الفصل –4 شفرات توثيق الرسائل ودوال النحت المقاومة للتصادم

4.1 الاتصال الخاص وسلامة الرسالة

ذكرنا في ما سبق كيف يمكن استخدام التشفير للحفاظ على **خصوصية الرسالة** message privacy المرسلة ، بحيث لايستطيع الخصم ان يعرف اي معلومة من النص المشفّر. لاتقتصر مخاوف الاطراف المتواصلة على خصوصية الرسالة المرسلة فحسب ، بل تشمل ايضا **سلامة الرسالة** message integrity. على سبيل المثال ، تصوّر ان سوبرماركت طلب عبر الاميل من المجهّز قائمة بشراء 10,000 علبة صودا. حين يستلم المجهز طلب الشراء يسأل نفسه سؤالين:

1. هل هذا الطلب موثّق ؟ بمعنى هل فعلا اصدر صاحب السوبرماركت الطلب ام تم اصدار الطلب من قبل خصم انتحل شخصية صاحب السوبرماركت.
2. اذا كان الطلب صادر من السوبرماركت فعلا ، عندها يسأل المجهّز فيما اذا كان محتوى الطلب يطابق ما ارسله السوبرماركت ام تم تغييره من قبل الخصم اثناء الارسال.

لاحظ ان طلب الشراء بحد ذاته ليس سريّا لذا لم يكن الاهتمام منصبّا حول خصوصيته. بدلا من ذلك ، المشكلة هي في كيفية التحقق من سلامة الطلب وهو مايعرف **بوثوقية الرسالة** message authentication. يمكن تعميم هذا المثال على الكثير من التطبيقات: كالشراء غير المحمي ، البريد الالكتروني ، وحتى الرسائل النصيّة.

في هذا الفصل ، سوف نرى كيفية استخدام تقنيات التشفير لمنع تغيير الرسائل المرسلة عبر خط اتصال مفتوح. في نهاية الفصل سوف نري كيفية اجراء التشفير الموثّق الذي يجمع بين الحفاظ على خصوصية وسلامة الرسالة معا.

4.2 توثيق الرسالة باستخدام التشفير

- يبدو للوهلة الأولى ان استخدام التشفير يمكن ان يحمي سلامة الرسالة ، وذلك لكون النص المشفّر يخفي محتوى الرسالة تماما. لذلك يبدو ان الخصم لايستطيع تغيير محتوى رسالة عشوائية.
- لكن هذا التصور خاطئ. فلو فرضنا ان الرسالة m تم تشفيرها بطريقة التشفير الانسابي ،

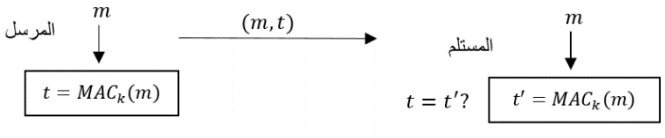
$$\mathrm{Enc}_k(m) = G(k) \oplus m$$ ، بمعنى ان

حيث G هو مولّد اعداد شبه عشوائية. هذه النصوص المشفّرة يمكن تغييرها بسهولة ، حيث ينتج قلب اي ثنائية من c الى استرجاع الرسالة m ولكن بثنائية مقلوبة. يعتبر هكذا تغيير عملا خطرا ، خصوصا اذا كانت الرسالة المرسلة هي قيم لتحويلات مالية او ثنائيات اعدادات لتطبيق معيّن.
- يكون تطبيق المهاجمة اعلاه على التشفير الكتلي اكثر صعوبة ، لكون قلب ثنائية واحدة قد يؤثر على محتوى كتلة كاملة بعد فك تشفيرها.
- لذا يلجأ الخصم الى اساليب اخرى تمنع اكتشاف التلاعب. نناقش هذه الاساليب على ضوء نمط التشفير المستخدم.
  - عند استخدام نمط ECB قد يقوم الخصم بتغيير ترتيب الكتل ، وهو يعتبر مهاجمة ناجحة غير مكتشفة.
  - تستخدم الانماط OFB ، CFB ، و CTR لتوليد سلسلة عشوائية ، لذا ينطبق عليها ماقلناه من مهاجمة التشفير الانسيابي.
  - اما في حالة النمط CBC فإن تغيير اي ثنائية في قيمة IV ستؤثر على تغيير ثنائية واحد فقط في اول كتلة.

نتيجة لفشل التشفير في حماية سلامة الرسالة ، فقد دعت الحاجة الى استخدام آليات جديدة ، تُعرف بشفّرات توثيق الرسائل ، لتمكّن الاطراف المتواصلة من معرفة فيما اذا كانت الرسائل المرسلة متلاعب بها ام لا.

4.3 شفرات توثيق الرسائل

تندرج **شفرات توثيق الرسائل** Message Authentication Codes (MAC) ضمن مجال التشفير بالمفتاح الخاص، لاعتمادها على مفتاح خاص k مشترك بين طرفين. الفكرة هي ان يقوم المرُسل باستخدام المفتاح الخاص k بحساب **شفرة توثيق** t، تعرف بـ MAC tag، للرسالة m التي يرغب بارسالها. ترسل هذه الشفرة مع الرسالة الى المستلم الذي بدوره يحسب شفرة توثيق t' للرسالة المستلمة.



شكل (4.1): فكرة استخدام MAC

يقبل المستلم الرسالة في حالة $t = t'$ فقط. تتطلب أمنية التوثيق انه لايوجد اي خصم يستطيع ان يولّد شفرة t لاي رسالة m' لم يتم ارسالها من قبل المرُسل، بحيث تؤدي الى قبول المستلم للرسالة. يوضّح الشكل (4.1) كيفية عمل شفرة التوثيق MAC.

تعريف(4.1)**:** تتكون **شفرة توثيق الرسالة** او MAC من ثلاث خوارزميات: Gen، Mac، و Vrfy.

