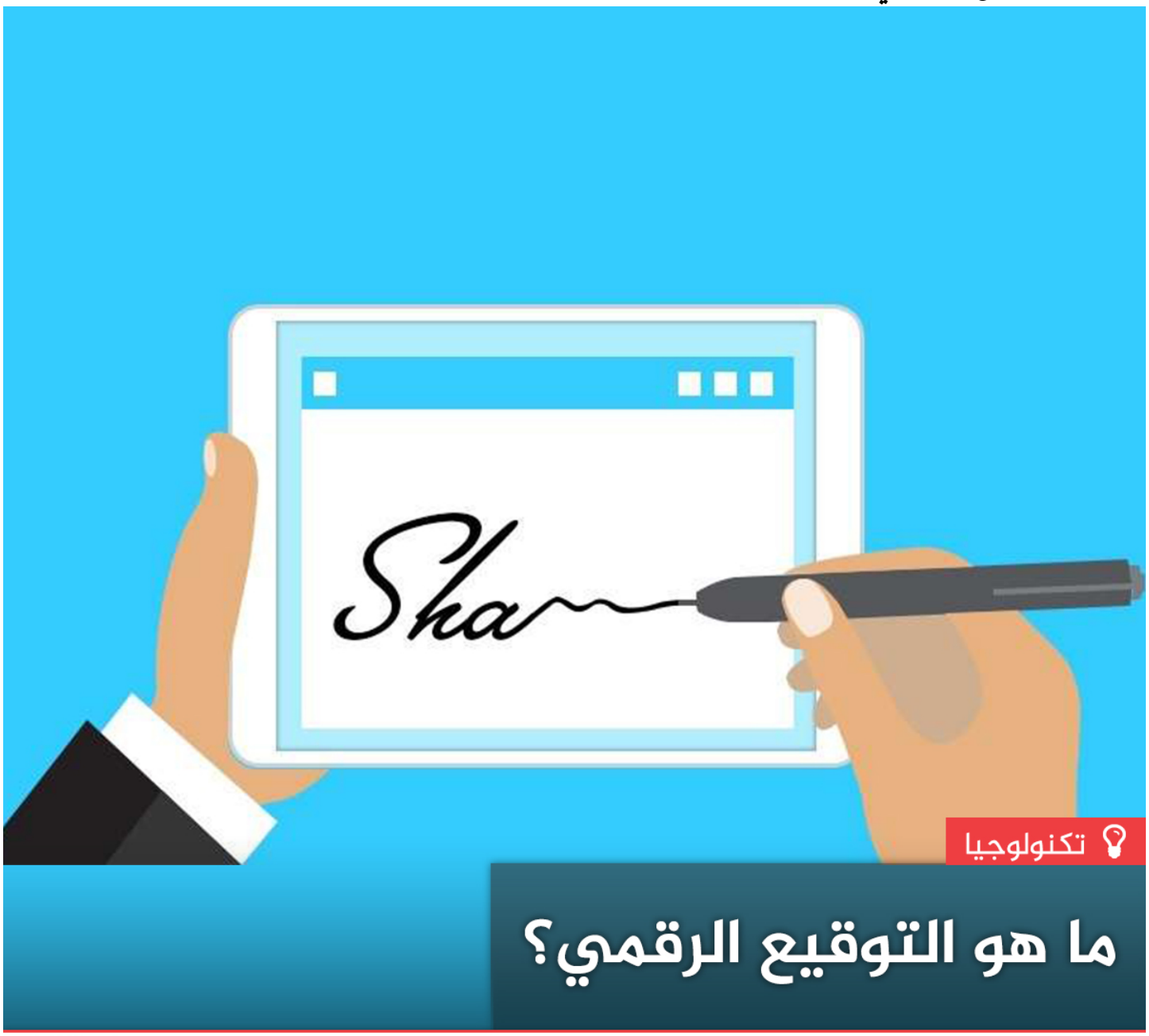
ما هو التوقيع الرقمي؟



التوقيع الرقمي هو في الأصل وسيلةٌ لضمان كون الوثيقة الإلكترونية (البريد الإلكتروني وجدول البيانات والملف النصي وما إلى ذلك) أصيلةٌ، بمعنى أنك تعرف من أنشأ المستند وتعلم أيضًا أنه لم يُغيَّر بأيّ شكلٍ من الأشكال منذ إنشائه.

