(31)التعميه

(1) التشفير أو الترميز (علم الأسرار), لم يكن علماً إلا مؤخراً, فهو علم يبحث عن تشفير معطيات حساسة وتحليلها. يمكن القول أنه فن قديم وعلم جديد, ففن لأن يوليوس قيصر قد استخدمه قديماً, أما علم فلأنه ارتبط ببعض العلوم الأخرى التي ظهر بعضها في 1970وما بعدها كالجبر ,نظرية الأعداد , نظرية التعقيد, ونظرية المعلومات.

(2) ينقسم علم التعمية إلى قسمين: • التشفير . • كسر التشفير.
فواضع التعمية يكون هدفه الأساسي هو ضمان سرية المعلومات المنقولة وعدم تعرضها للمعتدي. أما محلل التعمية فإ ن هدفه مضاد تماماً وهو كسر التعمية ومعرفة محتوى المعلومات المنقولة أو تحريفها بشكل يؤدي إلى قبولها على أنها المعلومات الصحيحة.

(3) وبناءاً على ذلك فإننا نستطيع تعريف التعمية على أنها تحويل نص واضح مقروء إلى نص غير مفهوم باستخدام إحدى طرق التعمية والتي قد تكون غير سرية ولكنها تستخدم مفتاحاً سرياً يمكن من يمتلكه من أن يعيد النص المعمي إلى النص الواضح . أما كسر التعمية فهي العملية العكسية للتعمية , أي محاولة معرفة المفتاح السري من النص المعمي ومن ثم الحصول على النص الواضح. يتضح لنا أن علم التعمية قائم على العناصر التالية: مرسل- مستقبل - رسالة - النص الواضح - النص المعمى - مفتاح التعمية . الآن نقدم تعريف رياضي لنظام التعمية.

(4) علم التعمية او علم التشفير هو علم وممارسة إخفاء البيانات؛ أي بوسائل تحويل البيانات (مثل الكتابة) من شكلها الطبيعي المفهوم لأي شخص إلى شكل غير مفهوم بحيث يتعذّر على من لا يملك معرفة سرية محددة معرفة فحواها. يحظى هذا العلم اليوم بمكانة مرموقة بين العلوم، إذ تنوعت تطبيقاته العملية لتشمل مجالات متعددة نذكر منها: المجالات الدبلوماسية والعسكرية، والأمنية، والتجارية، والاقتصادية، والإعلامية، والمصرفية والمعلوماتية. في شكلها المعاصر, التعمية علم من أفرع الرياضيات وعلوم الحوسبة.

(5) استعمل العرب هذا المصطلح كناية عن عملية تحويل نص واضح إلى نص غير مفهوم باستعمال طريقة محددة، يستطيع من يفهمها أن يعود ويفهم النص. غير أن في الوقت الحالي كثر استعمال مصطلح التشفير.

(6) استخدم التشفير منذ أقدم العصور في المراسلات الحربية بين وكذلك في الدبلوماسية والتجسس في شكليهما المبكرين. يعتبر العلماء المسلمون والعرب أول من اكتشف طرق استخراج المعمّى وكتبها وتدوينها .تقدمهم في علم الرياضيات أعطاهم الأدوات المساعدة الأزمة لتقدم علم التعمية، من أشهرهم يعقوب بن إسحاق الكندي صاحب كتاب علم استخراج المعمّىوابن وَحشيّة النبطي صاحب كتاب شوق المستهام في معرفة رموز الأقلام، المؤلف الذي كشف اللثام عن رموز الهيروغليفية قبل عشرة قرون من كشف شامبليون لها .وكثلك اشتهر ابن دريهم الذي كان لا يشق له غبار في فك التشفير فكان تعطى له الرسالة معماة فما هي إلا أن يحلها حتى يحولها في الحين إلى العربية ويقرئها وله قصيدة طويله يشرح فيها مختلف الطرق في تعمية النصوص وكان يحسن قراءة الهيرغليفية من أمثلة استخدام التعمية قديما هو ما ينسب إلى يوليوس قيصر من استعمال ما صار يعرف الآن بخوارزمية روت 13 لتعمية الرسائل المكتوبة باللاتينية التي يتبادلها مع قواده العسكريين، وهو أسلوب تعمية يُستبدل فيه كل حرف بالحرف الذي يليه بثلاثة عشر موقعا في ترتيب الأبجدية اللاتينية، مع افتراض أن آخر حرف في الأبجدية يسبق الأول في حلقة متصلة.

(7) في العصر الحديث, تعد آلة إنجما التي استخدمها الجيش الألماني في الحرب العالمية الثانية, أبرز مثال على استخدام التعمية لتحقيق تفوق على العدو في مجال الاتصالات، وكانت الأبحاث التي جرت بشكل منفصل في كل من المؤسستين العسكريتين الأمريكية والبريطانية في سبعينيات القرن العشرين فتحا جديدا فيما صار يعرف الآن بتقنيات التعمية القوية المعتمدة على الحوسبة، وارتبطت التعمية بعلوم الجبر ونظرية الأعداد ونظرية التعقيد ونظرية المعلوميات.

(8) توسع نطاق تطبيقات التعمية كثيرا في العصر الحديث بعد تطور الاتصالات وحدوث ثورة الاتصالات بما تتطلبه أحيانا من استيثاق وحاجة إلى ضمان عدم التنصت ومنع التجسس والقرصنة الإلكترونية وتأمين سبل التجارة

(8) توسع نطاق تطبيقات التعمية كثيرا في العصر الحديث بعد تطور الاتصالات وحدوث ثورة الاتصالات بما تتطلبه أحيانا من استيثاق وحاجة إلى ضمان عدم التنصت ومنع التجسسوالقرصنة الإلكترونيين وتأمين سبل التجارة الإلكترونية.