1. تقوم خوارزمية Gen بتوليد المفتاح السري k، اعتماد على معامل الأمنية n.
2. تقوم خوارزمية Mac بتوليد قيمة Mag tag t من الرسالة m والمفتاح السري k، وتكتب بالصورة $\mathrm{Mac_k(m)}$.
3. تستلم خوارزمية Vrfy الرسالة m، المفتاح السري k، و قيمة t وتعطي اما 1 (بمعنى صالح) او 0 (بمعنى غير صالح). يمكن السماح ببعض الخطأ في عمل شفرة التوثيق بحيث يكون:

$$\Pr\left[\mathrm{Vrfy_k}\left(\mathrm{Mac_k(m)}\right) = 1\right] > 1 - \mathrm{negl}(\lambda)$$

أمنية شفرات توثيق الرسائل. فكرة أمنية شفرات توثيق الرسائل انه لايوجد خصم يستطيع ان يولّد شفرة MAC صحيحة لاي رسالة هو يزيّفها.

شفرات توثيق الرسالة و مهاجمة الاعادة Replay attack. افترض السيناريو التالي: ترسل المستخدمة Alice الى المصرف طلبا بتحويل مبلغ قدره 1000 دولار من حسابها الى حساب المستخدم Bob. تعتبر المستخدم Alice طرف شرعي وموثّق لدى المصرف. تطبّق Alice خوارزمية Mac على طلب التحويل، لذا يتأكد المصرف من هويتها. لايستطيع المستخدم Bob ان يغيّر محتوى الطلب لان ذلك يتطلب تزييف شفرة التوثيق وهذا متعذر كما ذكرنا. ولكن، لا شئ يمنع المستخدم Bob من اعادة ارسال الطلب عشر مرات الى المصرف. اذا قبل المصرف جميع الطلبات، سيتم تحويل مبلغ 10,000 دولار لحساب Bob بدلا من 1000 دولار. هذه المهاجمة تعرف بمهاجمة الاعادة replay attack ولاتستطيع MAC لوحدها ان تمنع هذه المهاجمة.

هناك تقنيتان لمنع مهاجمة الاعادة في المعاملات، هما:

- **الارقام المتسلسلة الفريدة** unique sequence numbers
- و **الاختام الزمنية** timestamps.

تتضمن تقنية الارقام المتسلسلة الفريدة عدم السماح لمعاملتين ان يكون لهما نفس الرقم. عند ذلك، يتم تطبيق MAC على الرسالة بالاضافة الى الرقم المتسلسل. يكون للختم الرقمي نفس التأثير، حيث يكون لكل معاملة ختم يعتمد على الوقت الحالي، وبالتالي لايسمح بقبول معاملتين لديهما نفس الختم.

4.3.1 تصميم شفرات توثيق الرسالة

يتم تصميم شفرة توثيق الرسالة بالاستعانة بالدوال شبه العشوائية pseudorandom function، التي تم ذكرها سابقا.

- يتم تطبيق الدالة شبه العشوائية على الرسالة m للحصول على الشفرة t. يتطلب تزييف قيمة t معرفة ادخال الدالة عن طريق اخراجها عندما يكون طول الاخراج n، تقدّر احتمالية نجاح هذه العملية 2^{-n}، وهي احتمالية ضئيلة جدا.
- ان استخدام الدوال شبه العشوائية يثير مشكلة تقنية، وذلك لكون تلك الدوال تتعامل مع مدخلات ثابتة الطول n. في حين يفترض بشفرات التوثيق ان تتعامل مع رسائل متغيرة الطول. سوف نبتدأ بتصميم شفرات MAC آمنة لرسائل ثابتة بطول n، وبعد ذلك نغيّر

Construction (4.1): Fixed length MAC

Assumption: let $F_k(.)$ be pseudorandom function of length n

Gen(n): on receiving security parameter, n, it chooses randomly $k \leftarrow \{0,1\}^n$.

Mac$_k$(m): on the message, $m \in \{0,1\}^n$ and the key $k \in \{0,1\}^n$ it computes $t = F_k(m)$.

Vrfy$_k$(m,t): on message $m \in \{0,1\}^n$, the key $k \in \{0,1\}^n$, and the tag, t, it output 1 if and only if $t = F_k(m)$, otherwise it output 0.

التصميم لرسائل متغيّرة الطول. يوضّح المنهج (4.1) كيفية تصميم شفرة MAC لرسالة ثابتة الطول.

- لاحظ ان أمنية المنهج (4.1) تعتمد على "افتراض" وجود دالة شبه عشوائية.
- يقدر المنهج (4.1) على التعامل مع رسائل ثابتة الطول فقط، وهو قصور غير مقبول في الكثير من التطبيقات. في هذا المقطع، سوف نوضّح كيفية تصميم شفرة MAC عامة من رسائل متغيّرة الطول. قبل عرض المنهج المقترح نقدّم بعض الحلول البسيطة التي قد تخطر على البال. جميع هذه الحلول تفترض تقسم الرسالة الى كتل وتطبيق $F_k(.)$ على كل كتلة.

1. تطبيق الدالة $F_k(.)$ على الكتلة الأولى فقط: يعتبر هذا الحل غير أمن لقدرة الخصم على تغيير الكتل الاخرى.
2. تطبيق عملية XOR على جميع الكتل للحصول على كتلة B ومن ثم تطبيق $F_k(B)$: يعتبر هذا الحل غير أمن ايضا لأن الخصم يستطيع تغيير كتل الرسالة بحيث لاتتغير الكتلة B.
3. تطبيق $F_k(.)$ على كل كتلة بصورة منفصلة: هذا الحل غير مقبول ايضا لأن الخصم يستطيع تغيير ترتيب الكتل او حذف بعضها وتكرارها بدون ان يلاحظ الطرف المستلم.

