خوارزميّة Diffie-Hellman !

إعداد: أحمد الشنقيطي.

الحمد لله الذي بحمده يُستفتح كل كتاب و بذكره يُصدر كل خطاب وبفضله يتنعم أهل النعيم في دار الجزاء و الثواب والصلاة و السلام على سيد المرسلين و إمام المتقين المبعوث رحمة للعالمين محمد ابن عبد الله الصادق الأمين و على صحابته الأخيار و من تبعهم بإحسان إلى يوم الدين أما بعد :

في هذه المقالة, سأضع بين أيديكم شرحا لخوارزمية Diffie-Hellman و كلي أمل بأن يستفيد الجميع.

قمتُ بإدخال بعض الروابط المهمة في بعض الكلمات للذين يريدون الاستزادة, الكتابة الغليظة ذات اللون الأزرق تدل على وجود رابط, مثل هذه الكتابة الفريق العربي للبرمجة.

شُكر خاص للأخ الفاضل Fear.83 الذي قام بتصميم غلاف الكتاب.

تاريخ كتابة المقالة 06/08/2012

الكاتب في سطور:

الإسم: أحمد ابن محمد

اللقب: الشنقيطي

سنة الميلاد: 1992

الدولة: بلاد شنقيط و أرض المليون شاعر .. موريتانيا

الهواية: programming & Security

المستوى الأكاديمي: خريج كلية العلوم و التقنيات.

للتواصل: ahmed.ould_mohamed@yahoo.fr

فهرس المحتويات

1. مُقدمة 5
1.1 - ما هو التشفير ؟ 5
1.2 - التشفير في العصر القديم 5
1.3 - التشفير الحديث 6
2. نظرة تحليلية على الخوارزمية 8
2.1 - فكرة الخوارزمية 8
2.2 – البروتوكول 8
2.3 – مثال تطبيقي 10
2.5 - التعقيد الزمني 10
3. الخاتمة 11
4. المراجع 11

1. مُقدمة

- ما هو التشفير ؟
- التشفير في العصر القديم
- التشفير الحديث

1.1 - ما هو التشفير ؟

هو عملية يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية, حيث يمكن للشخص الذي يعرف المفتاح و خوارزمية التشفير, فك الشفرة (أي استعادة المعلومات الأصلية), يمكن أيضاً أن يقوم شخص آخر لا يعرف المفتاح و لا الخوارزمية بفك الشفرة !! و تُسمى العملية هنا "عملية غير مخولة".

في عام 1900 قبل الميلاد لم تكن هناك سوى مصطلحات هيروغليفية, استخدم الإنسان التشفير منذ حوالي ألفي عام قبل الميلاد لحماية رسائله السرية, وبلغ هذا الاستخدام ذروته في فترات الحروب, خوفا من وقوع الرسائل الحساسة في أيدي الأعداء, فالحروب دائما كانت الملهم الأكبر لظهور خوارزميات التشفير.[1]

1.2 - التشفير في العصر القديم

يُعد **علم التشفير** من أقدم العلوم الموجودة في يومنا هذا حيث تمتد أصوله إلى زمن **الفراعنة** و **القياصرة** أيضا, فقد كان الفراعنة أول من قام بعملية التشفير للتراسل بين قطاعات الجيش, دون أن ننسى أن أفضل طريقة استُخدمت في القدم هي طريقة يوليوس قيصر (**Julius Caesar**) وهو أحد قياصرة الروم, كما استخدم الصينيون القدامى طُرقا عديدة في علم التشفير والتعمية لنقل الرسائل السرية أثناء الحروب, فقد كانوا يستخدمون التشفير من أجل إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه يصعب عليه فهمها.

