ويكيبيديا
الموسوعة الحرة

خوارزمية آر إس إيه

خوارزمية رافيست وشامير وأدلمن	
Rivest–Shamir–Adleman	
معلومات عامة	
المطورون	ليونارد أدليمان وآدي شامير ورونالد ريفست
تاريخ النشر	1977
معلومات التشفير	
طول المفتاح	2,048 أو 4,096 بت
[الإنجليزية]	
تعديل مصدري - تعديل	

في علم التعمية، آر إس إيه (بالإنجليزية: RSA) هي خوارزمية تعمية بواسطة مفتاح عام.[1][2][3] ولعلها الأولى المعروفةً على هذا الصعيد. هي مناسبة للتّوقيع بالإضافة إلى التعمية. كانت أحد التقدّمات العظيمة الأولى في التعمية بواسطة مفتاح عامّ. آر إس إيه مستخدم في بروتوكولات التّجارة الإلكترونيّة على نطاق واسع، وهي آمنة طالما كان طول المفتاح طويلا جدا مثل: 1024 بت. تعتمد بشكل كبير على أنَّه لا توجد خوارزمية لتحليل عدد لعوامل بسرعة عالية.

آر إس إيه هي نسبيا خوارزمية بطيئة. لهذا السبب، لا تستعمل عادة من أجل تعمية كمية كبيرة من البيانات، بل تستعمل من أجل تعمية المفاتيح المستعملة في خوارزمية أخرى ثم تبادلها، كالخوارزميات ذات المفاتيح المتناظرة. بعدئذ، تستعمل الخوارزميات ذات المفاتيح المتناظرة من أجل تعمية كمية كبيرة من البيانات.

تاريخ الخوارزمية

وُصِفَتْ الخوارزمية علناً في عام 1977 من قبل ليونارد أدليمان وآدي شامير ورونالد ريفست في معهد ماساتشوستس للتقنية، الأحرف آر إس إيه هي الحروف الأولى من اسمائهم. وَصفَ كليفورد كوكس، عالم رياضيّات بريطانيّ يعمل مع جي سي إتش كيو (GCHQ) وكالة مخابرات المملكة المتّحدة، نظاماً مكافئاً في وثيقةٍ داخليةٍ في عام 1973. لكنّه نظرا لغلاء الحواسيب نسبيا الضرورية لتنفيذ هذا النظام في ذاك الوقت، تم اعتبار هذا النظام وكأنه فضول فقط، فلهذا لم يُنْشَر أبدًا. لكنّ اكتشافه لم يُكْشَف حتّى 1997 بسبب تصنيفه السّرّيّ للغاية، وريفيست وشامير وأدليمان ورثوا أو أكملوا آر إس إيه (RSA) عن شغل كليفورد كوكس.

مُنِحَ معهد مساشوستس للتكنولوجيا براءة اختراع ل«نظام وطريقة اتصالاتِ مشفّرة» الذي استعملت الخوارزميةَ في عام 1983. انتهت صلاحية براءة الاختراع في 21 سبتمبر 2000. ولأنه تم نشر ورقة تصف الخوارزميةَ في أغسطس 1977، قبل ديسمبر 1977 (وهو تاريخ تقديم الطلب لبرائة الاختراع)، أعاقت القوانين في مُعظم بقيّة العالمِ براءاتَ الاختراع في مكان آخر وبراءة الاختراع الأمريكيّة فقط هي التي كانت تمنح.

إنتاج المفاتيح

تَتضمّنُ خوارزمية آر إس إيه مفتاحا عامّا ومفتاحا خاصّا. المفتاح العامّ هو مفتاح التعمية فقط ويجب أن يكون معلوما لكل من يحاول الاتصال بمالك المفتاح. كما يدل على ذلك اسمه، هو مفتاح عام. لابأس في أن يعلمه جميع الناس. يمكن أن تُفَكّ الرسائل المشفّرة بالمفتاح العامّ فقط باستخدام المفتاح الخاصّ. كما يدل على ذلك اسمه، هو مفتاح خاص. لا ينبغي أن يعلمه أحد. المفاتيح لقاعدة آر إس إيه تُولد بالطريقة التالية:

1. اختيار عددين أوّليّن عشوائيّن كبيرين مختلفين q و p.
2. حساب $n = p \cdot q$. يُسْتَخْدَم n معاملا لكلا المفتاحين الخاصّ والعامّ.
3. حساب $\phi(n) = (p-1)(q-1)$.حيث أنَّ الدالة $\phi(n)$ تعطي عدد الأعداد التي بين 2 و n والتي هي أولية مع n أي أنه $GCD(n,i) = 1$ حيث $2 \le i \le n$. تسمى هذه الدالة مؤشر أويلر.
4. اختيار عدد صحيح بشكل عشوائي e حيث $2 \le e \le \phi(n)$ و $GCD(\phi(n), e) = 1$ (أي أنَّ العددين e و- $\phi(n)$ (يعني أنَّ $e \in \mathbb{Z}_n^*$) أوليين فيما بينهما). هذا العدد e سوف يكون الأُس العمومي.
5. ايجاد قيمة d أو المفتاح الخصوصي، بحيث أنَّه يُحقق التالي: $d \cdot e \equiv 1 (mod\ \phi(n))$, ويمكن حساب المعادلة الاخيرة بواسطة خوارزمية اقليدس المُوسعة. d سوف يكون الأُس الخصوصي.

المفتاح العمومي يتكوّن من المعامل n والأُس العمومي e (encryption)

المفتاح الخصوصي يتكوّن من المعامل n والأُس الخصوصي d (decryption), والذي يجب أن يكون سريا للحفاظ على امان الخوارزمية.

تعمية الرسائلِ

لنفرض أن A وB يريدان أن يتواصلا فيما بينهما. لنفرض أنَّ مفتاح A العمومي هو (n_A, e_A) أما المفتاح الخصوصي هو (n_A, d_A) ومفتاح B العمومي هو (n_B, e_B) والمفتاح الخصوصي (n_B, d_B) .

لنفرض أنَّ A يريد أن يرسل رسالة إلى B , لذا عليه فعل التالي:

1. يحصل على المفتاح العام للمستقبل B والذي هو (n_B, e_B) .
2. وجد ناتج التعمية لهذا الرقم عن طريق المعادلة $c = m^{e_B} (mod\ n_B)$
3. يُرسِل c إلى B.

ملاحظة:

- إذا كانت الرسالة مكتوبة بالحروف حينها يجب أولا تحويلها لشكل مناسب حيث يتوافق مع العمليات الحسابية ويمكن أن يتم هذا بتحويل الرسالة إلى نظام أسكي.

فك تعمية الرسائلِ

ليحصل B على الرسالة يفعل التالي:

يستخدم مفتاحه الخاص (n_B, d_B) ويحسب $m = c^{d_B}\,(mod\; n_B)$. حينها m هي الرسالة التي بعث بها A

صحة الخوارزمية

في كل نظام تعمية أهم خصلة يجب ان تتوفر فيه أنَّه يحقق الصفة التالية: $D(E(m,e),d) = m$ أي أنَّه إذا شفرنا رسالة ثم فككنا التعمية نحصل على نفس الرسالة. وهذا أيضا صحيح ل-RSA : $E(m,e) = m^e\,(mod\; n)$ وفك التعمية هو:

$$D(E(m,e),d) = (m^e)^d\,(mod\; n) \;= m^{ed}\,(mod\; n) \;= m^{ed\;(mod\;\phi(n))}\,(mod\; n) \;= m^1\,(mod\; n) = m$$

مثال

1. اختيار اثنين من الاعداد الأولية: $p = 61$ and $q = 53$
2. حساب $n = p \cdot q$ أي نفذ التالي $n = 61 \cdot 53 = 3233$
3. حساب $\phi(n) = (p-1)\cdot(q-1)$ حيث أنَّ $\phi(n)$ هو مؤشر أويلر. $\phi(n) = (61-1)(53-1) = 3120$.
4. اختيار $e > 1$ الذي ليس له أي عامل مشترك مع 3120 , مثل $e = 17$.
5. نختار d بحيث: $d \cdot e \equiv 1(mod\;\phi(n))$, مثلا نختار: d = 2753 وهو ملائم لانه: $2753 \cdot 17(mod\; 3120) \equiv 46801(mod\; 3120) \equiv 1$

المفتاح العمومي هو (n= 3233, e= 17). لذا فإنَّ التعمية كالتالي: $c = m^e\,(mod\; n) = m^{17}\,(mod\; 3233)$

المفتاح الخصوصي هو (n=3233, d=2753)، لذا فإنَّ فك التعمية كالتالي: $m = c^d\,(mod\; n) = c^{2753}\,(mod\; 3233)$

لنفرض انَّه يُراد تعمية m = 123، وهذا يكون كالتالي: $c = 123^{17}\,(mod 3233) = 855(mod\; 3233)$

وفك تعمية c = 855، يكون ب- $m = 855^{2753}\,(mod\; 3233) = 123$.