4.3.2 منهج CBC-MAC

نعرض الأن منهج CBC-MAC لتوليد شفرة توثيق الرسائل متغيّرة الطول باستخدام دوال شبه عشوائية محدّدة الطول. يعتمد تصميم CBC-MAC على نمط التشفير CBC وهو شائع الاستخدام عمليا. يعمل هذا التصميم على تقسم الرسالة الى كتل ، ويتم تطبيق التشفير الكتلي بعدها على هذه الكتل. لحساب شفرة لرسالة بطول ℓn ، حيث n هي طول الكتلة ، و ℓ هو عدد الكتل ، يتم تطبيق التشفير الكتلي ℓ من

Construction (4.2): Basic CBC– MAC

Assumption: Let $F_k(.)$ be pseudorandom function of length n

Gen(n): on receiving security parameter, n, it chooses randomly $k \leftarrow \{0,1\}^n$.

$Mac_k(m)$: on the message, $m \in \{0,1\}^{\ell n}$ and the key $k \in \{0,1\}^n$ it works as follows:

- Let $m = m_1, \dots, m_\ell$, s.t m_i is block of length n
- For $i = 1$ to ℓ: compute: $t_i = F_k(t_{i-1} \oplus m_i)$
- Output is t_ℓ.

$Vrfy_k(m, t)$: on message $m \in \{0,1\}^{\ell n}$, the key $k \in \{0,1\}^n$, and the tag, t, it output 1 if and only if $t = Mac_k(m)$, otherwise it output 0.

المرات. يكون حجم الشفرة الناتجة هو n من الثنائيات للرسالة ككل.

- يوضّح المنهج (4.2) طريقة عمل منهج CBC-MAC الاساسية.

يفترق CBC-MAC عن التشفير بنمط CBC باختلافين رئيسين ، هما:

1. التشفير بنمط CBC يستخدم المتغير العشوائي IV وهذا شئ حاسم للأمنية ، في حين لا يستخدم CBC-MAC هذا المتغّير.
2. في تشفير CBC يتم اخراج جميع الكتل المشفّرة ، وذلك كي تسهل عملية فك الشفرة. في حين CBC-MAC يخرج فقط الكتلة الاخيرة ، كون اخراج جميع الكتل غير ضروري ويعرّض الأمنية للخطر.

4.4 دوال النحت المقاومة للتصادم

لدى **دوال النحت المقاومة للتصادم** collision-resistant hash functions العديد من التطبيقات في التشفير وامنية الحاسوب. احد ابرز تلك الاستخدامات هو تصميم شفرة توثيق الرسالة. بصورة عامة ، تقوم دوال النحت hash functions بضغط خيوط رمزية متغيرة الطول الى خيوط رمزية اقصر تعرف **بالبصمة** fingerprint ، بحيث عند تغيير البيانات لاتعود البصمة صالحة.

- لتكن دالة النحت H ، ولتكن x هي البيانات متغيرة الطول. تدعى $y = H(x)$ بالبصمة (عادة مايكون طولها 160 ثنائية). عندما تتغير الرسالة الى x' فانه يمكن اكتشاف هذا التغيير بمقارنة $y \neq y'$، حيث $y' = H(x')$

- تستخدم هياكل البيانات دوال نحت تقليدية كطريقة لاسترجاع البيانات بوقت $\mathcal{O}(1)$، حيث يخّزن العنصر x في الجدول بالخلية التي عنوانها $H(x)$. عند استرجاع العنصر x يكفي التحقق من محتوى الخلية $H(x)$. لاحظ ، انه من الممكن ان **يتصادم** collide العنصران x و x' على نفس الخلية بحيث $H(x) = H(x')$.
- تشبه دوال النحت المقاومة للتصادم من حيث المبدأ دوال النحت التقليدية المستخدمة في هياكل البيانات من حيث ضغط البينات. يكمن الفرق الجوهري بين هاتين الدالتين في كون التصادم في الأولى يجب ان يكون منعدما ، بمعنى لايوجد خصم يستطيع ان يجد تصادم ما ، في حين يسمح بوجود التصادم في دوال النحت التقليدية.

4.4.1 تعريف الدالة المقاومة التصادم

يعّرف التصادم في الدالة H على انه زوج من المدخلات المختلفة x و x' بحيث يكون $H(x) = H(x')$. تكون الدالة H مقاومة للتصادم اذا تعذّر ايجاد اي خصم يستطيع ايجاد تصادم في تلك الدالة. بما ان الدالة H تقبل رسائل بأطوال مختلفة وتحوّلها الى رسالة بطول ثابت ، اذن التصادم موجود ولكن يصعب ايجاده.

قبل الشروع بتعريف دالة النحت نفترض وجود **عائلة** لدوال النحت بحيث يمكن تمييز دوالها بالمفتاح s. لايعتبر s مفتاح تشفير وانما هو وسيلة لتمييز الدالة H^s ضمن العائلة ،ويمكن ان يكون معلنا.

تجربة ايجاد التصادم $\text{Hash} - \text{coll}_{\mathcal{A},H^s}(n)$

1. يتم اختيار s ، بحيث $s \leftarrow \text{Gen}(n)$
2. يعطى s الى الخصم $\mathcal{A}$ ويخرج بدوره زوج من القيم x و x'.
3. اخراج التجربة يكون 1 اذا وفقط اذ $x \neq x'$ و $H^s(x) = H^s(x')$.

تعريف(4.2)**:** تكون دالة النحت π **مقاومة للتصادم** اذا كان لجميع الخصوم $\mathcal{A}$ ، توجد دالة ضئيلة negl بحيث:

$$\Pr[\text{Hash} - \text{coll}_{\mathcal{A},\pi}(n) = 1] \leq \text{negl}(n)$$

سوف نستخدم كل من الرمز H ، H^s ، و (Gen, H) للاشارة الى مصطلح دالة النحت المقاومة للتصادم.