تستند التواقيع الرقمية على أنواعٍ معينةٍ من التشفير لضمان المصادقة. والتشفير هو عملية أخذ كافة البيانات التي يرسلها جهاز الكمبيوتر إلى جهازٍ آخر وترميزها بشكلٍ يمكن فقط للحاسوب الآخر فك تشفيره. والمصادقة هي عملية التحقق من أن هذه المعلومات تأتي من مصدرٍ موثوقٍ به. وتعمل هاتان العمليتان جنبًا إلى جنب لإنتاج التوقيعات الرقمية.

هناك عدة طرق لمصادقة شخص أو معلومات على جهاز حاسوب:

- كلمة المرور **Password**:

يوفر استخدام اسم المستخدم وكلمة المرور الشكل الأكثر شيوعًا من المصادقة. إذ أنه حالما تقوم بإدخال اسمك وكلمة المرور عندما يطلبها الحاسوب، فإنه يتحقق صحتهما بمقارنتهما مع ملفٍ آمنٍ. فإذا لم يكن الاسم أو كلمة المرور متطابقين، فلن يُسمح لك الوصول إلى أبعد من ذلك.

- المجموع الاختباري **Checksum**:

تُعتبر واحدةً من أقدم الطرق لضمان صحّة البيانات، يُوفر المجموع الاختباري أيضًا شكلًا من أشكال المصادقة، لأن المجموع الاختباري الخاطئ يشير إلى تعرّض البيانات للتغيير بطريقةٍ ما. يُحدَّد المجموع الاختباري بإحدى طريقتين. لنفترض أن طول المجموع الاختباري للحزمة هو 1 بايت، مما يعني أنه يمكن أن يكون الحد الأقصى للقيمة هو 255، إذا كان مجموع البايتات الأخرى في الحزمة 255 أو أقل، فإن المجموع الاختباري يحتوي على القيمة الصحيحة. أما إذا كان مجموع البايتات الأخرى أكثر من 255، هذا يعني أن المجموع الاختباري هو الباقي من القيمة الإجمالية بعد أن قُسِّم على 256. انظر إلى هذا المثال:

البايت 1 = 212
البايت 2 = 232
البايت 3 = 54
البايت 4 = 135
البايت 5 = 244
البايت 6 = 15
البايت 7 = 179
البايت 8 = 80
المجموع = 1151

1151 مقسومًا على 256 يساوي 4.496 (يُقرب إلى أربعة). ناتج ضرب 256 بـ 4 يساوي 1024.
1151–1024 يساوي 127، وهو المجموع الاختباري للبايتات.

- فحص الخلل الدوري **Cyclic Redundancy Check** أو اختصارًا (**CRC**):

يتشابه مفهوم الخلل الدوري مع مفهوم التحقق الاختباري، ولكنه يستخدم قسمة متعدد الحدود **Polynomial division** لتحديد قيمة الخلل الدوري، التي يكون طولها عادةً 16 أو 32 بت. الشيء الجيد المفيد حول الخلل الدوري أنه دقيقٌ جدًا، إذ أنه في حال كان بتًّا واحدًا غير صحيحٍ فلن تكون قيمة الخلل الدوري متطابقةً. كلٌّ من التحقق الاختباري والخلل الدوري مُفيدان في منع الأخطاء العشوائية أثناء عملية توصيل البيانات، ولكن في المقابل يؤمنان حمايةً ضئيلةً من هجومٍ مُتعمدٍ على بياناتك.

تقنيات التشفير الواردة أدناه هي تقنياتٌ أكثر أمانًا

- التشفير بالمفتاح الخاص **Private key encryption**:

لكلّ حاسوبٍ مفتاحًا سريًّا (رمز) يُمكن أن يُستخدم لتشفير حزمة من المعلومات قبل إرسالها عبر الشبكة إلى حاسوبٍ آخر. يتطلب المفتاح الخاص معرفة الحواسب التي ستتصل مع بعضها البعض ويقوم بتثبيت المفتاح على كلٍّ منها. يشابه تشفير المفتاح الخاص في الأساس مفهوم الرمز السري الذي يجب على جهازيّ الكومبيوتر معرفته من أجل فك ترميز المعلومات. في المقابل سيؤمن الرمز المفتاح اللازم من أجل فك ترميز الرسالة. فكّر بالأمر كالتالي:

تقوم بإنشاء رسالة مشفرة وإرسالها إلى صديق، حيث أن كل حرف سيستبدل بالحرف الذي يليه، وبهذا الحالة يصبح حرف الألف باءً وحرف الباء تاءً.... وهكذا. وتكون قد سبق وأخبرت صديقًا موثوقًا بأن المفتاح هو إزاحة بمقدار اثنين. يحصل صديقك على الرسالة ويقوم بفك ترميزها، وأيّ شخصٍ آخر سيرى الرسالة لن يرى إلا كلامًا لا معنى له.

