تحليل الأعداد إلى عواملها الأولية.



عندما يكون التشفير بواسطة النظام غير المتماثل في الاتجاه المعاكس، كما توضحه الصورة أدناه، نكون أمام حالة إثبات الأصالة والعملية بهذا الشكل تسمى توقيعا.



- **النظام الهجين**: وهو الذي يجمع بين النظامين المتماثل وغير المتماثل بهدف الاستفادة من الجوانب الإيجابية لكلا النظامين وتجنب عيوبهما في الوقت نفسه. يتيح هذا النظام لمستخدميه توازنا مثاليا بين الحماية والأداء حيث يمكن استخدام النظام المتماثل لسرعة الأداء وبساطة خوارزميات التشفير وقلة الموارد المستخدمة، في حين تتم الاستفادة من النظام غير المتماثل للكفاءة والأداء القوي.



4. أشهر علماء التشفير عبر التاريخ

ومن يُنظر إليه على نطاقٍ واسعٍ على أنه أبو علوم الكمبيوتر النظرية والذكاء الاصطناعي هو آلان ماتيسون تورنغ (Alan Mathison Turing).

آلان

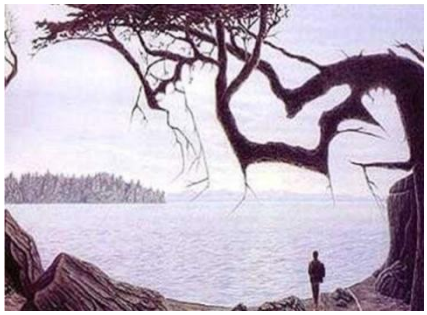
ماتيسون

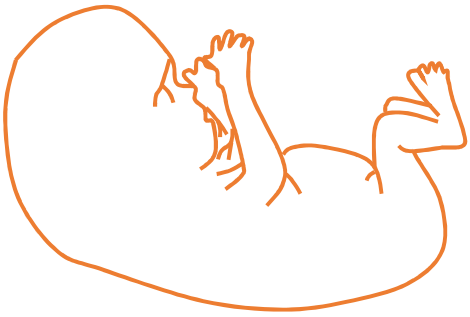
تورنغ

(1912-1954)

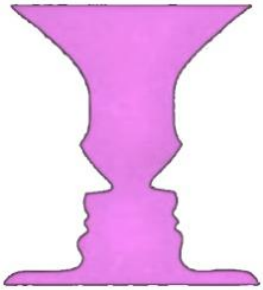
5. التعمية

المتأمل لأول مرة في اللوحة على اليمين قد يتصور أنّ الفنان الذي رسمها أراد أن يبرز جمال الطبيعة بأشجارها وأنهارها، ولكنه لو أمعن النظر فيها جيدا للاحظ أن اللوحة تخفي شيئا لا يلتفت إليه الرائي لأول وهلة وهو ما تبرزه الصورة على اليسار.



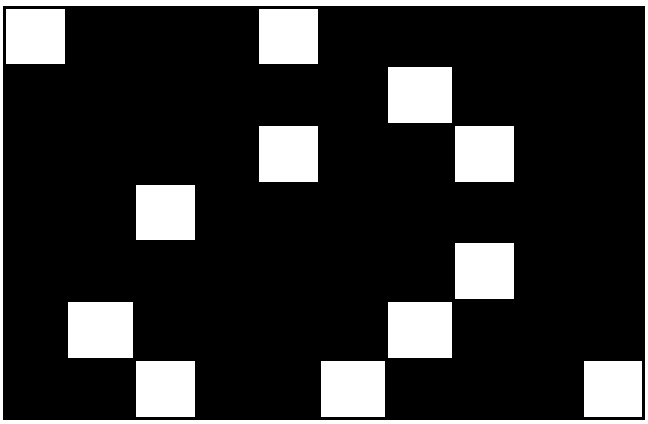


كما أن الناس منقسمون إلى قسمين بين من ينظر إلى الصورة التالية فيرى كأسا ورديا، ومنهم من يرى وجهين متقابلين. هذا النوع من الفن يسمّى فن التعمية (Steganography).



قد تبدو هذه التقنية فنًّا من الفنون فحسب، ولكنها قديمة جدًا، تم استخدامها منذ العصور الغابرة. يعود أقدم مثال معروف لها إلى القرن الخامس قبل الميلاد، حيث قام أريستاغوراس (Aristagoras) حاكم مدينة ميليتس (Miletus)، من أجل إيصال رسالة سرية، بوضع وشم على جمجمة عبد وانتظر حتى ينمو شعره مرة أخرى قبل أن يرسله في طريقه إلى الوجهة المحددة.

ومن بين أشهر الطرق القديمة للتعمية نجد مبدأ شبكة جيرولامو كاردانو (Gerolamo Cardano)، حيث تتم العملية بوضع شبكة أو نمط به ثقوب فوق نص يبدو في الظاهر أنه غير معقول المعنى، ليتم بعدها رفع الحروف أو الكلمات الموجودة أسفل الثقوب فقط للحصول على النص المخفي.