تعاريف اضعف لامنية دوال النحت.يعتبر تعريف (4.2) لأمنية دوال النحت تعريفا قويا ويصعب جدا تحققه. يكفي في الكثير من التطبيقات الاعتماد على تعاريف أمنية ابسط. هناك ثلاث تعاريف أمنية مرتبطة بدوال النحت:

1. **مقاومة التصادم** collision resistance: يعتبر اعلى مستوى وسبق وان ذكرناه. تعرف الدالة التي يصعب فيها ايجاد التصادم بدالة النحت المقاومة للتصادم.
2. **المقاومة المسبقة الثانية** second preimage resistance: تعتبر دالة النحت آمنة في ظل هذا التعريف اذا كان عند اعطاء x فمن الصعب على الخصم ايجاد x' بحيث يكون $H^s(x) = H^s(x')$. تعرف دالة النحت التي تحقق شرط المقاومة المسبقة الثانية بدالة النحت ذات المقاومة المسبقة الثانية.
3. **المقاومة المسبقة** preimage resistance: هنا ، تكون دالة النحت آمنة اذا صعب على الخصم ايجاد x تحُقّق $H^s(x) = y$ ، بحيث y تكون معطاة.تُعرف دالة النحت التي تحقق المقاومة المسبقة **بدالة الاتجاه الواحد** one-way function او دالة النحت ذات المقاومة المسبقة.

مهاجمة يوم الميلاد Birthday attack. تعتبر مهاجمة يوم الميلاد من ابرز الطرق المستخدمة لايجاد التصادم في دوال النحت. حيث تضع الحد الادنى لطول البصمة التي تنتجها دالة النحت كي تكون مقاومة للتصادم.

- يتم التعبير عن هذه المهاجمة كما يلي: اذا تم اختيار $y_1, \dots, y_q \in \{0,1\}^{\ell}$ بصورة عشوائية فما هي احتمالية وجود قيمتين i وj بحيث $y_i = y_j$؟. تنص هذه المهاجمة على انه اذا كان $\mathcal{O}(q) = \mathcal{O}\left(\sqrt{2^{\ell}}\right) = O(2^{\ell/2})$ فإن هذه المهاجمة تستطيع ايجاد التصادم باحتمالية $1/2$.
- تشبه هذه المهاجمة مسألة يوم الميلاد والتي تنص: اذا كان هناك q من الاشخاص في غرفة فما هي احتمالية وجود شخصين لهما نفس يوم الميلاد؟ ثبت في محلّه انه اذا كان هناك 23 شخص فإن احتمالية ايجاد شخصين لهما نفس يوم الميلاد هي 50%.
- بصورة عامة يكون عدد المحاولات لايجاد التصادم في الدالة التي طول بصمتها 2^{ℓ} هي $q = \sqrt{2(\ln 2)n} = 1.18\sqrt{n}$.

في ضوء هذه المهاجمة فانه يتم ايجاد تصادم لدالة النحت التي طول اخراجها ℓ ثنائية بـ$q = \mathcal{O}(2^{\ell/2})$ من الوقت. على سبيل المثال لو كان طول بصمة دالة النحت 128 ثنائية فإن مهاجمة يوم الميلاد تتطلب $\mathcal{O}(2^{64})$ من الحسابات لايجاد التصادم لها. نؤكد ان هذه المهاجمة مخصصة فقط للعمل مع دوال النحت مقاومة للتصادم فقط ولاتتعامل مع دوال النحت من نوع preimage resistance و second preimage. توضّح خوارزمية (4.1) كيفية ايجاد تصادم لدالة نحت باستخدام مهاجمة يوم الميلاد. حيث تم تقريب قيم q الى $2\sqrt{n} + 1$.

Algorithm (4.1): Birthday attack
Input: hash function, H^s, of ℓ-bit fingerprint
Output: pair of messages (x_i, x_j)
Set $q = \lceil 2\sqrt{2^{\ell}} \rceil + 1$
Generate q uniform random messages $x_1, \dots, x_q$
for $i = 1$ to q:
  $y_i = H^s(x_i)$
find distinct $i, j \in \{1, \dots, q\}$ such that $y_i = y_j$
if such i, j exist and $x_i \neq x_j$ then
  return the pair (x_i, x_j)

4.4.2 تحويل Merkle − Damgard

يعتبر تحويل Merkle − Damgard من اهم الطرق المستخدمة لتصميم دوال النحت المقاومة للتصادم. يعمل هذه التحويل على توسيع دالة النحت ثابتة الطول والتي تعرف **بدالة الضغط** compression function الى دالة عامة تستلم مدخلات مختلفة الطول. لغرض التبسيط ، سوف نفترض ان دالة الضغط تقلّص حجم المدخلات الى النصف. بمعنى انها تستلم مدخلات بطول $2\ell(n)$ وطول اخراجها هو $\ell(n)$.

تصميم تحويل $Merkle-Damgard$. لتكن h^s دالة نحت ثابتة الطول بمدخلات طولها $2\ell(n)$ واخراجات طولها $\ell(n)$. يتم تشكيل دالة النحت H^s متغيرة الطول كما موضح بالمنهج (4.3)، حيث يتم تقسيم الرسالة المدخلة x الى عدد من الرسائل القصيرة $(x_1, \dots, x_B)$بطولℓ. يتم حشو الكتلة الاخيرة x_B بالثنائيات 10^* الى ان تصبح بطول ℓ. تطبّق دالة النحت h^s بطريقة تكرارية على هذه الكتل ، حيث تستلم دالة الضغط كل من البصمة السابقة z_{i-1} و الكتلة الحالية x_i وتضغطهما معا للحصول على البصمة.z_i في الاخير يتم نحت البصمة ما قبل الاخيرة z_{B-1} مع طول الرسالة L للحصول على البصمة النهائية z_B. نشير الى ان القيمة الابتدائية للمتغير z_0 يمكن ان

Construction (4.3): Merkle – Damgard Transfrom

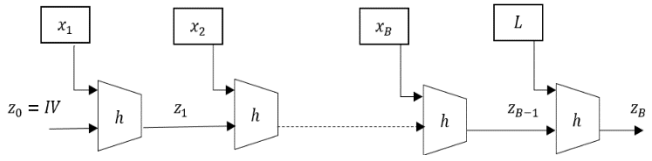
Assumption: Let $h^s(x)$ be fixed-length hash function of length $2\ell(n)$ and output $\ell(n)$

Gen(n): choose s.

