الفصل العاشر

التعمية التقليدية
Classical Cryptography

التعمية هي عملية التواصل (نقل معلومات) بين طرفين مع وجود من يتنصت عليهم (أعداء)[1]. أهم الأمثلة على ذلك هو الحفاظ على سرية المعلومات أثناء التواصل باستخدام قناة اتصال غير آمنة. ويتم ذلك بقيام المرسل بتحريف محتوى الرسالة بحيث يكون من الصعب على من يعترضها من معرفة محتواها ولكن من السهل قراءتها من قبل المُسْتَقبل (الصديق). وبهذا يمكن اعتبار عملية التعمية على أنها تقنية رياضية لحماية المعلومات (من الأعداء أو غير المصرح لهم معرفتها) وذلك بإجراء بعض التحويلات على هذه المعلومات.

إضافة إلى السرية، من الممكن استخدام التعمية لتحقق العديد من أهداف أمن المعلومات التي تعرف بالموثوقية (authentication) أو إثبات الأصالة التي تقدم لنا إثباتاً على التأكد من صواب مصدر الرسالة (أو أصل البيانات). أما سلامة البيانات (data integrity) فتكشف لنا التلاعب في البيانات من حيث تغييرها أو تأخير وصولها أو الرد غير الموثوق على الرسائل. ويكون دور المطابقة (identification) لإثبات التحقق من

---

(١) رايفست (Rivest)، انظر [71].

صحة هوية المستخدم. وعدم الإنكار (nonrepudiation) هي خدمة عدم السماح للمرسل التنصل (الإنكار) من أنه هو الذي قام بإرسال الرسالة. والتوقيع الإلكتروني (digital signature) هو رديف التوقيع الاعتيادي على الرسالة ويعد من أساسيات خطط الموثوقية.

تحليل التعمية (cryptanalysis) هو العملية العكسية للتعمية، وهي التقنية الرياضية المستخدمة لمحاولة كسر الرسالة المعماة ومن ثم قراءتها. تسمى عمليتي التعمية وتحليل التعمية بعلم التعمية (cryptology). يعد تحليل التعمية من العناصر المهمة لعلم التعمية التطبيقي حيث يلقى الضوء على مقدار ثقتنا بأمن خطة التعمية المستخدمة عند عدم وجود البرهان الرياضي على أمن هذه الخطة.

نقدم في البند (١٠,١) الإطار الأساسي المستخدم في الفصول العاشر والحادي عشر والثاني عشر. يعتمد أمن التواصل في التعمية التقليدية على سر يشترك فيه المتراسلون وندرس في البند (١٠,٢) بعض هذه الخطط التي تسمى خطط المفتاح المتماثل (symmetric-key schemes). إحدى هذه الخطط هي خطة اللفافة لمرة واحدة (one-time pad) وهي خطة بسيطة لا يمكن كسرها (آمنة تماماً) مهما كانت القدرة الحسابية التي يملكها العدو. ولكن هذه الخطة ليست عملية ويرجع السبب وراء ذلك لكبر المفتاح السري المستخدم. نناقش في البند (١٠,٣) نظام تعمية البيانات القياسي DES (Data Encryption Standard) وهو أفضل نظام تعمية متماثل المفتاح معروف لحد الآن. وعلى عكس الأمن التام لنظام اللفافة لمرة واحدة فقد صمم نظام DES لتكون كمية الحسابات اللازمة لكسره كبيرة جداً.

إحدى الخصائص الأساسية في أنظمة التعمية ذات المفتاح المتماثل هو معرفة المفتاح السري من قبل جميع المتراسلين حيث لا يمكن فصل القدرة على تعمية الرسالة عن القدرة على قراءتها. وفي العام ١٩٧٦م، نشر ديفي وهيلمان (Diffie and Hellman)

بحثهما المشهور (انظر [27]) حيث اكتشفا نظام التعمية ذو المفتاح المعلن (public- key cryptography). حيث كانت أحد خصائصه هي الفصل بين مفتاح التعمية ومفتاح كسر التعمية ويعتمد أمن هذا النظام على صعوبة حل بعض المسائل الحسابية. نقدم في الفصل الحادي عشر بعض مواضيع نظرية الأعداد التي يعتمد عليها هذا النظام وفي الفصل الثاني عشر نقدم نظام التعمية ذو المفتاح المعلن وطرق تنفيذه.

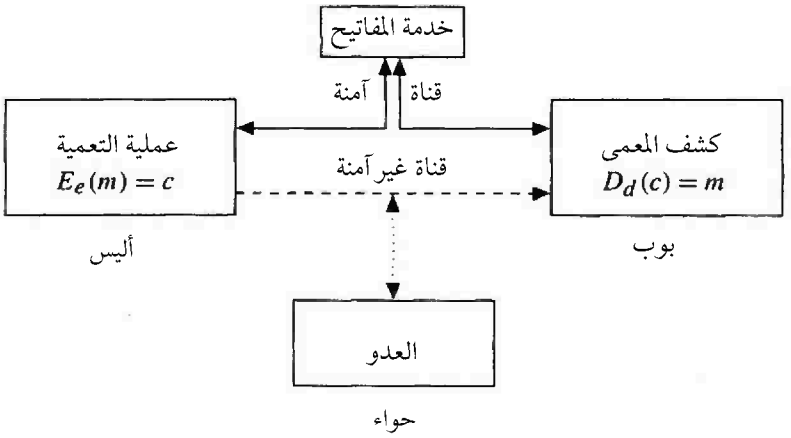
(١٠,١) خطط التعمية

Encryption Schemes

الهيكلية التالية هي التي نستخدمها عند دراسة أدوات عملية التعمية :

- هجائية منتهية $\mathcal{A}$.
- فضاء الرسائل $\mathcal{M}$ على $\mathcal{A}$ يتكون من كلمات رموز الهجائية. فعلى سبيل المثال، إذا كانت $\mathcal{A}=\{0,1\}$ فالرسائل هي عبارة عن كلمات تستخدم الرمزين 0 و 1. يرمز لمجموعة الرسائل من الطول n بالرمز $\{0,1\}^n$ ، كما أن $\{0,1\}^*$ هي مجموعة جميع الرسائل المنتهية الطول.
- تتكون خطة التعمية (أو التعمية) من فضائي رسائل $\mathcal{M}$ و $\mathcal{C}$ ومن مجموعة $\mathcal{K}$ (تسمى فضاء المفاتيح) ودالتين $E_k : \mathcal{M} \to \mathcal{C}$ و $D_k : \mathcal{C} \to \mathcal{M}$ لكل $k \in \mathcal{K}$ حيث $D_k\big(E_k(m)\big) = m$ لكل $m \in \mathcal{M}$. تسمى E_k دالة التعمية وتسمى D_k دالة كشف المعمى. كما تسمى عناصر $\mathcal{M}$ ، النص الواضح وعناصر $\mathcal{C}$ ، النص المعمى.
- تكتب المفاتيح في بعض خطط التعمية كأزواج مرتبة $k=(e,d)$ حيث يستخدم e في عملية التعمية و d في كشف المعمى. وفي هذه الحالة يسمى الزوج (e,d) ، زوج مفتاح ونكتب $E_e = E_k$ و $D_d = D_k$.

يبين الشكل (١٠,١) مخططاً لعملية تعمية أساسية حيث تريد أليس (Alice) إرسال رسالة سرية m إلى بوب (Bob) مع محاولة حواء (Eve) وهي العدو، التنصت على قناة الإرسال غير الآمنة.



الشكل (١٠,١). التواصل باستخدام التعمية.

عند استخدامنا نظام تعمية متماثل المفاتيح (انظر البند (١٠,٢)) نحتاج إلى قناة آمنة لإرسال المفاتيح نفسها وهذا يتطلب أحياناً إلى وجود ناقل مفاتيح موثوق به أو أي طريقة آمنة أخرى للحفاظ على السرية. أما عند استخدامنا لأنظمة التعمية ذوات المفتاح المعلن (انظر الفصل الثاني عشر) فتزودنا القناة بطريقة للتحقق من موثوقية الجزء المعلن من المفتاح.

هناك نوعان من الأعداء، الأول منهما وهو العدو غير الفعال يقتصر عمله على التنصت على جزء من القنوات غير الآمنة ومحاولة معرفة جزء من معلومات الرسالة المرسلة من أليس إلى بوب. أما النوع الثاني فهو العدو الفعال حيث يحاول إضافة إلى التنصت، محاولة تحريف أو إرسال رسائل أو حتى قطع الإرسال تماماً بين

أليس وبوب. إن مهمة التعمية هي محاولة الحفاظ على أمن المعلومات واكتشاف الرسائل المحرفة والمزورة. ولهذا فعملية التعمية لا تضمن لنا عملية إرسال رسائل آمنة تماماً طالما هناك عدو فعال وأحياناً يتم إرسال رسائل بصفة دورية لمحاولة اكتشاف نقاط ضعف قنوات الاتصال.

من الممكن القول إن نظام التعمية يكون قابلاً للكسر (غير آمن) إذا استطاع العدو الحصول على النص الواضح من النص المعمى (والأسوأ من ذلك هو استطاعة العدو من حساب المفتاح السري للنظام). يمكن تقسيم أمن النظام إلى الأنواع التالية:

- يكون النظام آمن تماماً إذا كان من المستحيل معرفة النص الواضح من قبل العدو (ما عدا طول النص الواضح) مهما كان النص المعمى المتوفر لديه ومهما كانت مصادر الحسابات المتوفرة لديه.
- يكون النظام آمن حسابياً إذا كانت عملية كسره حسابياً غير ممكنة مع وجود مصادر معقولة للحسابات ومع استخدام التقنية المعروفة لتحليل النظام.
- يكون النظام آمن برهاناً إذا أمكن برهان أن كسره على الأقل يكافئ حل مسألة رياضية من المعلوم أنها صعبة الحل.

سنقدم في البنود القادمة بعض التفاصيل عن هذه الأنواع المتعلقة بأمن أنظمة التعمية.

وصف خان (Kahn) الكتاب الذي نشره كرتشوف (Kerchhoffs) في العام ١٨٨٣م بأنه ثاني أعظم كتب التعمية[٢]. احتوى كتاب كرتشوف على عدة شروط أساسية لاختيار نظام التعمية منها: يجب أن يكون النظام غير قابل للكسر (على الأقل من

---

(٢) ذكر خان (انظر [48] Kahn): يعود الفضل الأول لوضع خطة مترابطة منطقياً لفكرة علم التعمية إلى جيوڤاني باتيستا بورتا المولود في مدينة نابيلوس في بحثه المنشور عام ١٥٦٣م، ولكن هذه النظرة إلى التعمية لم تعد كافية بعد اكتشاف التيلغراف.

الناحية التطبيقية) إذا كان من غير الممكن أثبات أمنه رياضياً. لا يجب أن يؤثر التغاضي عن بعض خصائص النظام على عملية الإرسال. سهولة تذكر وتغيير مفتاح التعمية السري. إمكانية إرسال النص المعمى باستخدام التيلغراف. يجب أن يكون هناك مرونة في نقل أدوات ووثائق النظام وأن تكون قابلة للتنفيذ من قبل شخص واحد فقط ويجب أن يكون النظام سهلاً بحيث لا يحتاج إلى معرفة مسبقة لقواعد كثيرة ولا يحتاج إلى تفكير ذهني. وهذه الأخيرة تسمى أحياناً بقاعدة كرتشوف التي تنص على أن أمن النظام يجب أن يعتمد فقط على مفتاح التعمية. أي أنه يمكن المحافظة على أمن النظام حتى لو كان العدو على دراية بنظام التعمية المستخدم.

يكون هدف العدو أثناء عملية التعمية المبينة في الشكل (١٠,١) هو معرفة النص الواضح من النص المعمى أو معرفة المفتاح نفسه، وأحياناً يكون الهدف محدود بمعرفة نص واضح معين. وعند اعتراضه لبعض الرسائل المعماة يحاول دراسة أنماط الإرسال لمعرفة معلومات عن الرسالة. على سبيل المثال، يمكن ملاحظة التدفقات المفاجئة للمعلومات حتى مع عدم معرفة ماهية الرسالة. إن هدفنا هو محاولة كسر النظام نفسه وهناك عدة مستويات لذلك:

(١) معرفة النص المعمى فقط (cipher text-only attack). يحاول العدو هنا معرفة النص الواضح أو مفتاح التعمية من النص المعمى الذي بحوزته. يعدُّ النظام الذي يمكن كسره بهذه الطريقة غير آمن كلياً.

(٢) معرفة النص الواضح (known-plaintext attack). في هذه الطريقة يكون بحوزة العدو جزء من النص الواضح وما يقابله من النص المعمى. وفي هذه الحالة يحاول العدو معرفة المفتاح السري أو كشف تعمية نصوص معماة إضافية سبق وأن استخدمت المفتاح نفسه لتعميتها.