S	T	R	Y	T	O	P	O	M	F
A	J	N	E	Y	M	G	T	P	Q
E	H	I	S	A	N	H	N	E	Y
R	Q	O	J	K	L	A	R	J	T
Q	W	D	C	Q	O	Z	G	K	R
X	R	S	V	B	J	A	E	R	Y
C	V	P	B	N	H	M	A	Z	Y

S	T	R	Y	T	O	P	O	M	F
A	J	N	E	Y	M	G	T	P	Q
E	H	I	S	A	N	H	N	E	Y
R	Q	O	J	K	L	A	R	J	T
Q	W	D	C	Q	O	Z	G	K	R
X	R	S	V	B	J	A	E	R	Y
C	V	P	B	N	H	M	A	Z	Y

يمكن تنويع نمط الشبكة من حيث الحجم والشكل، مما يسمح بتخصيص عملية التعمية.

على مر القرون، أصبحت هذه التقنية أكثر تعقيدًا، لا سيما مع ظهور الكمبيوتر وشعار كل شيء رقمي. فعلم التعمية لا يرمي إلى تشفير البيانات ولكن إلى إخفائها في ملف ذي مظهر عادي لا يثير أي شك، كملفات صور أو فيديو أو صوت أو ملفات نصية متواضعة.

فيما يلي سنتعرض، على سبيل المثال، إلى تقنية التعمية باستعمال ملفات الصور، وعلى القارئ المهتم بهذا العلم أن يتوسع كما يشاء.

6. التعمية باستعمال ملفات الصور

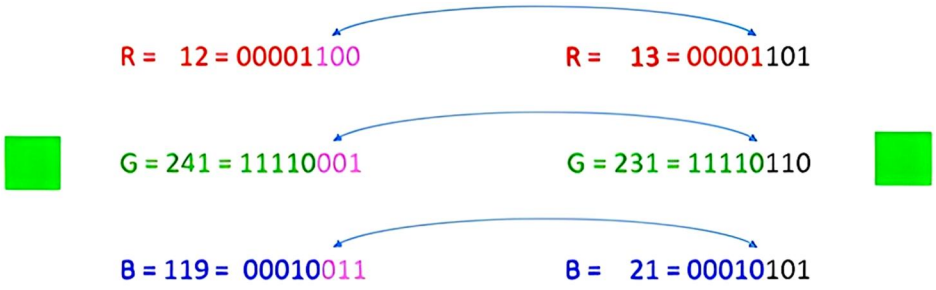
الصورة الرقمية هي عبارة عن مصفوفة من وحدات البكسل (pixels)، يتم تمثيل كل منها بثلاث وحدات تخزين (byte) يشير كل واحد منها على التوالي إلى مستويات الألوان الأساسية الأحمر والأخضر والأزرق (RGB). المربع التالي هو تكبير لبكسل مأخوذ من صورة تم إنتاجها بواسطة ماسح ضوئي (scaner)، يمثله الثلاثي RGB التالي:

1224119 ⟶ 000011001111000100010011

إذا تأملنا في كل وحدة تخزين من أحد الألوان الأساسية الثلاثة، نلاحظ أن البتات باللون الوردي تعتبر أقل البتات ثقلا لذلك تسمى LSB (Least Significant Bit)، مما يسمح باستبدالها ببتات المعلومة التي نريد إخفاءها في الصورة دون تشويهها.

1224119 ⟶ 000011001111000100010011

فعلى سبيل المثال إذا أردنا إخفاء السلسلة الثنائية 101110101 في بتات LSB داخل هذا البكسل فإنه ينتقل من لونه الأصلي على اليسار إلى اللون الجديد الذي، كما يلاحظ القارئ، لم يحصل له تغيير يُدرك بالعين المجردة:



ونظرًا لأن البكسل يمكن أن يحمل من المعلومة السرية إلى 9 بتات، فيمكن لصورة ذات حجم $n \times m$ بكسل أن تخفي رسالة من $\frac{9nm}{8}$ حرفا. لذلك يمكن لصورة ذات حجم 1024 × 768 بكسل مثلا أن تحتوي على أكثر من 884736 حرفًا، أي ما يكفي لإخفاء كتاب بحجم 280 صفحة بصيغة A4.

على سبيل المثال ومن خلال تطبيق برمجي، تم إنشاؤه بمشاركة فريق البحث الذي نرأسه بالمخبر الذي نتشرف بإدارته -الموسوم بالعلوم الأساسية في الإعلام الآلي والبحوث العملياتية والتوافيقية والاقتصاد القياسي (L'IFORCE)- تم إخفاء الصورة على اليمين في الصورة على اليسار فكانت الحصيلة الصورة الثالثة. ولك أيها القارئ أن تجد الفرق بين الصورة الأصلية والصورة الحاملة للمعلومة الخفية.