$H^s(x)$: on receiving s and $x \in \{0,1\}^*$ of length at most $2^{\ell(n)} - 1$, compute:

1. Let $L = |x|$ and $B = \left\lceil \frac{L}{\ell} \right\rceil$. Pad x with 10^* s.t its length is an exact multiple of ℓ
2. Define $z_0 = 0^\ell$, and then
3. for $i = 1$ to B:
   compute: $z_i = h^s(z_{i-1} || x_i)$.

تكون اي ثابت. تعرف هذه القيمة عادة بالمتجة الابتدائي IV.كما ان كتلة طول الرسالة الاخيرة يتم حشوها بعدد من الاصفار(عند الحاجة) وذلك لكي نحصل على طول كتلة بطول ℓ تماما من الثنائيات. تتم عملية حشو الكتلة الاخيرة بالشكل $0^k||L||$ ، حيث $||L||$ يمثل عدد الثنائيات المطلوبة لتمثيل L اما k فيمثل عدد الاصفار المطلوبة والتي تحسب بالشكل $k = \ell - ||L||$.يوضّح الشكل (4.2) طريقة عمل هذا التحويل.



شكل (4.2): تحويل $Merkle-Damgard$

4.4.3 مناقشة أمنية دوال النحت التطبيقية

لاتستخدم دوال النحت التطبيقية اي مفتاح خاص وبذلك فإن دالة النحت H تكون ثابتة ولايعود هناك داع لاستخدام خوارزمية Gen لاختيار المفتاح s. هناك مشاكل تواجهنا في تعريف مقاومة التصادم للدوال غير المفتاحية. فعندما نجد تصادم في دالة غير مفتاحية H ، فإن هذه الدالة لاتعود مقاومة للتصادم مطلقا. من جانب اخر عند وجود تصادم في الدالة H^s ، فانه يمكن استبدالها بالدالة $H^{s'}$.

يظهر الفرق الاخر عندما يكون طول بصمة H ثابتا ، وهي حالة اغلب دوال النحت التطبيقية: عند هذه الحالة لايعود هناك اي معنى لمعامل الأمنية ولايكون هناك معنى لايجاد خوارزمية كفوءة تجد التصادم باحتمالية ضئيلة ، لذا رأينا كيف ان مهاجمة يوم الميلاد تستطيع كسر هذه الدوال (بمعنى ايجاد التصادم) باحتمالية $1/2$ وبوقت ثابت!.

يمكن اعادة صياغة أمنية هذه الدوال بالشكل التالي: "تكون دالة النحت آمنة اذا تعذر ايجاد خوارزمية تعمل بوقت معتد به تستطيع ان تجد تصادم في الدالة H باحتمالية معتد بها".

مع ذلك فإن دوال النحت التطبيقية تستخدم بكثرة في الحياة العملية وان تعريف الأمنية اعلاه يعتبر كافٍ. على وجه الخصوص ، عندما يكون طول البصمة ℓ كبير نسيبيا فإن ايجاد التصادم بوقت ثابت $2^{\ell/2}$ يكون غير مقلق. على الرغم مما ذكرناه اعلاه ، يمكن تحويل دوال النحت التطبيقية الى دوال نحت مفتاحية. نقدّم طريقة المعالجة: تستخدم دوال النحت التطبيقية متّجه ابتدائي IV كجزء من شفرتها. يمكن اعتبار هذه القيمة كمفتاح سري S.

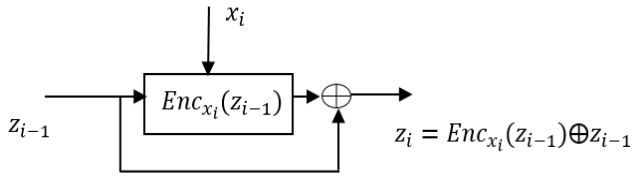
4.4.4 تصميم دوال الضغط

ذكرنا قبل قليل ان تحويل $Merkle-Damgard$ يستخدم لتوسيع دالة نحت ثابتة الطول h تعرف بدالة الضغط الى دالة نحت H تتعامل مع رسائل اطول. نتعرف في هذا الجزء على كيفية تصميم دوال الضغط h.

احد الطرق المستخدمة لتصميم دوال الضغط هي باستخدام دوال البعثرة شبه العشوائية (التشفير الكتلي). على سبيل المثال ، يمكن استخدام شفرة AES ، التي تطرقنا لها في الفصل السابق. تصمم دالة الضغط بالشكل:

$$h(x,y) = Enc_x(y) \oplus y$$

بحيث ان طول البصمة الناتجة يساوي طول مخرجات دالة البعثرة شبه العشوائية المستخدمة (عند استخدام AES يكون طول البصمة 128 ثنائية). عند دمج دالة الضغط هذه مع تحويل $Merkle-Damgard$ يكون لدينا $y = z_{i-1}$ (البصمة السابقة) و $x = x_i$ (جزء الرسالة رقم i). لاحظ ان هذا التصميم لم يشفّر اجزاء الرسالة بل يستخدم تلك الاجزاء كمفاتح للتشفير ، وهو اسلوب غير معتاد لاستخدام التشفير الكتلي. تعرف هذه الطريقة بطريقة $Davies\text{-}Meyer$ لتصميم دوال الضغط والتي يوضحها الشكل (4.3).