(٣) اختيار نص واضح (chosen-plaintext attack). في هذه الحالة يكون العدو قد استطاع الدخول مؤقتاً على أدوات التعمية (ليس المفتاح) ومن ثم أجرى عملية تعمية لبعض النصوص الواضحة. إذا تم اختيار النص المعمى بطريقة تعتمد على نتائج مسبقة فتسمى الطريقة بالهجوم التكيفي (adaptive attack).

(٤) اختيار نص معمى (chosen-ciphertext attack) في هذه الحالة يكون العدو قد استطاع الدخول مؤقتاً على أدوات التعمية ومن ثم يختار نصوص معماة ويجد ما يقابلها من النص الواضح.

هناك طرق أخرى لمحاولة كسر بعض الأنظمة التي تعتمد على خصائص أدوات التعمية، مثل ملاحظة الزمن اللازم للحسابات وغيرها (انظر [52] و [53]). وفي بعض الأحيان استخدمت الرشوة والابتزاز لمعرفة مفتاح التعمية.

(١٠,٢) التعمية ذات المفتاح المتماثل
Symmetric-Key Encryption

في عديد من أنظمة التعمية التقليدية يكون هناك كلمة سر (مفتاح) مشتركة بين المتراسلين وبمعرفة هذا السر يكون بإمكانهما التعمية وكشف المعمى. وبصورة أدق، نقول إن نظام التعمية متماثل المفتاح إذا كان إيجاد D_d من e و E_e من d يتطلب الوسائل نفسها.

يتكون نظام تعمية تعويض بسيط (Simple Substitution Cipher) من تطبيق آحادي k على الهجائية المستخدمة. تتم عملية التعمية بتطبيق k على كل من رموز الرسالة. أي إذا كان $m = m_0 m_1 \ldots$ حيث m_i رموز من الهجائية فإن:

$$E_k(m) = E_k(m_0 m_1 \ldots) = k(m_0)k(m_1)\ldots$$

مثال (١٠,٢,١)

نظام الإزاحة (shift cipher) هو حالة خاصة من نظام التعويض. يكون المفتاح k ، $0 \leq k \leq n$ عبارة عن إزاحة ثابتة على رموز الهجائية $\{a_0, a_1, \ldots, a_{n-1}\}$ حيث :

$$a_j \overset{(٣)}{\mapsto} a_{(j+k) \bmod n}$$

دالة التعمية المشهورة $\mathrm{rot}13$ تقابل $k = 13$ على الهجائية $\{a, b, \ldots, z\}$ وذلك بالتدوير 13 موقعاً. أي أن الحروف تقابل الأعداد $0,1,\ldots,25$ وأن $\mathrm{rot}13$ تعني إضافة 13 إلى كل من حروف الهجائية ومن ثم نحسب الناتج قياس 26 [٤].

سنستخدم عادة الحروف الصغيرة للنص الواضح والحروف الكبيرة للنص المعمى. على سبيل المثال،

$$\begin{aligned} \mathrm{rot}13(\text{rotate}) &= \mathrm{rot}13(17,14,19,0,19,4) \\ &= (4,1,6,13,6,17) \\ &= \text{EBGNGR} \end{aligned}$$

وبهذا فالنص الواضح "rotate" قد تمت تعميته إلى النص المعمى "EBGNGR". نظام الإزاحة هذا يحقق الخاصية $\mathrm{rot}13(\mathrm{rot}13(m)) = m$. أي أن دالة التعمية ودالة كسر التعمية هما الدالة نفسها. استخدم يوليوس قيصر (Julius Ceasar) نظام الإزاحة بمفتاح $k = 3$.

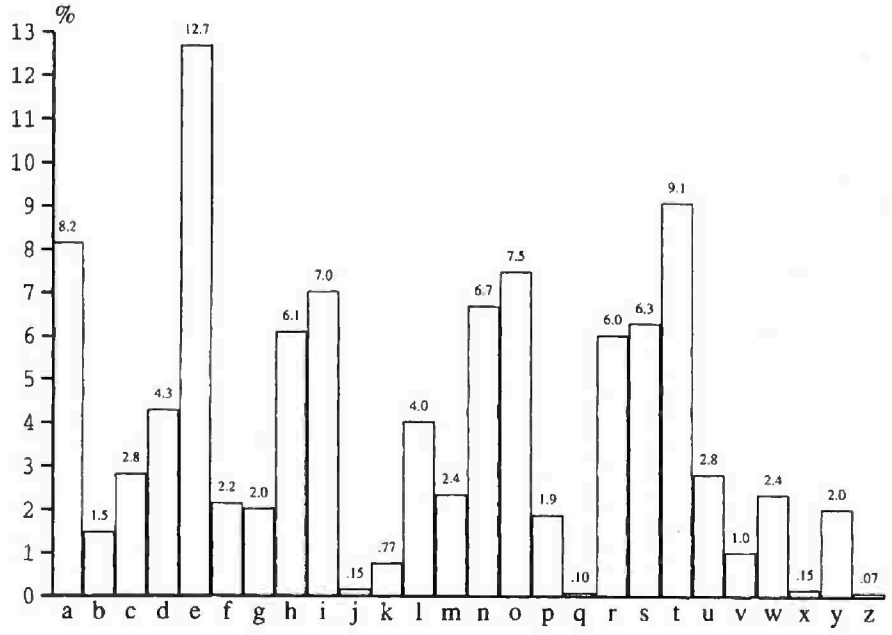
نظام الإزاحة غير آمن ويمكن كسره باستخدام طريقة اختيار النص الواضح. وهو غير آمن أيضاً باستخدام طريقة النص المعمى فقط ؛ لأن عدد المفاتيح هو 26 ومن الممكن تجريبها واحداً واحداً حتى نجد مفتاح التعمية. ▲

---

(٣) ندرس المفهوم " mod " في الفصل الحادي عشر وهنا يعني " $(i+k) \bmod n$ " باقي قسمة $i+k$ على n .

(٤) تستخدم $Rot13$ أحيانًا في USENET لتعمية العبارات التي تعتبر عدوانية.

قد يصعب كسر نظام تعمية تعويض بسيط باستخدام استنفاد المفاتيح حتى لو كان عدد رموز الهجائية صغيراً، ولكن يمكن كسره باستخدام تحليل التردد إذا كانت خواص الهجائية المستخدمة معروفة. على سبيل المثال، يبين الشكل (١٠,٢) ترددات حروف الهجائية الإنجليزية التي استندت إلى عينة مختارة من الصحف والروايات (انظر [3]). أي نص معمى لنظام تعمية تعويض بسيط يحقق توزيع ترددات الهجائية المستخدمة. فإذا كانت الهجائية المستخدمة هي الإنجليزية فنرى استناداً إلى الشكل (١٠,٢) أن الحرف الأكثر تردداً في النص المعمى يجب أن يقابل الحرف e (الأكثر تردداً في الهجائية الانجليزية) وأن ترددات الحروف $\{j, q, x, z\}$ صغيراً ومن ثم فإن ظهورها في النص المعمى نادر. من الممكن أيضاً الاعتماد على ترددات الثنائيات (حرفان متتاليان) والثلاثيات (ثلاثة حروف متتالية) بالأسلوب نفسه.



الشكل (١٠,٢). ترددات حروف الهجائية الانجليزية.

مثال (١٠,٢,٢)

لنفرض أن الهجائية هي الإنجليزية $\{a,b,\ldots,z\}$ وأن مفتاح نظام التعويض هو تبديلاً على الهجائية، على سبيل المثال،

$$k=\begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ T & U & V & W & X & Y & Z & B & I & K & E & A & C & D & F & G & H & J & L & M & N & O & P & Q & R & S \end{pmatrix}$$

حيث صور الصف الأول هي المقابلة لها في الصف الثاني، فمثلاً $E_k(\text{trek})=\text{MJXE}$. من السهل تذكر هذا التبديل؛ لأن بداية الكلمة BIKE واقعة تحت الحرف h ومن ثم نملأ بقية الحروف بالترتيب. هذا النظام غير آمن ويمكن كسره باستخدام طريقة اختيار النص الواضح (من الممكن إيجاد المفتاح بتعمية الرسالة $m=abc\ldots z$). أما استخدام طريقة النص المعمى فقط لكسر النظام فتحتاج إلى بعض الجهد ولكنها تنجح في نهاية الأمر في كسر النظام. أما طريقة الاستنفاد لمعرفة مفتاح التعمية فهي مستحيلة؛ لأن عدد عناصر فضاء المفاتيح هو $26!\approx 4\times 10^{26}$. ▲

يدعى نظام تعمية التعويض البسيط أحياناً بنظام تعمية التعويض الأحادي (monoalphabetic). إذا كانت الهجائية المستخدمة في نظام التعمية كبيرة فتصبح عملية تحليل (كسر) النظام باستخدام الترددات صعبة جداً. من الممكن إضافة رموز إضافية إلى هجائية صغيرة كالمستخدمة في المثال (١٠,٢,٢) لجعل فضاء الرسائل كبير ومن ثم يصعب كسره بتحليل الترددات. نظام البيانات القياسي DES (The Date Encryption Standard) الذي سندرسه في البند (١٠,٣,٢) هو عبارة عن نظام تعويض على هجائية سعتها 2^{64}.

الأنظمة التعددية

يمكن وصف الأنظمة التعددية على أنها أنظمة تحاول حجب ترددات المصدر الأصلي بحيث تُعمىَ كل من رموز النص الواضح إلى واحد من عدة رموز في النص المعمى. نظام فيجينير (Vigenere Cipher) هو مثال شائع على هذه الأنظمة. في هذا النظام يتم مقابلة رموز هجائية $\mathcal{A}$ مع الأعداد الصحيحة في الفترة $[0,|\mathcal{A}|]$ ومن ثم يتم اختيار

مفتاح $k = k_0k_1 \ldots k_{n-1}$ حيث $k_i \in \mathcal{A}$. تتم عملية التعمية بتعمية قوالب من الهجائية طولها n ؛ وذلك بمقابلة رموز الرسالة مع رموز المفتاح قياس $|\mathcal{A}|$. على سبيل المثال، لنفرض أن $\mathcal{A}$ هي الهجائية الإنجليزية $\{a, b, \ldots, z\}$ وتقابل مجموعة الأعداد $\{0, 1, \ldots, 25\}$. الجدول التالي يوضح طريقة التعمية لنص واضح قصير باستخدام المفتاح "KEY".

النص الواضح	she sells sea shells by the seashore
المفتاح +	KEY KEYKE YKE YKEYKE YK EYK EYKEYKEY
النص المعمى	CLC CIJVW QOE QRIJVW ZI XFO WCKWFYVC

حيث عملية الجمع هي قياس 26. ويتم كشف المعمى بطرح كلمة المفتاح من النص المعمى قياس 26.

إن استخدام ترددات رموز المصدر (الهجائية) لكسر النظام التعددي أصعب قليلاً هنا ؛ وذلك لإمكانية تعمية رمز من النص الواضح إلى عدد من الرموز المختلفة في النص المعمى وهذا يعتمد على موقع الرمز، فمثلاً تمت تعمية الحرف "e" في المثال أعلاه إلى الحروف $\{C, I, O\}$. ومع ذلك، إذا استطعنا معرفة طول المفتاح l فمن الممكن استخدام تحليل الترددات لنظام أحادي على رسائل جزئية مكونة من الأحرف التي تكون المسافة بينها مضاعفات الطول l في النص المعمى. في المثال المقدم أعلاه، تتكون الرسائل الجزئية في النص المعمى من الأحرف في المواقع $0, 3, 6, \ldots$ ويتم إنجاز ذلك بإضافة (قياس 26) الحرف الأول من الحروف الثلاثة لكلمة المفتاح إلى حروف النص الواضح في المواقع المقابلة.

اكتشف فردريك كاسيسكي (Friedrick Kasiski) في العام ١٨٦٣م طريقة تعرف الآن باسم اختبار كاسيسكي (Kasiski test) لمعرفة طول المفتاح بدراسة المسافات التي تفصل بين أجزاء متطابقة من النص المعمى[٥]. في الغالب تقابل الكلمات المتطابقة في

(٥) كتب خان [48] أن كاسيسكي توفي في العام ١٨٨١م قبل أن يدرك تأثير الثورة التي سببها اكتشافه في علم التعمية.

النص الواضح الجزء نفسه من مفتاح التعمية مما ينتج عنه كلمات متطابقة في النص المعمى. في المثال السابق، يحدث ذلك في الجزء "ells" من النص الواضح. من الممكن وجود أجزاء متطابقة في النص المعمى لا تقابل أجزاء متطابقة من النص الواضح ولكن كلما زاد طول الرسالة كان احتمال ظهور مثل هذه الأجزاء صغيراً. ولهذا فعملية تطبيق اختبار كاسيسكي تبدأ في البحث عن كلمات مكررة في النص المعمى ونحسب المسافات بين هذه التكرارات فيكون طول كلمة السر هو أحد قواسم القاسم المشترك الأكبر لهذه الأطوال. لاحظ أن اختبار كاسيسكي يؤكد على أنه إذا وجدت كلمتان في النص الواضح بحيث يكون طول المسافة بينهما مضاعفاً لطول المفتاح فسيظهر هذا العدد كقيمة مسافة بين كلمتين متطابقتين في النص المعمى. هذا بالتأكيد ليس بالضرورة أن يكون صائباً دائماً ففي حالة الرسائل القصيرة يكون احتمال تطابق كلمتان في النص المعمى صغيراً على الأرجح. وأما في حالة الرسائل المعماة الطويلة جداً فمن الممكن حدوث ذلك لأسباب أخرى.

