التشفير بالمفتاح غير المتناظر (المفتاح العلني)

التشفير بالمفتاح الغير متناظر (Asymmetric key encryption) هو أسلوب من أساليب التشفير يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر، ولهذا السبب سمي بالتشفير الغير متناظر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير، وبالتالي فإنه يسمح بتوزيع صلاحيات التشفير وفك التشفير على الجهات المختلفة بأن يعطي لبعضهم مفاتيح التشفير فقط ويعطي للآخرين مفاتيح فك التشفير.

ويسمى هذا النوع من التشفير أيضا بالتشفير بالمفتاح العلني (public-key encryption)، لأنك تستطيع أن تنشر أحد المفتاحين وهو يسمى المفتاح العلني (public-key)، وتحتفظ بالآخر سريا، ويسمى المفتاح الخاص (private-key).

وعندما تقوم بنشر المفتاح العلني، فإن أي أحد يستطيع استخدامه لتشفير البيانات التي يريدك أن تحصل عليها، لكن لن يتمكن أحد من فك تشفير هذه البيانات باستخدام هذا المفتاح العلني، لأن المفتاح العلني ينفع للتشفير فقط ولا يمكن استخدامه لفك التشفير، أما فك التشفير فيكون باستخدام المفتاح الخاص الذي يكون عندك أنت فقط، وبالتالي أنت ستكون الشخص الوحيد الذي يمكنه قراءة الرسائل التي شفرت لك باستخدام مفتاحك العلني.

وأشهر خوارزميات هذا النوع من التشفير هي خوارزمية RSA (Rivest, Shamir and Adleman) نسبة إلى العلماء الثلاثة الذين وضعوا هذه الخوارزمية.

تبادل البيانات عبر خط معرض للتنصت

إذا احتاج جهازان من أجهزة الكمبيوتر لتبادل المعلومات فيما بينهما على الإنترنت، فإنهما سيواجهان مشكلة سهولة التنصت على اتصال الانترنت لأن بياناتها تنتقل على الشبكة على خطوط غير آمنة. التشفير بالمفتاح العمومي هو أفضل حل لهذه المشكلة.

بعبارات أخرى، إذا كان لديك جهازين هما (أ) و(ب)، وأراد (أ) أن يرسل رسالة مشفرة إلى (ب)، فإن عليه أن يحصل على المفتاح العمومي للجهاز (ب) ويستخدمه لتشفير الرسائل المرسلة إليه، وبما أن (ب) هو الوحيد الذي يملك المفتاح الخاص فإنه الوحيد الذي يستطيع فك تشفير هذه الرسالة، ولنفرض الآن بأن هنالك جهاز ثالث (ج) وهو أيضا يريد أن يرسل رسالة مشفرة إلى (ب) فإنه يستطيع أن يستخدم المفتاح العلني نفسه للجهاز (ب) الذي استخدمه (أ) ليرسل إليه رسالته، وفي نفس الوقت فإن (أ) لا يستطيع أن يعرف محتوى المعلومات التي يرسلها (ج) إلى (ب) ولا (ج) يستطيع أن يعرف محتوى المعلومات التي يرسلها (أ) إلى (ب).

بهذه الطريقة نكون قد اقتربنا كثير من ايجاد حل شامل للاتصال الآمن عبر الشبكة لارسال البيانات الحساسة إلى الخدمات الآمنة، مثل المواقع التي تّظهر القفل الذهبي الصغير في شاشة المتصفح وتبدأ عناوينها بالمقطع https بدلا من http.

عندما نقوم بزيارة واحدة من المواقع الآمنة فإننا نستقبل منها مفتاحها العمومي لنتمكن من تشفير البيانات الحساسة وإعادة ارسالها إلى الموقع، لكن المشكلة التي تطرح نفسها هي: ما الذي يضمن لك بأن الذي أرسل لك هذا المفتاح العمومي هو الموقع الذي تريد التعامل معه؟
ما يحدث في هذا النوع من الهجمات هو أن المخترق يقوم باعتراض الاتصال بينك وبين المزود، بحيث يأخذ البيانات التي أردت ارسالها منذ البداية من جهازك إلى المزود ويرسلها هو إلى المزود من جهازه هو، فيعتقد

المزود بأنك موجود على جهاز المخترق، وفي نفس الوقت، يقوم المخترق بالرد عليك ويرسل إليك المفتاح العلني الخاص به، بدلا من أن تحصل على المفتاح العلني الخاص بالمزود الحقيقي الذي تريد التعامل معه، وعندما تقوم بتشفير البيانات بالمفتاح العلني للمخترق، فإنه سيتمكن من فك تشفيرها باستخدام المفتاح الخاص به.

والحل لهذه المشكلة يكون باستخدام أمر يسمى الشهادات الالكترونية، وهي أيضا تعتمد على تقنية التشفير بالمفتاح العلني.