شكل (4.3): تصميم دالة الضغط

4.4.5 دوال النحت التكرارية

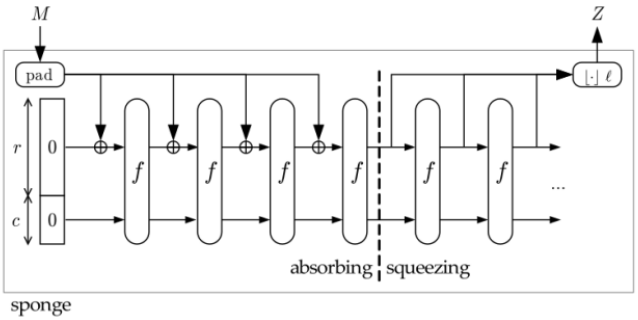
توجد هناك خوارزميات متخصصة لتصميم دوال النحت المقاومة للتصادم بدون استخدام التشفير الكتلي الذي اشرنا اليه في الجزء السابق.

- تعتمد اشهر خوارزميات النحت على تحويل $Merkle-Damgard$ ، حيث قُدّمت اول خوارزمية من قبل $Rivest$ عام 1990 والتي تدعى $MD4$.
- حدّث $Rivest$ خوارزمية $MD4$ للحصول على خوازمية $MD5$ عام 1992.
- اصدرت $NIST$ عام 1993 خوارزمية SHA (عرفت فيما بعد بخوارزمية $SHA\text{-}0$)، والتي تم تحديثها قليلا للحصول على $SHA\text{-}1$ التي اعلن عنها عام 1995.
- وجد في عام 2004 اول تصادم في خوارزمية $SHA\text{-}0$. كما شهد نفس العام ايجاد تصادمات وثغرات في خوارزمية $DM5$ وخوارزميات اخرى.

- وجد اول تصادم لخوارزمية SHA-1 المشهورة عام 2017، حيث ان اسلوب مهاجمتها كان اسرع بمقدار 100000 مرة من مهاجمة يوم الميلاد والتي تتطلب $O(2^{80})$ من المحاولات كما ذكرنا.
- نود ان نذكر ان ايجاد تصادم في خوارزمية معينة لايعني انها غير آمنة تماما بل يمكن استخدامها في التطبيقات التي لاتتطلب مقاومة التصادم.كدوال الاتجاه الواحد.
- تضمنت SHA-2 اربع خوارزميات، وهي SHA-224، SHA-256، SHA-385، و SHA-512. تشير اللواحق "224"، "256"، "384"، و "512" الى طول بصمة هذه الخوارزميات الاربع. تعتبر هذه الخوارزميات الاربع من الخوارزميات التكرارية ولكن لها تفاصيل عمل اعقد من خوارزمية SHA-1. تم اعتبار اخر ثلاث خوارزميات معايير دولية عام 2002. اما خوارزمية SHA-224 فأقرت عام 2004. نود الاشارة الى ان خوارزميات SHA-2 لم تستخدم بصورة شائعة كما هو حال خوارزمية SHA-1.
- تعتبر SHA-3 أخر اصدار من عائلة SHA، حيث تعتمد على هيكل مختلف عن تحويل $Merkle - Damgard$، الذي اعتمدت عليه جميع الخوارزميات السابقة. يدعى هيكل SHA-3 **بالهيكل الاسفنجي** sponge construction، والذي سوف نناقشه في الجزء التالي. اقُرّت SHA-3 كمعيار دولي عام 2015.
- قبل ختام هذا الفصل نود تقديم وصف مختصر لخوارزمية SHA-1. تنتج خوارزمية SHA-1 بصمة بطول 160 ثنائية. يتم توسيع الرسالة المدخلة x بكتلة اضافية بطول 512 ثنائية. تعمل الخوارزمية وفق تحويل $Merkle - Damgard$، حيث تقّسم الرسالة الى كتل بطول 512 ثنائية. تعمل دالة الضغط على تحول كتلة بيانات بطول 512 ثنائية والبصمة السابقة بطول 160 ثنائية الى بصمة بطول 160 ثنائية. تتعامل هذه الخوارزمية مع كلمات بطول 32 ثنائية.

4.4.6 دوال النحت ذات الهيكل الاسفنجي

اعتمدت خوارزمية SHA-3 على هيكل جديد يعرف بالهيكل الاسفنجي. يفترق هذا الهيكل عن تحويل $Merkle - Damgard$ بعدم استخدام دالة ضغط h وانما يستخدم دالة شبه بعثرة عشوائية f بدون مفتاح. تعمل هذه الدالة على تحويل خيط ثنائي الى خيط ثنائي اخر بنفس الطول وبمبدأ 1-1، بمعنى ان كل خيط ادخال له خيط اخراج وحيد. يمكن استخدام الهيكل الاسفنجي في الكثير من ادوات التشفير ولايقتصر استخدامه على تصميم دوال النحت فقط. مما يمّيز هذا الهيكل هو امكانية نحت الرسالة باي طول كان الى بصمة بأي طول.



شكل (4.4): التصميم الاسفنجي

- افترض ان الدالة f تتعامل مع خيوط رمزية بطول b. بمعنى ان لدينا $f: \{0,1\}^b \rightarrow \{0,1\}^b$.
- يعرف العدد الصحيح b بالعرض width ويمكن كتابته بشكل جمع عددين، وليكن $b = r + c$، بحيث r يمثل نسبة الثنائيات bitrate و c يمثل السعة capacity.
- تؤثر قيمة r على كفاءة **الدالة الاسفنجية** sponge function، بحيث سوف تعالج الرسالة M بمعدل r من الثنائيات في كل مرة.

- تؤثر قيمة c على أمنية الدالة الاسفنجية. يكون مستوى الأمنية تجاه نوع معين من انواع مهاجمة التصادم حوالي $2^{c/2}$.
- يوضّح الشكل (4.4) كيفية تصميم الدالة الاسفنجية المعتمدة على الدالة f.
- تعمل الدالة الاسفنجية كما يلي: يتم حشو الرسالة المدخلة M اولا بحيث يكون طولها من مضاعفات r. ومن ثم يتم تقسيم الرسالة المحشوة الى كتل بطول r.