كما يُعتبر علماء المسلمين و العرب أول من اكتشف طرق استخراج المعمَّى [2], من أشهرهم العلامة **يعقوب بن إسحاق الكندي** و **ابن وَحشِيَّة النبطي** الذي كشف اللثام عن رموز الهيروغليفية قبل أن يكتشفها العالم الفرنسي **Jean-François Champollion** بعشرة قرون !! [3], و كذلك اشتهر **ابن دريهم** الذي كان لا يشق له غبار في فك التشفير فكانت تُعطى له الرسالة معماة فما إن يراها حتى يحولها في الحين إلى العربية ويقرئها .. وله قصيدة طويلة يشرح فيها مختلف الطرق في تعمية النصوص وكان يحسن قراءة الهيرغليفية.[4]

يعتبر البعض أن طريقة الألغاز كانت من أوائل الطرق المُستخدمة قديما في التشفير, فكانوا يأخذون مثلا جملة مثل (ادفع لي أجرا) ويدخلون كل حرف في بداية كلمة جديدة فتصبح (إذا دخل فاروق عليه لباس يبدو أكثر جمالا راتبه أكثر) وللحصول على الجملة المطلوبة نأخذ الحروف التي تبدأ بها كلمات الجملة الجديدة فتحصل على (ادفع لي أجرا).

لكن هذه الطريقة صعبة جداً خاصة إذا كانت حجم المعلومات المُراد إرسالها كبيراً حيث تكمن صعوبتها في إيجاد جمل تحمل المعلومات المطلوبة ولها مدلول واضح لا يثير الشك، لذا فإن هذا النوع نادراً ما يُستخدم في الوقت الحالي.

1.3 - التشفير الحديث

في العصر الحديث, تُعد آلة **Enigma** 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 المعلوماتية.

في نهاية السبعينات من القرن المنصرم, و مع الاستخدام المُكثف لأجهزة الكمبيوتر, دخل علم التشفير مرحلة جديدة حيث أصبح البعض يُسميه "التشفير الحديث" (Modern cryptography) و مع التطور السريع الذي يشهده مجال الحماية و الأمن, أصبحت الحاجة ملحة لطرق تشفير قوية, لأن زيادة سرعة الكمبيوتر تعني قصر الوقت الذي يحتاجه الأخير لكسر أو كشف مفتاح تشفير معين.

يرجع الفضل في إظهار مفهوم التشفير الغير متناظر إلى الرائدين **Whitfield Diffie** و **Martin Hellman**, حيث قدَّما هذا المفهوم لأول مرة في **المؤتمر الوطني للحاسوب** في عام 1976 [5] قبل أن يتم نشره بعد بضعة أشهر في "التوجهات الجديدة في علم التشفير" (New Directions in Cryptography) [6].

يظل المخترع الأب مُختفيا خلف الكواليس - كما يحدث دائما في تاريخ التشفير - إذْ يعتبر البعض [7] أن الباحث الأمريكي **Ralph Merkle** هو أول من اكتشف فكرة "تشفير المفتاح العام" (**Cryptography Asymmetric**) بشكل مستقل, رغم أن كتاباته [8] عن الموضوع لم تُنشر إلا مؤخرا.

لم يستطع كل من W. Diffie و M. Hellman تقديم مثال حي على نظام المفتاح العام في البحث الذي قدماه سنة 1976. كان يجب عليهم أن ينتظروا سنة1978 للحصول على مثال واقعي[9] مُقدم من طرف الثلاثي المميز :

Adi Shamir, Ronald Rivest and Leonard Adleman

2. نظرة تحليلية على الخوارزمية

2.1 - فكرة الخوارزمية

2.2 - البروتوكول

2.3 – مثال تطبيقي

2.5 - التعقيد الزمني

2.1 - فكرة الخوارزمية

تُعتبر **خوارزمية D-H** الأول من نوعها في موضوع تبديل **المفاتيح**, حيث تسمح لشخصين (عادة ما يُطلق عليهما Alice و Bob) بتبادل بيانات حساسة دون أن يفهمها الطرف الثالث (المتصنت) حتى و لو حصل على نسخة منها. تعتمد الخوارزمية في عملها على إنشاء مفتاح سري مشترك يمكن استخدامه فيما بعد لتشفير المحادثات باستخدام خوارزمية تشفير مفتاح متماثل Symmetric-key.