توثيق صحة البيانات ومصدرها (التوقيع الالكتروني والشهادات الالكترونية)

التبادل الالكتروني الآمن على الانترنت يتطلب وجود طريقة نتأكد منها من شخصية الطرف الذي نتصل به ومن أن الرسائل التي نستقبلها منه قادمة بالفعل منه وأنها ليست رسائل مزورة، والتقنية المستخدمة لتحقيق ذلك تسمى التوقيع الالكتروني (Digital Signing).
في التوقيع الالكتروني، يقوم المزود الذي سيقوم بإرسال رسالة ما للزبون (بغض النظر عن حالة الرسالة من حيث كونها مشفرة أو لا) بتشفير هذه الرسالة النهائية مرة أخيرة باستخدام المفتاح الخاص به، وعندما تصل الرسالة إلى الزبون فإنه يقوم بفك تشفيرها باستخدام المفتاح العلني للمزود، فإذا نتج عن فك تشفير هذه الرسالة النتيجة التي يتوقعها الزبون فإنه يعلم بأن المزود هو بالفعل مصدر هذه الرسالة.

فلاحظ هنا بأننا نقوم بعملية عكسية، فبدلا من أن نشفر الرسالة بالمفتاح العلني ونرسلها للمزود، بحيث لا يتمكن أحد من فكها إلا المزود، فإن المزود يقوم هو بتشفيرها بمفتاحه الخاص ويرسلها إلى الزبون، بحيث يتمكن أي شخص من فك تشفير الرسالة باستخدام المفتاح العلني للمزود، لكن المزود وحده فقط يكون قادرا على تشفيرها باستخدام المفتاح الخاص لأنه وحده الذي يملك المفتاح الخاص، وبالتالي نكون متأكدين من أن الرسائل التي تقبل فك التشفير باستخدام المفتاح العلني للمزود هي رسائل مرسلة من المزود نفسه.

ولاحظ أيضا بأن الرسائل في هذه الحالة تكون عادة مشفرة مرتين، في المرة الأولى تشفر الرسالة الأصلية المحتوية على المعلومات الحساسة بالمفتاح العلني للزبون حتى لا يتمكن أحد من فك تشفيرها سوى الزبون، وتشفر بعد ذلك هذه الرسالة المشفرة نفسها مرة أخرى باستخدام المفتاح الخاص للمزود ليثبت للزبون بأنه هو الذي قام بارسال الرسالة وذلك بأنها تقبل فك التشفير بالمفتاح العلني للمزود.

خوارزمية ال ار اس ايه RSA

في علم التشفير، RSA (ليونارد أدليمان وأدي شامير ورون ريفيست) هي قاعدة للتشفير بواسطة مفتاح عام. كانت القاعدة الأولى المعروفةً بكونها مناسبة للتّوقيع بالإضافة إلى تشفير، وكانت أحد التقدّمات العظيمة الأولى في التشفير بواسطة مفتاح عامّ. آر إس إيه مستخدم في بروتوكولات التّجارة الإلكترونيّة على نطاق واسع، ويُعْتَقَد أن تكون مضمونة على اعتبار انه يوجد مفاتيح طويلة بشكل كافي واستعمالَ أحدث التطبيقاتِ.

-

طريقة عمل الخوارزميةَ

خوارزمية آر إس إيه تَتضمّنُ مفتاح عامّ ومفتاح خاصّ. المفتاح العامّ يُمْكِنُ أَنْ يُعْرَفَ إلى كُلّ شخصِ ومستعملُ لتَشْفير الرسائلِ. الرّسائل المشفّرة بالمفتاح العامّ يمكن أن تُفَكّ فقط باستخدام المفتاح الخاصّ. المفاتيح لقاعدة آر إس إيه وُلِّدَتْ بالطّريقة التّالية:

(1) اختر عددين أوّليّين عشوائيّين كبيرين تختلفين P و Q

(2) حساب $n = p * q$ ، n يُسْتَخْدَم كالمعامل لكلا المفاتيح الخاصّة والعامّة

(3) نحسب ال $\varphi(n) = (p-1)(q-1)$، $\varphi(n)$ كمّ من الأعداد بين 1 و n أوليه نسبيًا إلى n

(4) اختر عدد صحيح e بشرط أن يكون $1<e<\varphi(n)$ و $\gcd(e, \varphi(n)) = 1$

(5) باستخدام خوارزمية اقليدس الموسعة نحسب العدد الصحيح المميز d, حيث $1<d<\varphi(n)$

المفتاح العامّ يتكوّن هو (e,n) المفتاح السري هو (d,n)

تَشْفير الرسائل

المرسل A يفعل التالي:

(1) يحصل على المفتاح العام للمستقبل B والذي هو (n, e). (مفتاح التشفير العام)
(2) يحول الرساله من لغه إلى رقم صحيح عن طريق بروتوكول قابل للعكس .
(3) ايجاد ناتج التشفير لكل رقم عن طريق المعادله $c = m^e \bmod n$
(4) إرسال الناتج عن القسمه c إلى المستقبل.B

فك تَشْفير الرسائل

المستقبل B يفعل التالي:

(1) يستخدم مفتاحه الخاص (d, n) لحساب $m = c^d \bmod n$
(2) يستخلص اللغة أو محتوى الرساله الأصلي من العدد الصحيح m

مثال:

(1) اختيار اثنين من الاعداد الأولية: p=61 and q=53
(2) حساب $n= pq$ $n=61*53 = 3233$
(3) حساب $\varphi(n) = (p-1)(q-1$ $\varphi(n)= (61-1)(53-1) = 3120$
(4) اختيار $e > 1$ ، $e=17$ الذي ليس له اي عامل مشترك غير ال 1 مع ال 3120
(5) حساب d خوارزمية اقليدس الموسعة d=2753

المفتاح العام هو (n= 3233, e= 17). ومعادلة التشفير هي $c= m^e \% n = m^{17} \% 3233$:

المفتاح الخاص هو(n=3233, d=2753) ، ومعادلة فك التشفير هي $m=c^d \% n = c^{2753} \% 3233$:

على سبيل المثال، لتشفير $m = 123$ ، نحسب $c = 123^{17} \bmod 3233 = 855$

أو لفك تشفير $c = 855$ ، نحسب $m=855^{2753} \bmod 3233 = 123$

علينا أولا أن نختار عددين أوليين وليكن p و q (يفضل أن يكونا أعداد كبيرة)

1- نحسب جداء p و q وليكن الناتجه هو n
2- نجري عملية التالية $(p-1)*(q-1)$ وليكن الناتج هو z
3- نختار عدد اولي أكبر من الواحد وأقل من z وليكن e
4- نطبق خوارزمية اقليدس الممددة Extended Euclidean algorithm لكي نحصل على العدد d

5- المفتاح العام سيكون (e,n) والمفتاح الخاص سيكون(d,n)

6- عملية التشفير ستجرى كالتالي : c = ASCII code ^ e mod n

7- عملية فك التشفير ستكون كالتالي : m = ASCII code ^ d mod n

خوارزمية إقليدس هي خوارزمية لحساب القاسم المشترك الأكبر لعددين طبيعيين، تظهر أهميتها الأساسية في عدم الحاجة لتحليل العددين للتمكن من حساب قاسمهما المشترك الأكبر

لقاسم المشترك الأكبر لعددين طبيعيين A ، B يساوي القاسم المشترك الأكبر للعدد الثاني B وباقي قسمة A على B، ونكرر العملية نفسها حتى يصبح باقي القسمة مساويا الصفر، عندئذ يكون القاسم المشترك الأكبر هو العدد الآخر .

$$GCD(A,B) = GCD(B,r) \cdots\cdots GCD(N,0)$$

حيث r هو باقي قسمة A على B. N هو القاسم المشترك الأكبر.

الخوارزمية الإقليدية الممددة Extended Euclidean algorithm

يمكن تمثيل القاسم المشترك الأكبر للعددين عن طريق دمج خطي مع عددين آخرين ، وذلك كالتالي

GCD(x،y) = m*x + n*y

يمكن أيجاد قيمتي n و m وذلك عن طريق خوارزمية اقليدس الممتدة وهناك ثلاثة طرق لمعرفة هذه القيم (الطرق هي مشابه لبعض، لكن يمكن القول أنها مختصره من الأخريات). الطريقة الأولى: وهي يمكن ان نطلق عليها التراجع وفي هذه الطريقة نقوم بالحل عن طريق خوارزمية اقليدس وبعدها تقول بالتراجع الخلفي لايجاد قيمتي m، n كما في المثال التالي:

مثال: قم بتمثيل العددين 26 و 21 بطريقة اقليدس الممتدة : فنبدأ بالحل كما هو الحال في طريقة اقليدس :

26 = 21 *1 + 5

و 21 = 5 * 4 + 1

و 5 = 1 * 5 + 0

وتتوقف عند الصفر.

الآن المعادلة التي قبل المعادلة التي باقيها صفر أي المعادلة الثانية نقوم بكتابتها بالشكل التالي 1 = 21 - 5 * 4

أيضا المعادلة الأولى بنفس الشكل $5 = 26 - 1 * 21$ ، نعوض هذه المعادلة في المعادلة السابقة

1 = 21 – 4 * (26 – 1 * 21)

ومن غير أجراء عملية حسابية، فقط نفك القوس لينتج:

1 = 21 - 4*26 + 4*21

1 = 1*21 - 4*26 + 4*21

1 = - 4*26 + 5*21

اذاً قيمة m هي 5 وقيمة n هي - 4 .