- يتم في البداية تهيئة خيط ثنائيات بقيم b من الاصفار يدعى هذا الخيط بالحالة state.
- يتم تطبيق عملية XOR بين ثنائيات اول كتلة مع اول r من ثنائيات الحالة.
- بعدها تطّبق الدالة f مما يسبب تحديث الحالة.
- تكرّر هذه العملية على الكتل المتبقية من الرسالة المحشوة. يمثل هذا الاجراء طور الامتصاص absorbing phase من الدالة الاسفنجية.
- بعد طور الامتصاص يأتي طور العصر squeezing phase لانتاج البصمة.
  - افترض ان طول البصمة المرغوب هو v. نبدأ بأخذ اول r ثنائية من الحالة لنشّكل كتلة الاخراج.
  - اذا كان $v > r$، فأننا نطبّق الدالة f على الحالة الحالية ونأخذ منها اول r من الثنائيات ككتلة اخراج اخرى.
  - نكرّر هذا الاسلوب عدد من المرت لحين الحصول على اخرج يزيد عن v.
  - نقتطع من الاخرج عدد من الثنائيات بحيث يكون الاخراج هو v ثنائية فقط والذي يمثل البصمة المطلوبة.

نوضّح الأن بصورة مقتضبة كيفية وصف عملية الامتصاص رياضيا. افترض الرسالة المحشوة

$$M = m_1 || \dots . || m_k$$

بحيث ان $m_1, \dots, m_k \in \{0,1\}^r$. نعرّف الأن

$$y_0 = \underbrace{00 \dots 0}_{c} \text{ و } x_0 = \underbrace{00 \dots 0}_{r}$$

ثم نحسب القيم التالية

$$f(x_0 \oplus m_1 || y_0) = x_1 || y_1$$
$$f(x_1 \oplus m_2 || y_1) = x_2 || y_2$$
$$\vdots$$
$$f(x_{k-1} \oplus m_k || y_{k-1}) = x_k || y_k$$

بحيث ان $x_i \in \{0,1\}^r, y_i \in \{0,1\}^c : \forall i \geq 0$

- تعتمد أمنية الدالة الاسفنجية على افتراض ان تكون f دالة عشوائية. حيث يوجد تصادم في الدالة الاسفنجية عند تطبيق الدالة f تقريبا $2^{c/2}$ من المرّات.
- يدعى التصادم في الدالة الاسفنجية بالتصادم الداخي internal collision ويتم الحصول عليه عند تطبيق الدالة f والحصول على تكرار للجزء y من الحالة بمعنى $y_h = y_k$ بحيث $h < k$. وبما ان قيم $y_1 \dots y_k$ تتحصل من تطبيق الدالة f على خيوط بطول 2^c ، اذن تكون لدينا مهاجمة يوم الميلاد والتي تتطلب $2^{c/2}$ من المحاولات للحصول على تصادم.

SHA-3. تتكون SHA-3 من اربع خوارزميات نحت ، والتي تدعى SHA3-224، SHA3-256، SHA3-384، و SHA3-512. ايضا هذه التوابع تمثل اطوال بصمات تلك الخوارزميات (بمعنى أخر قيمة **v**.التي ذكرناها في اعلاه). تم اشتقاق هذه الخوارزمية من خوارزمية نحت اخرى تدعى keccac ، والتي اقترحت في المنافسة على SHA-3. توضّح قيم **b** ، **r** ، و**c** لهذه الخوارزميات في الجدول (4.1). لاحظ ان طول البصمة لهذه الخوارزميات هو اصغر من **r**.

جدول (4.1): معلمات خورزمية SHA-3

c	***r***	***b***	دالة النحت
112	1152	1600	SHA3-224
128	1088	1600	SHA3-256
192	832	1600	SHA3-384
256	576	1600	SHA3-512

- تكون الدالة **f** دالة تقابلية تتعامل مع خيوط ثنائيات بطول 1600. تتألف الدالة من 24دورة ، تتركب كل دورة من خمسة خطوات فرعية. تكون العمليات الداخلية شبيهةبالتي ذكرناها لخوارزمية SHA-1.

4.5 منهج HMAC

تطرقنا فيما سبق الى كيفية تصميم شفرة توثيق رسالة MAC بالاعتماد على الدوال شبه العشوائية (التشفير الكتلي). سوف نرى خلال هذا الفصل كيفية تصميم شفرة MAC باستخدام دوال النحت المقاومة للتصادم. تجمع هذه الطريقة بين السرعة (من حيث استبدال التشفير بدوال النحت) والامنية (من حيث اضافة مفتاح لدوال النحت).

تدعى طريقة توثيق الرسائل هذه HMAC ، وهي شائعة الاستخدام بسبب كفائتها وسهولة تصميمها مما جعلها من اكثر طرق حساب الـMAC شهرة. تستخدم HMAC خوارزمية النحت SHA-1 يعتمد تصميم HMAC على مفتاح **k** بطول 512 ثنائية. تستخدم هذه الخوارزمية ثابتين opad و ipda. كلا الثابتين بطول 512 ثنائية. يتشكل الثابت opad بتكرار الرقم السداسي عشر 36 حسب الحاجة. يتشكل الثابت ipad بنفس طريقة تشكيل opad ولكن بتكرار العدد 5C. يبين المنهج (4.4) عمل خوارزمية HMAC.

يبدو ان تطوير SHA3 قد يؤثر على استخدام HMAC مستقبلا. حيث يمكن استخدام SHA3 لنحت المفتاح مع الرسالة معا — SHA3(k||m) بدون محاذير أمنية للحصول على شفرة رسالة موثقة. يعرف هذا المقترح بأسم KMAC.

Construction (4.4): HMAC

$\boldsymbol{Gen(n)}$: choose $k \leftarrow \{0,1\}^{512}$.

$\boldsymbol{Mac_k(m)}$: on receiving k, and message $m \in \{0,1\}^*$ it computes:

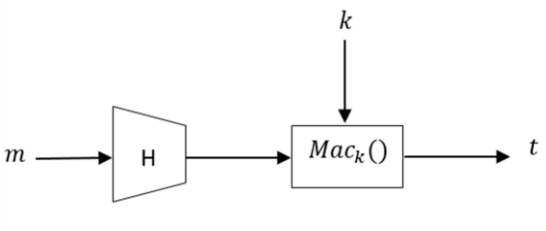
$HMAC_k(m) = SHA-1(k \oplus opad||SHA-1(k \oplus ipad||x))$.

