الفصل الثاني عشر

أنظمة التعمية ذوات المفتاح المعلن
Public–Key Cryptography

الخاصية الأساسية التي تميز بين أنظمة التعمية ذوات المفتاح المعلن وأنظمة التعمية التقليدية (أنظمة التعمية ذوات المفتاح المتماثل) هي الفصل بين عمليتي التعمية وكشف المعمى. ولكي نكون أكثر دقة، يتكون المفتاح k في أنظمة التعمية ذوات المفتاح المعلن من زوج مرتب $k = (e,d)$ حيث يستخدم e للتعمية و d لكشف المعمى. وفي هذا الإطار يكون e مفتاح معلن و d مفتاح سري يحتفظ فيه فقط من يحتاج لكشف الرسائل المعماة. ولكي يكون النظام آمناً كنظام تعمية يجب أن يكون من الصعب على العدو الذي بحوزته e والنص المعمى c من حساب m حيث $E_e(m) = c$.

كان أول ظهور لفكرة أنظمة التعمية ذوات المفتاح المعلن في العام ١٩٧٦م أثناء محاولة ديفي (Diffie) وهيلمان (Hellman) توزيع مفاتيح عبر قناة غير آمنة ولكنها موثوقة. إن هذا يعني في إطار الشكل (١٠,١) أن كل من أليس وبوب متأكدين من أصل وموثوقية الاتصالات عبر قناة غير آمنة مع وجود تنصت من قبل العدو حواء. والمسألة هنا هي المحافظة على السرية (على الرغم من تنصت حواء على قناة الاتصال) دون الاعتماد على جزء القناة السري في الشكل لنقل المفاتيح أو أي معلومات أخرى. الخطة المطروحة لتبادل المفاتيح هي على النحو التالي:

يختار كل من أليس وبوب عدداً أولياً p ومولِّداً α للزمرة $\mathbb{Z}_p^*$ ويعلنان عنهما. تختار أليس سراً عددًا عشوائيًا a ، $1 \leq a < p$ ثم ترسل α^a إلى بوب علنا (على مرأى وسماع حواء)[1]. وبالمثل، يختار بوب سراً عدداً عشوائيًا b ، $1 \leq b < p$ ويرسل α^b إلى أليس. تقوم أليس بحساب $\left(\alpha^b\right)^a \pmod p$ ويقوم بوب بحساب $\left(\alpha^a\right)^b \pmod p$. وبهذا يحصلان على المفتاح السري المشترك $k = \alpha^{ab} \pmod p$ ويستخدمانه بعد ذلك كمفتاح تعمية لنظام تقليدي مثل نظام DES. من المؤكد أن حواء تتمنى معرفة المفتاح السري k ولكي تستطيع ذلك يكون عليها حل مسألة ديفي وهيلمان (DHP) المرتبطة بمسألة اللوغاريتم المنفصل (DHP).

DHP : إذا كان p عدداً أولياً وكان α مولِّداً للزمرة $\mathbb{Z}_p^*$ وإذا علمت α^a و α^b فجد α^{ab}.

DLP : إذا كان p عدداً أولياً وكان α مولِّداً للزمرة $\mathbb{Z}_p^*$ وإذا علمت α^x فجد x.

من الواضح أن DHP ≤ DLP. أي يمكن حل مسألة DHP بزمن حدودي بمعرفة خوارزمية حدودية لحل مسألة DLP. وفي بعض الحالات الخاصة يكون أيضاً DLP ≤ DHP ولكن الحالة العامة مسألة تنتظر الحل (انظر [63]). يعتمد أمن اتفاقية ديفي وهيلمان لتبادل المفاتيح على افتراض صعوبة حل مسألة DHP.

تستخدم أنظمة التعمية ذوات المفتاح المعلن للتغلب على بعض الصعوبات التي تواجهها أنظمة التعمية التقليدية. فمثلاً، تقترح اتفاقية ديفي وهيلمان لتبادل المفاتيح إمكانية المحافظة على سرية التواصل من خلال قنوات غير آمنة (من المهم هنا افتراض موثوقية قناة الاتصال حيث إن اتفاقية تبادل المفاتيح ليست آمنة بوجود عدو نشط وسنوضح ذلك في البند (**١٢,٥**)) ولذا نستطيع القول إن توزيع المفاتيح لا يحتاج إلى

---

(١) α^a يعني $\alpha^a \pmod p$ ولكننا حذفنا "$\mod p$" للسهولة طالما أن المعنى واضح من السياق.

ناقل مؤتمن بافتراض إمكانية توثيق المفاتيح المعلنة. وبما أنه من المفترض أن يكون التوثيق أسهل من تبادل المفاتيح السرية لأنظمة التعمية التقليدية فنرى عدم ضرورة شرط السرية في أنظمة التعمية ذوات المفتاح المعلن.

ومن الميزات الأخرى لأنظمة التعمية ذوات المفتاح المعلن هي استخدام عدد أقل من المفاتيح. على سبيل المثال، إذا كان عدد مستخدمي نظام تعمية هو n فنحتاج إلى توزيع $\binom{n}{2}$ من المفاتيح في النظام التقليدي مقارنة مع توزيع $2n$ من المفاتيح في النظام المعلن وهو توفير كبير وخاصة عندما يكون n كبيراً.

أحد التطبيقات الأخرى على أنظمة التعمية ذوات المفتاح المعلن هو التوقيع الإلكتروني (Digital Signature) الذي سنناقشه في البنود اللاحقة. في هذه التطبيق يكون بمقدور أليس توقيع رسالة بطريقة تقنع بها بوب أن الرسالة مصدرها هو بالفعل أليس. وأكثر من ذلك حيث يستطيع بوب أيضاً إقناع مصدر ثالث بذلك. المشكلة الأساسية في استخدام أنظمة التعمية التقليدية في التوقيع الإلكتروني تكمن في أن المعلومات التي بحوزة أليس هي نفس المعلومات التي بحوزة بوب، ولذا فهما بحاجة إلى مصدر ثالث موثوق للتوقيع، وهذه المشكلة محلولة عند استخدام أنظمة التعمية ذوات المفتاح المعلن حيث تزودنا هذه الأنظمة بحل رياضي عملي لهذه المشكلة.

(١٢,١) دوال الاتجاه الواحد ودوال التمويه
One-Way And Hash Functions

نناقش في هذا البند مفهومين أساسين للتعمية، هما دوال الاتجاه الواحد ذوات الباب السري وهذا المفهوم من أساسيات أنظمة التعمية ذوات المفتاح المعلن. أما المفهوم الآخر والشائع الاستخدام في خطط التوقيع الإلكتروني فهو دوال التمويه (أو الدوال التعموية).

دوال الاتجاه الواحد

نقول إن الدالة $f : M \to C$ دالة اتجاه واحد إذا كان من السهل حساب $f(m)$ لكل $m \in M$ ولكن لكل $c \in C$ من الصعب حسابياً إيجاد m يحقق $f(m) = c$. يعتقد أن الدالة التي قدمناها في البند (**١٠,٣,٢**) لكلمات السر المستخدمة في يونكس (Unix) هي دالة اتجاه واحد (تحت سقف بعض القدرات الحسابية) حيث يتم تخزين (كلمة السر واسم المستخدم) f عوضاً عن كلمة السر نفسها[٢]. ودالة أخرى يعتقد أنها دالة اتجاه واحد هي دالة القوة المنفصلة. أي الدالة $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ المعرفة بالقاعدة $f(a) \equiv \alpha^a \pmod p$ حيث p عدد أولي و α مولِّداً للزمرة $\mathbb{Z}_p^*$.

لا يوجد برهان رياضي على وجود دوال اتجاه واحد. ولذا فأنظمة التعمية ذوات المفتاح المعلن تفترض أن بعض الدوال المعينة هي دوال اتجاه واحد آمنة للفترة المستخدمة. سنناقش في البنود القادمة بعض دوال الاتجاه الواحد المستخدمة في أنظمة التعمية ذوات المفتاح المعلن.

نقول إن دالة اتجاه واحد هي دالة ذات باب سري (trapdoor) إذا توفرت معلومات اضافية تسمح بإيجاد m يحقق $f(m) = c$ لكل c. دوال الاتجاه الواحد ذوات الباب السري هي الدوال المستخدمة في أنظمة التعمية ذوات المفاتيح المعلنة.

مثال (١٢,١,١) (تطبيقات على دوال الباب السري)

المحافظة على السر (Confidentiality): يختار كل مستخدم A دالة اتجاه واحد ذات باب سري خاصة به f_A ثم يعلن عنها. لإرسال رسالة سرية m إلى A يقوم المرسل باستخدام f_A ومن ثم يرسل الرسالة $c = f_A(m)$. وبما أن A هو الوحيد الذي لديه

---

(٢) كان هناك اعتقاد أن القيم المخزنة معلومة لجميع مستخدمي النظام مما يؤدي إلى كسر النظام ومن ثم معرفة كلمة السر حيث أن معظم المستخدمين للنظام يستعلمون كلمات سر سهلة التخمين. تطلب الأنظمة الحديثة كلمات سر أفضل وتقوم بتخزين المعلومات بشكل سري.

المعلومات السرية التي تسمح بإيجاد معكوس f_A فيكون بإمكانه معرفة الرسالة $m = f_A^{-1}(c)$. لاحظ عدم استطاعة المرسل من الحصول على m من c. لم نحتاج في هذه التطبيق إلى تبادل المرسل و المستقبل معلومات سرية ولكن من الضروري التأكد من موثوقية المفتاح المعلن.

منع التزوير (non-repudiation): هذا التطبيق هو رديف التوقيع الكتابي. المطلوب هو توقيع أليس لرسالة m بحيث يكون بإمكان بوب اقناع طرف ثالث بأن مصدر الرسالة m هو بالفعل أليس. لنفرض أن m مذيلة بمعلومات زائدة. إذا كانت $f_A : M \to M$ هي دالة اتجاه واحد ذات باب سري التي اختارتها أليس فإنها تقوم بإرسال $s = f_A^{-1}(m)$ إلى بوب. يقوم بوب بحساب $m = f_A(s)$ وتكون الرسالة الموقعة هي الزوج المرتب (m, s). من الممكن أن يكون باستطاعة العدو حساب $m = f_A(s)$ لنص مختار s ولكن تذيل m يمنع مثل هذا التزوير. وإذا كانت السرية مطلوبة في هذا التواصل فبإمكان أليس إرسال $c = f_B(s)$ عوضاً عن s حيث f_B دالة الاتجاه الواحد ذات الباب السري التي اختارها بوب.

دوال التمويه التعموية

نقول إن $H : X \to Y$ دالة تمويه إذا لم تكن دالة أحادية. لكل $x \in X$ يسمى $H(x)$ تمويه x ويستخدم كمعَرِّف للعنصر x. وبما أن H دالة غير أحادية فلابد من وجود $x_1 \neq x_2$ بحيث يكون $H(x_1) = H(x_2)$. من بين أهداف إنشاء دالة تمويه هي وضع شروط تفصل بين التصادمات ووجود خوارزمية فعالة لحساب قيم التمويه $H(x)$.

في العادة تكون عمليات التعمية في أنظمة التعمية ذوات المفتاح المعلن مكلفة حسابياً وعملية توقيع رسائل طويلة يحتاج زمن طويل. ولهذا أثناء التطبيق العملي تستخدم دوال التمويه لإنشاء ما يسمى الرسالة الملخصة (message digest) للرسالة المطلوب توقيعها ومن ثم يتم توقيع الرسالة الملخصة. ولكي نضمن أمن هذه العملية فيجب أن تتحقق في دالة التمويه خواص إضافية.

تعريف (١٢,١,٢)

دالة التمويه التعموية هي دالة $H : \{0,1\}^* \to \{0,1\}^*$ تحقق ما يلي:

(١) توجد خوارزمية فعالة لحساب H.

(٢) (مقاومة الصورة العكسية). لكل $y \in \{0,1\}^n$ يكون من الصعب حسابياً إيجاد $x \in \{0,1\}^*$ حيث أن $H(x) = y$.

(٣) (مقاومة التصادم). يكون من الصعب حسابياً إيجاد $x_1 \neq x_2 \in \{0,1\}^*$ حيث $H(x_1) = H(x_2)$.

حتى الآن لم يتم البرهان على وجود دوال تمويه تعموية؛ (لأن الشرطين (١) و (٢) يؤديان إلى أنها دالة اتجاه واحد)، ومع ذلك يستخدم عدد من الدوال التي يعتقد أنها دوال تمويه تعموية في التحقق من صواب البيانات وخطط التوقيع.

مثال (١٢,١,٣) (تطبيق على التوقيعات)

لتوقيع رسالة m، تقوم أليس بحساب التمويه وتوقيعه وبعد ذلك ترسل كل من الرسالة والتوقيع على $H(m)$ إلى بوب الذي يقوم بحساب $H(m)$ والتحقق من صواب التوقيع. تسمى الخطة الذي تتطلب وجود الرسالة نفسها أثناء عملية التحقق بالتوقيع الإلكتروني مع الملحق (digital signature scheme with appendix). ▲

إذا لم تكن دالة التمويه H مقاومة للصورة العكسية فبإمكان العدو (وربما بوب) بعد أن يحصل على توقيع صائب على $H(m)$ من تزوير توقيع أليس وذلك بإيجاد رسالة m' تحقق $H(m') = H(m)$ ومن ثم الحصول على توقيع صائب للرسالة m'.

إذا كان $m \neq m'$ حيث $H(m) = H(m')$ فباستطاعة أليس الخداع بحيث توقع الرسالة m وتدعي أن الرسالة التي وقعتها هي m'. ومن الممكن أن يجد العدو مثل هذا التصادم ومن ثم يقنع أليس بالتوقيع على إحدى الرسالتين.

افترضنا في المثال السابق أن التوقيع يضمن عدم التلاعب في التمويه الذي قامت أليس بحسابه. وبصورة عامة إذا وجدت آلية لحماية قيمة التمويه فيكون باستطاعتنا

استخدام دالة التموية للتحقق من عدم التلاعب في البيانات المقابلة لذلك. وفي هذا الإطار، تسمى دالة التمويه هذه التي لا تحتاج إلى مفتاح سري (مفتوحة)، شفرة اكتشاف معدلة (modification detection code) أو اختصاراً MDC. أما دالة التمويه التي تحتاج إلى مفتاح سري (مقفولة) لتوثيق مصدر البيانات فتدعى شفرة توثيق رسالة (message authentication code)، اختصاراً MAC. الدالة CBC-MAC المقدمة في البند (**١٠,٣,٢**) مثال على مثل هذه الدوال.

يوجد عديد من دوال التمويه التي يتم تصميمها باستخدام أنظمة التعمية القالبية، أحدها هي الدالة المقفولة CBC-MAC ودالتين مفتوحتين نقدمهما في المثالين التاليين.

مثال (١٢,١,٤) (تمويه ماتياس ومايز وأوسيز)

لنفرض أن E نظام تعمية قالبي حيث $\mathcal{K}$ فضاء المفاتيح. لنفرض أن $E_k : \{0,1\}^n \to \{0,1\}^n$ وأن $g : \{0,1\}^n \to \mathcal{K}$ دالة معلنة وأن H_0 قيمة ابتدائية معلنة تنتمي إلى $\{0,1\}^n$. تعرف الدالة $H : \{0,1\}^* \to \{0,1\}^n$ على النحو التالي:

(١) نفرض أن $x = x_1 x_2 \dots x_t$ حيث x_i كلمة ثنائية طولها n.

(٢) نفرض أن $H_i = E_{g(H_{i-1})}(x_i) \oplus x_i$، $1 \le i \le t$. عندئذ، $H(x) = H_t$.