مثال (١٠,٢,٣)

تم استخدام نظام فيجينير لتعمية النص المعمى التالي حيث اللغة المستخدمة هي الانجليزية دون استعمال النقط والفواصل والفراغات. أي أن اللغة مكونة فقط من أحرف الهجائية $a, b, \ldots, z$ وعددها 26.

الأوفسيت	النص المعمى
0	UPVZB BVUPN KKFOL OGAKU FBTKF LFXUJ VIPZV KFZXO FIDLO ONLUP
50	KKFUZ OMQFQ MQXKU AFIUP VVVVK KFDFL DMFIU PVVFI ZVTMU XDBZY
100	FVVYF ZTHBA ZQHEY LTXVU JVXFM IDRSQ EJNCI PVZZQ HQEYJ BZQHB
150	YHTWL OUWND OLVUJ VREZA JHTWW VPTZW VLVDM TROPV XWIMN KJBVE
200	FITKV XRQEL FZOBY HSMND TVFOJ DZQHB YLOOZ QTQXK UISLS LNLUP
250	RESWB HOEZQ HERVC MRWJV XWIMR LSISR WMIHF TZQHN CXUBV UJVXF
300	JZTOJ VXGJA REMMU GPEEG PEEWP BYHXI KHS

الفراغات المبينة ليست ضمن النص المعمى ولكنها وضعت لتسهيل القراءة.

تظهر الكلمة من الطول 3 "ZQH" في عدد من المواقع حيث وضعنا خط تحت ثلاثة من هذه المواقع وهي 110 ، 138 ، 226 على التوالي. وبهذا من المرجح أن يقسم طول كلمة السر l الفرق بين أي عددين من هذه الأعداد، وهذه الفرو قات هي :

$$226 - 110 = 2^2 \cdot 29 \qquad \text{و} \qquad 138 - 110 = 28 = 2^2 \cdot 7 .$$

هذا يقترح علينا أن $l \mid \gcd\left(2^2 \cdot 7, 2^2 \cdot 29\right)$. أي أن $l \mid 2^2$. إذا كان $l = 1$ فيكون النظام هو نظام الإزاحة الأحادي.

في هذه المرحلة يقوم محلل التعمية بدراسة توزيع الترددات لكل من أطوال المفتاح المقترحة لمحاولة معرفة فيما إذا كان لها خواص الهجائية المستخدمة. الجدول التالي يبين هذه الترددات لكل من طولي المفتاح. فمثلاً، إذا كان $l = 2$ فالجدول يبين ترددات الرسائل الجزئية المكونة من رموز أوفسيت زوجية ومن ثم المكونة من رموز أوفسيت فردية. وهذا يعطينا :

ℓ	رسائل جزئية أوفسيت	ترددات أحرف الرسائل الجزئية (مرتبة تنازليًا)
2	0, 2, 4, ...	19 16 12 12 11 10 9 8 8 7 6 6 5 5 5 5 5 4 4 3 2 2 2 1 0 0
	1, 3, 5, ...	14 14 13 10 10 10 9 9 9 8 8 7 6 6 5 5 5 3 3 3 2 2 2 2 1 0
4	0, 4, 8, ...	12 10 10 7 6 6 6 5 5 4 2 2 2 1 1 1 1 1 1 0 0 0 0 0 0 0
	1, 5, 9, ...	10 9 8 7 5 5 5 5 5 5 4 3 3 2 2 2 1 1 1 0 0 0 0 0 0 0
	2, 6, 10, ...	12 11 8 8 7 5 5 5 4 4 2 2 2 2 2 1 1 1 1 0 0 0 0 0 0 0
	3, 7, 11, ...	9 9 8 8 7 5 5 5 4 3 3 3 3 3 2 2 2 1 1 0 0 0 0 0 0 0

من المتوقع أن يعكس كل سطر من السطور (في حالة الطول الصحيح للمفتاح) توزيع ترددات الهجائية المستخدمة. ومع أن الرسالة في هذا المثال قصيرة نسبياً إلا أنه يمكن ترجيح أن يكون طول المفتاح هو $l = 4$ وليس $l = 2$. وباستخدام توزيع الترددات المبينة في الشكل (١٠,٢) نجد أن الحرف "e" هو الأكثر تردداً في اللغة الانجليزية. وبهذا فمن الممكن أن يقابل أحد الحروف ذات الترددات العالية في النص المعمى (لكل صف من صفوف $l = 4$) "e". وفي هذا المثال من الممكن اختيار 3 أو 4 (أو

ربما أكثر من ذلك) من حروف النص المعمى (لكل صف من صفوف $l = 4$) لتقابل الحرف "e".

يبين الجدول التالي الحروف الأربعة الأكثر تردداً في كل من صفوف $l = 4$ وما يقابلها من حروف المفتاح (باعتبار أن كل من هذه الحروف تقابل الحرف "e").

حروف النص المعمى الأكثر ترددًا لصفوف $\ell = 4$		حروف المفتاح المقابلة
F J U P	$(c - \text{e}) \bmod 26$	B F Q L
B V M I	$\longrightarrow$	X R I E
V Z R X		R V N T
K Q H L		G M D H

في هذه المرحلة يقوم محلل التعمية بكشف المعمى وذلك باستنفاد جميع كلمات المفتاح الممكنة والتي عددها في هذا المثال يساوي $4^4 = 256$.

في كثير من الأحيان يتم اختيار كلمة المفتاح من قاموس اللغة (أي أن المفتاح كلمة ذات معنى) مما يوفر على محلل التعمية الكثير من الجهد. ففي المثال أعلاه، يقود هذا البحث إلى الكلمتين "LEND" و "BIRD" وباستخدام الكلمة الثانية نرى أن النص الواضح هو:

النص المعمى	UPVZB BVUPN KKFOL OGAKU FBTKF LFXUJ VIPZV KFZXO FIDLO ONLUP
المفتاح	BIRDB IRDBI RDBIR DBIRD BIRDB IRDBI RDBIR DBIRD BIRDB IRDBI
النص الواضح	thewa terof thegu lfstr etche doutb efore hergl eamin gwith

والنص الواضح هو نص باللغة الإنجليزية ويكون كشف المعمى (بعد إعادة الفواصل والنقط) هو:

> The water of the Gulf stretched out before her, gleaming with the million lights of the sun. The voice of the sea is seductive, never ceasing, whispering, clamoring, murmuring, inviting the soul to wander in abysses of solitude. All along the white beach, up and down, there was no living thing in sight. A bird with a broken wing was beating the air above, reeling, fluttering, circling disabled down, down to the water.(٦)

(٦) من كتاب "اليقظة" لمؤلفته Kate Chopin.

تقابل كلمة النص المعمى "ZQH" التي استخدمناها في اختيار كاسيسكي لإيجاد طول المفتاح الكلمة الواضحة "ing". كان من الممكن استخدام كلمات أطول تكررت في النص المعمى، مثل "NLUP" و "ZQHBY" ويقابلان "with" و "ingth" حيث تكرر كل منها مرتان. لاحظ أيضاً أن الكلمة "PVZ" تكررت في الموقعين 1 و 135 وهذه تقابل "hew" و "mur" ومن ثم تعمدنا عدم استخدامها على اعتبار أن ذلك حدث مصادفة. هاتان الكلمتان يقترحان أن طول المفتاح يقسم 134 وهو ليس الطول الصحيح للمفتاح. ▲

يمكن إيجاد أمثلة أصعب على تحليل نظام فيجينير في كل من المرجعين [48] و [86] على وجه الخصوص نجد أن استخدام معامل الصدفة (index of coincidence) المعرف في المرجع [86] طريقة أفضل لإيجاد طول المفتاح وكلمة المفتاح.

نظام التعويض البسيط ونظام فيجينير هما مثالان على أنظمة التعمية القالبية (block ciphers) حيث يتم في هذه الأنظمة تحويل الرسالة باستخدام دالة ثابتة تؤثر في قوالب مكونة من عدد ثابت من الرموز. وهذه دوال عديمة الذاكرة، بمعنى أن الدالة المؤثرة على القالب لا تعتمد على موقع هذا القالب في الرسالة. وأما أنظمة السيل (stream ciphers) فهي على العكس من ذلك حيث الدالة المؤثرة على القالب تعتمد على موقع هذا القالب في الرسالة، ولهذا فأنظمة السيل تسمى أحياناً، أنظمة المرحلة (state ciphers).

تستخدم عادة الهجائية الثنائية $\mathcal{A} = \{0,1\}$ لتعريف مثل هذه الأنظمة حيث يعرف النظام القالبي (ونظام السيل) باستخدام عدد ثابت من البايتات تسمى طول القالب (block length). وتتم معالجة الرسائل على الهجائية $\mathcal{A} = \{a_0,\ldots,a_{n-1}\}$ بمقابلة $a_j \leftrightarrow j$ ثم تحويل j إلى كلمة ثنائية من الطول $\lceil \log_2 n \rceil$. في الحالة الخاصة التي يكون فيها عدد رموز الهجائية 26 (الهجائية الإنجليزية) كما هو مبين في المثال (**١٠,٢,٢**) نقوم باستبدال كل من رموز الهجائية بكلمة ثنائية طولها 5. على سبيل المثال،

$g \leftrightarrow 6 = 00110$. عندئذ، تؤثر دالتي التعمية وكشف المعمى في هذه الأمثلة على قوالب طول كل منها يساوي 5.

إذا كانت m و m' رسالتين على $\{0,1\}$ من الطول نفسه فيكون $m \oplus m'$ هو الجمع قياس 2، على سبيل المثال، $1100 \oplus 1010 = 0110$. تسمى هذه العملية أحيانا بعملية الفصل المتنافية (exclusive or) وتكتب عادة XOR (عملية الجمع هذه تحقق حلم التلاميذ بإجراء عملية جمع دون الحاجة إلى حمل الأعداد للمرحلة التالية).

مثال (١٠,٢,٤)

نظام تعمية فيرنام (Vernam Cipher) هو نظام سيل على $\mathcal{A} = \{0,1\}$. وفضاء المفاتيح هو أيضاً كلمات على $A = \{0,1\}$. دالة التعمية هي $m \mapsto c = m \oplus k$. وبالحساب قياس 2 نستطيع الحصول على النص الواضح m من النص المعمى c على النحو التالي:

$$c \oplus k = m \oplus k \oplus k = m \oplus 0 = m$$

أي أن دالة كشف المعمى هي نفس دالة التعمية. ▲

إذا حصلنا على مراتب المفتاح (يسمى عادة مفتاح السيل) من محاولات بيرنولي المستقلة باحتمال $\frac{1}{2}$ (مثل، الرميات المستقلة لقطعة نقود غير منحازة) وإذا استخدم المفتاح مرة واحدة فقط فنحصل على نظام تعمية اللفافة الواحدة (one-time pad) وهو نظام آمن تماماً ضد محاولة كسره بمعرفة النص المعمى فقط. يرجع سبب أمن هذا النظام إلى أن طول مفتاح التعمية يساوي طول النص الواضح (ومن ثم طول النص المعمى) ويستخدم لمرة واحدة فقط. استخدم شانون (Shannon) في العام ١٩٤٠م [80] مفهوم الانتروبيا (entropy) لإثبات الأمن التام لنظام تعمية اللفافة الواحدة حيث برهن أن أي نظام تعمية متماثل المفاتيح يعد آمن تماماً طالما كان طول المفتاح مساوياً لطول الرسالة.

في بداية اكتشاف نظام فيرنام كانت معلومات المفتاح تكتب على ورقة (لفافة) ثم تتلف هذه اللفافة بعد كل عملية تعمية ومن هنا جاءت التسمية "اللفافة الواحدة". لاحظ أن استخدام المفتاح نفسه لتعمية أكثر من رسالة واحدة يؤدي إلى ضعف أمن النظام، على سبيل المثال، إذا كان $c = m \oplus k$ و $c' = m' \oplus k$ فنرى أن:

$$c \oplus c' = \big(m \oplus k\big) \oplus \big(m' \oplus k\big) = m \oplus m'$$

(على وجه الخصوص إذا كان $m = m'$ فيستطيع محلل التعمية اكتشاف ذلك بسهولة).