$\boldsymbol{Vrfy_k(m,t)}$: output 1 if and only if $t = Mac_k(m)$.

4.6 تطبيقات دوال النحت المقاومة للتصادم.

لغرض معرفة اهمية دوال النحت المقاومة للتصادم في مجال التشفير نذكر فيما يلي مجموعة من تطبيقاتها العملية.

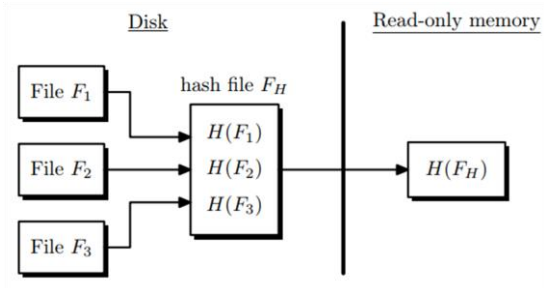
1. زيادة كفاءة شفرات توثيق الرسائل الامنة: احد التطبيقات المهمة لدوال النحت المقاومة للتصادم هي بتوسيع شفرات التوثيق التي تتعامل مع رسائل قصيرة الى شفرات تتعامل مع رسائل اطول. لحساب MAC للرسالة الطويلة m ، نقوم اولا بتطبيق دالة النحت عليها ومن ثم حساب $Mac_k()$ على الناتج. تتم عمليه الفحص بنحت الرسالة المستلمة للحصول على بصمة ومن ثم فحص شفرة تلك البصمة. يوضّح الشكل (4.5) طريقة المزج بين النحت والتوثيق (hash-then-MAC).
2. تصميم شفرات توثيق الرسائل:كما وضحنّا في طريقة HMAC.
3. التوقيع الرقمي: يعد التوقيع الرقمي من ابرز تطبيقات دوال النحت المقاومة للتصادم ، حيث يتم استخلاص بصمة الرسالة اولا ومن ثم يتم توقيع هذه البصمة. يسمح هذا الاسلوب بتوقيع رسائل مختلفة الطول ويوّفر أمنية تجاه عدد من المهاجمات.
4. سلامة الملفات: ليكن لدينا عدد من الملفات المهمة ، مثلا ملفات نظام التشغيل ، التي نريد ان نتأكد من عدم تغييرها من قبل بعض البرامج الخبيثة. يتم تطبيق دالة النحت المقاومة للتصادم على كل ملف. نخزّن بصمات الملفات في ذاكرة قراءة فقط مثلا USB. للتأكد من سلامة ملف معين يتم اعادة حساب بصمته ونقارنها مع البصمة المخزونة مسبقا. عند عدم وجود تطابق فإن الملف يعتبر متغيّر.



شكل (4.5): النحت ثم التوثيق

- تتطلب هذه الطريقة الوصول الى ذاكرة القراءة فقط عند محاولة اختبار سلامة كل ملف. تعد هذه الطريقة غير عملية عندما يكون عدد ملفات النظام كبيرا. تحل هذه المشكلة باعتبار البصمات على انها ملف واحد F_H ويتم تطبيق دالة النحت على هذا الملف. تخزن بصمة هذا الملف في ذاكرة القراءة فقط كما موضح في الشكل (4.6).

5. تستخدم دوال النحت المقاومة للتصادم في تصميم مولّدات الارقام شبه العشوائية من الناحية العملية ، حيث تكون مخرجاتها شبيها بارقام شبه عشوائية.
6. تستخدم دوال النحت المقاوم للتصادم في تخزين كلمات المرور. passwords في الخادمات servers غير الموثوقة ، حيث يتم تطبيق هذه الدوال على كلمة المرور للحصول على بصمة يتم تخزينها بدلا من كلمة المرور في الخادم.



شكل (5.6): سلامة الملفات

4.7 انظمة التشفير بامنية CCA

تطرقنا سابقا الى مفهوم الأمنية من نوع chosen ciphertext attack (CCA). في هذا الفصل سوف نستخدم شفرات توثيق الرسائل (ومناهج التشفير من نوع CPA) لتصميم مناهج تشفير من نوع CCA.

سوف يكون لمنهج التشفير المقترح خاصية منع الخصم من الحصول على اي نص مشفّر صحيح مالم يكن مشفّر من قبل الاطراف الشرعيين. وهذا له تأثير على الغاء الاستفادة من خوارزمية فك التشفير التي يتمتع بها الخصم في مهاجمة CCA. بصورة دقيقة ، يقوم منهج التشفير بتشفير الرسالة الصريحة اولا ، ومن ثم تطبيق MAC على النص المشفّر. مما يعني انه ستكون عملية فك الشفرة ممكنة فقط للرسائل المتولدة بصورة قانونية. يوضّح المنهج (4.5) تصميم منهج تشفير CCA أمن.

Construction (4.5): CBC–secure encryption scheme

Assumptions: let $\Pi_E = (Gen_E, Enc, Dec)$ be CBA-secure encryption scheme. Let $\Pi_M = (Gen_M, Mac, Vrfy)$ secure MAC scheme

$Gen'(n)$: on receiving n, it choose two keys $k_1 \leftarrow \{0,1\}^n$ and $k_2 \leftarrow \{0,1\}^n$.

$Enc'(m)$: on receiving (k_1, k_2), and message $m \in \{0,1\}^*$ it output $c = Enc_{k_1}(m)$, $t = MAC_{k_2}(c)$, and output (c, t).

$Dec'(c, t)$: on receiving (k_1, k_2), and (c, t), it checks if $Vrfy_{k_2}(c, t) = 1$. If so, output $Dec_{k_1}(c)$, otherwise output $\perp$.