2.2 – البروتوكول

- ليكن n و B العددان الصحيحان اللذان اختارهما كل من Alice و Bob علناً, n و B يجب أن يكونا أوليين فيما بينهما.
- سريا, تختار Alice بدورها عددا صحيحا بشكل عشوائي, نُسميه a, ثم تحسب العدد $A = B^a \% n$ ثم تُرسل - علناً - العدد الجديد إلى Bob.
- يقوم Bob بنفس الحركة السابقة: يختار بشكل سري عددا عشوائيا g ثم يحسب $G = B^g \% n$ ثم يُرسل الناتج إلى Alice.

☜ من الآن فصاعدا, كل طرف يملك نتيجة حساب الآخر, Alice ما عليها سوى حساب $G^a \% n$ و Bob $A^g \% n$ و انتهى الأمر !

في الحقيقة, فإن العددان السابقان متساويان :

$$\begin{cases} G = B^g \% n \Rightarrow G^a \% n = (B^g)^a \% n = B^{ag} \% n; \\ A = B^a \% n \Rightarrow A^g \% n = (B^a)^g \% n = B^{ag} \% n; \end{cases}$$

الآن, أصبح Alice و Bob يمتلكان العدد $B^{ag} \% n$ و الذي لا يعرفه أحد سواهما, يمكنهما استخدام هذا العدد كمفتاح, و يمكنها أن يتبادلا البيانات الحساسة أمام الجميع ...!

لكن, **كيف يمكن هذا ؟؟**

لا يُمكن للطرف الثالث (المتصنت) أن يعرف العدد a أو g (هذا العددان ضروريان لإيجاد $B^{ag} \% n$), العددان السابقان لا يدخلان ضمن المعلومات المتبادلة علنا, المعلومات التي يمكن للمتصنت الحصول عليها هي n, B, A and G و لتحديد a انطلاقا من A يجب تخطي عقبة **Discrete logarithm** التي من المستحيل "عمليا" كسرها حتى يومنا هذا.

كيف تتأكد Alice من وصول الرسالة إلى Bob و عدم تحريفها ؟

عندما تُرسل Alice رسالة سوف يتم تشفيرها بالمفتاح الخاص بها أو المفتاح العام التابع لـ Bob، بحيث تتحول هذه الرسالة إلى رموز لا يمكن فهمها ويتم إرفاق معها توقيع المُرسل.

عند إذن يقوم المستقبل بإرسال نسخه من التوقيع الالكتروني إلى الجهة المختصة بإصدار الشهادة، لتتأكد من صحة التوقيع ومن ثم تقوم أجهزة الكمبيوتر التابعة للجهة المختصة بالتحقق من صحة التوقيع وتُعاد النتيجة للمستقبل مرة أخرى، ليتأكد من صحة وسلامة الرسالة، فيقوم المستقبل بقراءة الرسالة وذلك باستخدام مفتاحه الخاص إذا كان التشفير قد تم على أساس رقمه العام أو بواسطة الرقم العام للمرسل إذا تم التشفير بواسطة الرقم الخاص للمرسل، ومن ثم يجيب على المرسل باستخدام نفس الطريقة وهكذا تتكرر العملية، و يُستخدم أيضا مع التوقيع الالكتروني عملية الهاش التي توفر تكلفة أقل من تشفير الرسالة بحيث تقوم بإنشاء قيمة رقمية معينة تكون أصغر من الرسالة بحيث تضمن عدم تغييرها, عندما يستقبل المستخدم الرسالة و الهاش يقوم بعملية الهاش مرة أخرى على هذه الأخيرة ومن ثم يقارن ما بين الهاش الأصلي و الهاش المُستقبل, إذا كانت القيم متساوية فهذا يدل على سلامة البيانات من التحريف والتزوير وإذا اختلفت القيم دل ذلك على تزوير الرسالة. [10]