جرت عدة محاولات من قبل محللي التعمية لكسر النظام؛ وذلك بالحصول على بعض المفاتيح والاحتفاظ بها حيث صرح ضابط المخابرات البريطانية، بيتر رايت (Peter Wright) (انظر [101]) أن تكرار الاتحاد السوفيتي لاستخدام مفتاح تعمية في أكثر من عملية تعمية واحدة (قام بإرسال اللفافة نفسها إلى عديد من سفاراته في الغرب أثناء الحرب العالمية الثانية) أدى إلى كسر نظام اللفافة الواحدة حيث قام محللو التعمية المعروفة باسم VENONA من اختبار عديد من الرسائل المعمية ومقارنتها مع الرسائل المرسلة من الاتحاد السوفياتي عبر قنوات مختلفة(٧).

يتنازل نظام DES المشهور عن استخدام اللفافة الواحدة ويستخدم خطط تعمية أكثر مرونة يعتقد أنها آمنة حسابياً حيث توجد طرق شائعة لتوليد المفاتيح عشوائياً. تولِّد هذه الطرق متتالية من الأعداد يتم تحديدها تماماً بمعرفة بذرة بدائية (initial seed)

---

(٧) قدمت محطة CNN التلفزيونية مسلسلاً عام ١٩٩٨م "خبرة الحرب الباردة" وكجزء من هذا المسلسل ذكرت أن مجموعة VENONA التابعة لهيئة USNSA تمكنت من كسر العديد من أنظمة التعمية (ومن ضمنها نظام تعمية اللفافة الواحدة) التي استخدمها الاتحاد السوفياتي خلال الفترة من ١٩٤٣م إلى ١٩٨٠م حيث تم الكشف عن هذه المصادر السرية في العام ١٩٩٥م. ولكن محطة CNN تجاهلت حقيقة استخدام المفتاح أكثر من مرة واحدة، الأمر الذي أخل لأمن النظام وادعت أن نظام اللفافة الواحدة قابل للكسر بتجريب عدة ملايين من الرسائل المعماة.

يتم اختيارها من مجموعة منتهية. وعلى الرغم من أن هذه المتتاليات لها العديد من الخصائص اللازمة للمحاكاة إلا أنها ليست عشوائية بالمعنى المطلوب في عملية التعمية[٨].

تمارين

(١٠,٢,٥) استخدم نظام فيجينير المبين في المثال **(١٠,٢,٣)** للحصول على النص المعمى التالي:

العداد	النص المعمى
0	VHVVG NRWGA EGCLJ RVHVO GAUHT OWWJE FSROJ LVIFQ KNKKG IIDPG
50	VUJAM HLUJW CLCRY EUWJE DVGLM HUBFW JTFEG CFPGV LOPEI DDLVW
100	QOLUE ALVGM VVJAC OCTKD EKKKG MRVBE BHRLR QPEUW QMFUT ONLPD
150	RBNIX KVBLM

جد مفتاح التعمية إذا علمت أن الكلمات من الطول 3 التي تحتها خط تقابل كلمة طولها 3 شائعة الاستخدام و أن الحرفين AE هما الحرفان an التي تبدأ بهما كلمة طولها 3.

(١٠,٢,٦) اكتب برنامجاً لتنفيذ نظام تعويض مماثل للمقدم في المثال **(١٠,٢,٢)** (استخدم المؤلفون المفتاح awk). يجب أن يقبل البرنامج كلمة المفتاح والصفوف على أنها مدخلات. بعد ذلك اختار نص واضح من اللغة الانجليزية طوله على الأقل 300 حرف ثم استخدم البرنامج للحصول على النص المعمى المقابل وبعد ذلك استخدم تردد اللغة لكسر النظام على اعتبار عدم معرفتك لكلمة المفتاح.

(١٠,٢,٧) هذا التمرين مخصص لكسر نظام فيجينير بالأسلوب المتبع في المثال **(١٠,٢,٣)** حيث نقدم معلومات كافية لمعرفة مفتاح التعمية ومن ثم النص الواضح

---

(٨) اكتشف جولدبيرج (Goldberg) وواجنر (Wagner) (انظر [39]) أن مولد الأعداد العشوائية المستخدم في تصفح الشبكة العنكبوتية Netscape أضعف مما ادعى مالك الموقع وهذا يؤدي إلى عدم ضمان أمن الصفقات التجارية وتسبب ذلك في الإحراج لمالك الموقع حيث منع الجمهور من استخدام خوارزميات أمن النظام.

دون استخدام الحاسب الآلي. ونترك خيار مثال أكثر واقعية للقارىء الذي يملك برنامج آلي لكسر النظام. استخدم نظام فيجينير للحصول على النص المعمى التالي:

العداد	النص المعمى
0	TU1RD SFOGK YLBVL OORXX RVDPL SHRSB POCBT TLQPG AOMHM SVONM
50	HDHDN TRTCX RYCJL NHGHT BRIIM HHQWB NHGTI ERDAX BHWCZ IQGEB
100	RHRQR TKSGX VRZJM IRBXG BXQWT RHGIU ELXXG GDIIA OUWIB EVAPR
150	DHQXW EWCTQ THBSF AUHXT LOOLN NWWAM HHOHB AQUPF EVGRA EGIAX
200	DICGL ESHTF BHFGX MRJXG GPOGM IDZAT WZCJE DESPL IJBPE AGWEE
250	OPOIL ALREX OSZTP OXZSM ANSXM TRATT NWVPM WKOIA ASDTG EGPTY
300	OUSRH UORHM AUHJI AJOXG IQOHM AWSRH UQQXE MHSIB NJCCP EGBTL
350	DDMBK LLRTY EQRTW BHWYB NJGJL ERTBB LLHPK YICGV EWCRK AFYSH
400	WQCCM HHGIN DHBIF OYSBX NWHWX CUIHA IQUDY TKSRH UQHTK RHJDE

الكلمة المكررة "MHH" تقع في المواقع 74 ، 179 ، 404 (خيارات أخرى ممكنة مثل الكلمة الأطول "SRHU").

(أ) إذا كان l هو طول كلمة المفتاح (غير المعلومة) فيمكن توقع أن $l \mid (179-74) = 3 \cdot 5 \cdot 7$ وأن $l \mid (404-179) = 3^2 \cdot 5^2$. إذا افترضنا أن هذه الكلمات المكررة من النص المعمى تقابل أجزاء متطابقة من النص الواضح فأثبت أن $l \in \{1,3,5,15\}$.

(ب) لنفرض أن l لا يمكن أن يكون 15.

الجدول التالي يبين ترددات أحرف النص المعمى (عددها 830) لبقية قيم l :

فسر لماذا يكون $l = 5$ هو طول المفتاح المرجح.

(ج) جد حرف المفتاح المقابل لعدة أحرف كثيرة التردد في النص المعمى في الحالة $l = 5$ على اعتبار أن هذه الأحرف تقابل الحرف e من النص الواضح.

(د) إذا افترضنا أن واضع التعمية اختار كلمة المفتاح من القاموس (أي كلمة ذات معنى) فجد كلمة المفتاح، ثم جد جزء من النص الواضح. لاحظ أن بعض الرسائل الجزئية تحتوي على حروف ترددها كبير.

ℓ	العداد	ترددات حروف الرسائل
1	0, 1, ...	60 53 45 42 40 40 39 39 39 39 38 37 33 32 30 27 27 26 25 25 21 20 17 13 13 10
		H T R E O W B D G I S A X L Q C P U M N F V K J Y Z
3	0, 3, ...	22 19 18 18 16 14 13 13 13 13 13 11 11 9 9 9 8 8 8 8 6 5 5 4 3 1
		H E B R T O A G I S W C U D Q X F L N P M K V Z J Y
	1, 4, ...	22 17 16 15 15 14 14 13 13 11 11 10 10 10 9 9 9 9 8 8 8 7 6 6 4 3
		H T G D W O X A E Q R I K S B C N V L P U M J Y F Z
	2, 5, ...	20 16 16 16 16 15 15 12 12 12 12 11 11 10 10 10 10 9 8 7 7 6 6 4 3 2
		T H I L R D S B M O W A P E G Q X F N C U V Y J Z K
5	0, 5, ...	24 15 15 13 12 12 11 11 7 7 6 5 5 4 4 3 3 3 3 2 1 0 0 0 0 0
		E A N T O R I S B D U H L C G M P W Y V F J K Q X Z
	1, 6, ...	22 15 14 14 13 12 12 10 8 8 6 6 6 5 4 3 2 2 1 1 1 1 0 0 0 0
		H Q D U W L R O K V F G J P X S I Y B E N Z A C M T
	2, 7, ...	18 15 13 13 12 11 9 9 9 8 7 7 6 5 5 4 3 3 2 2 2 2 1 0 0 0
		S O H W Q C G I R B A F Z D V M T U J P X Y K E L N
	3, 8, ...	24 14 13 12 12 11 11 10 9 8 7 7 6 6 5 2 2 2 2 2 1 0 0 0 0 0
		T P I C X D H G A E R W B S J L N Q V Y U F K M O Z
	4, 9, ...	18 17 15 13 13 10 9 9 8 7 7 6 5 4 4 4 3 3 3 3 2 2 1 0 0 0
		M B X L T G E H K F N A R I W Y O P V Z D U Q C J S

(١٠,٢,٨) تؤدي عملية ضغط البيانات إلى إزالة بعض البيانات الزائدة. إذا استخدمنا عملية ضغط البيانات ثم عملية التعمية فهل يؤدي ذلك إلى نظام أكثر أمناً ؟

(١٠,٣) أنظمة تعمية فيستل و DES

Feistel Ciphers and DES

ندرس في هذا البند بصورة مختصرة صنف من أنظمة التعمية يتضمن نظام المفتاح المتماثل الأكثر شهرة وهو نظام DES. يتركز اهتمامنا هنا على بناء هذه الأنظمة وأمنها وعلى القارئ المهتم بتفاصيل نظام DES الرجوع إلى المراجع المقدمة في البند (١٠,٤).

نقدم هنا نظامي تعمية هما نظام البيانات الجديد المحكم (New Date Seal) أو اختصارا DES ونظام تعمية البيانات القياسي (Date Encryption Standard) أو اختصاراً DES حيث يعتمد بناء كل منهما على نظام فيستل. أنظمة فيستل هي أنظمة قالبية ينبثق عنها أنظمة مثل DES تستخدم أساليب بناء بحيث يمكن اعتبار خطة التعمية على أنها

خطة نظام سيل . إن أهم شروط بناء أنظمة التعمية القالبية هو سعة فضاء المفاتيح التي يفترض أن تكون كبيرة ليستعصي على محلل التعمية كسر النظام (معرفة المفتاح) بطريقة الاستنفاد. كما يشترط أن يكون طول القالب كبيراً لكي يجعل عملية تجميع بيانات من النص المعمى لتخمين المفتاح أمراً صعباً جداً. يكون هدف التشويش (confusion) هو تعقيد العلاقة بين المفتاح والنص المعمى وأما هدف النشر (diffusion) فهو محاولة نشر النص المعمى بحيث يعتمد حرف من حروف النص المعمى على عدد كبير من حروف النص الواضح. كما يتطلب بناء نظام تعمية عدم تجاهل سرعة وسعة ذاكرة الجهاز المستخدم لتنفيذ عملية التعمية.

يكون طول النص المعمى في نظام فيستل مساوياً لطول رسائل النص الواضح وليكن $2n$ حيث $n \in \mathrm{N}$. مدخل الخطة هو الرسالة نفسها والمفتاح k ويتم تنفيذ خوارزمية التعمية بسلسلة من المراحل عددها r.

- خوارزمية جدولة المفاتيح حيث يتم توليد مفاتيح جزئية $k_1, k_2, \ldots, k_r$ من مفتاح معطى k. كل من هذه المفاتيح الجزئية تعرف دالة:

$$f_{k_i} : \{0,1\}^n \to \{0,1\}^n$$

- تقسم الرسالة m من الطول $2n$ إلى قسمين أيسر وأيمن وتكتب $m = (m_0, m_1)$. ويتم كتابة المراحل على النحو التالي:

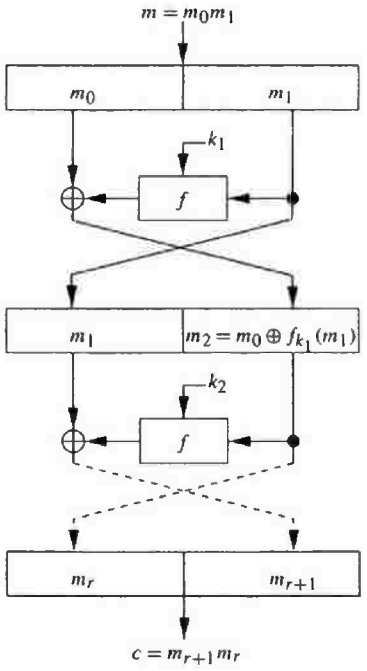
$$\begin{aligned}
&1 : (m_0, m_1) \mapsto \left(m_1, m_2 = m_0 \oplus f_{k_1}(m_1)\right) \\
&2 : (m_1, m_2) \mapsto \left(m_2, m_3 = m_1 \oplus f_{k_2}(m_2)\right) \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
&r : (m_{r-1}, m_r) \mapsto \left(m_r, m_{r+1} = m_{r-1} \oplus f_{k_r}(m_r)\right)
\end{aligned}$$

يقوم المخرج بتبديل النصف الأيمن مع النصف الأيسر للمرحلة الأخيرة لنحصل على $c = (m_{r+1}, m_r)$.

