#أمنك_مسؤوليتك

كيف نحافظ على ملفاتنا ورسائلنا محمية من خلال عملية "التشفير" ؟

اجعل بياناتك المخترقة غير مجدية لمن تقع بيده

كيف نحافظ على ملفاتنا ورسائلنا محمية من خلال عملية "التشفير" ؟
اجعل بياناتك المخترقة غير مجدية لمن تقع بيده

كلّ ما يمكن تخزينه ونقله عبر شبكة الإنترنت، قد يكون معرضاً للاختراق أو الحصول عليه من قبل طرف ثالث غير مصرح له بذلك، وهو ما يفرض علينا العمل على تشفير ملفاتنا ورسائلنا ذات الأهمية، الأمر الذي ينطبق على جميع مستخدمي الإنترنت، وبخاصة العاملين في مجالات حساسة كالصحافة وتوثيق الانتهاكات والجرائم.

> "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمسّ شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات".
> المادة ١٢ من الإعلان العالمي لحقوق الإنسان

فقد يكلفنا وقوع رسائلنا السرية، أو بياناتنا التي نود مشاركتها بشكل انتقائي، بيد خصومنا خسارات كبيرة، ربما تصل لتعرضنا للاعتقال في بعض الأحيان، أو حتى فقدان الحياة في أحيان أخرى، خاصة في فترات النزاعات والحروب، أو في ظل سيطرة حكومات مستبدة تجد أنه من حقها اختراق كل المعلومات والرسائل، والقضاء على كل ما يخالف توجهاتها وآراءها، بعيداً عن حق الأفراد في الخصوصية وحرية التعبير.

ومن هنا تأتي أهمية **تشفير المعلومات** كقيمة جوهرية في الحفاظ على الأمن الرقمي للمستخدمين وحماية سرية معلوماتهم وخصوصيتها، إذ يُتيح التشفير إخفاء محتوى الرسائل المتبادلة بين شخصين عن أي شخص ثالث قد يعترضها، كما أنه في حال وقوع الملفات المشفّرة بالخطأ في أيدي أشخاص غير مصرّح لهم قراءتها سيبقى محتوى الرسائل غير مقروء بالنسبة لهم.

ويُعد التشفير هو الطريقة المُثلى لحماية المعلومات القيّمة ـ سواءَ كانت مستندات أو صور أو معاملات إلكترونية عبر الإنترنت ـ من الوقوع في أيدي الشخص الخطأ وما قد يترتب على ذلك من مخاطر أمنية.

> يُطلق التشفير على عملية تحويل المعلومات من شكلها المقروء أو الواضح إلى شكل لا يمكن معه قراءتها أو معاينتها إلا للمُصرّح لهم بذلك، وهو يدخل ضمن إطار علم التعمية.

وقد شهدت أساليب التشفير تطوراً واضحاً منذ نشأته وعلى مر العصور حتى يومنا هذا، كما تنوعت تطبيقاته العملية لتشمل مجالات عدة، كالمعلوماتية، والأمنية، والعسكرية، والدبلوماسية، والتجارية والمصرفية.

نشأة علم التشفير وتطوره

ربما لا نخطئ حين نقول إنه ومع بداية الوجود البشري، واكتشاف الإنسان لأهمية التواصل ومشاركة المعلومات مع الآخرين، ظهرت أهمية التواصل الانتقائي وإخفاء المعلومات عن البعض.

فمع تنظيم البشر لأنفسهم ضمن مجموعات تتنافس على الموارد والمأكل والمشرب، كان من الضروري إيجاد طريقة تتواصل فيها كل مجموعة بشكل سري وآمن بعيداً عن المجموعات الأخرى.

ومع ظهور الكتابة ظهر فنّ تشفير الرسائل أو كتابتها على شكل رموز تُتيح للأشخاص المُصرّح لهم فقط قراءتها وفهمها، ورغم اختلاف المؤرخين حول الحضارة التي يُنسب لها ظهور التشفير، يُجمعون على أنه كان لكل حضارة طرقها الخاصة للتواصل بشكل آمن من خلال تشفير الرسائل.

وقد استُخدم التشفير على نحو واسع في المجالين الحربي والعسكري، إذ استخدمه الفراعنة بين قطاعات الجيش عام 2000 قبل الميلاد، كما استخدمه الصينيون لنقل الرسائل أثناء الحروب.

تُعتبر الهيروغليفية والتي كانت تستخدم من قبل المصريين القدماء أقدم تقنية من تقنيات التشفير، ويعود ظهورها لعامي 3200 و3500 قبل الميلاد [1]، إذ كانت الرموز التي تُكتب في هذه التقنية معروفة فقط من قبل الكتبة الذين يقومون بإرسال الرسائل والبرقيات بالنيابة عن الملوك، على عكس الخطين الهيراطيقي الذي حُصر استخدامه بالكهنة، والديموطيقي الذي استُخدم من قبل عامة الشعب.