يبين الشكل (**١٢,١أ**) مخطط هذه الدالة. ▲

إذا بدلنا x_i مع H_{i-1} في المثال السابق فسنحصل على دالة التمويه التالية مع ملاحظة التغيير في كتابة x.

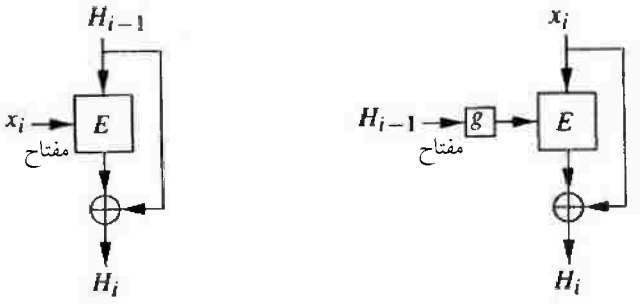
مثال (١٢,١,٥) (تمويه ديفز ومايز)

لنفرض أن E نظام تعمية قالبي طول قالبه يساوي n مرتبة ثنائية ويستخدم مفاتيح طول كل منها يساوي k مرتبة ثنائية. لنفرض أن H_0 قيمة ابتدائية معلنة تنتمي إلى $\{0,1\}^n$. تعرف الدالة $H : \{0,1\}^* \to \{0,1\}^n$ على النحو التالي:

(١) نفرض أن $x = x_1 x_2 \dots x_t$ حيث x_i كلمة ثنائية طولها k.

(٢) نفـــرض أن $H_i = E_{x_i}(H_{i-1}) \oplus H_{i-1}$ حيـــث $1 \le i \le t$. عندئـــذ، $H(x) = H_t$.

مخطط هذه الدالة مبين في الشكل (**١٢,١ب**).



(أ) تمويه ماتياس ومايز وأوسيز (ب) تمويه ديفز ومايز

الشكل (١٢,١). دوال تمويه مفتوحة تعتمد على نظام تعمية قالبي.

يجب أن يكون طول الرسالة المدمجة التي تولدها دالة تمويه مفتوحة كافياً لمنع هجوم تاريخ الميلاد (بحث عشوائي للحصول على تصادم). من المتوقع الحصول على تصادم في دوال التمويه ذات الطول n بعد $2^{n/2}$ عملية على الأكثر. على وجه الخصوص كل من دالتي التمويه المقدمتين في الشكل (**١٢,١**) غير محصنة لمنع التصادم إذا كان $E = DES$. طول الرسالة المدمجة لدالة التمويه المشهورة المعروفة باسم خوارزمية التمويه الآمنة (secure hash algorithm) أو اختصاراً $SHA-1$ يساوي 160 مرتبة ثنائية وطول الرسالة المدمجة لدالة تمويه مشهورة أخرى تدعى الرسالة المدمجة الخامسة أو اختصاراً $MD5$ يساوي 128 مرتبة ثنائية (كلا الدالتين يعتمد على $MD4$ والرمز MD يعني خوارزمية رسالة ملخصة والرقم 4 يعني ترتيب الخوارزمية في سلسلة خوارزميات قدمها رايفست).

تمارين

(١٢,١,٦) لنفرض أن $g : \{0,1\}^* \to \{0,1\}^*$ دالة تمويه مقاومة للتصادم. ولنفرض أن الدالة h معرفة على النحو التالي:

$$h(x) = \begin{cases} 1 \,||\, x & \text{إذا كان طول } x \text{ يساوي } n \text{ مرتبة ثنائية} \\ 0 \,||\, g(x) & \text{ما عدا ذلك} \end{cases}$$

حيث الرمز '||' يعني ضم أو تسلسل (concatenation). أثبت أن h دالة تمويه طولها $n+1$ مقاومة للتصادم ولكنها ليست مقاومة للصورة العكسية (انظر [63] ، ملحوظة **(٩,٢٠)**).

(١٢,١,٧) هذا التمرين هو المثال **(٩,٦٤)** من [63] ويبين الحيطة الواجب أخذها عند إنشاء MAC من MDC. لنفرض أن h هي MDC معرفة استقرائياً على رسالة $x = x_1 \dots x_t$ على النحو التالي:

$$H_i = f(H_{i-1}, x_i)$$
$$h(x) = H_t$$

حيث H_0 هي قيمة ابتدائية معطاة. يمكن تحويل h إلى MAC بضم مفتاح سري k بحيث تكون MAC على الرسالة x هي:

$$M = h(kx)$$

أثبت إمكانية استخدام معرفة الزوج المرتب (M,x) في تزوير MAC على xy دون الحاجة لمعرفة المفتاح السري k.

(١٢,١,٨) هذا التمرين مأخوذ من التمرين **(٧,٤)** (انظر [86]). لنفرض أن p و q عددان أوليان حيث كل من $p' = 2p+1$ و $q' = 2q+1$ عدداً أولياً. ولنفرض أن $n = p'q'$. لنفرض أيضاً أن $\alpha \in \mathbb{Z}_n^*$ من الرتبة $2pq$. لتكن الدالة $h : \mathbb{Z} \to \mathbb{Z}_n^*$ معرفة بالقاعدة:

$$h(x) \equiv \alpha^x \pmod{n}$$

إذا كان $h(x_1) = h(x_2) = h(x_3)$ فأثبت وجود خوارزمية فعالة لتحليل n بمعرفة تصادم مناسب على x_i. وضح الخوارزمية عندما يكون $n = 77$ و $\alpha = 2$ حيث $h(9) = h(69) = h(129)$.

(١٢,٢) نظام RSA

RSA Cipher

يستخدم نظام RSA المشهور الذي تم اكتشافه في العام ١٩٧٧م من قبل رايفست وشامير وأدلمان (Rivest, Shamir, and Adleman) في أغراض التعمية وخطط التوقيع الإلكتروني. يعتمد أمن نظام RSA على فرضية صعوبة مسألة تحليل الأعداد. يعرف نظام RSA على النحو التالي:

(١) لنفرض أن $p \neq q$ عددان أوليان كبيران وأن $n = pq$ و $\varphi = (p-1)(q-1)$.

(٢) اختار قوة تعمية عشوائياً e ، $1 < e < \varphi$ حيث $(e, \varphi) = 1$.

(٣) استخدم خوارزمية إقليدس لإيجاد قوة كشف المعمى d ، $1 < d < \varphi$ حيث $ed \equiv 1 (\mathrm{mod}\, \varphi)$.

(٤) عرف $f : \mathbb{Z}_n \to \mathbb{Z}_n$ على النحو التالي:

$$f(m) \equiv m^e (\mathrm{mod}\, n)$$

يعتقد أن دالة RSA (الدالة f) هي دالة اتجاه واحد ذات باب سري d. فإذا كان d معلوماً فتوجد خوارزمية فعالة لإيجاد m من $c = f(m)$ وذلك باستخدام الخاصية $ed \equiv 1 (\mathrm{mod}\, \varphi)$. لإثبات ذلك، نفرض أولاً أن $p \nmid m$. بما أن:

$$ed = 1 + k\varphi = 1 + k(p-1)(q-1)$$

حيث $k \in \mathbb{Z}$ وأن $m^{p-1} \equiv 1 (\mathrm{mod}\, p)$ (استناداً إلى مبرهنة فيرما الصغرى) نجد أن:

$$m^{ed} = m^{1+k\varphi} = m\left(m^{p-1}\right)^{k(q-1)} \equiv m (\mathrm{mod}\, p)$$

أما إذا كان $p \mid m$ فنجد أن $m^{ed} \equiv 0 \equiv m(\mathrm{mod}\, p)$. وبالمثل، يمكن إثبات أن:

$$m^{ed} \equiv m(\mathrm{mod}\, q)$$

وبما أن p و q أوليان نسبياً فنخلص إلى أن:

$$m^{ed} \equiv m(\mathrm{mod}\, n)$$

إذن،

$$c^d \equiv \left(m^e\right)^d \equiv m(\mathrm{mod}\, n)$$

وبهذا يمكن إيجاد m من c باستخدام خوارزمية التربيع وهي خوارزمية فعالة.

تسمى مسألة إيجاد f^{-1} دون معرفة d مسألة RSA وتنص على:

لنفرض أن $n = pq$ حيث $p \neq q$ عددان أوليان ولنفرض أن e عدد صحيح موجب أولي نسبياً مع $\varphi = (p-1)(q-1)$ وأن c عدد صحيح. جد m بحيث يكون:

$$m^e \equiv c(\mathrm{mod}\, n).$$

إذا كان تحليل n معلوماً فمن الممكن حساب d ومن ثم الحصول على m بطريقة فعالة. ولكن من المعلوم أن تحليل n حيث p و q عددان أوليان مختاران بعناية مسألة صعبة المنال.

يقدم التمرين (**١٢,٢,١٢**) خوارزمية فعالة لتحليل n إذا علمنا قيمة d. وبهذا تكون مسألة تحليل n ومسألة حساب d بمعرفة n و e متكافئتان حسابياً. بهذا التكافؤ يكون لدينا دليل على أن مسألة RSA ومسألة تحليل n هما مسألتان درجة صعوبتهما متساوية ولكن لم يتم تقديم برهان رياضي لذلك(٣).

في نظام RSA، المفتاح المعلن هو (n,e) والمفتاح السري هو d. إذا كان $0 \leq m \leq n-1$ فإن تعمية m هي:

$$c \equiv m^e(\mathrm{mod}\, n)$$

---

(٣) قدم كل من بونيه وفانكاتيسان (Boneh and Venkatesan) في المرجع [15] دليلاً على أن كسر نظام RSA حيث قوة التعمية e صغيرة لا يمكن أن تكافئ مسألة التحليل.

وكشف المعمى هو:

$$m = c^d (\mathrm{mod}\, n).$$

مثال (١٢,٢,١) (مثال صفي على RSA)

لنفرض أن العددين $p = 7$ و $q = 13$ استخدما لتوليد مفتاح نظام RSA. عندئذ:

$$\varphi = (p-1)(q-1) = 72$$

ولنفرض أن $e = 5$. باستخدام الشرط:

$$ed \equiv 1 (\mathrm{mod}\, \varphi)$$

نجد أن قوة كشف المعمى هو $d = 29$. المفتاح المعلن هو $(n = 91, e = 5)$ والمفتاح السري هو $d = 29$. الرسائل m هي أعداد صحيحة تقع في الفترة $[0, 91)$. إذا كان $m = 23$ فنجد أن:

$$c \equiv m^e \equiv 23^5 \equiv 4 (\mathrm{mod}\, 91)$$
$$c^d \equiv 4^{29} \equiv 23 (\mathrm{mod}\, 91)$$

حيث استخدمنا خوارزمية التربيع في الحسابات. ▲

عند استخدام نظام RSA لتعمية رسائل فمن الممكن أن تكون تعمية بعض الرسائل هي ذاتها، أي توجد m بحيث يكون $c \equiv m^e \equiv m (\mathrm{mod}\, n)$. على سبيل المثال، تعمية كل من الرسائل $m \in \{0, 1, n-1\}$ هي ذاتها (لاحظ أن قوة التعمية e عدد فردي). لإيجاد جميع هذه الرسائل، لاحظ أولاً أن $m^e \equiv m (\mathrm{mod}\, n)$ إذا وفقط إذا كان $m^e \equiv m (\mathrm{mod}\, p)$ و $m^e \equiv m (\mathrm{mod}\, q)$.

الآن، إذا كان $m^e \equiv m (\mathrm{mod}\, p)$ فإما أن $m \equiv 0 (\mathrm{mod}\, p)$ أو أن $m^{p-1} \equiv 1 (\mathrm{mod}\, p)$. ومن ثم استناداً إلى التمرين (١١,١,٢٢) نجد أن عدد الحلول هو $1 + (e-1, p-1)$. وبالمثل، عدد حلول التطابق $m^e \equiv m (\mathrm{mod}\, q)$ يساوي $1 + (e-1, q-1)$. وباستخدام مبرهنة الباقي الصينية نجد أن عدد حلول التطابق $m^e \equiv m (\mathrm{mod}\, n)$ يساوي $[1 + (e-1, p-1)][1 + (e-1)(q-1)]$. على وجه

الخصوص، بما أن كلاً من e و p و q فردي فيوجد على الأقل 9 رسائل تعمى إلى ذاتها. في المثال (**١٢,٢,١**) يوجد 15 رسالة تعمى إلى ذاتها، احدى هذه الرسائل هي $m = 8$. التمرين (**١٢,٢,٣**) يبين عملية تعمية جميع رسائلها تعمى إلى ذاتها.

في العادة لا تستخدم طريقتي معرفة أو اختيار النص الواضح لكسر أنظمة التعمية ذوات المفاتيح المعلنة. ولكن من الممكن كسر النظام بطريقة اختيار النص المعمى ويتم ذلك على النحو التالي: لنفرض أن حواء (العدو) اختارت رسالتين معميتين c_1 و c_2 وحسبت النصين الواضحين m_1 و m_2 على التوالي في نظام RSA. عندئذ،

$$(m_1 m_2)^e \equiv m_1^e m_2^e \equiv c_1 c_2 (\mathrm{mod}\, n)$$

ومن ذلك نرى أن $c \equiv c_1 c_2 (\mathrm{mod}\, n)$ هي تعمية الرسالة $m \equiv m_1 m_2 (\mathrm{mod}\, n)$. الآن، تقوم حواء باختيار $x \in \mathbb{Z}_n^*$ وترسل $\bar{c} = cx^e$ إلى أليس لغرض كشف المعمى. عندئذ، تحصل أليس على النص الواضح $\overline{m} \equiv \left(\bar{c}\right)^d (\mathrm{mod}\, n)$. وبما أن:

$$\overline{m} = (\bar{c})^d \equiv \left(cx^e\right)^d \equiv c^d x^{ed} \equiv mx (\mathrm{mod}\, n)$$

فيكون بإمكان حواء الحصول على الرسالة m وهي:

$$m \equiv \overline{m} x^{-1} (\mathrm{mod}\, n)$$

يمكن لواضع التعمية هزيمة مثل هذا الهجوم بإضافة بعض المعلومات الزائدة على الرسائل الواضحة قبل تعميتها.

من المهم أن يكون عدد القياس في مفتاح نظام RSA كبيراً جداً لضمان عدم القدرة على تحليله. اقترح مينيزس (Menezes) في العام ١٩٩٦م أن يكون طول n أكبر من أو يساوي 768 مرتبة ثنائية ورشح أن يكون هذا الطول يساوي 1024 مرتبة ثنائية لضمان أمن طويل الأجل (انظر [63]). أما في العام ١٩٩٩م استنتج كل من لينسترا وفيرهول (Lenstra and Verheul) أن 768 مرتبة ثنائية ليست كافية لأمن RSA مقارنة

مع أمن نظام DES (انظر [55]). هناك أيضاً شروطاً إضافية على العددين الأوليين p و q وذلك لتحاشي طرق التحليل المعروفة، على سبيل المثال، يجب أن يكون p و q من الطول نفسه ولا يجب أن يكون $|p-q|$ صغيراً نسبياً.

خطة توقيع نظام RSA (مع معرفة الرسالة)

يمكن استخدام نظام RSA لتوقيع الرسائل إلكترونياً على النحو التالي:

إذا أرادت أليس توقيع الرسالة m فيكون التوقيع هو $s \equiv m^d \pmod{n}$ حيث d مفتاح أليس السري وترسل s إلى بوب. يقوم بوب بحساب $m \equiv s^e \pmod{n}$ باستخدام مفتاح أليس المعلن (n,e). وبهذا يحصل على الرسالة الموقعة (m,s).