- إن هذا التبديل يسهل عملية كشف المعمى بحيث يسمح باستخدام المراحل r نفسها (نفس الترتيب) وبعكس ترتيب المفاتيح الجزئية. ولرؤية ذلك، بوضع $c_j = m_{r+1-j}$ نرى أن $c = (c_0, c_1)$ ويمكن إيجاد m_{r-1} من المراحل لنحصل على:

$$c_2 = m_{r-1} = m_{r+1} \oplus f_{k_r}(m_r) = c_0 \oplus f_{k_r}(c_1)$$

وهذا هو الشكل الذي نحصل عليه من المرحلة 1.



سلم فيستل ملتو

إن استخدام المراحل على هذه الصورة يسمح لنا باستخدام دالة بسيطة عند كل مرحلة. وعند استخدام مراحل متعددة (يستخدم DES عدد $r = 16$ من المراحل) نستطيع إدخال تشويش ونشر. ومن الضروري أن تكون سعة فضاء المفاتيح كبيرة لتمنع

العدو من إمكانية الحصول على المفتاح بطريقة الاستنفاد على اعتبار أن لديه أدوات حسابية سريعة.

(١٠,٣,١) نظام البيانات الجديد المحكم

نظام NDS من أنظمة فيستل البسيطة؛ وذلك لأن جدول المفاتيح يتكون من مفتاح واحد فقط. ولذا فهو سهل الكسر بطريقة اختيار النص الواضح كما سنرى في هذا البند.

ندرس هنا الحالة التي يكون فيها $n = 64$ (وبهذا يكون طول الرسائل هو $2n = 128$ مرتبة) وعدد المراحل هو $r = 16$. المفتاح هو الدالة $k : \{0,1\}^8 \to \{0,1\}^8$. من الواضح أن الشرط اللازم (وليس الكافي) على طول المفتاح لكي يمنع كسر النظام بطريقة استنفاد المفاتيح محققاً؛ لأن طول المفتاح هو $\left(2^8\right)^{2^8} = 2^{2048}$ وهذا عدد كبير جداً.

يحتوي النظام على دالتين (غير سريتين) $S_0, S_1 : \{0,1\}^4 \to \{0,1\}^4$ ويتكون جدول المفاتيح من المفتاح الوحيد k المستخدم في كل مرحلة من مراحل التعمية. لحساب $f_k\left(m_i\right)$ لنصف رسالة m_i من الطول 64 نقوم بتنفيذ التالي:

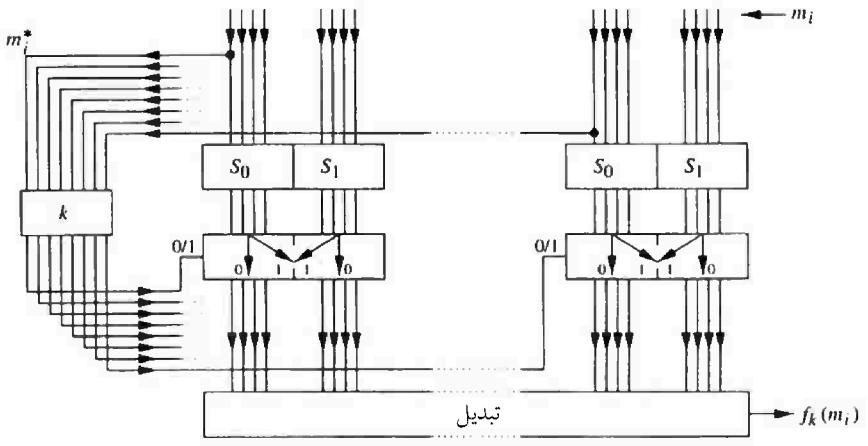
(١) نقوم بتجزئة m_i إلى 8 بايتات طول كل منها 8 مراتب ونفرض أن m_i^* هي البايت التي نحصل عليها من المرتبة الأولى لكل من بايتات m_i.

(٢) نقوم بتجزئة كل من بايتات m_i إلى كلمتين طول كل منها يساوي 4 ثم نجعل الدالة S_0 تؤثر على النصف الأيسر و S_1 تؤثر على النصف الأيمن.

(٣) إذا كانت المرتبة j من $k\left(m_i^*\right)$ تساوي 1 فنقوم بتبديل نصفي البايت j لمخرج S_0S_1.

(٤) نستخدم تبديلاً ثابتاً (غير سري) لتبديل المراتب المخرجة والتي عددها 64.

يبين الشكل (١٠,٣) مرحلة من مراحل NDS حيث التبديل النهائي يمنع من تقسيم الخطة إلى ثمان خطط أصغر مستقلة.



الشكل (١٠,٣). الدالة f في مرحلة من مراحل NDS .

كسر نظام NDS باختيار النص الواضح

إن أحد عيوب نظام NDS هو استخدام المفتاح نفسه في جميع المراحل مما يقود إلى معرفة المفتاح ثم كسر النظام باختيار النص الواضح، ويتم ذلك على النحو التالي:

نفرض أن $T = T_k$ هو التحويل المقابل لمرحلة من مراحل NDS. أي أن:

$$T\left(m_{i-1}, m_i\right) = T_k\left(m_{i-1}, m_i\right) = \left(m_i, m_{i-1} \oplus f_k\left(m_i\right)\right)$$

ولنفرض أن $F = T^{16}$ يرمز للمراحل الـ 16 جميعاً. الملاحظة الأهم هنا هو أن F يتبدل مع T وذلك لأن:

$$FT\left(m\right) = T^{16}T\left(m\right) = TT^{16}\left(m\right) = TF\left(m\right).$$

وبافتراض أن محلل التعمية على علم بالنظام المستخدم (من مبدأ كيرتشوف) ومن ثم يتم كسر النظام إذا استطاع الحصول على المفتاح k.

وبفرض أن $q \in \{0,1\}^8$ فيكون بإمكان محلل التعمية معرفة المفتاح إذا استطاع معرفة $k(q)$ لكل $q \in \{0,1\}^8$. ولانجاز ذلك يقوم بتنفيذ الخطوات التالية:

(١) يقوم بطمر q في الرسالة $m=(m_0,m_1)$ بحيث يكون $m_1^*=q$. وبهذا يحصل على النص المعمى $F(m)=(m_{16},m_{17})$ المقابل للنص الواضح المختار m.

(٢) لنفرض أن $\tilde{k}$ هي إحدى بايتات $k(q)$ وعددها 2^8. ولنفرض أن $\widetilde{T}=T_{\tilde{k}}(m)$ هو صورة الرسالة عند مرحلة واحدة تحت تأثير $\tilde{k}$.

(٣) إذا كانت $\tilde{k}=k(q)$ فنرى أن $\widetilde{T}=T(m)$ وأن:

$$F\left(\widetilde{T}\right)=FT(m)=TF(m)=T(m_{16},m_{17})=(m_{17},?)$$

وبهذا نجد أن النصف الأيسر من $F\left(\widetilde{T}\right)$ يتفق مع النصف الأيمن من $F(m)$. ويكون بإمكان محلل التعمية (العدو) الحصول على النص المعمى $F\left(\widetilde{T}\right)$ المقابل للنص الواضح المختار $\widetilde{T}$. وعليه، إذا كان النصف الأيمن من $F(m)$ يساوي النصف الأيسر من $F\left(\widetilde{T}\right)$ فيمكن اعتبار أن $\widetilde{T}$ تساوي $T(m)$ ومن ثم يقبل $\tilde{k}$ على أنه قيمة $k(q)$. لاحظ أن محلل التعمية يحتاج لتجريب $2^8=256$ قيمة للمفتاح $\tilde{k}$ على الأكثر ليحصل على مثل هذا التطابق.

وبتطبيق هذه الخطوات على كل $q\in\{0,1\}^8$ نحصل على مفتاح مرشح k باختيار $2^8(2^8+1)=65792$ نصاً واضحاً على الأكثر.

من الممكن أن نحصل على المفتاح الخطأ k حيث من المحتمل أن يكون $\widetilde{T}$ (في الخطوة ٣) "مطابقاً" دون أن تكون قيمته مساوية للمقدار $T(m)$. ومع ذلك إذا كان النظام مصمماً بحيث يضيف تشويش ونشر فمن الممكن افتراض عدم وجود أكثر من قيمة $\tilde{k}$ لنحصل على التطابق.

نحتاج أيضاً في الخطوة (٣) أن يكون $\tilde{k}=k(q)$ عندما يكون $\widetilde{T}=T(m)$. والمجهول الوحيد عند حساب $T(m)$ في هذه المرحلة هو شرط تبديل $k(m_1^*)$ على مخرج التحويليين S_0 ، S_1. فإذا اتفق مخرج S_0 و S_1 على إحدى بايتات m_1 فلا يمكن

تحديد مرتبة $k\left(m_1^*\right)$ المقابلة بمعرفة $T\left(m\right)$. وبناء على ذلك، نحتاج إلى اختيار m بحيث يختلف مخرج S_0 و S_1 عند كل بايت من بايتات m_1 إضافة إلى كون أن $m_1^* = q$ (عدم التمكن من اختيار مثل هذا الـ m يعدُّ مؤشراً على إمكانية كسر النظام بأسلوب أسهل)

مثال توضيحي

نأخذ نظام شبيه بنظام NDS حيث $n = 4$ وعدد المراحل هو $r = 3$. طول الرسائل هو $2n = 8$ مرتبة ودالة المفتاح هي $k : \{0,1\}^2 \to \{0,1\}^2$. (كل من المفاتيح الجزئية الثلاثة يساوي k). سعة فضاء المفاتيح هي $\left(2^2\right)^{2^2} = 256$. لنفرض أن S_0 هو التحويل المحايد وأن S_1 هو التحويل المتمم (على كل مرتبة). التبديل هو كتابة المراتب بالترتيب العكسي. والمخطط الشبيه في مخطط الشكل (**١٠,٣**) يحتوي على صندوقين S_0 و S_1 كل منهما يقبل مرتبة واحدة من مراتب m_i والتي عددها $n = 4$.

لنفرض أن المفتاح k معرف على النحو التالي:

$$k\left(00\right) = 10 \;،\; k\left(10\right) = 11 \;،\; k\left(01\right) = 00 \;،\; k\left(11\right) = 10$$

وأن الرسالة المراد تعميتها هي $m = \left(m_0, m_1\right) = \left(0111,1100\right)$.

يتم حساب $m_2 = m_0 \oplus f\left(m_1\right)$ على النحو التالي:

$$m_1 = 1100 \xrightarrow{S_0S_1} 1001 \xrightarrow{k} 0110 \xrightarrow{\text{تبديل}} 0110 \xrightarrow{\oplus m_0} 0001 = m_2 .$$

والمراحل الأخرى مشابهة، وبهذا نحصل على:

$$\begin{aligned}\left(m_0, m_1\right) &\mapsto \left(0111,1100\right) \mapsto \left(1100,0001\right) \mapsto \left(0001,1101\right) \\ &\mapsto \left(1101,0011\right) = \left(m_3, m_4\right) = F\left(m\right)\end{aligned}$$

سنوضح كسر النظام باختيار النص الواضح والحصول على $k\left(q\right)$ للحالة $q = 10$.

(١) نريد اختيار $m=(m_0,m_1)$ حيث $m_1^*=q$ بحيث تختلف مخرجات S_0 و S_1 عند التأثير على نصفي الرسالة m. فإذا اخترنا $m=(0111,1100)$ فنجد أن $F(m)=(1101,\underline{0011})$.

(٢) الجدول التالي يوضح مرحلة تعمية لقيم $\widetilde{T}$، قيمة لكل تخمين $\tilde{k}$ للمفتاح $k(q)$. كما يوضح الجدول القيم $F(\widetilde{T})$ المقابلة لكل خيار $\widetilde{T}$ للنص الواضح.

$\tilde{k}$	00	01	10	11
m_1	1100	1100	1100	1100
S_0S_1	1001	1001	1001	1001
$\tilde{k}$ تأثير	1001	1010	0101	0110
تبديل	1001	0101	1010	0110
$\oplus m_0$	1110	0010	1101	0001
$\tilde{T}$	(1100, 1110)	(1100, 0010)	(1100, 1101)	(1100, 0001)
$F(\tilde{T})$	(0000, 1011)	(1100, 0100)	(<u>0011</u>, 1000)	(<u>0011</u>, 1011)

(٣) سنعتبر أن $\widetilde{T}$ هو النص المطابق إذا تساوي نصف $F(\widetilde{T})$ الأيسر مع نصف $F(m)=(1101,0011)$ الأيمن. وبالنظر إلى الجدول نجد هذا يحدث لقيمتين هما $(0011,1000)$ و $(0011,1011)$. ومن ثم نحصل في هذه المرحلة على قيمتين محتملتين للمفتاح $k(q)$ هما $\tilde{k}=10$ و $\tilde{k}=11$.