طوّر الرومان في الفترة ما بين 51 و 58 قبل الميلاد طريقة جديدة للتشفير اعتمدت على استبدال كل حرف في النص الصريح بالحرف المقابل له بعد عكس الترتيب الأبجدي للحروف، وعُرف تشفير الرسائل الموجهة لقادة الحرب آنذاك بإسم "تشفير قيصر" نسبةً إلى الإمبراطور الروماني يوليوس قيصر [2].

وقد كان للعرب والمسلمين دور في تطوير علم التشفير الذي استخدموه في الرسائل العسكرية وتحليل الشفرات، واعتمدوا مصطلح "التعمية" كناية عن عملية تحويل نص واضح إلى نص غير مفهوم باستعمال طريقة محددة.

أما التطور الحقيقي لعلم التشفير فقد شهده نهاية القرن التاسع عشر وبداية القرن العشرين، بعد اختراع آلات خاصة بهذا الغرض ومنها جهاز "إنيغما" الذي استخدمه الجيش الألماني في كتابة رسائله المشفرة إلى عناصر شبكته التجسسية.

---

[1] "تطور الكتابة الهيروغليفية عبر التاريخ، نعود إلى البدايات"، الباحثون السوريون، آخر زيارة 27 -11- 2018، https://www.syr-res.com/article/5230.html.

[2] "شفرة قيصر - ويكيبيديا، الموسوعة الحرة"، موقع ويكيبيديا، آخر زيارة 27 تشرين الثاني/نوفمبر 2018. https://ar.wikipedia.org/wiki/%D8%B4%D9%81%D8%B1%D8%A9_%D9%82%D9%8A%D8%B5%D8%B1

بيعت آلة تشفير الرسائل الألمانية "إنيغما" - والتي حيرت الحلفاء طويلاً خلال الحرب العالمية الثانية- بأكثر من 208 آلاف دولار في مزاد علني بلندن عام 2011، محطمة بذلك الأرقام المتوقعة.

ساهم تطور التشفير الإلكتروني في توسيع دائرة استخدام التشفير، وانتقاله من الاقتصار على المجال العسكري إلى ولوج عالم المؤسسات الحكومية والشركات الخاصة والأفراد.

وكانت "إنيغما" الجهاز الأكثر تطوراً من نوعه، خلال فترة الحرب العالمية الثانية، كما يعتبرها البعض نقطة الانطلاق لظهور الأجيال الأولى من أجهزة الحاسوب الحديثة. ولم يستطع الحلفاء فك رموز الرسائل المشفرة التي كان كانت تُرسل بواسطة تلك الآلة، إلى أن نجحوا في الحصول عليها في إحدى المعارك البحرية، ليتم نقلها إلى مجمع "حديقة بلتشلي" الأسطوري في بريطانيا، حيث تمكنوا من فك شفرتها[3]

ما هي آلية التشفير؟

يعمل التشفير باستخدام شيفرة صيغة رياضية معقدة "خوارزميات"، ومفتاح لتحويل البيانات من نص عادي قابل للقراءة، إلى نص مبهم أشبه بطلاسم لا يستطيع الآخرون فهمه.

تعتمد قوة وفعالية التشفير على عاملين أساسيين: الخوارزمية، وطول المفتاح مقدّراً بالبت (bit).

أما الشيفرة فهي المفتاح الخاص الذي يمكن من خلاله فقط فك التشفير، وهي عادة ما تكون عبارة عن سلسلة طويلة من الأرقام التي تحميها آليات المصادقة المشتركة مثل كلمات المرور، أو الرموز، أو القياسات الحيوية مثل بصمة الأصبع.

كسر التشفير:

يُقابل علم التشفير علم قائم بحد ذاته يعمل على "كسر التشفير" وخرق الاتصالات الآمنة، يستخدمه معترضوا البيانات المشفّرة للتعرّف على محتوى هذه البيانات.

إن ظهور وسائل كسر التشفير دفع مطوري البرامج إلى تحديث وسائل التشفير على نحو مستدام ومتسارع لتوفير وسائل تشفير أكثر جودة، وهو ما دفع أيضاً القائمون على كسر التشفير لرفع مستوى وسائلهم المتبعة، الأمر الذي أدّى إلى خلق حالة من المطاردة المستمرة بين هذين العلمين، في محاولة من كلّ طرف التفوق على الطرف الآخر.

---

[3] "بيع آلة "إنغما" النازية بسعر قياسي في مزاد"، سي ان ان بالعربية، آخر زيارة 27-11-2018، http://archive.arabic.cnn.com/2011/entertainment/9/30/Nazi.enigma/.

أنواع التشفير:

يوجد تقنيتين أو طريقتين يتم استخدامهما للتشفير، تعتمد كل طريقة على أنواع وطبيعة المفاتيح.

1. التشفير المتماثل:

يُطلق عليه أيضاً التشفير التقليدي، يتم من خلاله استخدام نفس المفتاح للتشفير وفك التشفير، لذلك يكون من المهم اعتماد طريقة آمنة لنقل المفتاح بين المرسل والمستلم، إذ يمكن للشخص الذي يملك المفتاح فك التشفير وقراءة محتوى الملفات أو الرسائل.

2. التشفير الغير المتماثل:

يُطلق عليه أيضاً تشفير المفتاح العام، وهو يعتمد على مبدأ زوج المفاتيح، أي يتم استخدام مفتاحين مختلفين في عمليتي التشفير وفك التشفير.