لغرض كشف الرسائل المزورة، لا بد من أن تزود الرسالة ببعض المعلومات الإضافية m قبل توقيعها. فمثلاً، إذا اختار المزور (العدو) s وقام بإرسال $m \equiv s^e \pmod{n}$ إلى بوب مستخدماً مفتاح أليس المعلن. عندئذ، يقبل بوب الرسالة الموقعة (m,s) فقط إذا كانت تتضمن المعلومات الزائدة (حواء ليس لديها هذه المعلومات الزائدة).

عادة يتم اختيار قوة تعمية صغيرة لتسريع عملية التعمية والتحقق من صواب التوقيع، ولكن توجد بعض التحفظات المبينة في التمرينين (**١٢,٢,٤**) و (**١٢,٢,٥**) على مثل هذا الاختيار. وبالمثل، اختيار عدد صغير لقوة كشف المعمى d يمكن أن يحسن من عملية كشف المعمى وزمن توليد التوقيع ولكن بين واينر (Wiener [95]) من إمكانية معرفة المفتاح السري إذا كان d صغيراً مقارنة مع n وذلك باستخدام طريقة الكسور المتواصلة وهذا هو فحوى التمرين (**١٢,٢,٧**).

يستخدم عند التطبيق العملي لنظام RSA نظاماً أكثر تطوراً من النظام الموصوف في هذا البند. تذيل الرسالة قبل تعميتها هو إجراء شائع، وذلك للتغلب على محاولة كسر النظام باختيار النص المعمى وبعض محاولات الكسر الأخرى حيث تذيل الرسالة

بمعلومات عشوائية مع تكرار تعمية الرسالة نفسها يؤدي على الأغلب إلى أربعة رسائل معماة مختلفة (انظر [4]). أجرى بونيه (انظر [12]) مسحاً على محاولات كسر النظام لعقدين من الزمن وكانت النتيجة غير مقلقة حيث أظهرت معظمها أن الخطر يكمن في سوء استخدام نظام RSA. وأخيراً، نلفت نظر القارئ إلى أن التنفيذ الآمن لنظام RSA ليس بالمهمة السهلة.

تمارين

(١٢,٢,٢) اختارت أليس $p = 31$ و $q = 47$ و $e = 77$ لاستخدامها في نظام RSA.

(أ) ما هو مفتاح أليس السري؟

(ب) جد النص المعمى للرسالة $m = 3$ باستخدام مفتاح أليس المعلن.

(ج) تحقق من صواب نتيجة الفقرة (ب)، وذلك بالكشف عن الرسالة المعماة لتحصل على الرسالة الأصلية m.

(١٢,٢,٣) إذا كان $p = 5$ ، $q = 17$ ، $e = 33$ في نظام RSA فأثبت أن جميع الرسائل تعمى لذاتها.

(١٢,٢,٤) يفضل استخدام قوة تعمية صغيرة في نظام RSA لغرض تسريع عملية التعمية. لنفرض أن قوة التعمية لثلاث مستخدمين هي $e = 3$ وأن قياسات نظام RSA هي n_1 ، n_2 ، n_3 على التوالي. اعترضت حواء (العدو) النصوص المعماة:

$$c_i \equiv m^e (\mathrm{mod}\, n_i) \qquad \text{حيث} \qquad 1 \le i \le 3$$

للرسالة الواضحة المشتركة m. إذا افترضنا أن n_i أولية نسبياً مثنى مثنى فبين كيفية استخدام خوارزمية جاوس لمعرفة الرسالة m.

يوضح التمرين السابق بعض نقاط ضعف نظام RSA. في العادة تستخدم قوة تعمية أكبر (مثل $e = 2^{16} + 1$ الذي يحتوي على عدد قليل من المرتبة 1 في التمثيل

الثنائي لضمان الفعالية) للتغلب على الضعف السابق. كما أن توليد كلمة ثنائية عشوائياً وتذيل الرسالة بها قبل إجراء كل عملية تعمية هو أسلوب متبع للتغلب على الضعف الناتج عن استخدام قوة تعمية صغيرة (يدعى هذا الإجراء تمليح (Salting)).

(١٢,٢,٥) وصف كوبرسميث (Coppersmith [24]) طريقة فعالة للتغلب على محاولة كسر نظام RSA الذي يستخدم قوة تعمية صغيرة وذلك في حالة تحقيق الرسائل الواضحة لعلاقة خطية معلومة. لنفرض أن قوة التعمية هي $e = 3$ وأن c_1 و c_2 رسالتين معميتان تقابلان الرسالتين الواضحتين m و $m+1$ (حيث m مجهول). أي أن:

$$c_1 \equiv m^3 (\mathrm{mod}\, n)$$
$$c_2 \equiv (m+1)^3 (\mathrm{mod}\, n)$$

(أ) أثبت أن:

$$\frac{c_2 + 2c_1 - 1}{c_2 - c_1 + 2} \equiv m (\mathrm{mod}\, n)$$

أي أنه يمكن معرفة m من النصين المعميين c_1 و c_2.

(ب) لاحظ أن $x - m$ قاسم مشترك للعددين $x^3 - c_1$ و $(x+1)^3 - c_2$. أثبت الصيغة المقدمة في الفقرة (أ) باستخدام خوارزمية إقليدس لإيجاد القاسم المشترك الأكبر للعددين $x^3 - c_1$ و $(x+1)^3 - c_2$. تحقق من أن مخرج الخوارزمية هو بالفعل كثيرة حدود خطية.

(١٢,٢,٦) (معرفة جزئية للمفتاح) لنفرض أن $n = pq$ حيث p و q عددان أوليان يحققان $5 \leq p < q < 2p$. ولنفرض أن e و d عددان صحيحان يحققان $1 < e, d < \varphi$ و $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$.

(أ) بما أن $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$ فيوجد عدد صحيح k يحقق $ed - k\varphi(n) = 1$. أثبت أن $1 \leq k < e$.

(ب) افرض أن $d_1 = \left\lfloor \frac{kn+1}{e} \right\rfloor$. أثبت أن $|d_1 - d| < 3\sqrt{n}$.

(ج) إذا كان $e = 3$ فأثبت أن $k = 2$.

(د) إذا علمت فقط القيمتان $e = 3$ و n فصمم خوارزمية فعالة لحساب النصف الأيسر من مراتب d الثنائية (بالتحديد، يفترض أن تختزل الخوارزمية القيم إلى قيمة واحدة أو قيمتين). هذا التمرين مأخوذ من [12].

١٢,٢,٧ (قوة كشف معمى صغيرة) افرض أن $n = pq$ حيث p و q عددان أوليان يحققان $p < q < 2p$. افرض أن e و d عددان صحيحان يحققان $1 < e, d < \varphi(n)$ و $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$.

افرض أيضاً أن $d < \frac{1}{3} n^{1/4}$ وأن k عدد صحيح يحقق $ed - k\varphi(n) = 1$.

(أ) أثبت أن $n - \varphi(n) < 3\sqrt{n}$. أي أن n هو تقريب جيد لقيمة $\varphi(n)$.

(ب) أثبت أن $\frac{e}{n}$ هو تقريب جيد للعدد $\frac{k}{d}$. بالتحديد، أثبت أن $\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}$.

(ج) استخدم الحقيقة أدناه لتصميم خوارزمية فعالة لحساب d إذا علمت فقط القيمتين n و e.

حقيقة: لنفرض أن $y_0 > x_0 \geq 1$ حيث x_0 و y_0 عددان صحيحان. عدد الأزواج المرتبة (x, y) حيث $y_0 > y \geq 1$ التي تحقق $\left|\frac{x_0}{y_0} - \frac{x}{y}\right| < \frac{1}{2y^2}$ محدوداً بالمقدار $2 \log_2 y_0$. إضافة إلى ذلك من الممكن إيجاد جميع هذه الأزواج المرتبة بخوارزمية فعالة (كمتقاربات للكسور المتواصلة للعدد $\frac{x_0}{y_0}$. انظر هاردي ورايت (Hardy and Wright [95]). هذه الطريقة لكسر النظام أخذت من [12,14] وتم اكتشافها من قبل واينر [95].

(١٢,٢,٨) (هجوم التحليل الخاطئ [13,47]) لنفرض أن بطاقة ذكية (smartcard) تستخدم مبرهنة الباقي الصينية لكشف المعمى في نظام RSA. أي أن كشف النص المعمى c يتم بحساب:

$$m_p \equiv c^{d \bmod (p-1)} (\bmod p)$$
$$m_q \equiv c^{d \bmod (q-1)} (\bmod q)$$

وبعد ذلك نجد m ، $0 \leq m < n$ الذي يحقق:

$$m \equiv m_p (\bmod p)$$
$$m \equiv m_q (\bmod q)$$

(أ) أثبت أن العملية تؤدي إلى كشف معمى صحيح. أي، أثبت أن $m \equiv c^d (\bmod n)$.

(ب) لنفرض إمكانية التعديل في البطاقة الذكية بحيث تحسب قيمة خاطئة m_p وتحسب قيمة صائبة m_q. لنفرض أن m' هو كشف المعمى الخاطئ للرسالة c الذي نحصل عليه بعد التعديل. أثبت إمكانية استخدام ذلك لتحليل n.

(١٢,٢,٩) هجوم دوري لكسر نظام RSA بإيجاد أصغر عددٍ صحيحٍ موجبٍ k يحقق $c^{e^k} \equiv c (\bmod n)$.

(أ) أثبت أن هذا العدد k موجود. ثم أثبت أن حواء (العدو) تستطيع الحصول على الرسالة الواضحة من $c^{e^{k-1}} \equiv m (\bmod n)$.

(ب) يمكن تعميم هذا الهجوم على النحو التالي:

نفرض أن u هو أصغر عدد صحيح موجب يحقق $\left(c^{e^u} - c, n\right) > 1$.

أثبت أن العدو يستطيع الحصول على قاسم غير تافه للعدد n أو أن ذلك يؤدي إلى الحصول على الهجوم الدوري الأساسي (أي أن $u = k$).

في الغالب الهجوم الدوري هذا لا ينجح بكسر النظام إذا كان $n = pq$ حيث قواسم $p-1$ و $q-1$ أعداد كبيرة جداً (انظر [63]). أما الهجوم الدوري المعمم فمن المتوقع توقفه قبل الدورة الأساسية ومن ثم يمكن النظر إليه على أنه كسر للنظام بمحاولة تحليل العدد. وبهذا فإن حظوظ نجاحه محدودة على اعتبار أن مسألة التحليل صعبة.

(**١٢,٢,١٠**) أثبت إمكانية استخدام القوة الشاملة (universal exponent) $\lambda(pq) = lcm(p-1, q-1)$ عوضاً عن $\varphi(n)$ لتوليد مفتاح نظام RSA. من الممكن أن يؤدي استخدام λ إلى قوة كشف معمى صغيرة.

(**١٢,٢,١١**) الحاجة إلى أعداد أولية كبيرة لتوليد مفتاح RSA. لنفرض أن مخرج اختبار أوليات احتمالي هو "محتمل أولي" حيث p هو في الحقيقة عدد مؤلف. لنفرض أن $p = p_1 p_2$ حيث $p_1 \neq p_2$ عددان أوليان مختلفان عن q. أثناء توليد المفتاح نحصل على e و d من $\varphi(p,q) = (p-1)(q-1)$ عوضاً عن الحصول عليهما من $\varphi(n) = (p_1-1)(p_2-1)(q-1)$.

(أ) لاحظ أن $\lambda = lcm(p_1-1, p_2-2, q-1) \mid \varphi(n)$.

إذا كان $\lambda \mid \varphi(p,q)$ فأثبت أن ذلك يؤدي إلى تعمية وكشف معمى صائبان.

(ب) استخدم $p = 15$ ، $q = 5$ لتوضيح الفقرة (أ). أي، احسب λ ، $\varphi(n)$ ، $\varphi(p,q)$.

(ج) افرض أن $p = 21$ و $q = 5$. أثبت أن λ لا يقسم $\varphi(p,q)$. جد d إذا كان $e = 3$. جد رسالة m بحيث يكون $c^d \not\equiv m \pmod n$ ولكن $c \equiv m^e \pmod n$.

(**١٢,٢,١٢**) الغرض من هذا التمرين هو إثبات أن معرفة قوة كشف المعمى في d نظام RSA تؤدي إلى وجود خوارزمية فعالة لتحليل n. الفكرة الأساسية هي الحصول على جذر تربيعي غير تافه للعدد 1 قياس n.

بما أن $ed \equiv 1 (\mathrm{mod}\, \varphi)$ فإن $m^{ed-1} \equiv 1 (\mathrm{mod}\, n)$ لكل $m \in \mathbb{Z}_n^*$. ضع $ed - 1 = 2^s t$ حيث t عدد فردي. يتألف البرهان بإثبات أنه يوجد $r \in [1, s]$ لعلى الأقل نصف الأعداد بحيث يكون:

$$m^{2^{r-1}t} \not\equiv \pm 1 (\mathrm{mod}\, n)$$
$$m^{2^r t} \equiv 1 (\mathrm{mod}\, n)$$

ومن ثم لمثل هذا العدد m يكون $(m^{2^{r-1}t} - 1, n)$ قاسماً غير تافه للعدد n.

يفشل $m \in \mathbb{Z}_n^*$ بالحصول على قاسم عندما يكون $m^t \equiv 1 (\mathrm{mod}\, n)$ أو إذا وجد $0 \leq r < s$ حيث $m^{2^r t} \equiv -1 (\mathrm{mod}\, n)$. الجهد الأساسي المبذول هنا هو إيجاد عدد حلول هذه التطابقات.

لنفرض أن $p - 1 = 2^i p'$ و $q - 1 = 2^j q'$ حيث p' و q' عددان فرديان. تذكر أن التطابق $ax \equiv b (\mathrm{mod}\, n)$ قابل للحل إذا وفقط إذا كان $(a, n) \mid b$. وفي هذه الحالة يكون عدد الحلول غير المتطابقة قياس n يساوي (a, n) (تمرين (**١١,١,٢٠**)).

الحالة $m^t \equiv 1 (\mathrm{mod}\, n)$:

ندرس أولاً التطابق قياس p. لنفرض أن $\alpha \in \mathbb{Z}_p^*$ مولِّد. سنجد عدد الحلول x للتطابق $(\alpha^x)^t \equiv 1 (\mathrm{mod}\, p)$.

(أ) أثبت أن p' يقسم t.

(ب) لاحظ أن:

$$\alpha^{xt} \equiv 1 (\mathrm{mod}\, p) \text{ إذا وفقط إذا كان } xt \equiv 0 (\mathrm{mod}\, p - 1).$$

أثبت أن عدد الحلول يساوي p'.

(ج) بالمثل، عدد حلول التطابق $m^t \equiv 1 (\mathrm{mod}\, q)$ يساوي q'. استخدم الآن مبرهنة الباقي الصينية لإثبات أن عدد حلول التطابق $m^t \equiv 1 (\mathrm{mod}\, n)$ يساوي $p'q'$.

الحالة $m^{2^r t} \equiv -1 (\mathrm{mod}\, n)$:

كما في الحالة السابقة نجد عدد الحلول قياس p ومن ثم عدد الحلول قياس q. نسعى للحصول على عدد الحلول x للتطابق $(\alpha^x)^{2^r t} \equiv -1 (\mathrm{mod}\, p)$.

(د) لاحظ أن. $\alpha^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$. ولذا فإن $(\alpha^x)^{2^r t} \equiv -1 (\mathrm{mod}\, p)$ إذا وفقط إذا كان $x 2^r t \equiv \dfrac{p-1}{2} (\mathrm{mod}\, p-1)$. أثبت وجود حل للتطابق إذا وفقط إذا كان $r < i$. إضافة إلى ذلك أثبت أن عدد الحلول يساوي $2^r p'$.