يوضح لنا هذا المثال احتمال فشل هذا الهجوم في تحديد قيمة وحيدة للمفتاح. ومن الممكن تجريب نصوص واضحة أخرى. على سبيل المثال، إذا كانت $m=(0101,1100)$ فسنجد قيمة وحيدة $\tilde{k}=11$ على أنها القيمة الصحيحة للمقدار $k(10)$. ▲

تمارين

١٠,٣,١ إذا كانت $c=(m_{r+1},m_r)=(1111,0100)$ هي مُخرج التعمية في المثال التوضيحي فجد الرسالة المقابلة m.

١٠,٣,٢ استخدم خطوات المثال التوضيحي لإيجاد $k(00)$.

(١٠,٣,٣) لتكن $f_1, f_2 : \{0,1\}^4 \to \{0,1\}^4$ دالتين معرفتين على النحو التالي :

$$f_1(x_1, x_2, x_3, x_4) = (x_2 \oplus x_4, 1, x_1 x_2, 1 \oplus x_3)$$
$$f_2(x_1, x_2, x_3, x_4) = (1, x_1 \oplus x_3, x_4, x_2)$$

لنفرض أن F نظام فيستل توضيحي معرف على النحو التالي :

- $n = 4$ (ومن ثم فطول الرسالة هو $2n = 8$ مرتبة)، عدد المراحل هو $r = 2$.
- مفتاح F هو زوج (k_1, k_2) من المراتب الثنائية.
- نستخدم الدالة f_{k_i} في المرحلة $i \in \{1,2\}$.

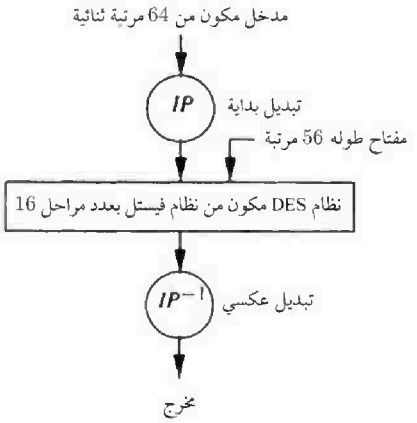
لنفرض أن c هو النص المعمى المقابل للنص الواضح m حيث مفتاح التعمية هو $(0,1)$. إذا كان :

$$c = m_{r+1} m_r = 10101011$$

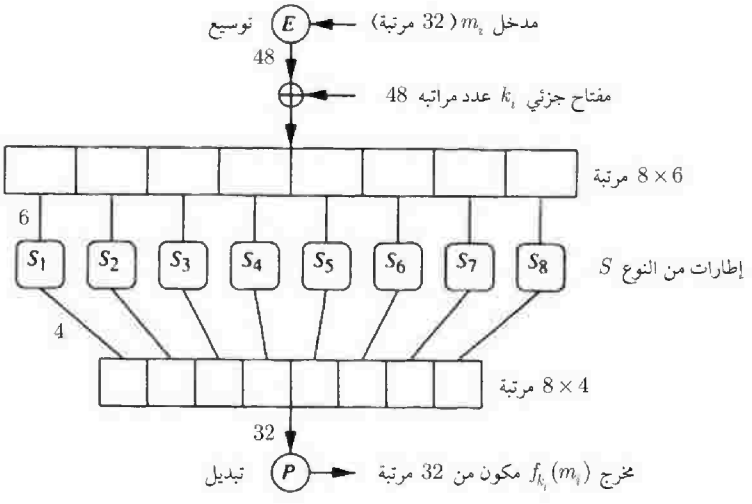
فجد النص الواضح m.

(١٠,٣,٢) نظام تعمية البيانات القياسي

بعد إعلان المعهد الوطني للقياس والتقنية NIST (National Institute of Standard and Technology) في العام ١٩٧٣م عن حاجته إلى نظام تعمية ليكون النظام الوطني القياسي قامت شركة IBM بالتعاون مع وكالة الأمن القومي (National Security Agency) بتطوير نظام يعتمد على نظام فيستل واعتمد النظام الجديد ليصبح نظام تعمية البيانات القياسي أو اختصاراً DES وكان ذلك في العام ١٩٧٧م. يستند نظام DES على نظام فيستل مكون من 16 مرحلة وطول المدخل يساوي 64 مرتبة ثنائية. يولِّد جدول المفاتيح مفاتيح جزئية k_i طول كل منها 48 مرتبة ثنائية في كل مرحلة من مفتاح معطى k طوله 56 مرتبة ثنائية. يُثَبِّت النظام ثمانية دوال إطار من النوع S وهي دوال أساسية لأمن النظام ومبينة في الشكل (١٠,٤).



(أ) هيكلية DES



(ب) دالة فيستيل الداخلية

الشكل (١٠,٤). مخطط نظام تعمية البيانات القياسي.

أحدث ظهور نظام DES في العام ١٩٧٧م تطوراً مهماً في علم التعمية حيث أصبح من أوسع أنظمة التعمية ذات المفتاح المتماثل استخداماً. وحصل بعض اللغط حول الاصطلاح "القياسي" وأحد أسباب هذا اللغط هو بقاء بعض أجزاء التصميم

سرية مما قاد البعض إلى الاعتقاد بوجود دالة ذات باب سري (trapdoor function) تتيح لوكالة NSA من كشف الرسائل المعماة.

واجهت سعة فضاء المفاتيح العديد من العقبات خلال فترة استخدامه حيث إن خطة التعمية معلنة ومن ثم فأمن النظام يعتمد تماماً على المفتاح. طول المفتاح هو 64 مرتبة ثنائية منها ثمان مراتب مخصصة لاختبار النوعية مما يجعل الطول المؤثر للمفتاح 56 مرتبة ثنائية وحذر بعض الأكاديميين من احتمال كسر النظام من قبل محلل تعمية عنيد وبحوزته حاسبات آلية سريعة بطريقة استنفاد المفاتيح.

اقترح ديفي وهيلمان (Diffie and Hellman) في العام ١٩٧٧م تصميماً لآلة تستطيع كسر نظام DES بطريقة الاستنفاد بيوم كامل كلفتها 20 مليون دولار أمريكي (انظر [28]). وقدم مايكل واينر (Michael Wiener) في العام ١٩٩٣م تفاصيل تصميم آلة بإمكانها استنفاد فضاء المفاتيح بسبع ساعات وكلفتها مليون دولار أمريكي (انظر [93]) وتم تصميم نموذجاً آخر لهذه الآلة في العام ١٩٩٧م بإمكانها استنفاد فضاء المفاتيح بحوالي ساعة من الزمن (انظر [94]).

في شهر يناير من العام ١٩٩٧م أعلنت شركة RSA لأمن البيانات عن جائزة مقدارها عشرة آلاف دولار أمريكي لمن يتمكن من إيجاد مفتاح DES باستنفاد المفاتيح باختيار ثلاثة أزواج من النصوص الواضحة. وفي شهر يونيو من العام ١٩٩٧م (بعد خمسة أشهر) تمكنت مجموعة تدعى DES-CHALL من الحصول على الجائزة بالاستعانة بشبكة كبيرة من الحاسبات المرتبطة بالإنترنت. احتاج هذا الجهد الجماعي إلى 96 يوماً وسبعون ألف حاسب، واحتاج اكتشاف المفتاح إلى استنفاد حوالي 25% من فضاء المفاتيح. وفي العام ١٩٩٨م تم كسر النظام بأسلوب مماثل ولكن بزمن 40 يوماً واستنفاد 88% من فضاء المفاتيح. وقبل انتهاء هذا التحدي سجلت مجموعة رقم قياسي وهو استنفاد $34 \cdot 109$ مفتاحاً في كل ثانية بواسطة حوالي 1400 فريقاً.

استطاعت المؤسسة الرائدة للإلكترونيات (EFF) من الحصول على جائزة تحدي DES حيث استغرق إيجاد المفتاح إلى 56 ساعة من البحث باستخدام آلة مصممة لهذا الغرض بكلفة 200 ألف دولار وفي العام ١٩٩٩م تضافرت جهود مؤسسة EFF ومؤسسة الشبكة للتوزيع من كسر تحدي DES بزمن يساوي 22 ساعة واستنفاد 245×10^9 مفتاحاً في كل ثانية. راجت شائعات عن تعمد حكومة الولايات المتحدة الأمريكية من المبالغة في تكاليف هذه الآلة والاستخفاف من قدرة كسر النظام باختيار النص الواضح لغرض حماية مصالح أخرى. وكما علق ديفي بعد نشر التفاصيل الكاملة للبرامج الإلكترونية والتصميم لآلة كسر النظام الذي اكتشفها (انظر [34]) بقوله "إن السؤال لا يقتصر فقط على اكتشاف مفتاح DES بطريقة الاستنفاد؛ لأنه يجب الأخذ بعين الاعتبار كلفة ذلك والغرض من ذلك". إن إمكانية كسر نظام DES باستنفاد المفاتيح طريقة غير فعالة ويمكن الحصول على طريقة استنفاد فعالة إذا كان بحوزة محلل التعمية معلومات جزئية إضافية مثل البناء المستخدم أو بعض المعلومات عن النص الواضح.

من الممكن استخدام عمليات تعمية مضاعفة (سنناقش ذلك لاحقاً)؛ إضافة إلى DES وذلك لتحسين أمن النظام بطريقة الاستنفاد ولكن ذلك يكون على حساب سرعة التعمية (انظر التمرين (**١٠,٣,٥**)) ومع ذلك فنظام DES يعد من الأنظمة المحصنة حيث علق ديفي في رسالة إلى مؤسسة EFF (انظر [34]) بالقول "إن أي جدل مهما كان مقنعاً حول عدم أمن نظام DES لن يحد من الاستثمار الواسع في أدوات DES حول العالم وسيستمر العالم باستخدام نظام DES مهما كانت عيوبه لقناعتهم بملاءمته لاحتياجاتهم".

البديل المحتمل لنظام DES هو نظام التعمية القياسي المتقدم أو اختصاراً AES (Advanced Encryption Standard) حيث قدمت خوارزمية تعمية لهذا النظام في العام ٢٠٠٠م. يحاول هذا النظام تجنب نقاط ضعف نظام DES؛ وذلك بتحصنه عن محاولات

كسره باستنفاد المفاتيح. اقترح بعض علماء التعمية المشهورين (انظر [9]). إن استخدام مفتاح طوله 75 مرتبة ثنائية سيجعل النظام المستخدم آمناً للعام ١٩٩٦م وأن استخدام مفتاح طوله 90 مرتبة ثنائية سيضمن أمن النظام للعشرين سنة القادمة مع ملاحظة أن "تكلفة تعمية قوية لا تزيد كثيراً عن تكلفة تعمية ضعيفة".

التعمية المتكررة

من الممكن تنفيذ عملية التعمية عدداً من المرات في أنظمة التعمية القالبية مثل نظام DES بهدف الحصول على فضاء مفاتيح ذي سعة كبيرة. على سبيل المثال، تتم عملية التعمية المضاعفة على النحو التالي:

$$E\left(M\right) = E_{k_2}E_{k_1}\left(m\right)$$ حيث k_1 و k_2 مفتاحان.

ليس بالضرورة أن تعزز عملية التعمية المضاعفة من أمن النظام، وأحيانا لا تزيد حتى من طول المفتاح الفعال. إذا كان نظام التعمية مغلقاً تحت عملية التحصيل، أي إذا وجد $k_3 \in \mathcal{K}$ بحيث يكون $E_{k_2}E_{k_1} = E_{k_3}$ لكل $k_1, k_2 \in \mathcal{K}$ فلا يكون للتعمية المضاعفة أي تأثير على أمن النظام. على سبيل المثال، نظام التعويض البسيط حيث فضاء المفاتيح هو جميع التبديلات k على هجائية (انظر المثال (٢،٢،١٠)) مغلق تحت عملية التحصيل حيث $k_3 = k_2 \circ k_1$.

إذا كان k مفتاحاً لنظام DES فيكون DES_k تبديلاً على الهجائية $\{0,1\}^{64}$. ويحتوي فضاء المفاتيح على عدد من التبديلات لا يزيد عن 2^{56} (من مجموعة تبديلات عددها $2^{64}!$). وهذه المفاتيح (التبديلات) ليست مغلقة تحت عملية التحصيل ولهذا يستخدم النظام عمليات تعمية متعددة على أمل حمايته من الكسر بطريقة استنفاد المفاتيح.

في حالة عملية التعمية المضاعفة يكون على محلل التعمية (العدو) تجريب عدد من المفاتيح يساوي $\left(2^{56}\right)^2 = 2^{112}$. ومع ذلك فالنظام غير آمن بطريقة كسر تدعى طريقة الالتقاء بالمنتصف (meet-in-the-middle attack) حيث يكون على محلل التعمية

تجريب عدد من المفاتيح يساوي 2^{57} ولكن ذلك يأتي على حساب تخزين 2^{56} من المفاتيح. إذا كان لدى محلل التعمية زوج واحد (m,c) على الأقل حيث $c = \mathrm{DES}_{k_2}\mathrm{DES}_{k_1}(m)$ فيستطيع معرفة المفتاحين k_1 و k_2 باتباع ما يلي:

(١) يقوم بعمل جدول للقيم $\big(i, \mathrm{DES}_i(m)\big)$ لجميع المفاتيح i.