خوارزميات مُساعدة

الرفع بواسطة التربيع المتكرر

فليكن a,k,n اعداد صحيحة عندها يمكن حساب $a^k\,(mod\; n)$ والتعقيد الحسابي للخوارزمية هو: $O((\log_2 k)(log_2^2 n))$ والخوارزمية كالتالي:

```
int exp_mod(a,k,n)
{
   int d=1;
   int aa=a;
   while(k>0)
   {
      if(k%2==1)
      {
         d=(d*a)%n;
      }
      k=(k-k%2)/2;
      aa=(aa*aa) %n;
   }
}
```

صحة هذه الخوارزمية تعتمد على أنّه يمكن كتابة كل عدد k بواسطة النظام الثنائي أي أنَّه: $k = k_0 + k_1 \cdot 2 + \cdots + k_{s-1} \cdot 2^{s-1}$ حينها كل ما علينا هو حساب $2^{2^j}\,(mod\; n)(j = 1, 2, \cdots, s-1)$

مثال: نريد أن نحسب: $y = 1311^{134}\,(mod\; 39979)$

1. نحسب 134 بالنظام الثنائي: وهو $134 = 128 + 4 + 2 = 2^7 + 2^2 + 2^1$
2. نحسب $T_j = 1311^{2^j}$ لكل $1 \le j \le 7$ بطريقة التربيع المتكرر أي:

$$T_1 = T_0^2\,(mod\; 39979)$$

$$T_2 = T_1^2\,(mod\; 39979)$$

$$\vdots$$

$$T_7 = T_6^2\,(mod\; 39979)$$

3. حينها y يكون حاصل ضرب كالتالي:

$$\ldots od\; 39979) \;= 1311^{2^7+2^2+2^1}\,(mod\; 39979) = 1311^{2^7}\,(mod\; 39979) \cdot 1311^{2^2}\,(mod\; 39979) \cdot 1311^{2^1}\,(mod\; 39979) \;= T_7 \cdot T_2 \cdot T_1 \;= 17236$$

حساب مقلوب عدد

في خوارزمية RSA أردنا أن نجد d بحيث يتحقق: $ed \equiv 1(mod\phi(n))$ لذا فإنه علينا أن نجد: $d \equiv e^{-1}(mod\phi(n))$ لذا سوف نستخدم خوارزمية اقليدس المُوسعة والسبب هو: بما أنَّ $gcd(e,\phi(n)) = 1$ حينها يمكن ايجاد عددين صحيحين a,b بحيث $a \cdot e + b \cdot \phi(n) = 1 \Rightarrow (a \cdot e + b \cdot \phi(n))(mod\ \phi(n)) = 1(mod\ \phi(n)) \Rightarrow a \cdot e = 1(mod\ \phi(n))$, لذا فان العدد a سوف يكون d . الخوارزمية تعقيدها: $O(log_2^2(n))$.

امان الخوارزمية

- أيسر الوسائل لخرق امان الخوارزمية هي ايجاد عوامل العدد n , لنقل انه يمكن ايجاد عوامل n بالإضافة لنفرض أنَّ $n = p \cdot q$ حينها وبما أنَّ المفتاح العمومي موجود ولنفرض أنّه e لنجد المفتاح الخصوصي d :

1- نجد مؤشر أويلر للعدد n : $\phi(n) = (p-1)(q-1)$

2- نحل المعادلة $ed \equiv 1(mod\ \phi(n))$

لذا فانه من السهل خرق الامان في الخوارزمية إذا ما توجد خوارزمية تحليل لعوامل بسرعة. ولكن لا يوجد خوارزمية سريعة لفعل هذا ! لذا يمكن اعتبار هذا الخرق غير مُعتبر.

ملاحظة: بيتر شور، في عام 1997 قدم خوارزمية سريعة لايجاد العوامل ولكن ذلك كان بمساعدة ادوات فيزيائية بالتحديد بواسطة الحسابات الكمومية. وهذه الخوارزمية لا تُعتبر قابلة للبرمجة لانها تحتاج حاسوب كمومي وهو غير موجود للأن (أي عام 2013) ولكن هناك بصيص من الامل لامكانية اختراع مثل هذه الحواسيب.