نستطيع افتراض أن $i \leq j$ دون المساس بالعمومية. الآن، نستخدم مبرهنة الباقي الصينية لإثبات أن عدد حلول التطابق $m^{2^r t} \equiv -1 (\mathrm{mod}\, n)$ يساوي $2^{2r} p'q'$ إذا كان $r < i$ ويساوي صفراً ما عدا ذلك. الآن، الحد الأعلى لعدد الأعداد $m \in \mathbb{Z}_n^*$ التي تحقق $m^{2^r t} \equiv -1 (\mathrm{mod}\, n)$ حيث $0 \leq r < s$ هو:

$$\sum_{r=0}^{i-1} 2^{2r} p'q' = p'q' \left(2^{2i} - 1\right) / 3 .$$

وبهذا يكون الحد الأعلى لعدد الأعداد $m \in \mathbb{Z}_n^*$ التي تؤدي إلى فشل تحليل n هو:

$$p'q' \left(1 + \frac{2^{2i} - 1}{3}\right) = p'q' \left(\frac{2}{3} + \frac{2^{2i}}{3}\right) .$$

وبما أن:

$$2^{2i} p'q' \leq 2^i p' 2^j q' = (p-1)(q-1) = \varphi(n)$$

فنجد أن:

$$p'q' \left(\frac{2}{3} + \frac{2^{2i}}{3}\right) \leq \frac{\varphi(n)}{6} + \frac{\varphi(n)}{3} + \frac{\varphi(n)}{2} .$$

إذن، يوجد $1 \leq r \leq s$ لعلى الأقل نصف الأعداد $m \in \mathbb{Z}_n^*$ بحيث يكون:

$$m^{2^{r-1}} \not\equiv \pm 1 (\mathrm{mod}\, n) \quad \text{و} \quad m^{2^r t} \equiv 1 (\mathrm{mod}\, n).$$

لتحليل n، نقوم باختيار $m \in \mathbb{Z}_n^*$ عشوائياً ونجد r. بعد ذلك نقوم بحساب $\left(m^{2^{r-1}t} - 1, n\right)$. من المتوقع الحصول على قاسم غير تافه للعدد n بعد محاولتين.

(١٢,٢,١٣) إذا كان من المعلوم أن عملية التعمية $c \equiv m^e (\mathrm{mod}\, pq)$ قد تمت عندما يكون $m \in [0, p)$ فمن الممكن إنجاز ذلك في المجموعة $\mathbb{Z}_p$ عوضاً عن المجموعة $\mathbb{Z}_{pq}$ وبهذا نحصل على النص الواضح كالتالي:

$$m \equiv c^d (\mathrm{mod}\, n) \equiv c^{d \bmod (p-1)} (\mathrm{mod}\, p).$$

اقترح شامير (Shamir [78]) نظام RSA غير متوازن حيث قام باختيار عددان أوليان $p < q$ من أطوال مختلفة تماماً، على سبيل المثال، طول p يساوي 500 مرتبة ثنائية وطول q يساوي 4500 مرتبة ثنائية. ويتم اختيار الرسائل الواضحة في الفترة $[0, p)$. وكانت نتيجة ذلك فشل محاولة كسر النظام بتحليل $n = pq$ وسرعة كشف المعمى في نظام RSA غير المتوازن مساوية لسرعة كشف المعمى في نظام RSA حيث طول القياس يساوي 500 مرتبة ثنائية. أثبت أنه يمكن كسر نظام RSA غير المتوازن تماماً بطريقة اختيار النص المعمى.

(١٢,٢,١٤) نشرت مجلة CRYPTO 96 [102] مقالاً بعنوان "جانب مظلم من صندوق أسود للتعمية". الفكرة الأساسية لهذا المقال هو افتراض تلوث صندوق أسود مع وجود تقنية تسمح للمُصَنِّع من الحصول على أسرار لا يمكن للآخرين من اكتشافها.

تعرف هذه التقنية باسم إخفاء معلومات سرية مع وجود حماية شاملة (Secretly Embedded Trapdoor with Universal Protection) أو اختصاراً SETUP. كان هدف المؤلفين المباشر لتقنية SETUP هو استخدامها على نظام RSA. الفكرة الأساسية لهذه الدراسة هو إخفاء معلومات كافية من قوة التعمية المعلنة e لنظام RSA بحيث تسمح للعدو من تحليل n. يختار الصندوق الأسود عددين أوليين $p \neq q$ ومن ثم يولد مفتاح تعمية $(n = pq, e, d)$ لنظام RSA. يتم تلويث العملية باستخدام مفتاح العدو (n', e') لمحاولة اختيار عدد أولي p حيث $e \equiv p^{e'} (\mathrm{mod}\, n')$ و $(e, \varphi(n)) = 1$.

(أ) ترك المؤلفين [102] بعض التفاصيل للقارئ. كيف يتمكن العدو من تحليل n باستخدام المفتاح المعلن (n, e) وما هي الفرضيات التي استخدمت لهذا الغرض؟

(ب) ناقش إمكانية اكتشاف SETUP مستنداً إلى الزمن اللازم لتوليد المفتاح أو شكل المفتاح المولَّد.

تقنية الـ SETUP المبينة أعلاه عديمة الفائدة في الحالات التي تكون فيها قوة التعمية e صغيرة. قدم المؤلفون خصوصية سيئة جداً (Pretty Awful Privacy) لتقنية SETUP مماثلة للخصوصية الجيدة جداً PGP (Pretty Good Privacy)، انظر [37,104]، ولكنهم أخفوا معلومات عن p في عدد القياس n. انظر أيضاً [103] والتمرين (**١٢,٥,٦**).

(١٢,٣) الأمن القابل للبرهان
Provable Security

يعتمد أمن نظام RSA على فرضية صعوبة مسألة تحليل الأعداد ومع ذلك تبين أن المحاولة المستمرة والمنظمة للحصول على النص الواضح من النص المعمى في نظام RSA

ليس معلوماً أن صعوبتها تكافئ صعوبة مسألة التحليل. ولذا فمن المحتمل أن تكون مسألة تحليل الأعداد مسألة صعبة ولكن كسر نظام RSA مسألة سهلة.

قدم رابن (Rabin [69]) في العام ١٩٧٩م نظام تعمية يمكن إثبات أنه آمن، وهذا يعني أن صعوبة الحصول على النص الواضح من نص معمى تكافئ مسألة حسابية يعتقد عدم وجود خوارزمية فعالة لحلها. إن الأمن القابل للبرهان يقلل من الفرضيات ويقدم لنا تعريفاً أكثر دقة لمفهوم الأمن. يجب توضيح نقطة مهمة هنا وهي أن البرهان يفترض صعوبة المسألة الحسابية ذات العلاقة فمن الممكن وجود معلومات مقنعة بصعوبة حل مسائل حسابية مثل مسألة التحليل أو مسألة اللوغاريتم المنفصل ولكن لم يتم تقديم برهان ذلك حتى الآن.

نظام رابن يشبه نظام RSA حيث دالة التعمية في كلا النظامين هي على الصورة $f(m) \equiv m^e (\mathrm{mod}\, pq)$. في نظام RSA تكون هذه الدالة قابلة للعكس وأما نظام رابن فيستخدم $e = 2$، ومن ثم فحساب الجذور التربيعية يقدم لنا الخيارات الممكنة للرسالة m. والتعريف الدقيق لنظام رابن يتم باختيار عددين أوليين $p \neq q$ ويكون المفتاح المعلن هو $n = pq$ والمفتاح السري هو (p, q). دالة التعمية هي $f : \mathbb{Z}_n \to \mathbb{Z}_n$ ومعرفة بالقاعدة:

$$f(m) \equiv m^2 (\mathrm{mod}\, n).$$

إذا كان c نصاً معمى فيتم كشف المعمى بحل التطابق $c \equiv m^2 (\mathrm{mod}\, n)$ لإيجاد الجذور التربيعية الأربعة كما هو مبين في البند (**١١,٤**).

مثال (١٢,٣,١)

لنفرض استخدام $p = 31$ و $q = 41$ في نظام رابن. لتعمية الرسالة $m = 814$ باستخدام المفتاح المعلن $n = pq = 1271$ نحصل على النص المعمى:

$$c = f(m) \equiv m^2 \equiv 814^2 \equiv 405 (\mathrm{mod}\, 1271).$$

ولكشف المعمى نستخدم المفتاح السري $p = 31$ و $q = 41$ لإيجاد الجذور التربيعية.

ولقد بينا في البند (**١١,٤**) وجود خوارزمية فعالة لحل التطابقين:

$$m^2 \equiv 405 \equiv 2 (\mathrm{mod}\, 31)$$
$$m^2 \equiv 405 \equiv 36 (\mathrm{mod}\, 41)$$

وإيجاد الجذور التربيعية m. لاحظ أن $p \equiv 3 (\mathrm{mod}\, 4)$. ولذا نجد أن الجذرين التربيعيين قياس p هما:

$$m \equiv \pm 2^{(p+1)/4} \equiv \pm 8 (\mathrm{mod}\, 31).$$

أما الجذران التربيعيان قياس $q = 41$ فأحدهما سهل لأن 36 مربع كامل. وبهذا نجد:

$$m \equiv \pm 6 (\mathrm{mod}\, 41)$$

الآن، نستخدم خوارزمية جاوس (**١١,١,٦**) ونحصل على الجذور التربيعية الأربعة m_1 ، m_2 ، m_3 ، m_4 بحل كل من أنظمة التطابقات التالية:

$$\begin{cases} m \equiv 8 (\mathrm{mod}\, 31) \\ m \equiv 6 (\mathrm{mod}\, 41) \\ m_1 = -240 \end{cases} \quad ، \quad \begin{cases} m \equiv -8 (\mathrm{mod}\, 31) \\ m \equiv 6 (\mathrm{mod}\, 41) \\ m_2 = 457 \end{cases}$$

$$\begin{cases} m \equiv 8 (\mathrm{mod}\, 31) \\ m \equiv -6 (\mathrm{mod}\, 41) \\ m_3 = -457 \end{cases} \quad ، \quad \begin{cases} m \equiv -8 (\mathrm{mod}\, 31) \\ m \equiv -6 (\mathrm{mod}\, 41) \\ m_4 = 240 \end{cases}.$$

(لاحظ أننا نحتاج فقط لحل النظامين الأول والثاني لأن الجذور هي $\pm m_1$ و $\pm m_2$).

وبهذا نحصل على أربعة خيارات مختلفة m_i للنص الواضح m. وبحالة عدم تذيل الرسالة بمعلومات إضافية قبل تعميتها فيكون من الصعب على المستقبل أن يخمن الرسالة الواضحة على أنها:

$$m_3 \equiv 814 (\mathrm{mod}\, n).$$

▲

لفهم أمن النظام نقدم مسألة رابن وهي المهمة بالنسبة للعدو.

مسألة رابن (RABIN): لنفرض أن $n = pq$ وأن $c \equiv m^2 (\mathrm{mod}\, n)$. جد x يحقق $c \equiv x^2 (\mathrm{mod}\, n)$.

هذه هي مسألة الجذور التربيعية التي قدمناها في البند (**١١,٤**). إذا كان $p \equiv q \equiv 3 (\mathrm{mod}\, 4)$ فإن العدد $n = pq$ هو عدد بلم ومن ثم يمكن إيجاد الجذور التربيعية بزمن حدودي. في المثال أعلاه، $q \equiv 1 (\mathrm{mod}\, 8)$. ولهذا فالعدد n ليس على الصيغة المطلوبة. لا توجد خوارزمية حدودية معلومة لحل التطابق $x^2 \equiv c (\mathrm{mod}\, q)$ عندما يكون $q \equiv 1 (\mathrm{mod}\, 8)$. ولكن توجد طريقة عشوائية ناقشناها في البند (**١١,٤**) زمن تنفيذها المتوقع حدودي. إذن، RABIN ≤ FACTOR. أي إذا وجدت خوارزمية زمن تنفيذها لتحليل العدد حدودي فمن الممكن حل مسألة رابن بزمن متوقع حدودي. ولبرهان العكس، أي برهان FACTOR ≤ RABIN، تذكر أولاً أنه إذا كان $x^2 \equiv y^2 (\mathrm{mod}\, n)$ وكان $x \not\equiv \pm y (\mathrm{mod}\, n)$ فإن $(x + y, n)$ قاسم غير تافه للعدد n. الآن، اختر $x \in \mathbb{Z}_n^*$ عشوائياً واحسب $c \equiv x^2 (\mathrm{mod}\, n)$. استخدم خوارزمية حساب رابن لإيجاد جذر تربيعي y للعدد c بزمن متوقع حدودي. احتمال أن يحقق y العلاقة $x \not\equiv \pm y$ يساوي $\frac{1}{2}$. وبهذا يكون $(x + y, n)$ قاسم غير تافه للعدد n (أي أحد العددين الأوليين).

إذن، نخلص إلى أن كسر نظام رابن يكافئ تحليل n. لاحظ أن البرهان السابق لا يضمن أمن النظام ضد محاولة كسره باختيار النص المعمى. إضافة إلى ذلك من الممكن تطبيق اتفاقية من النمط المبين في التمرين (**١٢,٢,٤**) على نظام رابن.

إحدى صعوبات كشف المعمى في نظام رابن هو صعوبة تخمين النص الواضح الصحيح من بين الأربعة نصوص (الجذور التربيعية). وللتغلب على هذه الصعوبة، عادة يتم تذيل الرسالة الواضحة قبل تعميتها بمعلومات إضافية (مثل تكرار بعض مراتبها) بطريقة يكون فيها من الصعب تحقيق أكثر من جذر من الجذور الأربعة لهذه

الخاصية. وهذه الطريقة تصلح أيضاً لمقاومة محاولة كسر النظام باختيار النص المعمى (لأن مخرج الخوارزمية لا يقدم معلومات مفيدة للعدو في هذه الحالة). ولكن برهان التكافؤ بين مسألة رابن ومسألة التحليل غير مضمونة في هذا النظام المعدل. يقدم التمرين (**١٢,٣,٣**) نظام شبيه بنظام رابن (على أعداد بلم) حيث يضمن هذا النظام معرفة الرسالة الأصلية.

تمارين

(**١٢,٣,٢**) ليكن $n = 551$ هو القياس في نظام رابن.

(أ) جد النص المعمى $c \equiv m^2 (\mathrm{mod}\, n)$ للرسالة $m = 53$.

(ب) جد النص الواضح للرسالة المعماة c بالحصول على الجذور التربيعية الأربعة المرشحة بأن تكون الرسالة m.

(ج) ناقش محاولة كسر النظام باختيار النص المعمى على النحو التالي:

اختار $x \in \mathbb{Z}_{551}^*$ عشوائياً وليكن $x = 53$. أدخل القيمة $c \equiv x^2 (\mathrm{mod}\, n)$ إلى خوارزمية RABIN. ماذا يحدث لو كان مخرج الخوارزمية 498 ؟ إذا كان مخرج الخوارزمية هو 517 فأثبت أن باستطاعتك تحليل n.

(**١٢,٣,٣**) يقدم هذا التمرين الشكل العام لنظام تعمية طرحه وليامز (Williams [96,97]) لعدد مؤلف مختار n وهو نظام شبيه بنظام رابن حيث الحصول على النص الواضح من النص المعمى يكافئ تحليل العدد n ولكن يسمح بمعرفة النص الواضح الأصلي من بين الجذور التربيعية الأربعة.

افرض أن $n = pq$ حيث $p \equiv q \equiv 3 (\mathrm{mod}\, 4)$ وأن:

$$d = \big((p-1)(q-1) \,/\, 4 + 1\big) \,/\, 2 .$$

اختر s يحقق $\left(\frac{s}{n}\right) = -1$. المفتاح المعلن هو (n, s) والمفتاح السري هو d.