2.3 – مثال تطبيقي

الجزء **الأخضر** يُمثل البيانات العامة التي يتم تبادلها أمام الجميع الجزء **الأحمر** يُمثل البيانات الخاصة بكل طرف:

Chez Alice	Publique (internet)	Chez Bob
	On choisit un nombre premier arbitraire commun: **p = 419** On choisit un nombre aléatoire commun inférieur à p: **g = 7**	
Alice choisit un nombre aléatoire secret: **Ax = 178**		Bob choisit un nombre aléatoire secret: **Bx = 344**
Ay = 7^{178} modulo 419 = 208		**By = 7^{344} modulo 419 = 49**
Ay = 208	⟶	**Ay = 208**
By = 49	⟵	**By = 49**
s = 49^{178} modulo 419 = 107		**s = 208^{344} modulo 419 = 107**
	⟵ échange de données chiffrées avec **s** ⟶	

يُمكن لـ Alice و Bob أن يستخدما العدد 107 كمفتاح لتشفير الرسائل المُتبادلة بينهما [11]، عمليا نستخدم أعداد ضخمة جدا و لكن الهدف هنا هو توضيح الفكرة فقط.

2.5 - التعقيد الزمني

عند تطبيق الخوارزمية سيتم حساب أربع exponentiations mod p, باستخدام خوارزمية **الأس المعياري السريع** فإن وقت التنفيذ يتغير بتغير حجم العدد p الذي عادة ما يكون عددا أوليا ضخما.

إذا أردنا تبادل مفتاح حجمه L سيكون عدد الـ binary operations يساوي:

$$\theta\left(4 * log^3(L)\right)$$

3. الخاتمة

إلى هنا أصل بك أخي القارئ إلى نهاية هذه الجولة السريعة, بالطبع الموضوع شيق و طويل أيضا, ما زالت هناك العديد من النقاط التي كنت أود التحدث عنها (لكن أخاف أن يزيد الحجم عن حجم المقالة القياسي) مثل كتابة **الخوارزمية بلغة الجافا** أو **السي++** و إدراج **خوارزمية DSS** في D-H من أجل إضافة التواقيع الرقمية (Digital **signature**) إلى البيانات المتبادلة و الكثير الكثير من النقاط المهمة التي ربما أكتب عنها لاحقا.

4. المراجع

(**1**) : **ما هو التشفير (Cryptographic) ؟** (موسوعة الأسئلة والإجابات الحرة)

(2) : THE CODEBREAKERS, David Kahn, page 93 ; Kahn on Codes, David Kahn, page 41

(**3**) : **كتاب علم التعمية واستخراج المعمَّى عند العرب.**

(**4**) : **ابن الدريهم وجهوده في علم التعمية (التشفير)**, الدكتور محمد حسان الطيان.

(5) : W. Diffie and M.E. Hellman, Multiuser cryptographic technics, Proceedings of AFIPS National Computer Conference, 109-112, 1976

(6) : W. Diffie and M.E. Hellman, New directions in cryptography, IEEE transactions on information theory, 22(1976), 644-654

(7) : A.J. Menezes, P.C Van Oorschot, S.A. Vanstone, Handbook of applied cryptography, CRC Press, 1997, p47

(8) : R.C. Merkle, Secure communications over insecure channels, Communications of the ACM, 21(1978),294-299

(9) : Ronald Rivest, Adi Shamir, Leonard Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM, 21(1978), 120-126

(**10**) : التوقيع الالكتروني .. خطوة إلى الأمام, جريدة الخليج الإماراتية – الملحق الاقتصادي

(**11**) : **Exemple d'algorithme asymétrique : Diffie–Hellman**

(**12**) : **La Naissance de la Cryptographie Asymétrique**, Guénaël Renault, SALSA – LIP6/UPMC – 14 mars 2012