(٢) لكل مفتاح محتمل j يبحث فيما إذا كان $\mathrm{DES}_j^{-1}(c)$ أحد عناصر القائمة. فإذا كان كذلك، فيوجد i حيث $\mathrm{DES}_j^{-1}(c) = \mathrm{DES}_i(m)$. وبهذا يكون $c = \mathrm{DES}_j \circ \mathrm{DES}_i(m)$. ومن ثم يجد أن $(i,j) = (k_1,k_2)$ هو أحد الخيارات المحتملة للقيمتين k_1 و k_2. وإذا توفر أزواج إضافية من النص الواضح وما يقابله من النص المعمى فبإمكان محلل التعمية استخدامها ليتخلص من التطابقات غير المنطقية. إذا كان بحوزة محلل التعمية زوجين من النصوص فيستطيع أن يكسر النظام.

يستخدم نظام DES عند التطبيق العملي له عمليات تعمية ثلاثية بفضاء مفاتيح سعته $\left(2^{56}\right)^3 = 2^{168}$ ودالة تعمية:

$$E(m) = E_{k_3}E_{k_2}E_{k_1}(m)$$

حيث $k_1, k_2, k_3 \in \mathcal{K}$ و $E_{k_i} = \mathrm{DES}_{k_i}$ أو $E_{k_i} = \mathrm{DES}_{k_i}^{-1}$.

كما يستخدم أحياناً حالة خاصة من عمليات التعمية الثلاثية (يستخدم مفتاحين) يكون فيها:

$$E_{k_2} = \mathrm{DES}_{k_2}^{-1} \quad \text{و} \quad k_3 = k_1.$$

لاحظ أنه لو كان $k_2 = k_1$ لحصلنا على DES. إن عمليات التعمية الثلاثية تضمن أمن النظام ضد محاولة كسره بطريقة الالتقاء بالمنتصف حيث يحتاج لتجريب عدد 2^{112} من المفاتيح. ولكن من الممكن كسر الحالة الخاصة (استخدام مفتاحين) إذا استخدم محلل التعمية عدداً أكبر من النصوص الواضحة أو عمليات التعمية (انظر [63]).

أشكال العمليات

تقوم الأنظمة القالبية في الغالب بتقسيم النص الواضح إلى أجزاء (عادة تكون بنفس طول القالب) ثم يتم تعمية كل جزء على حدة. نستخدم نظام DES في الأمثلة التوضيحية مع التأكيد على أن هذه الطرق تصلح لجميع الأنظمة القالبية.

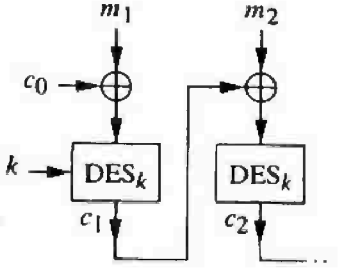
لنفرض أن $m = m_1 m_2 \ldots$ رسالة حيث m_i قالب (طوله 64 مرتبة في نظام DES). يقوم كتاب التعمية الإلكتروني (electronic codebook) أو اختصاراً ECB بتطبيق عملية DES على كل من هذه القوالب ليحصل على $c_i = \mathrm{DES}_k(m_i)$. ميزات هذه الطريقة هي سهولة تنفيذها وإذا حصل أخطاء في بعض مراتب قالب أثناء عملية التعمية فيبقى تأثير ذلك في القالب نفسه عند كشف المعمى. وأما العيب في هذه الطريقة هو أن النصوص الواضحة المتطابقة تعمى إلى نص معمى واحد وينتج عن ذلك تسريب بعض المعلومات لمحلل التعمية.

أما طريقة تعمية سلسلة قوالب (cipher-block chaining) أو اختصاراً CBC فتتم باختيار قالب بدائي c_0 وعملية التعمية تكون:

$$c_i = \mathrm{DES}_k(m_i \oplus c_{i-1}) \quad \text{لكل} \quad i \geq 1$$

وعملية كشف المعمى هي:

$$m_i = \mathrm{DES}_k^{-1}(c_i) \oplus c_{i-1}.$$



تعمية سلسة قوالب

يتم اختيار القالب الأول من النص المعمى عشوائياً للحيلولة دون الحصول على النص المعمى نفسه للنصوص الواضحة المتطابقة. وتختلف هذه الطريقة عن ECB بوجود سلسلة جزئية من سلسلة تعتمد حدودها على الحدود السابقة حيث c_j يعتمد على c_{j-1} (وهذا بدوره يعتمد على جميع القوالب السابقة).

وكما رأينا فالأخطاء التي تحدث في النص المعمى c تؤثر فقط في قوالب كشف المعمى المقابلة للقوالب الذي حدثت في الأخطاء عند استخدامنا تعمية ECB، في حين CBC تقوم بنشر الخطأ في القالب c_j بحيث يمنع الحصول على كل من m_j و m_{j+1}. في الحقيقة، إذا حاول العدو التغيير في القالب c_j فإن ذلك يحدث أخطاء في مراتب m_{j+1} (انظر التمرين (٤,٣,١٠)).

تطبيقات على مطابقة الهوية

يمكن استخدام الأنظمة المتماثلة المفاتيح للحصول على تطابق الهوية (authentication). نقدم مثالين على هذه التطبيقات، أولهما، استخدام تعمية سلسلة القوالب (CBC) لتطابق هوية الرسالة وأما المثال الثاني فيستخدم خطة لكلمة سر (password) تعتمد على نظام DES لتطابق الهوية الشخصية (identification) وممكن أن يكون الفرق بين التطابقين غير واضح في معظم الأحيان، إلا أن تطابق هوية الرسالة تكون مهمته معرفة الرسالة الحقيقية وليس فقط معرفة الهوية.

مطابقة هوية الرسالة

لنفرض أن بوب (Bob) وأليس (Alice) يتبادلان رسائل عبر قناة اتصال غير آمنة (مثلاً، البريد الالكتروني). عند استلام بوب لرسالة مفترض أن تكون مرسلة من أليس يتوجب عليه أن يقتنع أن هذه الرسالة فعلا مرسلة من قبل أليس. يوجد على الأقل طريقتان لاعتراض الرسالة هما انتحال الشخصية أو التغيير في محتوى الرسالة (تزوير الرسالة).

إحدى الخيارات المتاحة للتحقق من هوية الرسالة هي استخدام خطة تعمية لنظام متماثل المفاتيح مثل DES ويتم ذلك على النحو التالي: يتفق كل من بوب وأليس على مفتاح سري مشترك، تقوم أليس باستخدام هذا المفتاح لتعمية الرسالة m وترسل $c = E_k(m)$ إلى بوب. يقوم بوب بكشف تعمية c باستخدام المفتاح المشترك ويقبل الرسالة إذا "اعتقد أن محتوى الرسالة معقول". ولمنع العدو من التلاعب في محتوى الرسالة بحيث يرسل إلى بوب رسائل بديلة، تقوم أليس بتذييل الرسالة m بمعلومات زائدة مثل الزمن أو أي متتالية من المعلومات الزائدة قبل تعميتها. فإذا كان من الصعب استخدام عملية التعمية بحيث يكون لكشف المعمى معنى مقبول دون معرفة المفتاح السري فنكون قد ضمنا مستوى ملائم لإعاقة العدو من تزييف محتوى الرسالة. ولكن بعض أنظمة التعمية تسمح ببعض التغييرات المختارة دون التمكن من كشف هذه التغييرات، على سبيل المثال، إذا استخدم ECB لتعمية قوالب من الرسائل فهناك احتمال أن يتمكن العدو من إعادة ترتيب أو تعويض أو حتى حذف بعض قوالب النص المعمى. أما نظام اللفافة الواحدة فيتيح للعدو تغيير بعض المراتب، وذلك بتغيير المراتب المقابلة لها في النص المعمى.

من الممكن استخدام خطط أقوى باستخدام نظام CBC ويتم ذلك باختيار نظام تعمية قالبي E وكتابة الرسالة $m = m_1 m_2 \dots m_t$ حيث طول m_i يساوي سعة النظام القالبي (إذا كان $E = \text{DES}$ فطول القوالب يساوي 64 مرتبة). نقوم الآن باستخدام CBC لحساب:

$$c_i = E_k(m_i \oplus c_{i-1}) \quad \text{لكل} \quad 1 \le i \le t.$$

بعد ذلك، ترسل أليس الرسالة m و c_t الذي يدعى شفرة مطابقة هوية الرسالة (message authentication code) أو اختصار BAC. يقوم الآن بوب بحساب CBC-MAC (بالطريقة نفسها التي حسبت بها أليس) ويقبل الرسالة على أنها المرسلة من أليس إذا

تساوت هذه القيمة مع قيمة MAC المستقبلة. ولمنع كسر النظام باستنفاد المفاتيح، يستخدم مفتاحاً آخر k' ويتم تعمية القالب الأخير باستخدام عملية تعمية ثلاثية باستخدام مفتاحين بحيث ترسل أليس $E_k E_{k'}^{-1}(c_t)$ عوضاً c_t وهذه تكون قيمة MAC.

مطابقة الهوية الشخصية

تعتمد خطة كلمة السر على معلومات سرية بين المستخدم ونظام الاتصال ولا يمكن الدخول إلى النظام إلا إذا قدم المستخدم السر المشترك للنظام. نقدم هنا آلية عمل كلمة السر المستخدمة في معظم أنظمة يونكس (Unix) للحاسبات. لكي تستطيع الدخول إلى النظام يتوجب عليك تقديم زوج من المعلومات هما هوية المستخدم وكلمة السر وبعد أن يتأكد النظام بواسطة معلومات مخزنة مسبقاً أن كلمة السر تقابل هوية المستخدم عندئذ، يسمح لك بالدخول إلى النظام.

تستخدم كلمة السر التي لا يزيد طولها عن 8 رموز في تكوين مفتاح k لدالة تعمية معدلة لنظام DES. كل من الرموز تساهم بعدد 7 من مراتب المفتاح التي عددها 56. يضاف مراتب صفرية إذا كان طول كلمة السر أصغر من 8 رموز. يضاف 12 مرتبة أخرى (تسمى الملح) تؤخذ من ساعة النظام في لحظة تكوين كلمة السر يكون الغرض منها تعديل نشر E في الشكل (١٠,٤) حيث يتم تحديد واحدة من التغييرات التي عددها $2^{12} = 4096$. يقوم النظام بحساب $m_i = \mathrm{DES}_k^*(m_{i-1})$ لكل $1 \le i \le 25$ حيث DES* يرمز لنظام DES المعدل و m_0 كلمة صفرية طولها 64 مرتبة. يتم تخزين كلمة الملح التي طولها 12 مرتبة والكلمة m_{25} التي طولها 64 مرتبة (تسمى كلمة السر المموهة) على النظام، عادة في الملف (/etc/passwd). وعند تقديم هوية المستخدم وكلمة السر يقوم النظام بإجراء الحسابات نفسها ويسمح للمستخدم في الدخول إلى النظام إذا كانت الحسابات متفقة مع القيمة المخزنة.

تدعى هذه الحسابات، خوارزمية تعمية كلمة السر باستخدام يونكس. يستطيع العدو الذي بحوزته مدخل من الملف (/etc/passwd) من محاولة كسر النظام بطريقة اختيار النص الواضح. وعلى الرغم من صعوبة كسر النظام باستنفاد المفاتيح فمن الممكن كسر النظام باستخدام قاموس لكلمات السر المعروف أنها مفضلة لدى المستخدمين. ولكن إضافة مراتب الملح تجعل كسر النظام باستخدام قاموس كلمات السر أكثر صعوبة لوجود 4096 خياراً لكل كلمة من كلمات السر. كما تساعد إضافة مراتب الملح على عدم السماح باستخدام تصميم غير قانوني لآلة نظام DES لكسر كلمة السر.

غالباً ما يكون باستطاعة العدو الحصول على الملف (/etc/passwd) نفسه (في عديدٍ من الأنظمة يستطيع جميع المستخدمين من قراءة هذا الملف)، ومن ثم يحاول كسر النظام بطرق مختلفة. إن معرفة بعض كلمات السر هو تهديد لا يستهان به حتى مع الأعداء الذين يستخدمون أجهزة ذات قدرة حسابية محدودة[٩]. أجبر هذا الهجوم مستخدمي هذه الأنظمة إلى اختيار كلمات سر أفضل لمحاولة تحصين النظام من مثل هذا النوع من الهجوم وقاموا أيضاً بنقل كلمة السر المموهة إلى ملف منفصل تستلزم قراءته بعض المعلومات الإضافية.