التعمية: اختر رسالة m حيث $(m,n)=1$. احسب $b_1 \in \{0,1\}$ بحيث يكون $\left(\frac{m}{n}\right)=(-1)^{b_1}$ واحسب $m_0 \equiv s^{b_1}m \pmod n$. أرسل الثلاثي:

$$\left(c \equiv m_0^2 \pmod n, b_1, b_2 \equiv m_0 \pmod 2\right).$$

كشف المعمى: عند استلامك للثلاثي (c,b_1,b_2)، احسب $m_0 \equiv \pm c^d \pmod n$ حيث تختار الإشارة التي تحقق $m_0 \equiv (-1)^{b_2} \pmod 2$. عندئذ، الرسالة الواضحة هي $m \equiv s^{-b_1}m_0 \pmod n$.

(أ) إذا كان $\left(\frac{x}{n}\right)=1$ و $c \equiv x^2 \pmod n$ فأثبت أن $c^d \equiv \pm x \pmod n$.

(ب) تحقق من الحصول بالفعل على الرسالة m بإجراء كشف المعمى.

(ج) افرض أن $p=7$، $q=11$، $n=pq$. لاحظ أن $p \equiv q \equiv 3 \pmod 4$. أثبت أن $s=2$ تحقق $\left(\frac{s}{n}\right)=-1$. وضح التعمية وكشف المعمى للرسالة $m=31$.

السمة الأساسية لهذا النظام هو تمييز الجذر التربيعي الصحيح (من بين الأربعة جذور تربيعية) في حالة $n=pq$ حيث $p \equiv q \equiv 3 \pmod 4$. سنستخدم الترميز نفسه الذي استخدمه وليامز في بحثه. افرض أن $[a,b]$ يرمز لفصل الرواسب قياس n بحيث يتحقق ما يلي: إذا كان $y \in [a,b]$ فإن $y \equiv a \pmod p$ و $y \equiv b \pmod q$.

(د) أثبت أن $\left(\frac{-1}{p}\right)=-1$. استنتج من ذلك أنه إذا كان $(c,p)=1$ فإن واحداً فقط من بين العددين $\pm c$ هو راسب تربيعي قياس p.

(هـ) إذا كان $(y,n)=1$ فأثبت إمكانية كتابة الجذر التربيعي للعدد y^2 في $\mathbb{Z}_n$ على الصور $[a,b]$، $[-a,b]$، $[-a,-b]$، $[a,-b]$ حيث $a \in Q_p$ و $b \in Q_q$.

(و) إذا كان $y \in [a,b]$ أو $y \in [-a,-b]$ فنقول إن y هو جذر تربيعي للعدد y^2 من النمط 1 ونقول إن باقي الجذور التربيعية هي من النمط 2. أثبت أن y من النمط 1 إذا وفقط إذا كان $\left(\frac{y}{n}\right) = 1$. ومن ثم فالتحليل ليس ضروري لمعرفة النمط.

(ز) إذا كان y_1 و y_2 جذرين مختلفين من النمط 1 فأثبت أن $y_1 \equiv -y_2 (\mathrm{mod}\, n)$ وأن واحداً فقط منهما زوجي.

العدو الذي لديه القدرة على كشف المعمى يحصل على جذر تربيعي من النمط 1 وآخر من النمط 2 لعدد مختار ومن ثم يكون باستطاعته تحليل n.

(ح) يجد العدو عدد x يحقق $\left(\frac{x}{n}\right) = -1$ ثم يطبق عملية كشف المعمى على x^2.

إذا تمكن من كشف معمى كل نص من النصوص المعماة الصحيحة فعندئذ يمكن اختيار $x = s$. يقوم العدو الآن بكشف المعمى $\left(x^2, 0, 0\right)$ ويحصل على جذر تربيعي y من النمط 1. أثبت أن $(y - x, n)$ هو قاسم غير تافه للعدد n.

(١٢,٤) نظام الجمل
ELGamal Cipher

قدم الجمل (ELGamal [29]) في العام ١٩٨٥م نظام تعمية وخطة توقيع إلكتروني يعتمدان على فرضية صعوبة حل مسألة اللوغاريتم المنفصل. وكان توقيع الجمل هو أول توقيع تتبناه الحكومة الأمريكية في العام ١٩٩٤م حيث التوقيع الإلكتروني القياسي (Digital Signature Standard) أو اختصاراً DSS هو صيغة معدلة لخطة توقيع الجمل.

تحتاج عملية التعمية في نظام الجمل إلى عدد أولي p ومولداً $\alpha \in \mathbb{Z}_p^*$. يختار كل مستخدم عدداً عشوائياً a حيث $1 \le a \le p-2$ كمفتاح سري ويكون المفتاح

المعلن هو $\left(p, \alpha, \alpha^a (\mathrm{mod}\, p)\right)$. لإرسال رسالة m حيث $0 \le m < p$ باستخدام المفتاح المعلن يقوم المرسل باختيار عشوائي لعدد k حيث $1 \le k < p$ ثم يرسل الزوج المرتب $\left(\alpha^k (\mathrm{mod}\, p), m\left(\alpha^a\right)^k (\mathrm{mod}\, p)\right)$. وباستخدام المفتاح السري a يمكن كشف المعمى وإيجاد الرسالة m ؛ لأنه يمكن حساب α^{-ak}. وبهذا يكون $m\left(\alpha^a\right)^k \alpha^{-ak} \equiv m (\mathrm{mod}\, p)$.

مثال (١٢,٤,١) (مثال صفي على تعمية الجمل)

ليكن $p = 13$. وليكن $\alpha = 2 \in \mathbb{Z}_{13}^*$ مولِّداً. يمكن اختيار المفتاح المعلن a حيث $1 \le a \le 13 - 2$. لنفرض أن أليس اختارت $a = 6$. تقوم أليس بحساب:

$$\alpha^a \equiv 2^6 \equiv 12 (\mathrm{mod}\, 13)$$

ومن ثم تعلن عن $\left(p, \alpha, \alpha^a (\mathrm{mod}\, p)\right) = (13, 2, 12)$ كمفتاح معلن. لإرسال الرسالة $m = 9$ يختار بوب عدد عشوائي k حيث $1 \le k < p$ وليكن $k = 3$. وباستخدام مفتاح أليس المعلن يقوم بوب بإرسال:

$$\begin{aligned}(\gamma, \delta) &= \left(\alpha^k (\mathrm{mod}\, p), m\left(\alpha^a\right)^k (\mathrm{mod}\, p)\right) \\ &\equiv \left(2^3, 9(12)^3\right) \equiv (8, 4) (\mathrm{mod}\, 13)\end{aligned}$$

إلى أليس. بعد ذلك تستطيع أليس استخدام مفتاحها السري $a = 6$ لقراءة الرسالة وذلك بحساب:

$$\left(\alpha^k\right)^{-a} \equiv \gamma^{-a} \equiv \gamma^{p-1-a} \equiv 8^{13-1-6} \equiv 12 (\mathrm{mod}\, 13)$$

وبهذا تكون الرسالة هي:

$$m \equiv \delta \alpha^{-ak} \equiv 4 \cdot 12 \equiv 9 (\mathrm{mod}\, 13).$$

لاحظ أن توليد المفتاح في هذا المثال يؤدي إلى أن $\alpha^a \equiv -1 (\mathrm{mod}\, p)$ وهذا غير مفضل كما هو موضح في التمرين (١٢,٤,٥). ▲

إحدى نقاط قوة نظام الجمل هو وجود عشوائية صريحة في عملية التعمية ومن ثم فالرسالة m يمكن أن تعمى إلى نصوص معماة مختلفة اعتماداً على الاختيار

العشوائي للعدد k. ومن ثم يكون النظام محمياً ضد بعض محاولات كسره. لاحظ أننا سبق وأن أدخلنا العشوائية على نظام شبيه لنظام RSA وحصلنا على الحماية نفسها. أما إحدى نقاط ضعف نظام الجمل فهو تمديد سعة الرسالة ؛ لأن النص المعمى يتكون من زوج من الأعداد الصحيحة كل منها يساوي تقريباً الرسالة.

المسألة التالية تهم العدو :

مسألة الجمل (ELGAMAL): ليكن p عدداً أولياً وليكن $\alpha \in \mathbb{Z}_p^*$ مولّداً إذا علمت α^a ، α^k ، $m\left(\alpha^a\right)^k$ فجد m.

من الواضح أن وجود خوارزمية حدودية لحل مسألة اللوغاريتم المنفصل يؤدي إلى وجود خوارزمية حدودية لحل مسألة ELGAMAL. أي أن ELGAMAL ≤ DLP. ولذا فأمن نظام الجمل يعتمد على مسألة اللوغاريتم المنفصل ولكن ليس من المعلوم أن مسألة ELGAMAL تكافئ مسألة DLP.

لاحظ أن التبديل بين α^a و α^k هو جزء من اتفاقية ديفي وهيلمان للحصول على مفتاح مشترك α^{ak}. ومن ثم يستخدم نظام الجمل هذا المفتاح المشترك لتعمية الرسالة m بضربها بهذا المفتاح. ولذا فإن وجود خوارزمية لحل مسألة ديفي وهيلمان يؤدي مباشرة إلى حل مسألة الجمل. أي أن ELGAMAL ≤ DHP. ولبرهان أن DHP ≤ ELGAMAL نفرض وجود خوارزمية حدودية لحل مسألة الجمل. أي إذا كان لدينا $\left(p, \alpha, \alpha^a, \alpha^k, m\alpha^k\right)$ فنستطيع الحصول على مخرج الخوارزمية m بزمن حدودي. وفي مسألة ديفي وهيلمان يكون المطلوب إيجاد α^{ak} بمعرفة $\left(p, \alpha, \alpha^a, \alpha^k\right)$. ولذا بإدخال $\left(p, \alpha, \alpha^a, \alpha^k, 1\right)$ إلى خوارزمية الجمل نحصل على المخرج $m = \alpha^{-ak}$. وبعد ذلك نقوم بأخذ النظير (يحتاج ذلك إلى زمن حدودي) ونحصل على α^{ak}.

توقيع الجمل

تستخدم خطة توقيع الجمل دالة تمويه بحيث تكون صورة الرسالة m التي يمكن أن يكون طولها كبيراً جداً هي ملخص الرسالة x ومن ثم يتم توقيع x. يحتاج التحقق من صواب التوقيع إلى وجود الرسالة نفسها. ولهذا فخطة توقيع الجمل هي مثال على التوقيع بملحق.

يتم توليد المفتاح لغرض التوقيع بصورة مماثلة لتوليد مفتاح التعمية. لنفرض أن الرسالة المراد توقيعها هي $m \in \{0,1\}^*$. نستخدم دالة تمويه معروفة $H : \{0,1\}^* \to \{0,\ldots,p-1\}$ للحصول على ملخص الرسالة $x = H(m)$. يتم اختيار عدد عشوائي k ، $1 \le k < p$ حيث $(k, p-1) = 1$. يتم حساب $r \equiv \alpha^k \pmod p$. نستخدم الآن المفتاح السري a لحل التطابق:

$$x \equiv ar + ks \pmod{p-1}$$

لإيجاد s. توقيع الرسالة m هو الزوج (r,s).

يتم التحقق من صواب التوقيع من المفتاح المعلن باستخدام الحقيقة:

$$\alpha^x \equiv \alpha^{ar+ks} \equiv \left(\alpha^a\right)^r \left(\alpha^k\right)^s \pmod p$$

لنفرض أن (r,s) هو التوقيع المزعوم على الرسالة m. نقوم باستخدام دالة التمويه المعروفة لحساب $x = H(m)$. يتم قبول التوقيع إذا تحقق $\alpha^x \equiv \left(\alpha^a\right)^r \left(\alpha^k\right)^s \pmod p$ حيث $1 \le r < p$. (انظر التمرين (**١٢,٤,٣**)).

إذا حاول العدو تزوير التوقيع على الرسالة m فإنه يقوم بحساب $x = H(m)$ و $r = \alpha^k$ لأي k. ولكنه لا يستطيع إيجاد قيمة a و s بحل التطابق $x \equiv ar + ks \pmod{p-1}$ ولكن من الممكن إيجاد x وتوقيع (r,s) بحيث يكون شرط التحقق:

$$\alpha^x \equiv \left(\alpha^a\right)^r \left(\alpha^k\right)^s \pmod p$$

صحيحاً. ولإنجاز ذلك نقوم باختيار عددين صحيحين j و k حيث $1 \leq k < p$ و $(k, p-1) = 1$ وحساب:

$$r \equiv \alpha^j \left(\alpha^a\right)^k (\mathrm{mod}\, p)$$
$$s \equiv -rk^{-1} (\mathrm{mod}\, p-1)$$
$$x \equiv sj (\mathrm{mod}\, p-1)$$

وبهذا يكون التوقيع (r,s) على x صائباً لأن:

$$\left(\alpha^a\right)^r r^s \equiv \alpha^{ar}\alpha^{js}\alpha^{aks} \equiv \alpha^{js} \equiv \alpha^x (\mathrm{mod}\, p)$$

وبهذا يتم قبول التوقيع إذا استطاع العدو إيجاد رسالة m حيث $H(m) = x$. يسمى كشف المعمى هذا بالتزوير الوجودي (existential forgery)؛ لأن المعلومات التي يعرفها العدو عن محتوى الرسالة قليلة جداً.

إحدى الوسائل الأخرى التي يحاول العدو استخدامها لكسر خطة توقيع الجمل هو حل التطابق:

$$\alpha^x \equiv \left(\alpha^a\right)^r r^s (\mathrm{mod}\, p)$$

للتوقيع (r,s). من الواضح أن ذلك ممكناً إذا استطاع العدو معرفة المفتاح السري a (ربما من توقيع سابق معلوم). ولكن معرفة a من معلومات معلنة يكافئ مسألة اللوغاريتم المنفصل. وحل s بدلالة r هي أيضاً مسألة اللوغاريتم المنفصل. وأما محاولة حل r بدلالة s تؤدي إلى تطابق أسي في r ولا توجد خوارزمية فعالة لحل مثل هذا التطابق.

لضمان أمن النظام يجب أن يكون العدد الأولي p كبيراً جداً بحيث يتعذر حل مسألة اللوغاريتم المنفصل في الزمرة $\mathbb{Z}_p^*$. في العام ١٩٩٦م لاحظ مينيزس [63] أن استخدام عدد أولي p طوله 512 مرتبة ثنائية ليس آمناً واقترح الطول 768. وإذا أردنا أمن طويل الأجل فاقترح أن يكون طول العدد الأولي يساوي 1024 مرتبة ثنائية.

لاحظ أيضاً أن طول التوقيع هو ضعف طول العدد الأولي مما يعيق استخدامه في بعض التطبيقات مثل البطاقة الذكية.

استخدمت صورة معدلَّة لتوقيع الجمل في التوقيع الإلكتروني القياسي (DSS) في العام ١٩٩٤م. وعلى الرغم من أن طول القياس p يتراوح بين 512 و 1024 مرتبة ثنائية، إلا أنه من الممكن استخدام توقيع طوله 320 مرتبة ثنائية نحصل عليه من تمويه طوله 160 مرتبة ثنائية باستخدام زمرة جزئية من $\mathbb{Z}_p^*$. انظر [63] للحصول على تفاصيل خوارزمية التوقيع الإلكتروني (DSA) وخوارزمية التمويه الآمن (SHA-1) المستخدمة كدالة تمويه.