يُعرف المفتاح الأول بالمفتاح العمومي وهو يستخدم لتشفير الرسائل، أما الآخر فيَعرف بالمفتاح الخاص ويُستخدم لفك تشفير الرسائل. في هذه العملية يتم إرسال المفتاح العام لجميع المستخدمين، أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد.

الاتصال المشفّر:

يوفر تشفير البيانات أثناء نقلها من جهاز إلى آخر "عبر الإنترنت أو الاتصال اللاسلكي" حماية فعّالة من اعتراض الاتصال من قبل طرف ثالث، كما يُعتبر من الممارسات الجيدة أيضاً استخدام الاتصال المشفّر عند إرسال أي بيانات عبر شبكة اتصال لاسلكية مثل WIFI، أو عندما تمر البيانات عبر شبكة غير موثوق بها. يمكننا نقل بيانات مشفّرة عبر اتصال غير آمن وهو ما سيَبقي بياناتنا آمنة، كأن نقوم بإرسال مرفق مشفّر ضمن رسالة بريد إلكتروني.

VPN أو "الشبكة الخاصة الافتراضية"

هي الطريقة الأكثر أماناً للاتصال بالانترنت، إذ تقوم بالمحافظة على بيانات المستخدمين ونشاطاتهم مخفية ومشفرة عبر إنشاء نفق وهمي بين الجهاز ومزود خدمة VPN مما يعني عدم قدرة أي أحد على اعتراضها.

برنامج تشفير الملفات: VeraCrypt

هو برنامج مجاني مفتوح المصدر، يسمح لك بتعمية ملفاتك، وهو نُسخة مُحدّثة من مشروع تروكربت المتوقف، كما أنه يُعالج الثغرات الأمنية المُكتشفة في تروكربت.

تشفير الرسائل:

يُعتبر تشفير الرسائل أمراً في غاية الأهمية في الحالات التي يتم فيها نقل رسائل حساسة قد يشكل تبادلها مصدراً كبيراً للخطر على ناقليها، خاصةً في الدول التي تقمع الحريات، الأمر الذي قد يكلّفهم حياتهم.

إنّ إرسال الرسائل الإلكترونية العادية أمر غير محمي، إذ يمكن الوصول إليها واختراقها وسرقة المعلومات التي تحتويها، سواء من قبل قراصنة الإنترنت، أو من قبل الشركة التي توفّر هذه الخدمة، أو قد تقوم بذلك الحكومات.

يُمكن أن يوفر البريد الإلكتروني المشفّر القدرة على تشفير جسم ومرفقات الرسائل الإلكترونية، وهو يستخدم نوع تشفير غير متماثل.

يوجد العديد من البرامج التي تعمل على تشفير رسائل البريد الإلكتروني، الأمر الذي يقي من مخاطر كشف مضمونها أو حتى معرفة صيغة مرفقاتها الحقيقية.

برنامج تشفير الرسائل Kleopatra:

هو برنامج مجاني مفتوح المصدر، يمكّن المستخدمين من نقل رسائل البريد الإلكتروني والملفات بشكل آمن مع مساعدة من التشفير والتوقيع الرقمي.

المؤسسات المشاركة بالحملة:

منظمة سوريون من أجل الحقيقة والعدالة: منظمة سورية مستقلة، تأسست عام 2015، تعمل على توثيق انتهاكات حقوق الإنسان في سوريا، وقضايا المناصرة في المحافل الدولية.

جريدة عنب بلدي: مؤسسة إعلامية سورية مستقلة تأسست عام 2011 في مدينة داريا بريف دمشق، وتصدر مطبوعة أسبوعية، سياسية، اجتماعية، منوعة.

راديو روزنة: إذاعة سورية انطلقت عام 2013، تقدم نشرات ومواجز إخبارية متعددة وبرامج ثقافية وتوعوية وخدمية متنوعة، وتنشط أيضاً عبر موقعها الإلكتروني.

الشبكة السورية للإعلام المطبوع: تأسست عام 2014، وهي تجمّع لصحف ومجلات سورية مستقلة، تعمل على تنسيق الجهود فيما بينها من خلال تبادل الخبرات الصحفية والمهنية.

منظمة آرتا للإعلام والتنمية: وهي منظمة غير حكومية غير ربحية، مقرها في مدينة عامودا بمحافظة الحسكة، تعمل على تطوير مشاريع إعلامية مستقلة وتدريب ودعم صحفيين.

مشروع سلامتك: تأسس عام 2012، يهدف لنشر التوعية والمساعدة حول الأمن الرقمي، عبر تقديم الدعم التقني للمنظمات السورية، والمساعدة التقنية عبر الإنترنت، والتدريب الميداني.

موقع أنا إنسان: يركز على نشر القصص الإنسانية، وبشكل خاص قصص السوريين، بهدف طرح ومعالجة قضايا متعددة، وتوثيق معاناتهم والانتهاكات التي ارتُكبت بحقهم، إلى جانب عرض تجارب نجاحهم وإنجازاتهم.