- التشفير بالمفتاح العام **Public key encryption**:

يستخدم تشفير المفتاح العام مزيجًا من المفتاح الخاص والمفتاح العام. المفتاح الخاص معروف من قبل حاسوبك فقط، في حين أن المفتاح العام مُعطى من قبل حاسوبك إلى أيّ حاسوبٍ يريد أن يتصل معه بشكلٍ آمن. لفك ترميز وتفسير رسالة مُشفرة يجب على الحاسوب أن يستخدم المفتاح العام الذي زوّده به الحاسوب المرسل للرسالة، مع المفتاح الخاص به.

يستند المفتاح على قيمة هاشيّة **Hash value** (قيمة التجزئة)، وهي قيمةٌ لرقمٍ مُدخلٍ تُحسب باستخدام خوارزمية هاش **Hash algorithm**. أهم ما يميز القيمة الهاشية أنه من المستحيل تقريبًا استنتاج رقم الإدخال الأصلي بدون معرفة البيانات المستخدمة في إنشاء تلك القيمة.

هنا مثال بسيط:
رقم الإدخال: 10667
خوارزمية التجزئة (الخوارزمية الهاشية): القيمة المدخلة × 143
القيمة الهاشية: 1525381

يمكن أن تلاحظ مدى الصعوبة في معرفة أن قيمة 1525381 تأتي من ناتج ضرب 10667 وَ 143. ولكن إن كنت تعلم أن العدد المضاعف هو 143، عندئذ سيكون من السهل جدًا حساب قيمة 106667.

لكن في الواقع التشفير بالمفتاح العام أكثر تعقيدًا من هذا المثال، ولكن هذا هو جوهر الموضوع. تستخدم المفاتيح العامة عمومًا خوارزمياتٍ معقدةً، وقيماً هاشيةً كبيرة جدًا لتشفير أرقام بـ 40 بت أو حتى 128 بت.

يحتوي العدد الذي حجمه 128 بت 2 مرفوعة للأس 128 من التركيبات المحتملة، وهو عددٌ ضخمٌ مساوٍ لعدد جزيئات الماء في 2.7 مليون حوض سباحةٍ أولمبيٍّ. حتى قطرة الماء الواحدة بإمكانها أن تحتوي على مليارات المليارات من جزيئات الماء.

- الشهادات الرقمية:

يلزم تنفيذ التشفير العام على نطاقه الواسع وجود نهجٍ مختلفٍ، وهنا يأتي دور الشهادات الرقمية. الشهادات الرقمية في الأصل بت من المعلومات يقول إن مصدرًا مستقلًا يُعرف باسم سلطة التصديق **Certificate Authority** يثق بخادم الويب. تلعب الشهادات المرجعية دور الوسيط الذي يثق به كلا جهازي الكومبيوتر. فهي تؤكد على صحة ما يقوله كلّ حاسوبٍ عن نفسه، وتعمل على مشاركة المفتاح العام

لكلّ حاسوبٍ مع الحواسيب الأخرى.

يعتمد معيار التوقيع الرقمي **Digital Signature Standard** أو اختصارًا (**DSS**) على أسلوبٍ من أساليب تشفير المفتاح العام الذي يستخدم خوارزمية التوقيع الرقمي **Digital Signature Algorithm**، أو اختصارًا (**DSA**) وهي صيغةٌ من التواقيع الرقمية صادقت عليها حكومة الولايات المتحدة.

تتكون هذه الخوارزمية من مفتاحٍ خاصٍّ لا يعرفه سوى المُنشئ للوثيقة (المُوقّع) ومفتاحٍ عامٍّ.

يحتوي المفتاح العام على أربعة أجزاء، يمكنك أن تتعلم المزيد عنها في هذه الصفحة.

يمكن أن تصبح بطاقات الدفع الإلكتروني مستقبل العملة. استعن بـ الرابط إن أحببت معرفة كيف يمكن أن تساعد التوقيعات الرقمية في تأمين مستقبل الدفع الإلكتروني.

- التاريخ: 2018-08-12
- التصنيف: تكنولوجيا

#تكنولوجيا #علوم الحاسوب #التوقيع الرقمي #التشفير الرقمي

المصادر

- الصورة
- HowStuffWorks

المساهمون

- ترجمة
  - سهى قاسم
- مُراجعة
  - شريف دويكات
- تحرير
  - روان زيدان
  - رأفت فياض
- تصميم
  - رنيم ديب
- نشر

- يقين الدبعي