تعدُّ خطة كلمة السر من الأمثلة على تطابق الهوية الضعيفة حيث لا يكون المستَخدِم على إطلاع مفصل عن هوية النظام المستخدَم، فإذا كانت القناة غير آمنة فمن الممكن انتحال العدو شخصية النظام إضافة إلى التصنت على عملية التعمية. نقدم في الفصل الثاني عشر المزيد عن تطابق الهوية.

---

(٩) استطاع كل من فيلدمير وكارن (Feldmeier and Karn) انظر [32] في العام ١٩٨٩م من استخدام قاموس كلمات السر لمعرفة 30% من كلمات سر نظام معطى حيث قدما خوارزمية كشف معمى سريعة في هذا الهجوم واستطاعا معرفة كلمات السر المموهة.

تمارين

(١٠,٣,٤) (أخطاء في النص المعمى لنظام DES) لنفرض أنه تمت تعمية t من قوالب النص الواضح $m_1, m_2, \ldots, m_t$ باستخدام نظام DES ونتج عن ذلك قوالب النصوص المعماة $c_1, c_2, \ldots c_t$ على التوالي.

(أ) لنفرض أنه تم إرسال نص معمى واحد يحتوي على أخطاء وليكن c_j. اشرح باختصار الطريقة التي يمكن إتباعها لتحديد عدد ومواقع القوالب التي يحتوي النص الواضح لها على أخطاء لكل من النظامين ECB و CBC.

(ب) لنفرض أن النظام المستخدم هو CBC ولنفرض أن العدو بدل موقعي القالبين c_3 و c_6. ماهو عدد قوالب النص الواضح التي تحتوي على أخطاء؟

(ج) بين كيف يمكن للعدو أن يُحدث أخطاء في بعض مراتب m_{j+1} بالتلاعب بالقالب c_j إذا كان النظام المستخدم هو CBC.

(١٠,٣,٥) تقترح هذه المسألة طريقة لحماية DES ضد محاولة كسره بطريقة استنفاد المفاتيح. المفتاح هو $k = (k_1, k_2)$ حيث $k_1 \in \{0,1\}^{56}$ و $k_2 \in \{0,1\}^{64}$. لنفرض أن $m \in \{0,1\}^{64}$ نص واضح.

(أ) أثبت أن استخدام الدالة $E_k(m) = \mathrm{DES}_{k_1}(m) \oplus k_2$ لا يزيد من أمن النظام عند محاولة كسره باستنفاد المفاتيح. أي بين كيفية كسر النظام باستخدام 2^{56} من عمليات DES. يمكن أن تفترض أن لديك عدداً معقولاً من الأزواج $(m_i, c_i = E_k(m_i))$.

(ب) هل يزيد استخدام دالة التعمية $E_k(m) = \mathrm{DES}_{k_1}(m \oplus k_2)$ من أمن النظام باستنفاد المفاتيح؟

اقترح رايسفت (Rivest) في مقالة المنشور في مجلة "CRYPTO, 96 [49]" التمديد DESX لنظام DES حيث $k = (k_1, k_2, k_3)$ ودالة التعمية هي:

$$E_k(m) = k_3 \oplus \mathrm{DES}_{k_1}(m \oplus k_2).$$

إضافة إلى أدوات DES المعروفة يسمح أيضا باستخدام العملية " XOR pre-and post" الرخيصة التكاليف.

(١٠,٣,٦) لنفرض أن حواء (العدو) حصلت على ثلاثة أزواج (m_1, c_1) ، (m_2, c_2) ، (m_3, c_3) حيث استخدمت أليس لتعميتهم نظام DES ثلاثي ودالة تعمية هي:

$$E(m) = \mathrm{DES}_{k_3}\mathrm{DES}_{k_2}\mathrm{DES}_{k_1}(m)$$

صمم هجوم اللقاء بالمنتصف لمعرفة مفتاح أليس (k_1, k_2, k_3) بعدد من العمليات يساوي تقريباً 2^{112}.

(١٠,٣,٧) (خاصية التتميم لنظام DES). لنفرض أن $\overline{m}$ هي متممة m (مرتبة مرتبة). إذا كان $c = \mathrm{DES}_k(m)$ فمن السهل أن نرى أن $\bar{c} = \mathrm{DES}_k(\overline{m})$ (يمكن رؤية ذلك بالنظر إلى خطوات خوارزمية تعمية DES). هل من الممكن استخدام هذه الخاصية لتقليل الزمن اللازم لكسر النظام باستنفاد المفاتيح بطريقة معرفة النص الواضح؟ ماذا لو كانت الطريقة المستخدمة هي اختيار النص الواضح؟

(١٠,٣,٨) يقدم نظام CBC-MAC طريقة للتحقق من أمانة (صواب) المعلومات ولكنه لا يحافظ على سريتها. الاقتراح التالي يضيف المحافظة على السرية. نقوم بتذييل الرسالة $m = m_1 m_2 \dots m_t$ بـ MAC لنحصل على $m' = m m_{t+1}$. عندئذ يستخدم نظام CBC (باستخدام نفس المفتاح والقالب البدائي c_0) لتعمية m' لنحصل على النص المعمى $c_1, c_2, \dots, c_{t+1}$ حيث

$(c_i = E_k(m_i \oplus c_{i-1})$ لكل $1 \le i \le t+1$ وحيث أول t من الحسابات مماثلة لتلك المستخدمة للحصول على MAC. وبهذا نحصل على النص المعمى مباشرة من الحسابات التي أجريت للحصول على MAC. أثبت أن هذه الخطة تؤدي إلى قالب نص معمى أخير $c_{t+1} = E_k(m_{t+1} \oplus c_t)$ لا يعتمد على النص الواضح ولا على النص المعمى. اشرح لماذا تؤدي هذه الإضافة في التعمية إلى خطر على أمن مطابقة الهوية ثم بين كيف يتمكن العدو من الاستفادة من هذا الضعف.

(١٠,٤) حواشي
Notes

الجملة الأولى في بداية هذا الفصل مأخوذة من كتاب رايسفت [71] الشيق "مقدمة في علم التعمية". يحتوي كتاب سايمنز (Simmons [81]) على إسهامات العديد من المؤلفين بما في ذلك إسهامات ديفي (Diffie [26]) "السنوات العشر الأولى للتعمية ذات المفتاح المعلن". ننصح بقراءة كتاب التعمية التطبيقية لمؤلفيه مينيزز، أورشت، فانستون (Menezes, van Oorshot, Vanstone [63]) لتغطيته المادة العلمية بشكل عميق ومنظم.

كتاب كاسر الشفرات لمؤلفه خان (Kahn) يحتوي على أدبيات التعمية غير التقنية لما قبل العام ١٩٦٧م، كما تضم الطبعة الثانية من الكتاب الذي صدر في العام ١٩٩٦م على بعض الإضافات عن تطور التعمية. يناقش غارفانكل (Garfinkel [37]) بعض الجوانب السياسية والقانونية والخصوصية ومسألة اتخاذ القرارات المتعلقة بالتعمية علاوة على تاريخ التطبيق "خصوصية جيدة وبارعة ((Pretty Good Privacy (PGP))". أما كتابي ستنسون وكوبلتز (Stinson [86] and Koblitz [50]) فهما المكان الطبيعي لدراسة موسعة للمادة التي قدمناها في هذا الفصل.

يمكن الاطلاع على كمية هائلة من المعلومات عن المشروع (VENONA) الذي تبنته وكالة الأمن القومي على البوابة الإلكترونية :

http://www.nsa.gov

تبدأ المقدمة التاريخية بالفقرة التالية :

"بدأت في الأول من فبراير عام ١٩٤٣م خدمات مخابرات الإشارة التابعة للجيش الأمريكي وهو الاسم السابق لوكالة الأمن القومي برنامجاً سرياً صغيراً أطلقت عليه اسم حركي هو VENONA. كان الهدف الرئيسي لبرنامج VENONA هو متابعة وربما كسر أنظمة الاتصالات الدبلوماسية المعماة للاتحاد السوفيتي. بدأ تجميع هذه الرسائل من قبل خدمات مخابرات الإشارة (سميت لاحقاً وكالة الأمن القومي ويطلق عليها الاسم الشائع "ارلنغتون هول" نسبة إلى مكتبها الرئيسي في ولاية فرجينيا) منذ العام ١٩٣٩م ولكن لم يتم التحقق منها قبل ذلك. عينت المدرسة الشابة الآنسة جين غرابيل (Gene Grabeel) مسؤولة عن هذا المشروع."

الوصف المقدم لنظام البيانات الجديد المحكم (NDS) مأخوذاً من بيكر وبايبر (Berker and Piper [3]). ويمكن إيجاد تفاصيل نظام DES في المراجع [3, 86, 63]. من الممكن الرجوع إلى المقالات في سلسلة أعداد مجلة IEEE الذي بدأها [87] للاطلاع على الجدال حول أمن نظام DES. يمكن إيجاد بعض تصميمات الإطار S في المراجع [23]، [86]، [76]. البوابة الإلكترونية :

http://www.rsa.com

تحتوي على معلومات عن التحدي الذي أطلقته مجموعة RSA لكسر النظام DES. أما محاولات كسر نظام DES فمن الممكن الاطلاع عليها على بوابة المؤسسة غير الربحية EFF :

http://www.eff.org

تم تبني استخدام DES CBS كنظام قياسي من قبل المنظمة العالمية للقياس (ISO 9797) والمعهد القومي الأمريكي للقياس (ANSI X9.9) لأغراض تطابق الهوية [63]

حيث أن استخدام ANSI X9.9 منتشراً بين البنوك وفي التعاملات المالية. تمت الموافقة على استخدام نظام DES الثلاثي من قبل ANSI في نوفمبر من العام ١٩٩٨م واعتمد نظاماً قياسياً (ANSI X9.52). وفي العام ١٩٩٩م بدأ المعهد القومي للقياس والتقنية (NIST) بإجراء التحضيرات لتبني نظام DES الثلاثي كنظام التعمية القياسي للمعلومات التابع للحكومة الفدرالية للولايات المتحدة الأمريكية (FIBS 46-3) انظر:

http://csrc.nist.gov/cryptval

ومن ضمن ما جاء بوثيقة الإعلان عن ذلك:

"بالإضافة إلى ذلك ولمعرفتنا أن ضمان أمن نظام DES يقترب من نهايته فقد تم التعاون بين NIST وقطاع الصناعة من جهة وبينهما وبين العاملين في قطاع علم التعمية لتطوير نظام تعمية قياسي متقدم (AES) يخدم القرن الواحد وعشرين. وقد بدأ هذا المشروع قيد التنفيذ في الثاني من يناير عام ١٩٩٧م (62 FR 93) حيث ينوي هذا المشروع إلى جعل خوارزمية التعمية لنظام AES غير سرية ومعلنة للعامة ولها القدرة على حماية ملفات الحكومة السرية إلى بداية القرن القادم. وبما أن خوارزمية تعمية أي نظام تحتاج لبعض الوقت للتأكد من قدرتها فلا بد من أخذ الوقت الكافي قبل طرح AES واعتباره نظام آمن من قبل FIBS. يمكن الحصول على معلومات عن الجهد المبذول من قبل NIST لتطوير AES على البوابة الإلكترونية":

http://www.nist.gov/aes

منذ فترة قصيرة تم تصميم آلة خاصة لكسر نظام DES وبناء على ذلك فقد تخلت NIST عن استخدام نظام DES للعديد من التطبيقات. وكما هو الحال مع أدوات الأمن الأخرى فالتعمية يجب أن توازن بين التكلفة وخطر كسر النظام. منذ فترة قصيرة تم بناء آلة كسر بكلفة 250000 دولار أمريكي واستطاعت معرفة مفتاح رسالة واحدة بحوالي 56 ساعة وذلك بإتباع طريقة الاستنفاد. ومن المتوقع أن يكون الزمن اللازم لكسر رسالة باستخدام مثل هذه التقنية الخاصة ضعف الزمن السابق؛ لأنه تم كسر النظام بالزمن السابق باستنفاد ربع المفاتيح فقط. في بعض التطبيقات لا يسبب مثل هذا

الكسر خطراً مباشراً، وخاصة عندما يحتاج المستخدم الحفاظ على سرية المعلومات لفترة زمنية قصيرة. ومن المتوقع مع التقدم في صناعة التقنية أن يتم كسر النظام بزمن أقل ولهذا توصي NIST بتبني المقترحات التالية:

- على الأنظمة المستخدمة تطوير استراتيجية انتقال حصيفة إلى نظام DES الثلاثي. يجب أن يكون لهذه الاستراتيجية القدرة على حماية المعلومات من الخطر المصاحب.
- عند بناء نظام جديد، استخدم نظام DES الثلاثي لحماية البيانات الحساسة ولكن غير السرية.

أخذت هذه الاقتراحات بعين الاعتبار عند الشروع في كتابة مسودة مشروع (FIPS 46-3) حيث تم اعتبار نظام DES الثلاثي كما هو مبين في (ANSI X9.52) على أنه الخوارزمية التي وافقت عليها FIPS.