يستخدم توليد مفتاح DSA عدداً أولياً q طوله 160 مرتبة ثنائية وعدد أولي p حيث $q \mid (p-1)$ بحيث يكون طول p يساوي $512+64t$ مرتبة ثنائية، $0 \le t \le 8$ (بحد أقصى 1024 مرتبة ثنائية). لنفرض أن β مولِّداً للزمرة الجزئية الدورية من الرتبة q من $\mathbb{Z}_p^*$ (انظر التمرين (**١٢,٤,٤**)). يتم اختيار مفتاح سري a عشوائياً حيث $1 \le a < q$. المفتاح المعلن هو $\big(p, q, \beta, \beta^a \pmod p\big)$.

لتوقيع رسالة m نجد التمويه $x = H(m)$ الذي طوله 160 مرتبة ثنائية. يتم اختيار عدد k عشوائياً حيث $1 \le k < q$. وبعد ذلك يتم حساب التوقيع (r,s) على النحو التالي:

$$r \equiv \Big(\beta^k \pmod p\Big) \pmod q \quad \text{و} \quad s \equiv (x+ar)^{-1} k \pmod q$$

يتم قبول (r,s) كتوقيع صائب للرسالة m إذا تحقق ما يلي:

$$\left(\beta^{xs^{-1} \pmod q} \left(\beta^a\right)^{rs^{-1} \pmod q} \pmod p\right) \pmod q \equiv r$$

(انظر التمرين (**١٢,٤,٤**)).

تمارين

(**١٢,٤,٢**) مثال صفي على توقيع الجمل. لنفرض أن أليس اختارت $p = 17$ والمولِّد $\alpha = 3 \in \mathbb{Z}_{17}^*$ والمفتاح السري $a = 6$.

المفتاح المعلن هو $\big(p, \alpha, \alpha^a (\mathrm{mod}\, p)\big) = (17, 3, 15)$. دالة التمويه هي $H(m) \equiv m (\mathrm{mod}\, p)$.

(أ) جد قيمة التمويه x والتوقيع (r, s) للرسالة $m = 26$ بفرض أن أليس اختارت $k = 11$ (لاحظ أن $(k, p-1) = 1$).

(ب) بين تفاصيل التحقق من صواب التوقيع (r, s) على m مع توضيح عدم الحاجة إلى معرفة المفتاح السري a.

(**١٢,٤,٣**) إذا لم يتم التحقق من الشرط $1 \le r < p$ أثناء التحقق من صواب توقيع الجمل فيكون بالإمكان تزوير التوقيع على رسالة m' مع وجود شرط صواب التوقيع (r, s) على قيمة تمويه x حيث $(x, p-1) = 1$. في هذه الحالة نفرض أن $x' = H(m')$ وأن $u \equiv x' x^{-1} (\mathrm{mod}\, p-1)$. ضع $s' \equiv su (\mathrm{mod}\, p-1)$ واستخدم مبرهنة الباقي الصينية لحل النظام:

$$r' \equiv ru (\mathrm{mod}\, p-1)$$
$$r' \equiv r (\mathrm{mod}\, p)$$

لإيجاد قيمة r'. أثبت أن (r', s') توقيع مقبول للرسالة m' إذا تجاهلنا الشرط $1 \le r' < p$ (أُخذ هذا التمرين من [10]، انظر أيضاً [63] الملحوظة (١١,٦٦)).

(**١٢,٤,٤**) يناقش هذا التمرين تفصيلان من تفاصيل خوارزمية التوقيع الإلكتروني.

(أ) لنفرض أن $g \in \mathbb{Z}_p^*$ يحقق $\beta \equiv g^{(p-1)/q} (\mathrm{mod}\, p) \neq 1$. أثبت أن رتبة β تساوي q.

(ب) إذا كان $s \neq 0$ فأثبت صواب التحقق من التوقيع.

(١٢,٤,٥) في المثال **(١٢,٤,١)** حصلنا من توليد المفتاح على التطابق $\alpha^a \equiv -1 (\mathrm{mod}\, p)$.
لماذا كان هذا الاختيار سيئاً؟ [إرشاد: ما هي قيمة $m\left(\alpha^a\right)^k$ لكل خيار للعدد k؟].

(١٢,٤,٦) (مولدات ضعيفة) لنفرض أن $p \equiv 1 (\mathrm{mod}\, 4)$ وأن $\alpha \in \mathbb{Z}_p^*$ مولِّد يحقق $\alpha \mid (p-1)$. إذا كان حساب اللوغاريتمات في زمرة جزئية G من $\mathbb{Z}_p^*$ رتبتها α ممكناً فيكون بإمكان العدو إنشاء توقيع (r,s) على رسالة m على النحو التالي:
لنفرض أن مفتاح أليس المعلن هو α^a وأن r معرفاً بحيث يحقق $p-1=\alpha r$.

(أ) أثبت أن α^r مولِّد للزمرة G. وبهذا يكون من الممكن إيجاد z يحقق $\alpha^{rz} \equiv \left(\alpha^a\right)^r (\mathrm{mod}\, p)$.

(ب) أثبت أن $r^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$.

(ج) افرض أن $s \equiv \dfrac{p-3}{2}(H(m)-rz) (\mathrm{mod}\, p-1)$. أثبت أن (r,s) توقيعاً مقبولاً على الرسالة m.

(١٢,٤,٧) إعادة استخدام العدد العشوائي k في نظام الجمل يؤدي إلى مخاطر.

(أ) لنفرض أن k استخدم لتعمية الرسالتين m_1 و m_2.
أثبت أن حيازة العدو على النصين المعميين والرسالة $m_1 \neq 0$ يؤدي إلى معرفة الرسالة m_2 بطريقة فعالة.

(ب) لنفرض أن k استخدم لتوقيع الرسالتين m_1 و m_2.
أثبت إمكانية معرفة العدو للمفتاح السري a.

(١٢,٥) برتوكولات (معاهدات أو اتفاقيات) تعموية
Cryptographic Protocols

البرتوكول أو المعاهدة أو الاتفاقية هو هيكل عام من الإجراءات لتطبيق المفاهيم البدائية للتعمية. التعريف المقدم في [25] للبرتوكول هو "خوارزمية لتنفيذ صنف من التعاملات (وحدات منطقية لتنشيط الاتصال)". نقدم في هذا البند القصير عدة مفاهيم لها علاقة بالبرتوكولات حيث نناقش مسألتين تقليديتين هما:

برتوكول رمي قطعة نقود بين فريقين حيث كل منهما لا يثق في الآخر ويرغبان في حل خلاف بينهما برمي قطعة نقود باستخدام الهاتف. أما برتوكول عدم المعرفة مطلقاً (Zero-Knowledge) فيقدم برهاناً على حوزة أحدهم على سر دون إفشاء أي معلومة عن ذلك السر.

يبين الهجوم النشط على خطة ديفي وهيلمان لتبادل المفاتيح الحاجة إلى توضيح فرضيات البرتوكول. وحتى مع أن فرضيات البرتوكول واضحة فإنه ليس من المعلوم ما إذا كانت هذه الفرضيات تلبي المطلوب عند دراسة حالة معينة. ومثال على ذلك هو برتوكول لعبة البوكر الذهنية (لعبة بوكر عادلة (غير متحيزة) دون استخدام ورق اللعب) التي قدمها كل من شامير ورايفست وأدلمان في [79] حيث تبين لاحقاً أنها تقدم معلومات كافية للحصول على تعليم جزئي لأوراق اللعب.

عند اكتشاف ضعف في الأمن فإنه ليس من الواضح دائماً اكتشاف السبب، هل هو من البرتوكول أو من دالة التعمية. كتب مور (Moore [64]): "عند اكتشاف ضعف في نظام تعمية فيجب علينا التفريق بين أمرين فإذا كانت النتيجة لهذا الاكتشاف هي الحد من مدى التطبيقات أو تحديد مدى المتغيرات التي يجب استخدامها في الخوارزمية فمن الممكن أن يكون سبب هذا الضعف هو فشل البرتوكول. أما إذا كان تأثير هذا الاكتشاف هو عدم الصلاحية الكاملة للنظام المستخدم أو قصر مدى المتغيرات المستخدمة

بشكل مجحف بحيث يجعل دالة التعمية صعبة الحساب فيكون نظام التعمية قد تم كسره فعلياً." ولذا فالضعف المقدم في التمرين (١٢,٢,٤) هو نتيجة فشل البرتوكول حسب إدعاء مور. وفي التمرين (١٠,٣,٨) تم الدمج بين نظامين آمنين حيث تمت مقايضة بين التعمية والتوثيق. ولذا يمكن الجدال على أن هذا هو فشل في البرتوكول مع أن مقولة مور تدعى أن هذا هو كسر لنظام التعمية.

برتوكول الثلاث خطوات لشامير

يوضح برتوكول الثلاث خطوات لشامير الفرق بين البرتوكول والدالة التعموية. صمم شامير هذا البرتوكول للحصول على السرية دون التبادل المسبق للمفاتيح. يتم اختيار نظام تعمية تقليدي (متماثل المفتاح) يحقق الخاصية $E_{k_1}E_{k_2} = E_{k_2}E_{k_1}$ لكل $k_1, k_2 \in \mathcal{K}$. من الممكن النظر إلى عملية التعمية على أنها تضع "قفلاً" على الصندوق الذي يحتوي الرسالة. الخطوات التالية توضح البرتوكول لغرض إرسال رسالة m من A إلى B.

(١) يختار كل من A و B عشوائياً مفتاح سري K_A و K_B على التوالي.

(٢) تضع A قفلها على الرسالة وترسل $c_1 = E_{k_A}(m)$ إلى B.

(٣) يقوم B بوضع قفله و إعادة $c_2 = E_{k_B}(c_1) = E_{k_B}E_{k_A}(m)$ إلى A.

(٤) تقوم A بإزالة قفلها وترسل $c_3 = D_{k_A}(c_2)$ إلى B. يكشف B المعمى c_3 ليحصل على الرسالة m.

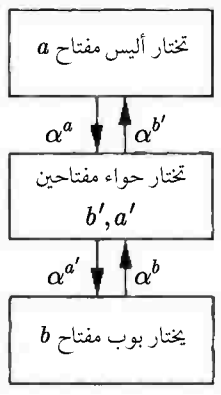
بوضع شروط مناسبة على E ، يبدو أن هذا التبادل مقاوماً لمحاولات الكسر. ولكن البرتوكول يضع شروطاً إضافية ضمنية على نظام التعمية. لنأخذ الحالة التي يكون فيها النظام هو نظام اللفافة للمرة الواحدة. عندئذ، $E_k(m) = k \oplus m$. إذا حصل العدو على:

$$c_1 = k_A \oplus m \quad ، \quad c_2 = k_B \oplus c_1 \quad ، \quad c_3 = k_B \oplus m$$

فنجد أن التبادل غير آمن على الإطلاق ؛ لأن $c_1 \oplus c_2 \oplus c_3 = m$. هذا مع أن النظام المستخدم في البرتوكول آمن تماماً. يقترح التمرين (**١٢,٥,١**) نظاماً آخر لاستخدامه في هذا البرتوكول.

(١٢,٥,١) اتفاقية ديفي وهيلمان لتبادل المفاتيح

في اتفاقية ديفي وهيلمان لتبادل المفاتيح المقدمة سابقاً يقوم أليس وبوب بتبادل $\alpha^a \pmod p$ و $\alpha^b \pmod p$ من خلال قناة اتصال مفتوحة (غير آمنة) للحصول على المفتاح السري المشترك α^{ab} . هذه الخطة آمنة ضد الهجوم السلبي ولكنها غير آمنة ضد الهجوم الإيجابي (النشيط).



الاعتراض في المنتصف

إذا لم تكن المفاتيح موثقة فبإمكان العدو النشط إضافة إلى انتحال الشخصية أن يصمم هجوم يدعى اعتراض في المنتصف (intruder-in the middle) بحيث لا يستطيع أي من أليس أو بوب اكتشافه. ويتم ذلك بأن تشارك حواء (العدو) السر $\alpha^{ab'}$ مع أليس و السر $\alpha^{a'b}$ مع بوب حيث a' و b' مختاران من قبل حواء. إذا أرسلت أليس رسالة معماة باستخدام مفتاح مشتق من $\alpha^{ab'}$ ، تقوم حواء باعتراض الرسالة وتكشف المعمى ثم تعيد التعمية باستخدام مفتاح مشتق من $\alpha^{a'b}$ وترسلها إلى بوب. وبهذا يكون بمقدور حواء الحصول على جميع النصوص الواضحة المتبادلة[٤].

يستعان أحياناً بمصدر مؤتمن أو ما يسمى سلطة الشهادات (Certification Authority) ، اختصاراً CA لغرض التوثيق. يقوم CA أولاً بالتحقق من هوية الشخص A ثم يُكَّون رسالة تحتوي على المعلومات الشخصية (اسم، عنوان، وهكذا) إضافة إلى مفتاح A المعلن (α^a في حالتنا). يوقع CA الرسالة وبهذا يصدر شهادة C_A تربط هوية A مع

(٤) انظر التمرين (**١٢,٥,٥**) الذي يقترح برتوكولاً يجبر حواء على التصرف بحذر.

مفتاحها المعلن. يقوم أليس وبوب بتبادل الشهادتين C_A و C_B المتضمنتين α^a و α^b على التوالي. عند استلام بوب للشهادة C_A يتحقق من صواب توقيع CA ومن ثم يقتنع بأن مفتاح أليس المعلن هو α^a. وبالمثل، تقوم أليس بالتحقق من أن مفتاح بوب المعلن هو α^b. لا يزال احتمال انتحال الشخصية قائماً هنا؛ لأنه من الممكن أن ترسل حواء (العدو) شهادة تنتمي إلى أليس ومع ذلك فإنها غير قادرة على حساب المفتاح السري المشترك α^{ab}.

يحتاج استخدام CA بهذا الأسلوب إلى دفع ثمن (مرة واحدة) إنشاء شهادة لكل مستخدم ولكن التحقق من التواقيع لا يحتاج إلى تدخل من قبل CA. يجب أن يكون مفتاح CA المعلن موثقاً ولكن السرية غير مطلوبة هنا. أما نقاط الضعف هنا فتكمن في أن CA يخدم عدد كبير من العملاء وبالتالي يكون مستهدف من قبل العدو، وبالمقابل فإن إلغاء خدمات CA يؤدي إلى فاجعة. أيضاً، من الممكن أن يضطر CA إلى إلغاء المعلومات وإعادة التوزيع مرة أخرى في حالة انتهاء صلاحية شهادة العميل أو توقيع CA.

أحد الاستخدامات الشائعة للشهادات هو تأمين شراء منتجات آمن من خلال شبكة الاتصال العالمية (الإنترنت). في العادة يكون التوثيق باتجاه واحد (يرسل التاجر شهادة إلى العميل)؛ لأن إرسال شهادات من قبل العميل نادرة الحدوث. يكون لدى العميل الذي يستخدم برنامج الدخول إلى مواقع الشبكة العالمية قائمة بسلطات الشهادات حيث يقبل تواقيع هذه السلطات. من الممكن لهذا البرتوكول أن يسمح للعميل من التحقق من الشهادة. فالشهادة الصالحة من http://www.delta.com يكون لديها معلومات مقنعة بأن المفتاح المعلن هو بالفعل مفتاح www.delta.com. ومن الممكن أن تحدث مفاجئة للشخص الراغب في شراء تذكرة سفر لاكتشافه أن عنوان شركة دلتا للطيران هو www.delta-air.com [٥].

---

(٥) لاحظت detta Comm أن حوالي 8000 زائر في اليوم يدخلون إلى www.delta.com بغرض البحث عن Delta Air. وتم في العام ١٩٩٩م تعديل على صفحة الانترنت لتقليل الدخول غير المرغوب.