- p و- q لا يجب أن يكون قريبين جدا خشية ان التحليل إلى العوامل على طريقة «فيرمات» ل n ان تكون ناجحة، إذا p و q على سبيل المثال هم اقل من $2n^{\frac{1}{4}}$ سوف يكون الحل ل p و q سهل. بالإضافة إلى ذلك إذا كانت أي من p -1 أو q-1 لهم عوامل اولية صغيرة فقط، ممكن ان تحلل n إلى عواملها يشكل سريع عن طريق «خوارزمية بولارد» وهذه القيم ل p و q يجب أن تهمل.
- من المهم ان يكون المفتاح السري كبير كفاية، حيث اثبت السيد michel wiener في عام 1990 انه إذا $q \leq p \leq 2q$ و $d < \frac{n^{1/4}}{3}$ فان d يمكن حسابها على نحو كاف من قيم n و e. لا يوجد هجوم معروف ضد الاسس الصغيرة العامة مثل e=3 باشتراط استخدام تبطين مناسب، على كل حال في حين عدم استخدام تبطين أو عمله بشكل خاطيء فان الاسس الصغيرة العامة لها مخاطرة أكبر تؤدي إلى هجوم، كما هو الحال في ضعف النص الصريح غير المبطن. 65537 هو قيمة تستخدم في غالب الأحيان ل e. هذه القيمة من الممكن ان تعتبر انها حل وسط بين تجنب الهجومات الاسية الصغيرة المحتملة ومع ذلك تسمح بالتعمية ات الفعالة.

إيجاد أعداد أولية

لإيجاد أعداد أولية p و q نختار بشكل عشوائي أعدادا ويتم فحصها. لذا كل ما يُحتاج إليه هو وسيلة لفحص الأولية بطريقة سريعة. هناك عدة خوارزميات منها خوارزميات احتمالية مثل اختبار ميلر-رابن لأولية عدد ما وأخرى حتمية مثل اختبار أ.ك.أس.

السرعة

RSA أبطا بكثير من ال DES ونظم التعمية المتناسقة. مع التجربة على سبيل المثال أحمد يقوم بتعمية رسالة سرية بواسطة خوارزمية متناسقة، يشفر المفتاح التناسق بواسطة ال RSA ومن ثم يبعث المفتاح المتناسق المشفر بواسطة الRSA والرسالة المشفرة تعمية ا تناسقيا إلى سهيلة. هذا الاجراء يرفع المزيد من الاحتياطات الأمنية. فعلى سبيل المثال: المهمة الكبرى هي استخدام مولد ارقام عشوائية قوي للمفتاح المتناسق لان توفيق (مختلس السمع يريد ان يرى ما تم بعثة) يمكن ان يجتاز الRSA فقط بتخمين المفتاح المتناسق.

توزيع المفاتيح

كما في كل الشيفرات، كيفية توزيع مفاتيح آر إس إيه العامة مهم جدا الأمن. يجب أن يكون توزيع المفاتيح آمنا جدا ضد هجوم الرجل في الوسط. لنفترض أن توفيق له طريقة ما لإعطاء أحمد مفاتيح تحكمية وجعله يصدق أن هذه المفاتيح هي مفاتيح سهيلة. لنفترض أيضا أن سهيلة قادرة على أن تقطع الرسائل بين أحمد وتوفيق. سهيلة تقوم بارسال مفتاحها العام لأحمد والتي يعتقد أحمد أنها مفاتيح توفيق، ومن ثم يستطيع توفيق أن يقطع أي نص مشفر مرسل بواسطة أحمد ومن ثم فك تعمية ه بمفتاحه السري الخاص وابقاء نسخة من هذه الرسالة ومن ثم تعمية ها بمفتاح سهيلة ثم إرسال النص المشفر الجديد لسهيلة. في الحقيقة أن أحمد وسهيلة لا يستطيعوا أن يكشفوا وجود توفيق. الدفاعات ضد هذه الهجومات كثيرا ما تكون معتمدة على الشهادات الرقمية أو مكونات أخرى للبنية التحتية للمفتاح العام.

انظر أيضا

- دالة وحيدة الاتجاه
- تبادل مفتاح ديفي-هيلمان
- نظرية التعقيد الحسابي

المراجع

1. Calderbank، Michael (20 أغسطس 2007). "The RSA Cryptosystem: History, Algorithm, Primes" (PDF)". مؤرشف من الأصل (PDF) في 2016-12-13.
2. Probabilistic encryption & how to play mental poker keeping secret all partial information, Annual ACM Symposium on Theory of Computing, 1982. نسخة محفوظة 31 مارس 2020 على موقع واي باك مشين.
3. Coppersmith، Don (1997). "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities" (PDF). *Journal of Cryptology*. ج. 10 ع. 4: 233–260. DOI:10.1007/s001459900030. مؤرشف من الأصل (PDF) في 2017-09-22.