(9) تعد تقنيات التوقيع الرقمي والتصويت الالكتروني والنقد الرقمي تطبيقات عملية معتمدة على التعمية.

(10) هو الحقل المهتم بالتقنيات اللغوية و الرياضية لتحقيق أمن المعلومات, حاصة في عملية الاتصال.تاريخياً, اهتم علم التعمية فقط بالتشفير أي وسائل تحويل المعلومات من شكلها الطبيعي المفهوم إلى شكل غير مفهوم ولقد اهتم الإنسان منذ آلاف السنين على هذا العلم لحجب المعلومات السرية عن أعداءه. وقد اقتصر استخدام علم التعمية في القرون الماضية في الحفاظ على أمن المعلومات العسكرية والمراسلات الدبلوماسية وحماية الأمن الوطني.لكن نطاق تطبيقات التعمية توسع كثيراً في العصر الحديث بعد تطور الاتصالات وحدوث ثورة الاتصالات لما تتطلبه من وثوقية أحيانا وضمان عدم الاختراق ومنع التجسس والقرصنة الإلكترونية وتأمين سبل التجارة الإلكترونية.

(11) تُصنف التعمية في منظومتين: التشفير والترميز، والفارق الرئيسي بينهما هو طول المقطع المعتمد من النص الواضح عند تحويله إلى نص معمّى. فالتشفير يتناول كل حرف من حروف النص الواضح أو مجموعة حروف لا تزيد على ثلاثة، في حين تتناول منظومة الترميز كلمة أو عبارة أو جملة بكاملها وفق لائحة متفق عليها.

(12) تقسم طرائق التعمية التقليدية، (التي لم يضف إليها جديد منذ نشأتها على يد الكندي حتى أواسط القرن العشرين)، إلى ثلاثة أنواع، ذكرها الكندي في كتابه «رسالة في استخراج الأعداد المضمرة»، وهي رسالة مذهلة في معلوماتها وأول مرجع معروف في علم التعمية واستخراج المعمى. وهي: التعمية بالقلب أو بتبديل مواقع الحروف ، والتعمية بالإبدال أو الإعاضة ، والتعمية بإضافة حروف «أغفال» أو حذف حروف. والطريقتان الأوليتان أساسيتان، ولكل منهما قاعدة عامة ومفتاح:

أ ـ التعمية بالقلب: تكون بتغيير مواقع حروف النص الواضح وفق ترتيب معين من دون أن يفقد الحرف فحواه، ويمكن أن يمثل عليها بقلب حروف كل كلمة في النص أو إزاحة حروفها أو خلطها.

ب ـ التعمية بالإبدال أو الإعاضة: فيها يبدل بكل حرف من النص حرف أو رمز وفق قاعدة محددة من دون تغيير في موقعه، أو يستبدل بالحرف الحرف الذي يليه أو يسبقه على ترتيب حروف الهجاء أو الأبجدية أو باستعمال حساب الجُمل أو باستعمال «سجل المرة الواحدة».

السؤال (1) : أسلوب الكاتب في القطعة :	
(أ) يسود بحيادية للطرفين	(ب) xxxx

السؤال (1) : أسلوب الكاتب في القطعة :	
(أ) يسرد بحيادية للطرفين	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (2) : ما الذي يجعل الشخص يعيد الرسالة بعدما علم محتواها :	
(أ) تضليل المرسل له الرسالة	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (3) : كلمة المفتاح السري في القطعة :	
(أ) تدل على أنه لا يعطي الحق لفتح الرسالة إلا المخول لذلك العمل	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (4) : من أقسام الشفرات(سري يحتوي على مفتاح واضح) ما القسم الأخر :	
(أ) غير سري ويحتوي على مفتاح غامض	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ) والعكس صحيح	

السؤال (5) : تتحدث الفقرة (1) بصفة رئيسية عن :	
(أ) تعريب علم التشفير	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (6) : محلل التعمية هدفه :

(أ) كسر الشفرة	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (7) : إن الذي يكسر الشفرة تقريبا يكون مطمئن (تقريبا) والسبب يرجع إلى أنه يكون معتمدا على اطمئنان المعمى الى :	
(أ) أمان المعلومات وسريتها	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (8) : الضمير في " لأن يوليوس قيصر قد استخدمه أيضاً " يعود على :	
(أ) علم التشفير	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (9) : تتحدث الفقرة (2) بصفة رئيسية عن :	
(أ) أقسام علم التشفير	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (10) : علاقة الفقرة (3) بالـ (2) :	
(أ) سببية	(ب) نتيجة
(ج) توضيح	(د) توكيد
الإجابة : (ب)	

Copy Select All

السؤال (11) : علاقة الفقرة (4) بالـ (1) :	
(أ) نتيجة	(ب) تفسير
(ج) سببية	(د) تحمل نفس المضمون
الإجابة : (د)	

السؤال (12) : تتحدث الفقرة (6) عن إستخدام علم التشفير في أغراض :	
(أ) حربية	(ب) مدنية
(ج) xxxx	(د) xxxx
الإجابة : (أ)	

السؤال (13) : أنسب عنوان للقطعة :	
(أ) علم التشفير تعريفه ، استخدامه	(ب) xxxx
(ج) xxxx	(د) xxxx
الإجابة : (أ)	