(١٢,٥,٢) براهين بدون معلومات

الهدف الذي تسعى أليس (المُبَرهِنة) إلى تحقيقه هو إقناع بوب (المتحقق) من أن بحوزتها سر s. أحد الخيارات لذلك هو أن تفصح أليس لبوب عن السر ومن ثم لا يبقى السر سراً. عند دراستنا لخطة توثيق كلمة السر التي ناقشناها في البند (١٠,٣,٢) حصل العدو على كلمة سر أليس ومن ثم أصبح باستطاعته انتحال شخصية أليس. يتيح برتوكول عدم المعرفة مطلقاً للمبرهن بتقديم إثبات مقنع أن بحوزته سراً دون إفشاء أي معلومات يستطيع المتحقق أن يستخدمها لاحقاً.

تحتاج المناقشة الدقيقة لبروتوكولات عدم المعرفة مطلقاً إلى معلومات ومفاهيم صعبة. ولذا ندعو القارئ المهتم لمثل هذه المناقشة الدقيقة اللجوء إلى المراجع المذكورة في البند (١٢,٦) حيث ذكرنا أيضاً مرجعين لمناقشة غير رياضية لمفهوم عدم المعرفة مطلقاً. سنقصر دراستنا في هذا البند على مناقشة غير دقيقة لهذا البرتوكول.

كتوضيح لأنظمة البراهين (ليست بالضرورة براهين عدم المعرفة مطلقاً) دعنا نناقش مسألة برهان أن $v \in J_n$ راسب غير تربيعي حيث n حاصل ضرب أعداد أولية كبيرة سرية. المبرهن الذي يعرف تحليل العدد n يستطيع تقديم برهان غير قابل للرفض بأن $v \in \overline{Q_n}$ وذلك بالكشف عن قواسم العدد ولكنه يكون قد قدم للمتحقق في هذه الحالة معلومات أكثر بكثير من اقناعه بأن v هو بالفعل راسب غير تربيعي.

قدم [40] البرهان التالي لهذه المسألة. لاحظ أن كلمة "برهان" في هذا السياق تعني "معلومات مقنعة" وليس معلومات مؤكدة.

(١) يقوم المتحقق B باختيار عدد $t > 0$ كوسيط لضمان الأمن ويختار أيضاً $b_i \in \{0,1\}$ عشوائياً. كما يختار $z_i \in \mathbb{Z}_n^*$ حيث $1 \le i \le t$. يتحدى B المبرهن A بالقيم:

$$w_i \equiv z_i^2 v^{b_i} (\mathrm{mod}\, n) \quad ، \quad 1 \le i \le t.$$

(٢) يحدد A (بطريقة ما) إذا كان كل من w_i راسباً تربيعياً ويكون رده:

$$c_i = \begin{cases} 0 & , \quad w_i \in Q_n \\ 1 & , \quad w_i \in \overline{Q_n} \end{cases}$$

لكل $1 \leq i \leq t$.

(٣) يتحقق B ما إذا كان $b_i = c_i$ لكل i ، و إذا كان كذلك يقبل B البرهان (أن v راسب غير تربيعي).

إذا كان v راسباً غير تربيعي فإن التحدي w_i راسب تربيعي إذا وفقط إذا كان $b_i = 0$. فإذا كان t كبيراً كفاية وأن الفريقين التزما بالبرتوكول فسوف يقتنع B أن v راسب غير تربيعي. ومن ناحية أخرى، إذا كان v بالفعل راسباً تربيعياً فإن كلاً من w_i راسباً تربيعياً وأن احتمال أن يكون $b_i = c_i$ لكل i يساوي 2^{-t} وبهذا يكون من غير المرجح أن يقبل B بالادعاء $v \in \overline{Q_n}$.

إذا التزم الفريقان بالبرتوكول فلا يتاح للمتحقق B من معرفة أي معلومات لا يستطيع حسابها دون A (عدا حقيقة أن المبرهن قادر بالفعل على النجاح بالتحدي). هذا البرتوكول ليس عدم معرفة مطلقاً. كما أن المتحقق ليس مجبراً على الالتزام بالبرتوكول؛ لأنه من الممكن أن يحصل على رد لأعداد w_i من اختياره، أي أنه من الممكن أن يستخدم المتحقق المبرهن (بافتراض أن المبرهن لا يلجأ إلى الغش) لتحديد فيما إذا كانت أعداد من اختياره (ليس بالضرورة أن يكون على الصيغة الموصوفة بالبرتوكول) رواسب تربيعية. الصيغة المقدمة لهذا البرتوكول في [40] تفرض على المتحقق أن يكون أميناً.

كما ذكرنا سابقاً فإن أحد تطبيقات مفاهيم عدم المعرفة مطلقاً هي إثبات الهوية الشخصية. صمم البرتوكول التالي على البرهان بعدم المعرفة مطلقاً لإثبات أن قيمة معينة v هي راسب تربيعي قياس n.

برتوكول (إثبات الهوية الشخصية لفيات وشامير)

يختار مركز موثوق به قياس $n = pq$ مشابهًا لقياس RSA ويبقى القواسم سرية. يحصل المبرهن A على عدد سري $s \in \mathbb{Z}_n^*$ من المركز الموثوق به ويكون $v \equiv s^2 (\mathrm{mod}\, n)$ مفتاح A المعلن. ينجح المبرهن في إقناع المتحقق B أن بحوزته s بتنفيذ الخطوات الثلاث التالية عدد t من المرات حيث $t > 0$ هو عدد لضمان الأمن:

(١) يختار A عشوائياً الالتزام (commitment) r حيث $1 \leq r < n$ ويرسل الشاهد $x \equiv r^2 (\mathrm{mod}\, n)$ إلى B.

(٢) يرد B بتحدي عشوائي $e \in \{0,1\}$.

(٣) يكون رد A هو $y \equiv rs^e (\mathrm{mod}\, n)$.

(٤) يتحقق B من أن $y \not\equiv 0$ وأن $y^2 \equiv xv^e (\mathrm{mod}\, n)$. يقبل B البرهان إذا نجحت جميع الجولات وعددها t.

ليس لدى المتحقق B أي معلومات عن السر s: لا يعتمد الرد $y = r$ على s والعدد العشوائي r في الرد $y = rs$ غير معلوم من قبل B. من الممكن أن يتمكن العدو في كل جولة من انتحال شخصية A وينجح إذا كان التحدي متوقعاً. فإذا توقع أن يكون $e = 0$ فإن الشاهد والرد لا يتغيران، وإذا توقع أن يكون $e = 1$ فيقوم باختيار $x = r^2 v^{-1}$ كشاهد و $y = r$ كرد. وبما أن التحديات يتم اختيارها بطريقة عشوائية فإن احتمال نجاح التوقع يساوي $\frac{1}{2}$ في كل جولة. يبين التمرين **(١٢,٥,٢)** أنه على الأغلب يتم اكتشاف مثل هذا المتطفل. يمنع أيضاً عدم القدرة على توقع التحدي محاولة الكسر بإعادة لعب الجولات من قبل عدو بحوزته شهادة من جلسة برتوكول صحيحة سابقة.

(١٢,٥,٣) رمي النقود والبوكر الذهني

نقدم في هذا البند برتوكولان تعمويان إضافيان لغرض تسليط الضوء على التطبيقات الواسعة لمثل هذه البرتوكولات وكذلك للتأكيد على التحديد الواضح لفرضيات البرتوكول والتحقق من ملائمة هذه المتطلبات. يحتوي البند (١٢,٦) مراجع للعديد من التطبيقات الأخرى ومحاولات كسر مثل هذه البرتوكولات.

قدم بلم (Blum [11]) اقتراح رمي قطعة النقود باستخدام الهاتف. قرر الزوجان أليس وبوب بعد العديد من المشاحنات الانفصال عن بعضهما ومن ثم الطلاق واتفقا على استخدام الهاتف لرمي قطعة نقود ليحسما من سيكون له حق الوصاية على الأطفال. المعضلة هنا أن كليهما غير مستعد أن يكون المتصل الأول أو أن يفصح عن نتيجة رمي قطعة النقود. تكمن الفكرة الأساسية وراء هذا البرتوكول بأن أليس ستلتزم بالاختيار "صورة" أو "كتابة" وتعلن عن التزامها بطريقة تسمح لها بإخفاء اختيارها مع التزامها بهذا الاختيار. يقوم بوب بتخمين خيارها ومن ثم تقوم أليس بتقديم معلومات تجعل التزامها معلناً. يعتمد أمن البرتوكول على صعوبة حل مسألة الرواسب التربيعية (QRP).

برتوكول رمي قطعة نقود

(١) تختار أليس $n = pq$ حيث $p \neq q$ عددان أوليان فرديان وتختار عشوائياً $x \in J_n$ وتعلن عن n و x لبوب.

(٢) يكون رد بوب إما "$x \in Q_n$" أو "$x \in \overline{Q_n}$" (باحتمال 50% أن يكون صائباً بفرض صعوبة مسألة QRP).

(٣) تقوم أليس بالإفصاح عن p و q. يقوم بوب بالتحقق من أن p و q هما أوليان بالفعل (ومن ثم $x \in J_n$). يتحدد صواب رد بوب بحساب $\left(\frac{x}{p}\right)$.

إذا فشل بوب بالتحقق من أولية العددين p و q فيكون بإمكان أليس الغش بأخذ $n = p_1p_2p_3$ حيث p_i أعداد أولية واختيار x يحقق $\left(\frac{x}{p_1}\right) = \left(\frac{x}{p_2}\right) = -1$ و $\left(\frac{x}{p_3}\right) = 1$ (أي أن $\left(\left(\frac{x}{n}\right) = 1\right)$) وبعد حصول أليس على رد (تخمين) بوب تقوم بالإفصاح عن الزوج $(p = p_1p_2, q = p_3)$ أو الزوج $(p = p_1, q = p_2p_3)$ وذلك يعتمد على النتيجة التي تفضلها (على سبيل المثال، إذا أرادت أن يعتقد بوب أن x راسب تربيعي فإنها نفصح عن الزوج الأول).

لعبة البوكر ذهنياً

يظهر أن علماء التعمية لهم اهتمامٌ خاصٌ في لعبة عادلة (غير متحيزة) للبوكر الذهني. اقترح كل من شامير ورايفست وأدلمان في العام ١٩٧٩م برتوكولاً للتوزيع نشر العام ١٩٨١م في المجلة العلمية (The Mathematical Gardner). الفكرة الأساسية هي استخدام برتوكول الثلاث خطوات لشامير. اتفق أليس وبوب على مجموعة رسائل m_i ، $1 \le m_i \le 52$ رسالة لكل ورقة لعب. تقوم أليس بتعمية هذه الرسائل وترسل $E_{k_A}(m_i)$ ، $1 \le i \le 52$ بترتيب عشوائي. يختار بوب خمسة نصوص معماة ويعتبرها أوراق لعب أليس ويعيدها إلى أليس. يقوم بعد ذلك بتعمية خمسة نصوص معماة إضافية باستخدام E_{k_B} ويرسلها إلى أليس التي تستخدم D_{k_A} لإزالة قفلها عن هذه الرسائل وتعيد النتيجة إلى بوب على اعتبار أنها أوراق لعب بوب.

اقترح لهذه اللعبة توليد مفتاح شبيه لنظام RSA حيث يتفق أليس وبوب على عدد قياس n (حاصل ضرب عددان أوليان فرديان مختلفان) وكل منهما يختار مفتاح سري $k = (e, d)$ بحيث يكون $(e, \varphi(n)) = 1$ و $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$. وبهذا تكون دالتي التعمية وكشف المعمى هما $E_k(m) \equiv m^e (\mathrm{mod}\, n)$ و $D_k(c) \equiv c^d (\mathrm{mod}\, n)$ على التوالي. يعلنان عن مفتاحيهما السريين بعد انتهاء اللعبة.

بعد نشر هذه الخطة بزمن قصير بين ليبتون (Lipton [25]) أن الدالة المقترحة تفشل ولا تحقق الفرضية الضمنية للبرتوكول التي تدعى عدم إمكانية تعليم أوراق اللعب ؛ وذلك لوجود خوارزمية فعالة لحساب رمز جاكوبي والمحافظة على القيمة بعد التعمية. أي أن :

$$\left(\frac{m}{n}\right) = \left(\frac{m}{n}\right)^e = \left(\frac{m^e}{n}\right)$$

فإذا لم تكن قيم رمز جاكوبي متساوية لكل m_i يكون بإمكان بوب اختيار أوراق لعب بقيم معينة لرمز جاكوبي ويعيدها إلى أليس وبهذا يحتمل حصوله على أفضلية. من الممكن هزيمة مثل هذا الهجوم باختيار تعمية لتكون جميعها رواسب تربيعية. يجد لاعب البوكر المهتم مراجع في البند (**١٢,٦**) لبرتوكولات مقترحة وطرق للغش.

تمارين

(**١٢,٥,١**) في برتوكول الثلاث خطوات لشامير افرض أن $E_k(m) \equiv m^k \pmod p$ حيث p عدد أولي مناسب.

(أ) أثبت أن دالة التعمية إبدالية وبهذا تحقق الشرط لاستخدام البرتوكول.

(ب) كيف يتم اختيار k_A و k_B ؟ جد c_1 ، c_2 ، c_3 .

(ج) ناقش أمن البرتوكول.

(**١٢,٥,٢**) يتعلق هذا التمرين ببرتوكول فيات وشامير لإثبات الهوية الشخصية.

(أ) إذا نجح منتحل الشخصية بتوقع التحدي e فأثبت أن الشاهد x والرد y سيقبلان بخطوة التحقق.

(ب) إذا كان التوقع خاطئاً فوضح كيفية اكتشاف منتحل الشخصية.

(١٢,٥,٣) (إثبات حوزة لوغاريتم منفصل (انظر [19,20])) افرض أن p عدد أولي وأن رتبة $g \in \mathbb{Z}_p^*$ هو العدد الأولي q. المفتاح السري للمستخدم A هو s حيث $1 \le s < q$ والمفتاح المعلن هو $S \equiv g^s \pmod p$. يقنع A المستخدم B بحوزته s في عدد $t > 0$ من الجولات.

(١) يختار A عشوائياً التزام x ، $1 \le x < q$ ويرسل الشاهد $X \equiv g^x \pmod p$ إلى B.

(٢) يرد B بتحدي عشوائي $e \in \{0,1\}$.

(٣) يكون رد A على النحو التالي

$$y = \begin{cases} x & ,e = 0 \\ sx^{-1} \pmod q & , \quad e = 1 \end{cases}.$$

يقبل B البرهان إذا تم نجاح جميع الدورات التي عددها t.

(أ) إذا التزم الفريقان بقواعد البرتوكول فتحقق من أن B سيقبل البرهان.

(ب) بين كيف يتمكن المتطفل من الغش بافتراض إمكانية تخمين التحديات (ولكن s غير معلوم).

(ج) ناقش المعضلة التي ستواجه العدو في حالة التخمين الخاطئ.

(١٢,٥,٤) خطة مقترحة لإثبات الهوية الشخصية. تقوم سلطة الشهادات بربط هوية أليس بالعدد $n = pq$ حيث n معلن والعددان الأوليان $p \neq q$ هما مفتاح أليس السري.

(١) يتحدى بوب أليس براسب تربيعي عشوائي x قياس n.

(٢) يكون رد أليس جذر تربيعي y للعدد x.

(٣) يتحقق بوب من صواب $y^2 \equiv x \pmod n$.

إذا نجحت الخطوات بعدد من الجولات فهل هذا كافياً لإقناع بوب بحوزة أليس على سر؟ بين أن هذه الخطة تحتوي على عيوب مقلقة.

(١٢,٥,٥) (تبادل مفاتيح بوجود أعداء نشطين) لنفرض أن أليس وبوب يعتمدان على تمييز الأصوات أثناء جلسة تبادل المفاتيح. ولهذا عوضاً عن استخدام سر ديفي وهيلمان المشترك α^{ab} مباشرة فإنهما يستخدمان وسيلة تمييز الأصوات وكل منهما سيقرأ جزءاً من السر α^{ab}. بعد التحقق من هذه الأجزاء للسر α^{ab} يكون الجزء المتبقي هو السر المشترك k.

(أ) بافتراض أن العدو غير قادر على معرفة k من α^a و α^b والأجزاء التي تم تسريبها من α^{ab}. هل هذا مقنع لكل من أليس وبوب بأن العدو لا يعرف k؟ اقترح رايفست وشامير [72] تغيير في هذا البرتوكول يجبر المعترض في المنتصف من إخفاء نشاطه (ومن ثم يحتمل الكشف عن وجوده). تختار أليس رسالة m وترسل نصف $E_k(m)$ حيث k هو المفتاح التي تم حسابه (من المحتمل أن يكون مشتركاً مع العدو وليس مع بوب). يقوم بوب بالرد بنصف النص المعمى الذي يختاره. بعد ذلك تقوم أليس بإرسال النصف الآخر من الرسالة $E_k(m)$ ويقوم بوب بالرد بصورة مماثلة.

(ب) افرض عدم امكانية اكتشاف بعض أجزاء النص الواضح من معرفة نصف $E_k(m)$ فقط. ناقش خيارات العدو (بالتحديد، ناقش ماذا يحصل إذا قام العدو بإرسال النصف الأول من رسالة أليس).

(١٢,٥,٦) (قناة مخفية Subliminal Channel) يمكن لخطط التوثيق أن تسمح بوجود قناة مخفية يتواصل بها فريقان دون التمكن من اكتشافها. اقترح سيمونز (simmons [82, 83]) التصور (السيناريو) التالي لمسألة يطلق عليها مسألة السجين:

ارتكب مجرمان جريمة مشتركة وتم اعتقالهم وسجنهم في زنزانتين منفصلتين بعيدتين عن بعضهما لحين تقديمهما للمحاكمة. طريقة التواصل الوحيدة بينهما هي عن طريق

إرسال رسائل لبعضهما من خلال طرف ثالث موثوق من إدارة السجن (يفترض أن يكون عميل لمدير السجن). يسمح مدير السجن للسجينين بالتواصل على أمل أن يتمكن من خداع على الأقل واحداً منهما بأن يقوم بإرسال رسالة من إدارة السجن إلى أحد السجينين وإقناعه أن من كتبها هو زميله السجين الآخر أو على الأقل تعديل في رسالة حقيقية أرسلت من زميله. وبما أن لدى مدير السجن قناعة تامة بأن السجينين سيحاولان الاتفاق على خطة تؤدي إلى تملصهم من ذنب ارتكاب الجريمة فإن مدير السجن سيسمح لهم فقط بالتواصل على شرط قراءته لجميع رسائلهم وبأن تكون رسائلهم غير ضارة. ومن ناحية أخرى فالسجينين ليس لديهما أي خيار إلا قبول شروط مدير السجن. أي، أن يقبلان باحتمال خداعهما أفضل من عدم تواصلهما إطلاقاً؛ وذلك لأنهما بحاجة إلى الاتفاق على وضع خطة للتملص من الجريمة. ولكي ينجحا في ذلك فيجب أن يجدا وسيلة لخداع مدير السجن؛ وذلك بإيجاد خطة سرية للتواصل بينهما. أي إيجاد "قناة مخفية" بينهما على مرأى ومسمع مدير السجن على الرغم من أن الرسائل بينهما لا يظهر أنها تحتوي على معلومات سرية (على الأقل لمدير السجن). وبما أنهما على يقين من نية مدير السجن لخداعهما بزج رسائل مزورة فإنهما يوافقان على التواصل بشرط أن يسمح لهما بتوثيق رسائلهما.

يسمح توقيع الجمل بوجود مثل هذه القناة المخفية بين السجينين أليس وبوب. توليد مفتاح أليس لا يتغير حيث تقوم أليس باختيار عدد أولي p ومولِّد $\alpha \in \mathbb{Z}_p^*$. وتختار عدداً عشوائياً سرياً a ، $1 \leq a \leq p-2$. وبهذا يكون مفتاح أليس المعلن هو $\big(p, \alpha, \alpha^a \pmod p\big)$. عادة، تقوم أليس بتوقيع الرسالة m باختيار عشوائي k حيث $k < p$ و $(k, p-1) = 1$ ومن ثم حساب (r, s) حيث $r \equiv \alpha^k \pmod p$ ونحصل على s بحل التطابق:

$$H(m) \equiv ar + ks \pmod{p-1}$$

عندئذ، تقوم بإرسال (m,r,s) إلى بوب عن طريق مدير السجن. أما إذا أرادت أليس مشاركة السر a مع بوب فمن الممكن استخدام k لنقل الرسالة المخفية[٦].

(أ) إذا اشترك كل من أليس وبوب في السر a ، فما هي الشروط التي يجب أن يحققها s بحيث يكون باستطاعة بوب إيجاد القناة المخفية k بطريقة فعالة بمعرفة (m,r,s) ؟

المعضلة التي تواجه أليس هي مشاركة مفتاحها السري مع بوب (مع احتمال أن يكون بوب قادراً على تزوير توقيعها). وعلى الرغم من ضرورة إرسال المفتاح a بطريقة آمنة إلا أن يونغ وينغ (Young and Yung) قدما SETUP (انظر التمرين (**١٢,٢,١٤**)) طريقة تسمح لأليس من الكشف عن مفتاحها السري لبوب باشتراط أن يكون مفتاح بوب المعلن $\left(p,\alpha,\alpha^b(\bmod p)\right)$ معروفاً لأليس. عندئذ، تقوم أليس بتلويث خطوات التوقيع وينتج عن ذلك (m_1,r_1,s_1) و (m_2,r_2,s_2) بطريقة تسمح للمستخدم الذي لديه b من معرفة a. ولكي تكشف أليس عن a تختار عشوائياً k_1 بحيث يكون كل من k_1 و $\beta \equiv \left(\alpha^b\right)^{k_1} (\bmod p)$ و $\alpha^{\beta^{-1}}(\bmod p)$ أولية نسبياً مع $p-1$ حيث β^{-1} هو النظير الضربي للعدد β قياس $p-1$. وعوضاً

---

(٦) على الرغم من أن توقيع الجمل (r,s) يحتاج إلى $2\log_2 p$ مرتبة ثنائية إلا أن $\log_2 p$ مرتبة ثنائية فقط تستخدم للسرية ومن ثم فباقي المراتب يمكن استخدامها للقناة المخفية. وبما أن $(k,p-1)=1$ فمن الممكن إرسال فقط $\varphi(p-1)$ من الرسائل السرية المختلفة k ويكون من الصعب اكتشافها لأن للتطابق $xs \equiv H(m) - ar(\bmod p-1)$ العديد من الحلول x. لاحظ سيمونز [84,85] إمكانية التغلب على نقاط الضعف هذه عند استخدام DSA والمفترض أن هذا النظام هو الأفضل بسماح وجود قنوات مخفية لحد الآن.

عن اختيار أليس للعدد k_2 عشوائياً فإنها تختار $k_2 = \beta^{-1}$. أخيراً، افرض كالعادة أن $r_i \equiv \alpha^{k_i} (\mathrm{mod}\, p)$ و $s_i \equiv (H(m_i) - ar_i)k_i^{-1} (\mathrm{mod}\, p-1)$، حيث $i \in \{1,2\}$.

(ب) أثبت أن باستطاعة بوب الحصول على a بحساب

$$r_2^{-1}\left(H(m_2) - s_2 \,/\, r_1^b (\mathrm{mod}\, p)\right) (\mathrm{mod}\, p-1).$$

(ج) لغرض التوضيح، افرض أن $p = 13$ ، $\alpha = 2$. أثبت أن كلاً من β و $\alpha^{\beta^{-1}} (\mathrm{mod}\, p)$ أولي نسبياً مع $p-1$ إذا كان $b = 5$ و $k_1 = 7$. إذا كان $b = 3$ فأثبت عدم قدرة أليس على إيجاد k_1 يحقق الخواص المطلوبة.

(١٢,٦) حواشي
Notes

إضافة إلى خطط التعمية التي درسناها في هذا الكتاب، توجد طرق تعمية أخرى ذات أهمية خاصية تعتمد على المنحنيات الناقصية. حيث تضمن هذه الطرائق أمن النظام بمفتاح أقصر مقارنة مع الأنظمة الأخرى كنظام RSA. فخوارزمية المنحنيات الناقصية للتوقيع الالكتروني (Elliptic Curve Digital Signature Algorithm) أو اختصاراً ECDSA هي رديف DSA وتم قبولها من قبل معهد القياس الوطني الأمريكي (American National Standards Institnte) أو اختصاراً (ANSI X9.62) في العام ١٩٩٩م. تجد في مرجع جونسن ومينيزس (Johnson and Menezes [44]) دراسة تتعلق بقرارات التصميم و الأمن و التنفيذ للتوقيع ECDSA كما يتضمن بحثهما مقدمة عن المنحنيات الناقصية. أما كوبلتز (Koblitz [50]) وستنسون (Stinson [86]) فيحتويان على مقدمة للمنحنيات الناقصية وتطبيقاتها في التعمية. وأما المواضيع المتقدمة في المنحنيات الناقصية فمن الممكن إيجادها في العديد من المراجع نذكر منها بلاك وسيروسي وسمارت (Blake, Seroussi, and Smart [8]) ومينيزس (Menezes [62]).

ذكر التقرير التقني الذي أعلن عنه في العام ١٩٩٧م من قبل مجموعة الأمن للاتصالات الإلكترونية، اختصاراً (CESG) أن علماء التعمية البريطانيون استخدموا أنظمة التعمية ذوات المفاتيح المعلنة في العام ١٩٧٠م حيث أطلقت عليه مجموعة CESG [30] العنوان "تعمية غير سرية" وظهر نظام تعمية شبيه بنظام RSA في المرجع كوكس (Cocks [21]). كما أن فكرة خطة ديفي وهيلمان لتبادل المفاتيح ظهرت في وليمسن (Williamson [100])[٧].

هناك عديد من التطبيقات المشهورة التي تستخدم أنظمة التعمية التقليدية وأنظمة التعمية ذوات المفاتيح المعلنة معاً للحصول على توثيق وسرية، ومن هذه التطبيقات "سرية جيدة جداً" (PGP)، انظر [37,104] وعلى صعيد الأنظمة، نظام ميكروسن المعروف باسم آلية إنجاز الاتصال البعيد (remote procedure call) أو اختصاراً RPC، انظر [70,88]. من المهم ذكره هنا أن جزءاً من أمن خطة ميكروسن تعتمد على أخذ القوة قياس عدد أولي طوله 192 مرتبة ثنائية والذي اعتبر غير آمن في العام ١٩٩١م [54]. ولاعتبارات عدم التعرض للهجوم يجب الأخذ بالاعتبار الإطار العام لأمن الشبكة و التي لا تعتمد فقط على مبادئ تعموية. في واقع الأمر، إن مسائل الأمن لا تعتمد في الغالب على التعمية. شهد العام ١٩٩٠م سيل من الإنذارات الأمنية

---

(٧) علقت مجموعة CESG بالقول "من المهم ذكره أنه على الرغم من اقتراح العديد من الأفكار لأنظمة التعمية ذوات المفاتيح المعلنة، إلا أن أفضل نظامين آمنين هما أول نظامين تم اكتشافهما. كما أنه من المهم ملاحظة أن ترتيب الأكاديميين لهذه الاكتشافات هو عكس ترتيب مجموعة CESG". كتب وليمسون [100] كلمات حذرة في مقدمة كتابه: "أحد الأسباب التي جعلتني أرجئ الكتابة هو أنني أجد نفسي في وضع محرج، وبعد كتابة الكتاب [99] بدأت أشك في مجمل نظرية التعمية غير السرية. والمشكلة تتلخص في أنني لا أملك برهاناً أن الطريقة المقدمة في [99] هي بالفعل آمنة. وبصيغة أخرى، فيما إذا كان لهذه الطريقة ضمانات لعدم كسرها".

بسبب بعض التجاوزات مثل الرسائل التي طولها يزيد عن الطول المفترض واحتواء بعض الرسائل على رموز غير متوقعة. وكانت بعض هذه التجاوزات في البرامج المعنية بآلية الأمن.

أخذت المواضيع التي تتعلق بالبراهين بدون معلومات من جولدواسر وميكالي وراكوف (Golodwasser, Micali, and Rackoff [40]) ومن مينيزس وفان أورشت وفانستون (Menezes, Van Oorshot, and Vanstone [63]). انظر أيضاً الفصل الثالث عشر من كتاب ستنسون [86]. صنف براسارد و سربيو (Brassard and Cre'peau [18]) المفاهيم المتعددة لبراهين بدون معلومات.

وما يثير الاهتمام (أو على الأقل التعجب) هو جلسات CRYPTO التي ناقشت مقدمة لبرهان بدون معلومات دون استخدام الرياضيات حيث قدم كوسيكواتر وجوليو وبرسون (Quisquater, Guillou, and Berson [68]) مقالة بعنوان "مغارة علي بابا الغريبة" التي يؤدي مدخلها إلى تشعبات من الطرق غير النافذة. وصمم اختبار عملي يبين قدرة المدعي على تقديم برهان مقنع من امتلاكه كلمات سحرية تمكنه من فتح ممراً بين النهايات غير النافذة دون الإفصاح عن السر نفسه. طلب من المدعي الذي دخل المغارة بمفرده سابقاً من العودة باستخدام طريق من اختيار شاهداً يقف عند التشعب. تكرر إعادة التجربة لغاية اقتناع الشاهد بأن المدعي يمتلك فعلاً كلمات سحرية(٨).

في العام ١٩٩٨م قدم مفهوم البرهان بدون معلومات في أحد لقاءات CRYPTO على شكل لعبة بعنوان أين والدو (Where's Waldo [41]) والهدف من هذه اللعبة هو تحديد مكان الشخصية والدو. في هذه اللعبة يكون المطلوب من أليس إقناع بوب بأنها

(٨) كان من الممكن تقديم البرهان لخطوة واحدة وذلك بسؤال المدعي بعمل دورة مبتدأ من التشعب، أو على الأصح إتلاف القصة.

وجدت والدو دون الإفصاح عن الحل (كيفية إيجاده). ستستخدم مقصاً خاصاً بها لإخفاء والدو من الخلفية ولكن هذا لا يقنع بوب حيث يتهمها باستخدام صورة أخرى من مصدر آخر. يكون حل أليس هو استخدام قطعة ورق معتمة حجمها ضعف حجم صورة والدو و تحتوي على نافذة صغيرة لعزل والدو.

تحتوي المراجع سالوما ([75] Salomaa) وسيبري وبيرايك (Seberry and Pieprzyk [77]) وشناير ([76] Schneier) على عديد من مجالات تطبيقات البرتوكولات مثل، مشاركة السر، القنوات المخفية، النقود الإلكترونية، خطط الاقتراع وغيرها. وقدم سيمونز ([84] Simmons) عرض شامل للقنوات المخفية حيث استهل هذا العرض بمقدمة تاريخية تتعلق بالتحقق من العرض المقدم لاتفاقية الحد من الأسلحة الإستراتيجية المعروفة باسم SALTII. يستطيع القارئ إيجاد بروتوكولات تقترح طرق الغش في لعبة البوكر الذهنية في فورتشن وميريت ([33] Fortune and Merritt) وكوبرسميت ([22] Coppersmith) وغيرها.